www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 4 April, 2013 Page No. 1346-1350

Protected Cash Withdrawal in Atm Using Mobile Phone

M.R.Dineshkumar[1] M.S.Geethanjali[2] R.Karthika[3] M.Nagaraj[4] N.Vijayanandam[5]

KNOWLEDGE INSTITUTE OF TECHNOLOGY, SALEM.
[1],[2],[3],[4] UG students, Department of Electronics and Communication Engineering,
[5] Assistant Professor, Department of Electronics and Communication Engineering.

ABSTRACT

In recent days different access control methods have been proposed to secure the ATM Transaction from unauthorized access. This paper describes a method of implementing two way authentication. The first one is normal PIN verification method and if the password is correct then it goes to the second step of authentication (i.e.,) two way authentication method. In that if the authorized person replied YES through their mobile, then corresponding transaction takes place. Otherwise it switches ON the buzzer, automatically close the door of ATM centre and LCD will show the detail about ATM theft to the higher authorities.

Keywords: ATM, Two way authentication, Reply Message Option, SMS.

1.INTRODUCTION

The ATM was invented to solve the problem of long queue in banks and to improve the quality of banking services to customers. With the ATM, customers can access their bank accounts in order to

make cash withdrawals and check their account balances as well as purchasing mobile phone prepaid credit. Being a machine, it is important that it authenticates the user each time he/she applies for access to ATM Services. This is usually done by the insertion of an ATM card which contains a unique card number and security information such as a PIN number which is unique to every user. Anybody can be in the possession of the card and the person may have knowledge of the users PIN. This makes this approach vulnerable to ATM fraud.

The two way authentications are many in use for cash withdrawal in ATM. Some of the two way authentications are using mobile phone as medium to involve second step of authentication. By using mobile phone, a One Time Password (OTP) or One off Transaction Password (OOTP) or Mobile Phone Authentication Approval is the second step authentication [1], [2], [4].

Multifactor Authentication (MFA) is a security system in which more than two form of authentication is implemented to verify the

legitimacy of a transaction. In this authentication system, the biometric authentication may be one way of authentication. Because of its multiple step or biometric verification to authenticate the user, the system complexity get increases but it provides higher level of security [3].

2. EXISTING METHODOLOGY

The existing system of two-factor authentication using mobile phones, are used to generate the one time password (OTP) [2].By definition, authentication is the use of one or more mechanisms in order to prove that you are who you claim to be. Once your identity is validated, access is granted [1]. Three universally recognized authentication factors exists today: what you know (passwords), what you have (tokens, cards) and what you are (biometrics). Recent work has been done in trying alternative factors, for example somebody you know, a factor that can be applied in social networking.

Two-factor authentication is a mechanism that implements two of the above mentioned factors and is considered stronger and more secure than the traditionally implemented one factor authentication system. For example, withdrawing money from an ATM machine uses two factor authentication: the ATM card (what you have) and the personal identification number (what you know).

Passwords are known to be one of the easiest targets of hackers. Therefore, most companies are searching more ways to protect their customers and employees. Biometrics are known to be very secure [2], but are used only in special organizations (such as military organizations) given the expensive hardware needed and their high maintenance costs. As an alternative, banks and companies are using tokens as a way of two-factor authentication.

A token is a physical device that generates passwords needed in an authentication process. Tokens can either be software or hardware. Hardware tokens are small devices that can be easily carried. Some of these tokens store cryptographic keys or biometric data. Anytime a user wants to authenticate in a service, he uses the one-time password displayed on the token in addition to his normal account password. Software tokens are programs that run on computers and provide a onetime password that it is changed after a short amount of time (usually 30 seconds). OTP algorithm's security is very important because no one should be able to guess the next password in sequence. The sequence should be random to the maximum possible extent, unpredictable and irreversible. Factors that can be used in OTP generation include names, time, seeds, etc. Several commercial two-factor authentication systems exist today such as RSA Secure ID [2].Multifactor authentication uses more than two form of authentication and it provides higher security [3].

3. PROPOSED METHODOLOGY

In this project we analyzed what are the problem people faced in the existing technology. Especially Multifactor Authentication (MFA) method provides more complexity to the user.

This project helps to overcome the problem of complexity and provides easiest way to secure the ATM card. Whenever ATM card is

inserted into the ATM card slot, the system requires PIN to authenticate the user. If PIN gets verified, it sends authentication message to the user's mobile. If the user replied to make a transaction, then transaction process takes place. Otherwise it switches ON the buzzer and gives detail about fraud to the higher authorities. The proposed system uses GSM modem for sending authentication message from ATM to the user and getting Reply Message Option (RMO) from user to ATM. If the authorized person transaction takes place Reply Message Option is YES otherwise no transaction occur.

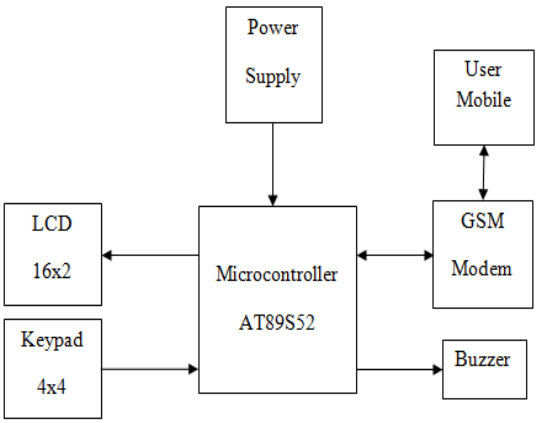

Figure-1: Block diagram of proposed model

3.1 HARWARE DESCRIPTION

ATMEL 89S52

The AT89S52 is a low-power, high-performance CMOS 8-bit microcontroller with 8K bytes of in-system programmable Flash memory. The device is manufactured using Atmel's high-density non volatile memory technology and is compatible with the industry-standard 80C51 instruction set and pin out.

