INTERNATIONAL JOURNAL OF RECENT TRENDS IN ENGINEERING & RESEARCH
Impact Factor 4.101 ISSN -2455-1457
RECENT ADVANCES IN ELECTRONICS & COMMUNICATION ENGINEERING (RAECE-2K17)

IMPROVED SECURITY IN AUTOMATED TELLER MACHINE

N.SNEHA
Student, ECE Department
Nalla Narasimha Reddy Group of Institutions

SNEHA TALARI
Assistant professor, ECE Department
Nalla Narasimha Reddy Group of Institutions

Abstract— **Security is provided to grant access to a legal user and to prevent the system from an illegal person. The problem of disclosure will often occur either through spywares like key loggers installed on target machine or a malicious onlooker who observes while the person enters the password in public space (password authentication). Virtual keyboards provide protection against key loggers but fail to avoid shoulder-surfing. Improvising of these keyboards by changing the layout to frustrate the hackers is planned in this proposed system. When the person enters his PIN in the touch screen, immediately the arrangement of the numbers in the screen will be changed from its original position. The person entering next wouldn't have the same arrangement of numbers in the touch screen. Even when the shoulder-Surfer observes the movement of the person entering the PIN number they can't able to hack the password. It is efficiently possible to avoid Shoulder-Surfing attacks by using Arduino IDE compiler with Arduino.**

Index Terms—**Shoulder-Surfing Attacks, Virtual Keyboards, PIN, Arduino IDE Compiler.**

I. INTRODUCTION

Nowadays, many people are dependent on computers for keeping major record of data. Data are sent in a cost-effective manner across wider area network. Automated Teller Machine is the automatic systems being used since 1967 by many of us. ATM was found by John Shepphardbaren on June 1967 at United Kingdom. It emerged in India in 1968. Today, people have some secret number and password to protect their secret files and also for verification. The personal identification number is one of the day-to-day user authentication technique used in multiple situations, such as depositing and to drawback cash from automated teller machine (ATM), releasing lock in a mobile device, to proceed electronic transactions and even for disclosing a door.

A. Authentication

Authentication is the method of verifying the identification of the person or thing. Authentication is usually done on the basis of passwords, in private and public system networks. Passwords are used in, entering into accounts, emails, accessing applications, networks, web sites, workstations, etc. The commonly used authentication techniques are, Token based authentication such as key cards, band cards, smart card etc., Biometric based authentication (Ex. Fingerprints, iris scan, facial recognition), and Knowledge based authentication (Ex. Text-based passwords, picture-based passwords)[15].

B. Passwords

Password is a covert (word or string) of characters that is used for user authentication to prove his identity and gain access to resources. Two types of Passwords are, Alpha Numeric Password and Graphical Password.

Alpha Numeric Password Ideally, the user should combine both upper and lower case letters and digits, which should be at least 8 characters. This password would not be a word that can be available in a dictionary or public directory. But two conflicts requirement of the Alpha numeric password is Easy to remember and very tough to guess. But most of the user tends to ignore the second requirement which leads to brittle passwords. Several solutions have been proposed to avoid this issue. Graphical password is one of the solutions.

C. Graphical Password

Graphical password is an authentication system that works by the user select password using the images, in a specific order, presented in a graphical user interface. For this reason, the graphical-password technique is sometimes called as graphical user authentication. It is more difficult to break graphical passwords using the traditional attack methods such as, brute force attack, spyware or dictionary attack. An example of a system that uses an image on the screen and lets the user chooses a password by some clicks. These clicks are the "password", and the user has to click closely to these points again in order to complete the authentication. Such passwords are easier to remember & hard to guess. Two types of Graphical password is, Recall Based Techniques and Recognition Based Techniques. In Recall Based Technique, A user is asked to reproduce something that the user created or selected earlier during the registration stage. In Recognition

Based Techniques, a user is accessible with a set of images and the user passes the authentication by recognizing and identifying the images that selected during the registration stage. One of the covert passwords is Personal Identification Number.

