International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 09 | Sep 2020 www.irjet.net p-ISSN: 2395-0072

FACE DETECTION BASED ATM SAFETY SYSTEM IN IOT USING SECURE TRANSACTION

Dr. V. Gokula Krishnan. M.Tech.Ph.D[1], G.N. Kirran[2], K.P. Deepkarasan[3], J. Kishore Kumar[4]

[1]ASSOCIATE PROFESSOR, DEPT OF CSE, PANIMALAR INSTITUE OF TECHNOLOGY, CHENNAI
[2-4]B.E STUDENT, DEPT OF CSE, PANIMALAR INSTITUE OF TECHNOLOGY, CHENNAI

ABSTRACT: A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. Proposed paper uses face recognition technique for verification in ATM system. The automated teller machine, or ATM, is such a complicated piece of technology that it does not have a single inventor. Instead, the ATMs we use today are an amalgam of several different inventions.

Traditionally we use ATM Cards with pin to enable any transaction of money from one account to another. In this proposed paper we implement a new generation ATM machine which can be operated without the ATM card. In this system we have some more webpages for the identification of the user and 3 rd. user. In first website we have two buttons one for user and another one for third user, if I am user means I want to click user button or otherwise click third user button. Maybe I am third user first I want to enter the authorized user name and password then camera take image mail to authorized person at the same time send alert SMS via IOT. And finally another new webpage is there, if the user should want to go there and should give okay then only third user moves to amount withdraw other its hold. The existing ATM model uses a card and a PIN which gives rise to increase in attacks in the form of stolen cards, or due to statically assigned PINs, duplicity of cards and various other threats .A new biometric ATM seeks to use biometric identity so that not cards and PINs is needed, as the keys to allow consumers to access their cash. The ATM offers a prompt to complete authentication via facial recognition on consumers. Therefore, the combination of face recognition algorithms, frees a user from an extra burden of remembering complex passwords.

KEY WORDS: Identification, Verification, Face Recognition, Biometrics, false rejection, false acceptance

INTRODUCTION:

Normally, human beings use faces to distinguish between individuals and current advancements in computer vision capability within the last few years have enabled similar recognitions automatically. Traditional face recognition algorithms used simple geometric models, which have progressively matured over the years into a science of complex mathematical models and representations, thus drawing face recognition technology into the limelight for both verification and identification purposes. Verification is the process of comparing one biometric patterning with another biometric pattern, resulting in either a rejection or acceptance decision, (Heseltine, 2005). Identification is the process of comparing one biometric pattern with a set of two or more biometric patterns in order to determine the most likely match, (Heseltine, 2005).

Authentication in computer information systems has been by tradition based on something that one has for example magnetic strip cards, smart cards or even keys, or what one knows for example usernames and passwords, PIN or other secret codes. In order for more reliability in verification or identification processes to be achieved, something that uniquely identifies and characterizes a given person should be adopted, and biometrics technology offers computerized methods of identity verification using the concept of measurable physiological or behavioral characteristics for instance iris, retinal or face sample. These characteristics are often referred to as bio-data and must be measurable and unique.

This paper presents my findings of facial recognition, a subset of biometric authentication techniques and its deployment possibility in banking applications.

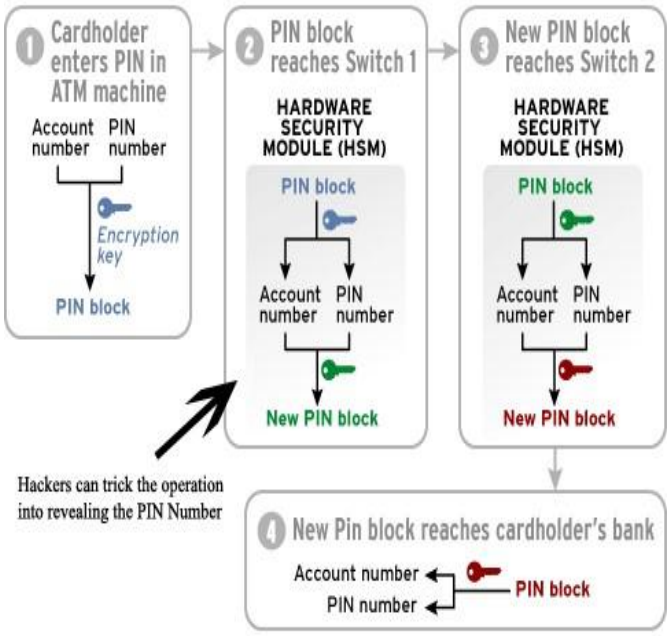
The standard ATM system uses a two level authentication:

1. Identification: to identify the customer

A **one** to **many**

2. Verification: to ensure that the identified user is using the system

A **one** to **one**



For enterprises that haven't revisited their authentication strategies in several years, it may be time to take a fresh look. According to Gartner Inc., a confluence of technology trends affecting enterprises such as mobility, social media, cloud computing and big data are having an effect on virtually every area of IT, including the market for enterprise authentication technology. It is inevitable to adopt two-factor authentication in one form or another.

