Contemporary Engineering Sciences, Vol. 7, 2014, no. 10, 449 - 455
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2014.4329

Two Factor Authenticated Cash Withdrawal Using Mobile Phones and Apprehend Insecure Users within the ATM Centre

A. C. Jayasudha

School of Computing, SASTRA University,
Thanjavur-613401, India

Abstract

In banking systems, cash cards are provided with pin facilities to withdraw cash and it is ubiquitous. Consequently, security risk are also emerged in all dimensions. Hence, this project proposes, two factor authentication method to have high privacy and detain the intruder or unauthorized user within the ATM center. Initially this claimed system, verifies the user is authenticated or not. If it is confidential server allows transaction or else certain detain functions are activated. Thus, the hackers, distributing the security protocol and password schemes by invading the ATM machines with the aid of duplicate card is restricted.

Keywords: Banking system, ATM, Authentication, Secure cash withdrawal, Intruders

1 INTRODUCTION

With the advancement in technology and communication, automatic machines are emerging to give sophisticated environment. Banking system remains as a very good platform to save, withdraw and transfer money from one place to another. This consumes large time and advancement in technology, embedded system launched ATM service machine. In spite of such services, unauthorized user gain data and they misuse the system. To tackle this problem, concept of embedded security was introduced. Many researchers formulated several security design for authenticated transaction[8] in banking application.

2 METHODOLOGIES

Secure cash withdrawal using mobile phone[9] describes the architecture for cash withdrawal in ATM machine using mobile phone and banking application. The design comprises RFID, NFC technology, security protocols viz WEP, WPA, biometric data. RFID reader is equipped with ATM machines, which senses the presence of signal emitted from mobile phone, then server provides service to the user aided by NFC technology[10]. If the user is authenticated, transaction is allowed. Updated information is send to the banking system. The main drawback includes, hacking the password is easy and security is not reliable. security threats such as replay attack, spoofing, guessing attack, phishing attack, modification attack, smurf attack, stolen verifier attack[6] are possible.

OTP based two factor authentication[2] [4] describes the method of increasing security from hacking password. Level of authentication provided to the user is based on two factor authentication[3] which sends SMS instantly to the user generated by the system server and changes from time to time. Using multiple OTPs and nested hash function[5] host delivers the username. Challenges must be satisfied by the user, server checks for authentication and allows further transaction.

Intruders try to hack these challenges knowing the schemes such as pre-play attack, forgery attack, insider attack and small challenge attack. These security risks are overcome by this algorithm possessing forward and infinite OTP generation[7] with two nested hash function. Computational risk of the algorithm and server clock synchronization is of less importance to improve the practical reliability. Also problems of SMS cost, delay and roaming[1] are also solved in this authentication process.

Inspite of strengthen password authentication system, hacking remains as a continuous process. To apprehend those hackers at the spot of trying to access unauthorized smart cards, we propose a new system. it explains that when someone try to misuse the ATM card by developing duplicate one and entered a wrong password, further transaction is blocked. Doors of ATM centre is locked and a camera connected to the system is turned ON . also ATM module number is sent to as a SMS to the user, banking system and nearby police station.

3 SYSTEM OVERVIEW

RFID reader is placed on the ATM machine and the user approaching services are read by sensing emitted signal from RFID tag enclosed in mobile phone. First host embarks service by offering certain challenges to the user's mobile phone owing through GSM module, which is developed for security purpose. Reply is sent via message. If it satisfies the data updated in host server, then driver switch to the relay, which allow further transaction. The amount to be withdrawn is sent as message from mobile phone. It must match the amount entered in ATM machine. Or else transaction will not be proceeded. If the reply for the challenges does not matches updated criteria in the server, system sends that transaction is blocked. Microcontroller permits driver to switch the relay for transaction blocked section. The overall proposed system model is shown in figure 1;