D. Personal Identification Number

A personal identification number(PIN) as a 4 digit numeric password in mobile or stationary systems, including smart phones, tablet computers, automated teller machines (ATM), and point of sale (PoS) terminals, a direct observation attack based on shoulder surfing becomes great concern. The PIN entry can be observed by nearby adversaries, more effectively in a crowded area. Usually the same PIN is chosen by a user for various purposes and used repeatedly; a compromise of the PIN may cause the user a great risk. To cope with this problem, which is between the user and the system, cryptographic prevention techniques are hardly applicable because human users are limited in their capacity to process information. Instead, there have been alternative approaches considering the asymmetry between the user and the system

E. Shoulder Surfing Attack

In computer security, shoulder surfing refer to using direct monitoring techniques, for example looking over someone's shoulder movement to hack the information. In early 1980s, Shoulder surfing was practiced near public pay phones to steal calling card digits and make long distance calls or sell them in the market for cheaper prices. Once a user's ID and the corresponding password are thieved by an adversary, the adversary can do anything with the user's account, which can ruin their account.

There are several technologies were introduced to avoid the shoulder surfing attack. Some of the techniques were discussed in the related work

II. RELATED WORK

A. Black and White Method

Mun Kyu Lee have proposed the Black and White(BW) Method [5] where the regular numeric keypad is colored at random, half of the keys in black and the other half in white (Fig.1), which is called as BW method. A user who knows the correct PIN digit can answer its color by pressing the separate color key. The basic BW method is aimed to resist a human shoulder surfing attack. But if the selected halves were memorized or written on a paper for m, consecutive rounds and recalled to derive their Grouping Patterns, the shoulder surfer could identify a single digit of the PIN. In this method a new strategy has been implemented that will entirely neglect shoulder surfing even a well practiced perceptual grouper could not break the PIN digit invade by the user in a standard way

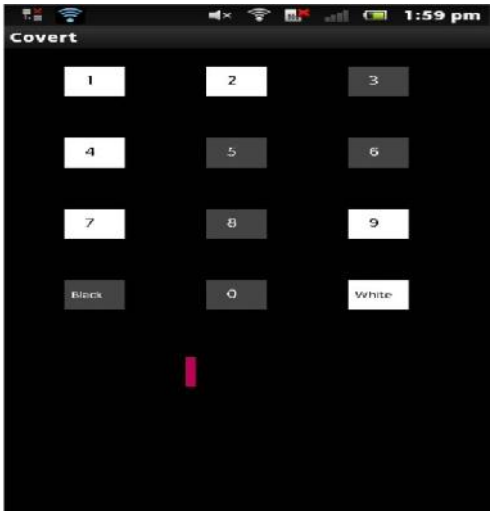

Fig 1. Black and White Method

B. Session Key Method

The session key method has the 4 rounds. The first round is the session key decision round, and the remaining three rounds are PIN-entry rounds. In the session key decision round, ten randomly arranged objects (Fig 2) are displayed to the user. The user can decide any of the symbols and assign it to the 1st digit of the PIN using the Up or Down buttons. If the user presses the Up button, then the symbols move immediately upper wards. If the user presses the Down button, then the symbols move immediately downwards. Using this Up and Down buttons, user moves the decided key to the PIN and then presses OK. While the user moves the symbols, then all the symbols will move Up and Down in which direction the user moving the symbols. So, if the shoulder surfer watches the user enters or even though if attacker records the process, can't find the PIN. In next round, the symbols were shuffled with new symbols too. So this is too tuff to guess or find the PIN by this Session key logon procedure. Now the Session key was decided by the user as well as the 1st digit of a PIN is validated. This same Session key (Symbol) must use for remaining 3 rounds which is the PIN entry method.

The remaining 3 rounds are PIN-entry rounds, in which the *i* th digit of the PIN is entered in the *i* th round (Here *i* = 2, 3, 4). In each of these each rounds, the 10 symbols were shuffle. The user wants to assign the session key for each round using the Up and Down button. In each round user presses the OK button. When the user presses the OK button, then the PIN considered.