The user is expected to provide a user identifier/token such as a card and a PIN to be authorized to access the system. When the system receives the Client ID and PIN, it compares the stored credentials with the received data. Access is granted only when there is a match between the captured details and the ones stored in the system. PINs are the most often used authentication mechanisms for ATMs.

At first, Shepherd-Barron envisioned a six-digit PIN number, but his wife nonetheless preferred four digits, which became the standard PIN length for all vending and ATM machines.

The user presents a valid identity (ID Number) and a password to access the account. A password should be kept secret and should also be short enough to be memorized. They can be digits, letters or alphanumeric codes. The use of passwords is known to be ancient.

Are defined as any pocket-sized card with embedded integrated circuits which can process information (smartcard alliance, 2009) It has a microchip embedded in it which makes it —smart|| and that allows other devices to communicate with it. The processing power of smart cards gives them the versatility needed to make payments, to configure your cell phones and connect to your computers via satellite or the internet (Guthery & Scott, 2001).

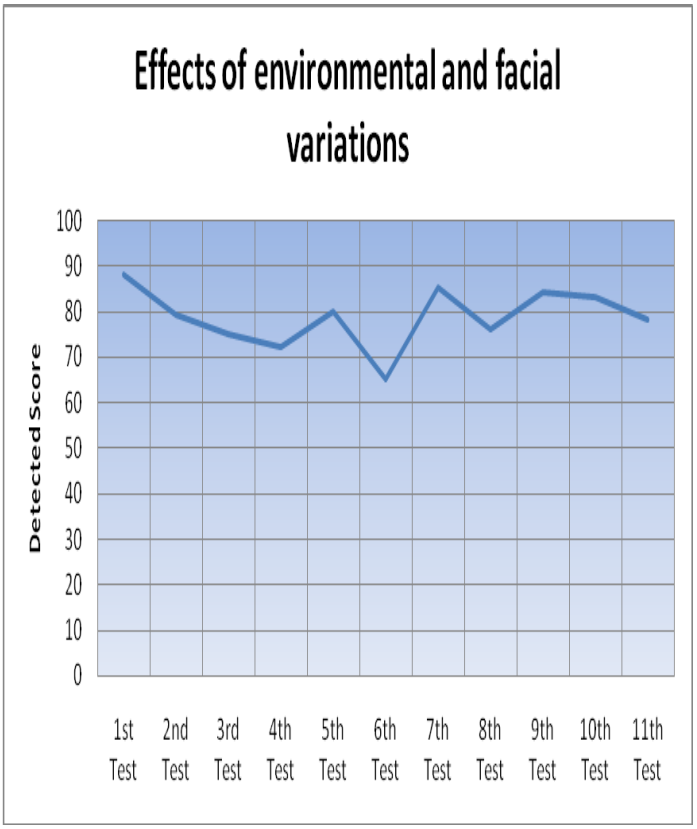
Password is the most used method of restricting access to computer system accounts. Usually, the user presents a valid ID and a password to use the account. Most systems print dots or asterisk instead of the real characters.

Passwords are prone to cracking. This is done by getting a copy of the 1-way hash code in the database, and then using the appropriate algorithm to decode until a match is found.

The most appropriate method of countering password cracking is ensuring that attackers do not even get access to the encrypted password in the server.

After identification of the requirements and scope of ATM security, we discussed how to integrate our facial recognition component in the ATM architecture.

According to figure 16 above, user plane is the plane that directly interacts with user. Therefore to meet the user's security objectives, user plane has to provide security services like access control, authentication, data confidentiality and integrity.



ATM machines face a lot of threats due to the fact that they are public utilities and that there are no measures to control who accesses them at any one point in time. There is lack of a formal model to guarantee security using biometrics technology and to describe secure software

system architecture with a stepwise refinement methodology. The methodology for system modelling and refinement specifies a set of architectural and operational components and how they interact with each other.

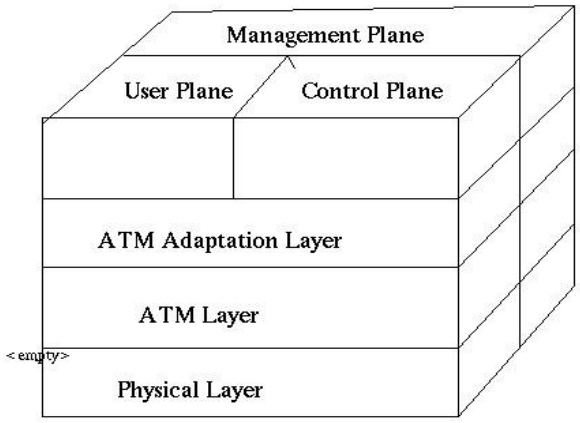
This is why we are interested in developing a two-factor authentication mechanism using a second factor authentication which is "something that is part of the user".