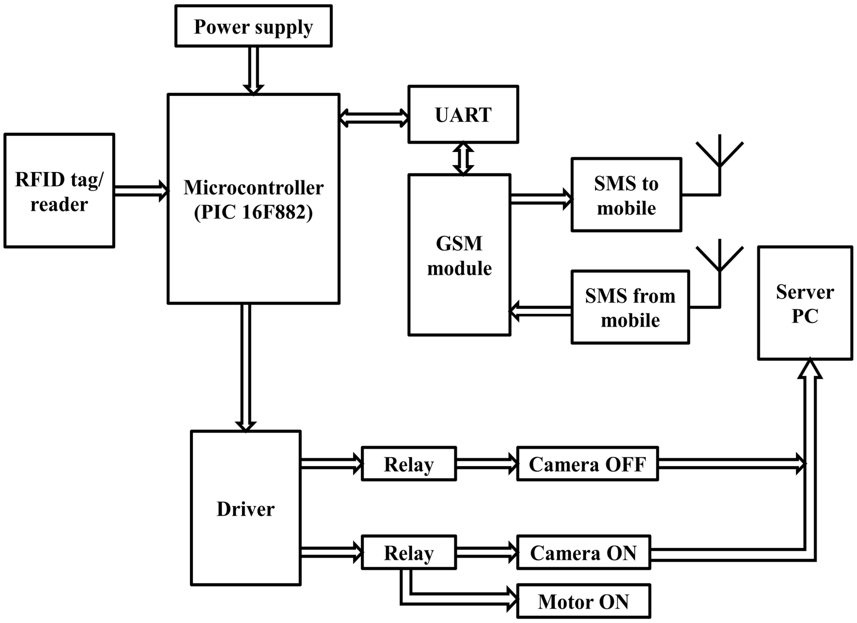


figure 1: Proposed system model

It pursuits the following action;
i) Buzzer is enabled to produce alert signal
ii) Doors of the ATM machine is locked by activating DC motor
iii) separate camera connected with this section is turned ON. Snapshot of the person will be taken. It is stored and sent by the server for immediate investigation
iv) Also ATM module number is sent to the user, nearby police station and banking system.

These system helps in immediate tracing of hacker.

4 SYSTEM HARDWARE ARCHITECTURE

5V power supply is required for the controller. So 230V, 5HZ single phase AC input voltage is converted into 5V DC supply using step down transformer, bridge rectifier, 2200µf capacitor and 7805 voltage regulator. Hence power supply is indicated using LED.

RFID tag/reader is embed along with user's mobile phone and ATM machine respectively. Passive RFID tag is chosen to tackle near field coupling. RFID tag acquires power from reader by following the design issues such as magnetic induction and electromagnetic wave capture. when the tag approaches the reader, an alternating voltage will be developed from the tag's smaller coil. Alternating voltage is rectified and by coupling it to the capacitor, power is obtained. Data from tag is identified and encoded by the reader. Tag's ID and associated details are sent to the microcontroller. Server checks for confirming user's account and begins the process.

PIC microcontroller (PIC16F882) is opted for my application. PIC16F882 are 8 bit CMOS microcontroller pursuing nanowatt technology. The signal from RFID reader is sent to the user and if it identifies as an authorized user, microcontroller start sending SMS generated from host system, through GSM module. It routes the reply from user to the host server. Based on the reply, it activates the driver to switch corresponding relay. At the same time, action performed is sent as message to the user.

Q2303A GSM module type is used to communicate with the user by sending text message. It act as a wireless interface between user and application system. The data from microcontroller are transmitted to Q2303A module using UART cable. PIC16F882 operating voltage is 5V and follows TTL logic. But UART works in RS232 logic. Hence, MAX 232 will convert TTL logic into RS232 logic, whose output is fed to UART, inturn connected to GSM module. Collected data are transmitted to mobile number updated in the banking server. Also reply sent from mobile user is received by GSM module and transmitted back to microcontroller.

ULN2003 driver is preferred for our application. It acts as a buffer circuit and used to drive large current or voltage upto 600mA and 50V. Microcontroller handles just 0V-5V. Based on the input either 0V or 5V, ULN2003 convert this TTL logic into large current/voltage respectively to drive heavy load devices. Depending on the reply from user, microcontroller sends information to the driver. Accordingly, one relay is switched ON, other remains idle. Audacity for opting and energizing the relay is made possible using driver.

Solid state relay is used in our application. It act as a electronic switch device and not as electromechanical device. It conducts electrical current to the device connected. Two relays present are present in this system. If the reply from user is satisfied, microcontroller switches the first rely that has transaction proceeding section. Cash withdrawal is done successfully. otherwise, if challenges are not met by the user, second rely is switched ON. It drives buzzer, camera and motor. Buzzer sound is produced, camera is turned ON to capture the image and transmitted. DC motor is run to lock the door.

Webcam is similar to videophones which make computer holding camera and communicate over the Internet. This type of camera is installed to an individual computer with the help of 'USB2.0 PC camera' software driver. It permits USB port of the computer to capture moving image legibly and is uploaded to the central server.

The following setup demonstrate the prototype of the proposed system as shown in the figure 2;