Fig 2. Session Key Method

C. Gaze based Password

Eye tracking technology has come a long way since its origins in the early 1900's. State of the art eye trackers offer non encumbering, remote video-based eye tracking with an accuracy of 1° of visual angle. Eye trackers are a specialized application of Computer vision. A camera is used to monitor the user's eyes. One or more infrared light sources illuminate the user's face and produce a glint – a reflection of the light source on the cornea. As the user looks in different directions the pupil moves but the location of the glint on the cornea remains fixed. The relative motion and position of the centre of the pupil and the glint is used to estimate the gaze vector, which is then mapped to coordinates on the screen plane.

Fig 2. Gaze based password

III. OBJECTIVES & OVERVIEW OF THE PROPOSED MECHANISM

A. Objectives

The main aim of this project is to prevent human shoulder surfing attack and to establish a secure transaction by implementing the Key Shuffling Method.

B. Overview of the proposed Mechanism

As an addition to the Credit/Debit card PIN Security a Key Shuffling Method is proposed for ATM machine installed at Point of Sale (POS). The Key Shuffling could overcome the Shoulder Suffering and Keypad Overlay frauds. The numeric digits of Digital Keypad get swapped after entering the PIN number in the keypad of the ATM machine. Every numeric digit gets replaced by other numeric digit; it would provide a new position to every digit. This particular way of representing the keypad will avoid the risk of shoulder surfing of PIN and remembered by any person, who is just trying to identify the digits of PIN by getting the idea of its place on the keypad.

i. KEY SHUFFLING TECHNIQUE

When the user insert card into an ATM machine the following process has to be done

1. Select Language
2. PIN number
3. Prompt for choose Account Type
4. Select the Activity choice
5. Input Transaction Amount.

When the above steps are over the Transaction Amount is obtained. The numeric digits of the Digital Keypad in the ATM Machine get shuffled for every user's entry. Thus the Shoulder Surfing Attack can be prevented during transactions in the ATM machine.

ii. ARCHITECTURE OF THE PROPOSED SYSTEM

Initially the program for creating random sequence is written in Embedded C language. Now the generated PN sequence is considered as a reference and based on the reference a unique key pattern is created where every numeric digit gets replaced by other numeric digit. It would provide a new position to every digit. Then the program is fed into Arduino UNO board through the UART port and the corresponding shuffling key pattern is displayed in the screen. For every perfect login by the user's the shifted key pattern is displayed in screen which is connected to the Arduino board by i2c protocol.

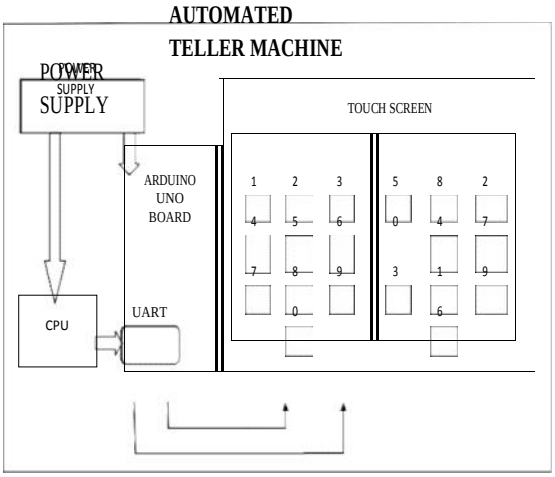

Fig 3. Proposed system

This distinct way of representing the keypad will avoid the risk of shoulder surfing of PIN and remembered by any person, who is just trying to identify the digits of PIN by getting the idea of its place on the keypad

iii. FUTURE WORK

Once the person is recognized the system display the message that Person is authorized and the window of ATM machine is open. The machine ask for bank selection if we choose the bank then it ask for pin number, after entering it the person can make their transactions related to banking like withdraw money, checking balance. Face recognition systems play an vital role in many applications like surveillance, biometrics and security. It is a challenging task in terms of software developing algorithmic solutions and hardware like creating physical implementations . The face recognition system is a set of two tasks one is *Face Identification*: Means to take one image and compares with data base of the person and tell
whose image it is and another is *Face Verification*: means to take one image face that is not in data base we need to verify that it is in the data base or not .