Human behavioral patterns (gait, handwriting, keystroke, voice, etc) fluctuate due to anxiety, exhaustion, or sickness. However, the physiological methods (retina, face, iris, fingerprint, palm, etc) are more stable than methods in the behavioral category, the reason being that physiological features are often non-alterable except by severe injury and have the benefit of non-intrusiveness.

Facial recognition is the primary focus in this study.

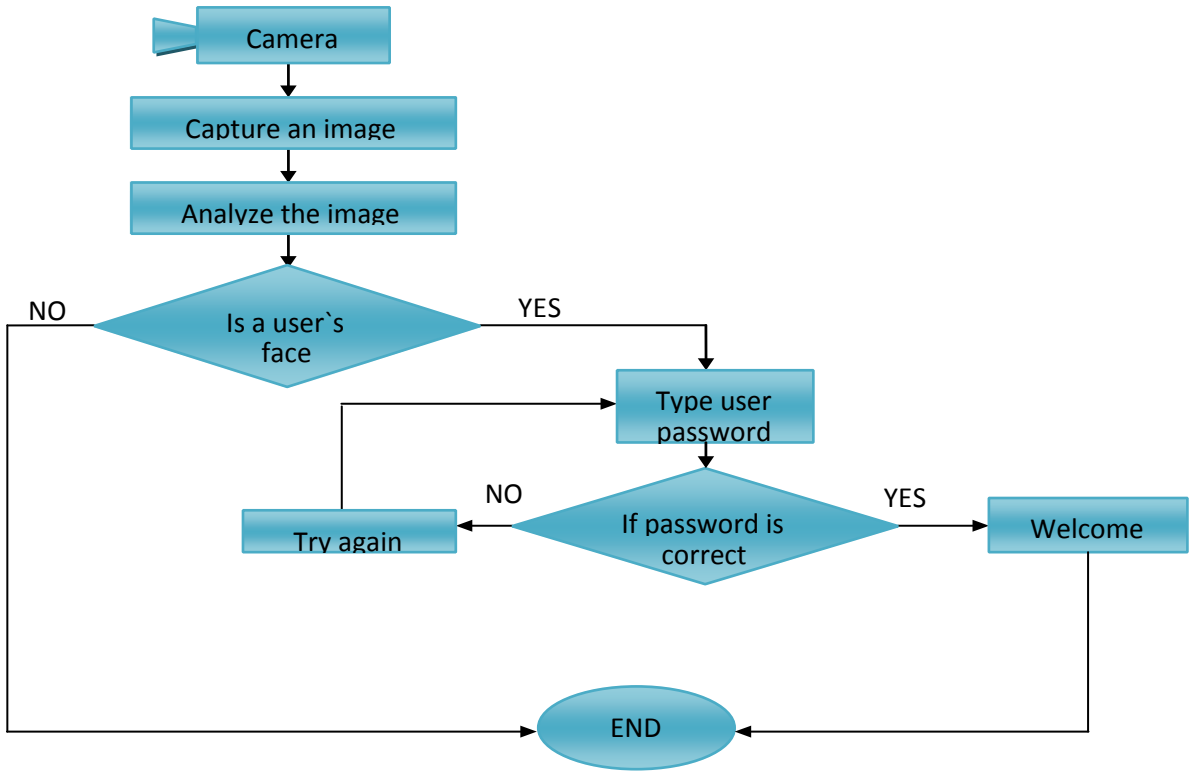
IMPLEMENTING SECURITY SERVICES ON ATM:

In this section, we discussed how to implement security services on ATM machine. We first examined the architecture of ATM and identified the ATM security scope, and then discussed how to place the facial recognition security feature in ATM architecture.



A plane consists of entities that are responsible for transferring user data.

Entities in control plane deal with connection establishment, release and other connection functions. Management plane entities perform management and coordination functions related to both the user plane and the control plane, and functions related to establishment of a routing infrastructure. Besides ATM layer entities perform ATM data transfer on behalf of the other entities in the three planes.



The user plane is the plane that directly interacts with user. Therefore, to meet the user's security objectives, user plane has to provide security services like access control, authentication, data confidentiality and integrity. Other services like key exchange, certification infrastructure and negotiation of security options might be useful to meet the variety of the customers' requirements. Therefore they also should be supported by user plane. Providing different security services options is important because of the various traffic classes in ATM network. Different connections have different security requirements. User plane security services have to provide enough flexibility to meet these requirements.