POWER SUPPLY UNIT

The power supply unit used here consists of two regulators: 7805 and 7812.7805 IC is used so as to get 5V supply to run ATMEL 89C51 microcontroller.7812 IC is used to get 12V supply to energize the relay and run the DC motor. The power supply should be of +5V, with maximum allowable transients of 10mv.To achieve a better /suitable contrast for the display, the voltage at pin 3 should be adjusted properly.

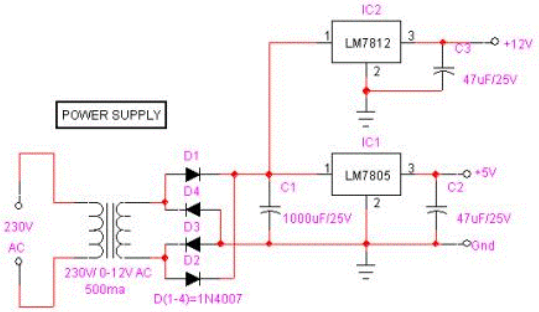

Figure-2: Circuit diagram of Power supply

GSM MODEM

The GSM modem is slightly different from the conventional modem. This utilizes the GSM standard for cellular technology. Here, one end being a wired connection, receives and transmits data. The other end is connected to a RF antenna. The GSM modem acts like a cellular phone and transmits text and voice data. It communicates with the GSM network via the SIM (Subscriber's Identity Module).

LCD

LCDs are common because they offer some real advantages over other display technologies. They are thinner and lighter and draw much less power than cathode ray tubes(CRTs).

KEYPAD

A **keypad** is a set of buttons arranged in a block or "pad" which usually bear digits, symbols and usually a complete set of alphabetical letters.

If it mostly contains numbers then it can also be called a **numeric keypad.** The keypad Switches are connected in a matrix of rows and columns : The rows of the matrix are connected to four output port lines. The columns of the matrix are connected to four input port lines.

3.2 SOFTWARE DESCRIPTION

KEIL MICRO VISION

Keil development tools for the 8051 microcontroller family support every level of developer from the professional applications engineer to the student just learning about embedded software development. The industry-standard Keil C Compilers, Macro Assemblers, Debuggers, Real-time Kernels, and Single-board Computers support ALL 8051-compatible derivatives and help you get your projects completed on schedule.

EMBEDDED C PROGRAMMING

The 'C' Programming Language was originally developed for and implemented on the UNIX operating system, by Dennis Ritchie in 1971. One of the best features of C is that it is not tied to any particular hardware or system. This makes it easy for a user to write programs that will run without any changes on practically all machines.

C is often called a middle-level computer language as it combines the elements of high-level languages with the functionalism of assembly language. To produce the most efficient machine code, the programmer must not only create an efficient high level design, but also pay attention to the detailed implementation.

4. CONCLUSION

The proposed system based on microcontroller is found to be more compact, user friendly and less complex which can readily be used in order to perform several tedious and repetitive tasks. Though it is designed keeping in mind about the need for industry it can extended for other purposes such as commercial and research applications. Due to the probability of high technology (GSM) used this "Protected Cash Withdrawal in ATM Using Mobile Phone" is fully software controlled with less hardware circuit. The feature makes this system is the base for future systems.

REFERENCES

[1] Kumar, K.Shailaja, G.Shailaja, A.Kavitha and A.Saxena, "Mutual authentication and key agreement for GSM", International Conference on Mobile Business (ICMB'06), pp. 25-26, 2006.

[2] Z.Li, Q.Sun, Y. Lian and D.Giusto, "An association based graphical password design resistant to shoulder surfing attack", IEEE International Conference on Multimedia and Expo, China, pp. 245-248, 2005.

[3] A.D.Luca, M.Langerich and H.Hussmann, "Towards understanding ATM security: a field of real world ATM use", In Proceedings of the sixth symposium on Usable Privacy and Security, ACM: Redmond, Washington, pp. 1-10, 2010.

[4] Zaslavskv.V and Strizhak.A, "Credit card fraud detection using self-organizing maps", Information and Security, pp. 48-63, 2006.

[5] Binachi.A, Oakley.I and Kwon.D.S, "Using mobile device screens for authentication", In Proceedings of the 23rd Australian Computer-

Human Interaction conference, OzCHI'11, ACM (NY, USA), pp. 50-53,2011.

[6] Boyd.J, "Here comes the wallet phone", IEEE Spectrum.42, Vol.11, pp. 12-14, 2005.

[7] Panjwani.S and Cutrell.E, "Useably Secure, low cost authentication for mobile banking", In Proceedings of the sixth symposium on Usable Privacy and Security, SOUPS'10, ACM (Redmond, Washington), ACM ID: 1837116, pp. 4:1-4:12, 2010.

[8] Furnell.S.M, Morrissey.J.P, Sanders.P.W, Stockel.C.T, "Applications of keystoke analysis for improved login security and continuous user authentication", Proceedings of Information Systems Security, pp. 283-294, 1996.

[9] Hamilton.D.J, Whelan.J, McLaren.A, MacIntrye.I, Tizzard.A, "Low cost dynamic signature verification system", IEEE conference Publication 408, England, pp. 202-206, 1995.

[10] T.S.Messengers, E.A.Dabbish and R.H.Sloan, "Examining Smart-Card Security under the Threat of Power Analysis Attacks", IEEE Trans. Computers, Vol.51, no.5, pp.541-552, May 2002.