In this paper the method of Face Recognition presented to improve the security of ATM. The face recognition is done successfully. And by face recognition security level of ATMs are increased. The transaction is more secure than before.

DUAL LINEAR REGRESSION MODEL BASED LEARNING

- On comparing the Input image from the gallery with the test frame, the algorithm tries to model the similarity between 2 clusters as the shortest distance between subspaces each spanned from the face images of one cluster.
- The distance between the virtual face images recreated from both the subspaces is taken as the distance between 2 subspaces.

ALGORITHM STEPS

1. Down sample and normalize the entire gallery, all the probe images into size axb.
2. Construct a matrix Y using the probe images.
3. For every subject in the gallery, construct a matrix X.
4. Find the estimation of virtual faces with respect to the objective function
5. Using the residual sum as the similarity between subject and probe.
6. Compare the similarity between all subjects and the probe; choose the subject close to the probe as the optimized solution.

iv. CONCLUSION

This proposed system provides a more secure PIN entry method for common user authentication with high usability. It provides compatibility and it is cost effective. The security is further enhanced by integrating the face recognition method. Dual linear regression algorithm is used in face recognition.

REFERENCES

[1] M. Kumar, T. Garfinkel, D. Boneh, and T.Winograd, Reducing shoulder-surfing by using gaze-based password entry", IEEE transactions on Usable Privacy and Security, vol 10, pp. 224-227, May 2012.

[2] Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto, "An Association- Graphical Password Design Resistant To Shoulder-Surfing Attack", International journal of Engineering and Advanced Technology, vol. 4, February 2013.

[3] M. Vijayalakshmi, "Automatic Human Facial Expression Recognition using Hidden Markov Model", In International Conference on Electronics and Communication Systems (ICECS -2014), pp 13 - 14, February 2014.

[4] Peipei Shi, Bo Zhu, and Amr Youssef, "A PIN Entry Scheme Resistant to Recording- based Shoulder-Surfing", In International Journal of Computer Science and Mobile Computing, Vol. 3, April- 2014.

[5] Sonia Rathi, Raunak Chitnis, Ramakant Yadav, Mrs. M.V.Bhosle, "Securing ATM Using Graphical Password Authentication Scheme ", In International Journal of Computer Trends and Technology (IJCTT) , vol . 8, no 3, July 2014.

[6] Er.Aman Kumar, Er.Naveen Bilandi, "A Graphical Password Based Authentication Based System For Mobile Devices", In International Journal of Computer Science and Mobile Computing, Vol. 3, December 2014.

[7] M.R.Divya, A.P.Janani, "Defending Shoulder Surfing Attacks in Secure Transactions Using Session Key Method", In International Journal of Science, Engineering and Technology Research (IJSETR), Vol . 4, February 2015.

[8] K.Manoj, S.Thiyagaraj, S.Sathyamoorthi, "Preventing Shoulder Surfing Attacks in ATM Using Base Pin and Base Character", In Journal of Engineering Research and Application vol. 5, June 2015

[9] Ms.R Revathy, Mrs.R.Bama, "Advanced Safe PIN-Entry Against Human Shoulder-Surfing", In IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 17, August 2015.

[10] Neelam S Khatkale, " Face Recognition Application in ATM Security", In International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, November 2015.

[11] Shweta Sankhwar, "A Safeguard Against ATM Fraud", In IEEE 6th Internation Conference on Advanced Computing, pp. 23-27, May 2016.

[12] Sivakami. R, "Security for Safety PIN Entry ", In International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, June 2016.

[13] Taekyoung Kwon and Sarang Na, "SteganoPIN: Two-Faced Human–Machine Interface for Practical Enforcement of PIN Entry Security", In IEEE Transactions On Human Machine Systems, vol. 46, pp. 314-317, September 2016.

[14] Sweta Singh, Akhilesh Singh, Rakesh Kumar "A Constraint-based Biometric Scheme on ATM and Swiping Machine", In International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), pp. 45-49, September 2016.