ENROLMENT AND IDENTIFICATION MODULES:

Package server.identification; import java.io.File; import server.ATMDialog; import server.ATMThread; import server.GlobalSettings; import server.database.Customer; import server.database.Face; public class IdentifyByFace extends Identification {

public IdentifyByFace(ATMThread aTMThreat) {

super(aTMThreat);

}

public ATMDialog identify(ATMDialog data) {

//Start of user code for Identification.identifyByNR if (state == 0) {

state++;

return new ATMDialog("Please look at the camera and press Capture\n","f","0");

}

Customer customer = null;

String faceFile = GlobalSettings.getDataDir()+ File.separator

+String.valueOf(aTMThreat.getConNr())+".jpg"; if (data.getReturnedInputFile(faceFile)) { Face face = new Face(faceFile); face.setUsedForTraining(false); customer = aTMThreat.getDatabase().getCustomerByFace(face);

}

if (customer == null) {

state++;

if (state >4) return this.identifyFail();

return new ATMDialog("Unknown face,\nPlease try again!","f","0");

} else { return identifyPass(customer);

//End of user code

} } }

RESULT :

Face recognition needs to be advanced to overcome instabilities due to variable illuminations, face expressions, poses and occlusion. 150 face images from 89 individuals have been used to train face the recognition algorithm and testing the system`s performance. Most of the images in the database are not sufficiently annotated with the exact illumination angle, face expressions, pose angle, and illuminant color. We carried out tests which included images in the database being matched with probe images from several individuals in different and exact capture environments. In the table above, we report the experimental results of face recognition performed using correlation matching and principal component analysis under various environmental conditions.

CONCLUSION:

Face recognition is a security measure in the field of computer vision, image analysis and pattern matching that is rather challenging to implement in systems to heighten system security and to curb unauthorized access. It has drawn much attention over the last few years because of its promising security features and its ability to be applied in various domains such as ID systems, voting systems, Automatic Teller Machines just to mention a few.

Past research in this field over the last few years have shown good progress and the results obtained so far shows that current facial recognition systems have reached acceptable and reasonable security threshold value while under operation in dynamic conditions and environments.

REFERENCES:

[1] M. Pantic and M. S. Bartlett, “Machine analysis of facial expressions,” in Face Recognition, K. Delac and M. Grgic, Eds. Vienna, Austria: I-Tech Educ., 2007, pp. 377–416.

[2] P. Ekman and W. V. Friesen, Facial Action Coding System: A Technique for the Measurement of Facial Movement. Palo Alto, CA, USA: Consulting Psychologists Press, 1978.

[3] P. Ekman, W. V. Friesen, and J. C. Hager, Facial Action Coding System: The Manual (Research Nexus). Salt Salt Lake City, UT, USA: Netw. Inf. Res. Corp., 2002.

[4] M. Pantic, A. Pentland, A. Nijholt, and T. S. Huang, “Human computing and machine understanding of human behavior: A survey,” in Artificial Intelligence

for Human Computing. Berlin, Germany: Springer, 2007, pp. 47–71.

[5] Z. Zeng, M. Pantic, G. I. Roisman, and T. S. Huang, "A survey of affect recognition methods: Audio, visual, and spontaneous expressions," IEEE Trans. Pattern Anal. Mach. Intell., vol. 31, no. 1, pp. 39–58, Jan. 2009.

[6] E. Sariyanidi, H. Gunes, and A. Cavallaro, "Automatic analysis of facial affect: A survey of registration, representation, and recognition," IEEE Trans. Pattern Anal. Mach. Intell., vol. 37, no. 6, pp. 1113–1133, Jun. 2015.

[7] M. F. Valstar, M. Mehu, B. Jiang, M. Pantic, and K. Scherer, "Metaanalysis of the first facial expression recognition challenge," IEEE Trans. Syst., Man, Cybern. B, Cybern., vol. 42, no. 4, pp. 966–979, Aug. 2012.

[8] M. F. Valstar et al., "FERA 2015—Second facial expression recognition and analysis challenge," in Proc. FG, 2015, pp. 1–8.

[9] Z. Meng, S. Han, and Y. Tong, "Listen to your face: Inferring facial action units from audio channel," IEEE Trans. Affective Comput., to be published.

[10] B. Martinez, M. F. Valstar, B. Jiang, and M. Pantic, "Automatic analysis of facial actions: A survey," IEEE Trans. Affective Comput., to be published.

[11] Y.-L. Tian, T. Kanade, and J. F. Cohn, "Evaluation of Gabor-waveletbased facial action unit recognition in image sequences of increasing complexity," in Proc. FG, Washington, DC, USA, May 2002, pp. 229–234.

[12] M. S. Bartlett et al., "Recognizing facial expression: Machine learning and application to spontaneous behavior," in Proc. CVPR, San Diego, CA, USA, 2005, pp. 568–573.