International Journal of Education and Science Research Review
Volume-11, Issue-2 March-April-2024 E-ISSN 2348-6457
(Peer-Reviewed, Open Access, Fully Refereed International Journal) P-ISSN 2349-1817
www.ijesrr.org Impact Factor - 7.02 Email- editor@ijesrr.org

Enhancing ATM Security: A Virtual Shuffling Keypad Approach

Dr. R.G. Zope[1], Avishkar Sawant[2], Atharav Kadam[3]

Department of Electronics and Telecommunication Engineering

[1,2,3]KJ College of Engineering and Management Research, Pune 411 048, Maharashtra, India.

Savitribai Phule Pune University, Pune

rajendrazope.kjcoemr@kjei.edu.in, sawantavishkar03@gmail.com,
kadamatharva2626@gmail.com

Abstract:

All keypad-based access and authentication systems carry a high risk of password oversight by an unauthorized a person standing nearby, or by someone lying in wait who may purposefully watch your finger motions on the keypad and look for the password. Particularly at the Automatic Teller Machine (ATM) counter, you must input your Personal Identification Number (PIN) in order to access your account and withdraw money. However, someone can figure out your PIN if they see how, you input it. All they need to do now is obtain your ATM card, which they can achieve by either attacking you or pickpocketing you and taking it. They may now enter your PIN and take out the money since they already have an idea of how your fingers move.

Keypads are used not only in ATMs but in many more applications. We have devised a clever solution to this issue by rearranging the keypad, which will fool those who are causing the security risks with our own finger movements. such that our finger movements on the keyboard would prevent them from detecting the PIN.

They may now enter your PIN and take out the money since they already have an idea of how your fingers move.
Keypads are used for many applications, including ATMs. Our finger movements pose a threat to our security, so we come up with the innovative idea of a shuffling keypad to confuse the malicious guys. so that our finger movements on the keyboard would prevent them from detecting the PIN.

Our objective is to create a shuffled keypad whose key configuration change with each usage, even if the PIN was not accepted the previous time. The keypad will display a different layout each time you use it.

Keywords: **Authentication, Security, Password, Virtual Keyboard.**

1. Introduction

In all keypad-based access system or authentication system there are high chances of password being overseen by unknown person who are standing near you. Or low-lying persons can intentionally note you finger movements on the keypad and try to guess the password. Especially in ATM counter whenever you want to withdraw money you have to enter pin and then get access to your account. But if someone sees how you are entering the password, they can make out you pin then only thing is they have to get you ATM card for that they can do pick pocketing or they can assault you and snatch the ATM card now as already they have finger movements of yours in the mind, they can enter you pin and withdraw the money.

Not only in ATM, we are using keypads at many places and our own finger movements are putting our security at risk, for this problem we have come up with an innovative solution of shuffling keypad which will confuse the culprits and they would not be able to detect the password from our finger movements on the keypad.

Our idea is to implement a shuffling keypad whose key arrangement will change after every use, even if in last use the password was not accepted. Every time you use the keypad next time you will get different layout.

To implement about idea, we have implemented the shuffling keypad using Graphics LCD which is the heart of the system. here we have used resistive touch screen keypad for entering the four-digit PIN. Our actual concept is that when we press first digit among four digit the key position will be shuffle in random manner according to the program of randomization. Similarly, for every digit the process will be same [2].

1.1 Background and observation:

The idea of this system is to add some complexity, through user computations performed by heart/hand or by computation devices, to prevent the three kinds of attacks. There is a tradeoff of how complex the computation by the users can be. One goal is to find an easy to compute but secure scheme for computing.

We believe that for some sensitive accounts such as on-line bank accounts, on-line credit card accounts, and ATMs, users are likely to choose a little additional complexity requiring some degree of human computing in order to make the account more secure.

As the number of ATM machines present in a single room, there are more chances of stealing the password. To overcome this problem in this system, we try to secured the user’s transaction from culprits, tracing the finger movements by the person stand nearby the user [1,2].

1.2 Proposed Approach

The unsecured ATMs is as shown in figure 1. We propose the virtual password scheme. We propose randomized linear generation functions. Which will shuffle the number in the Random way which will not all the intruder to guess the password easily.

The goal of this system is to help users to provide high security to user password being stolen by the culprits.