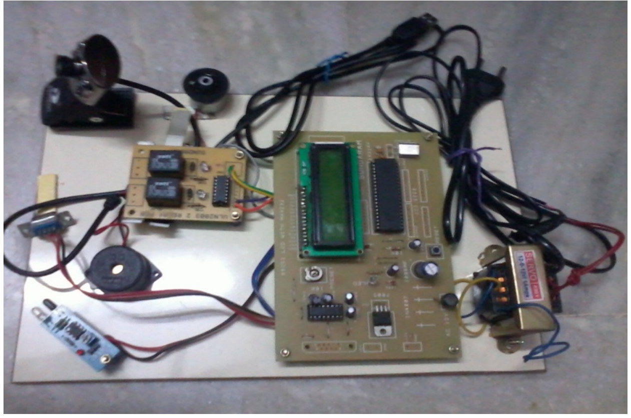
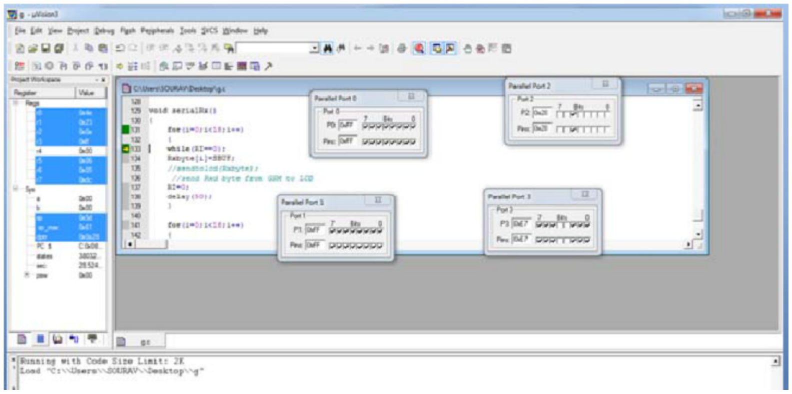


Figure 2: Hardware prototype used in the system

5 SOFTWARE ARCHITECTURE

The code required for the application is written based on embedded C programming. It adds more feature and user friendly. They are complied and executed with the support of keil C compiler. The debugging of the application code using keil C complier is shown in the figure 3.



```
void serialRx()
{
     for(i=0;i<18;i++)
     {
     while(RI==0);
     Rxbyte[i]=SBUF;
     //sendtolcd(Rxbyte);
      //send Rxd byte from GSM to LCD
     RI=0;
     delay(50);
     }

     for(i=0;i<18;i++)
     {
```

```
Running with Code Size Limit: 2K
Load "C:\\Users\\SOURAV\\Desktop\\g"
```

Figure 3: Code executed using Keil C complier

6 CONCLUSION

The consequences of using ATM cards for cash withdrawal in ATM machine, paves way for gaining data by unauthorized user. To strengthen the security issues of user's account, various password schemes were proposed; that includes touching, pointing, two factor authentication one time password, hash function and nested hash function. Inspite of these authenticated algorithm, hacking is done continuously. Our paper recommends the design and implementation, to avoid exploring the schemes during cash withdrawal and to lock the person at the moment of hacking process. This invokes confidentiality that hackers could not try to understand the security schemes. Hence frequent remedy for insecure cash withdrawal can be reduced.

REFERENCES

[1] Abdullahi Arabo, "Secure Cash Withdrawal through Mobile Phone/Device ", in Proceedings of the International Conference on Computer and Communication Engineering, 2008, 818-822.

[2] Daojing He, Maode Ma, Yan Zhang, Chun Chen, Jiajun Bu, "A strong user authentication scheme with smart cards for wireless communications", Computer Communications 34, 2011, 367-374.

[3] Francesco Buccafurri, Gianluca Lax, "Implementing disposable credit card numbers by mobile phones", in Springer Science+Business Media, LLC 2011.

[4] Kuo-Hui Yeh, Chunhua Su, N.W. Lo, Yingjiu Li, Yi-Xiang Hung, "Two robust remote user authentication protocols using smart cards", in The Journal of Systems and Software, 2010, 2556-2565.

[5] Manoj Kumar, "An Enhanced Remote User Authentication Scheme with Smart Card", International Journal of Network Security, 10(3) (2010), 175-184.

[6] Mohamed Hamdy Eldefrawy, Khaled Alghathbar, Muhammad Khurram Khan, "OTP-Based Two- Factor Authentication Using Mobile Phones", in 2011 Eighth International Conference on Information Technology: New Generations, 2011, 327-331.

[7] Ms. Trupti Hemant Gurav, Ms. Manisha Dhage, "Remote client Authentiction using mobile phone generated OTP", International Journal of Scientific and Research Publications, 2(5), 2012.

[8] Sagar Acharya, Apoorva Polawar, P.Y.Pawar, "Two Factor Authentication Using Smartphone Generated One Time Password", IOSR Journal of Computer Engineering, 11 (2) (2013), 85-90.

[9] Sagar Gajbhar, Shrikant Aher, Swapnil Auti, Shailesh Hodge, "Authentication using Mobile phone generated OTP", International Journal of Computer Science and Management Research 2(5) (2013).

[10] Välkkynen, P. Korhonen, I., Plomp, J., Tuomisto, T., Cluitmans, L., Ailisto, H. and Seppä, H. "A user interaction paradigm for physical browsing and near-object control based on tags": in Proc. Physical Interaction Workshop on Real World User Interfaces, 2003, 31-34.

Received: March 1, 2014