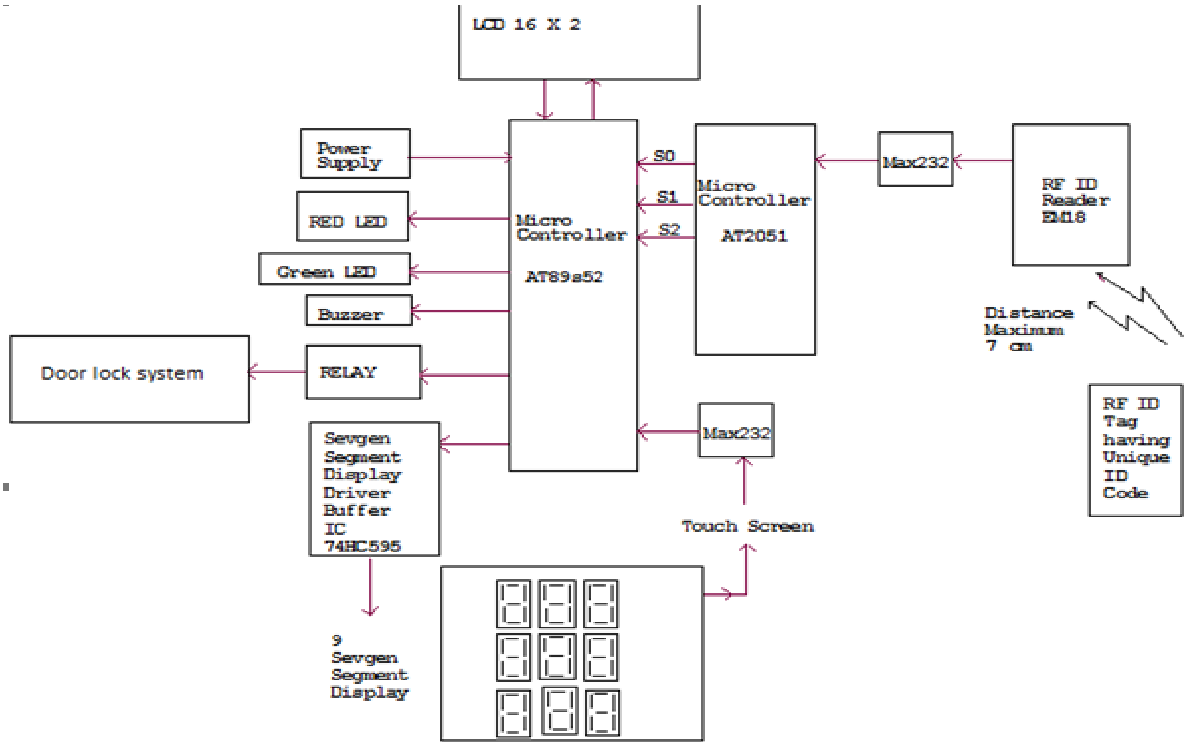
Figure 1: Unsecured ATMs.

2 System Overview:

Figure 2 shows the virtual shuffling keypad system overview for secure ATMs. In this system we are making a system which will help citizen to do things securely. We are implementing a system which will protect our PIN of ATM from hacking by culprits. Thus, we are developing a system that will fulfill our objectives.

Figure 2: System overview of virtual suffling keypad for secured ATMs.

RFID (Radio frequency identification) will be serving a purpose for authentication of ATM card from which we are interested to transact money. RFID reader gives the unique code of the tag when the tag comes in the range



of the RFID reader i.e. about 5 cm to 7cm. RF 'reader transmit the serial code to the microcontroller AT89c2051.

Microcontroller AT89c2051 receives this serially transmitted code by the RF reader and then it decodes same [2].

This signal will be the activation signal for main microcontroller AT89s52. AT89s52 microcontroller ask for the password by the Tx pin of Mmicrocontroller.

When the user enters first digit in a password the keypad gets shuffled randomly. This is done till all numbers of password get entered.

Random number generation algorithm is used to generate the shuffling of random numbers. Seven segment is used to display the numbers receives.

As soon as any citizen enter PIN of the ATM to our system, it will be recognized by microcontroller AT89s52. The Mmicrocontroller AT89s52 will then send command to LCD display for displaying notification text. Finally, transaction is successfully completed.

In this way we are providing protection to the PIN from stealing the password.

3. Experimental Observations:

In our laboratory, we have successfully tested and developed the virtual shuffling keyboard prototype is as shown in figure 3. Two RFID cards are used in our system; one is authorized and another is unauthorized.

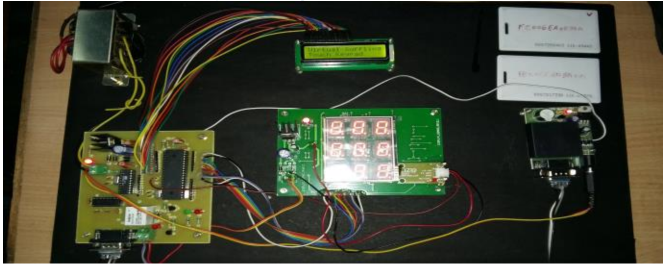


Figure 3: Virtual shuffling keyboard prototype

i) If the user shows the unauthorized card, then the notification of “Unauthorized Card” will be display on LCD is as shown in figure 4.

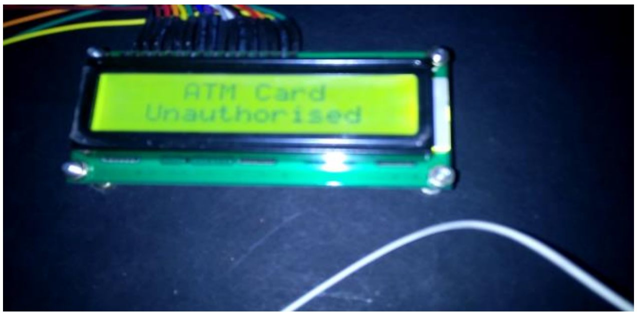


Figure 4: ATM card unauthorized

ii) If the users show the authorized card, then notification of “ENTER YOUR PIN” will display on the LCD is as shown in figure 5. After entering correct PIN, Green LED will turn ON as well as “ATM PIN Correct “and “Transaction Successfully Done” message will be display.

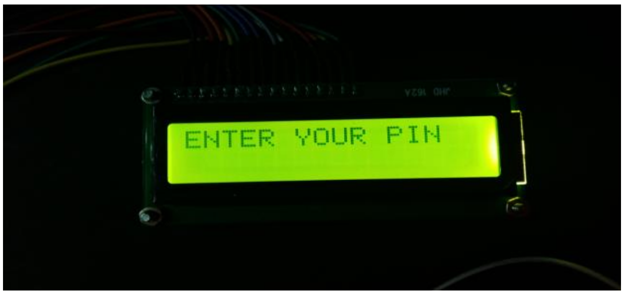


Figure 5: Enter your PIN

iii) Now If entered PIN is wrong then notification of “PIN Entered is Incorrect” will be display on LCD is as shown in figure 6.. Red LED will give visual indication as well as Buzzer will give audio indication.

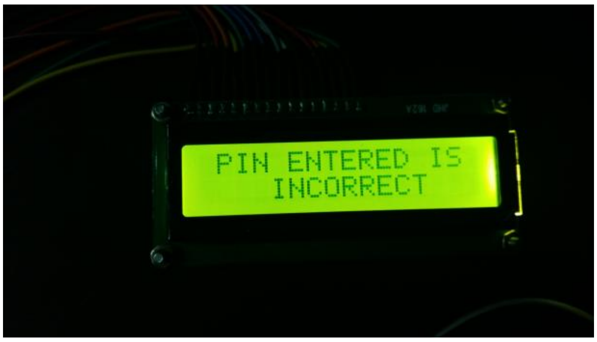


Figure 6: PIN entered is incorrect

4. **Conclusions:**

In our lab, we have successfully tested and built the virtual shuffling keypad prototype for secure ATMS, preventing users' passwords from being stolen by adversaries. A proposal for virtual passwords that secures user credentials in online settings, ATMs, and ubiquitous computing by using a little bit of human computation. Since a server has access to more information than any advertiser, we decided to employ user-determined randomized linear generating functions to secure users' passwords. We examined the system's defenses against shoulder-surfing attacks, Trojan horses like key loggers, and phishing. We felt that despite their shortcomings, the suggested virtual functions or their variations will be highly helpful for online services, ATMs, and pervasive computing.

5. References

[1]. Ankit Parekh, Ajinkya Pawar, Pratik Munot and Piyush Mantri, 2011.Secure Authentication using Anti-Screenshot Virtual Keyboard, International Journal of Computer Science Issues, 8(5): 3, September 2011.

[2]. Fujita, K. and Y. Hirakawa, 2008. A study of. password authentication method against observing Password based authentication. 6th International Symposium on Intelligent Survey. IEEE., SISY 2008.

[3]. V.Varalakshmi1,Mrs.P.Kanimozhi "Secure PIN Authentication for ATM Transactions Wireless Devices" International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 3, Special Issue 22, April 2016

[4]. Muhammad Ali Mazidi, Janice Gillispie Mazidi, Rolin D. Mckinlay, The 8051 Microcontroller and Embedded systems Using Assembly and C,2nd edition.

[5]. M.M. Shah, Design of Electronics Circuits and Computer aided design, Wiley Easten Limited Publication.

[6]. Kumaresan S,Suresh Kumar K, Dinesh Kumar G,Implementation of Secure ATM by Wireless Password Transfer and Shuffling Keypad

[7]. Prof .S.S. Punde , Takle Nikhil Dnyaneshwar , Thakare Samadhan Suresh,Virtual Shuffling Keypad and Wireless Password Transfer for Secure ATM Transactions

[8]. Kirankumar A, Bharath P N, Manjunath G,Virtual Shuffling Keypad for Secure ATMs

[9]. Zaid Imran and Rafay Nizami, "Advance Secure Login" International Journal of Scientific and Research Publications, Vol. 1, Issue 1, SSN 2250-3153, December 2011.

[10]. Gazal Betab and Ranjeet Kaur Sandhu, "Fingerprints in Automated Teller Machine-A Survey" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Vol.3, Issue-4, April 2014.