iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VI **Month of publication:** June 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Theft Prevention for Improvising Authenticity and Security of Automated Teller Machine System

Ayesha R. Syed[1], Vijay R. Wadhankar[2]
[1]*Electronics Engineering Department, R. T. M. Nagpur University*

Abstract— Attacks on ATM are on the increase world-wide. The cash handling, financial and banking companies have always taken the threat of villainous attacks very seriously and are constantly striving to improve their security measures. The main objective of this work aims at to develop an embedded system which is used for ATM security applications. This system would in turn benefit all the customers and the bankers will collect the customer mobile number who have a valid ATM card registered officially. On most modern ATM's the customer is identified by inserting a plastic ATM card with a magnetic stripe having a chip that contains a unique card number. Authentication is provided by the customer entering a personal identification number (PIN).
Keywords— ATM, PIN, RFID Module, GSM Module, GPS.

I. INTRODUCTION

An ATM card is any payment card issued by a financial institution that enables a customer to access an automated teller machine (ATM).An automated teller machine or automated banking machine (ABM), cash machine or cash point is an electronic telecommunications device that enables the customers to perform financial transactions, particularly cash withdrawal. Most ATM's are connected to interbank networks enabling people to withdraw and deposited money from machines not belonging to the bank where their accounts are held. ATM's rely on authorization of a financial transaction by the card issuer or other authorizing institution on a communications network. This is often performed through an ISO 8583 messaging system. ATM's typically connect directly to their host or ATM Controller or dial-up modem over a telephone line. The security of ATM transactions relies mostly on the integrity of the secure crypto processor. Encryption of personal information required by law in many jurisdictions, is used to prevent fraud. Sensitive data in ATM transactions are usually encrypted with DES, but transaction processors now usually required the use of Triple DES. The input device for an ATM is a card reader, which initially identifies the account. A keypad is used to enter passwords and select transactions. A depository allows the user to deposit cash or checks. The output devices include a currency dispenser, receipt printer, speaker and display screen. Inside most ATM's in the twenty-first century are PC's with an Intel processors chip running IBM's operating system. Software and hardware developed by ATM manufactures connects all of the peripheral devices of the ATM.

II. METHODOLOGY

In this Project Access to the ATM is given by using the Smart card Technology, which consist of two parts hardware and software. The hardware part consist of Microcontroller, Smart card Tag, Smartcard reader, GSM module, Keypad, LCD and some steps of software. The more details are as follows:

A. Hardware Description

The AT89S52 microcontroller is the main component of the entire system. Furthermore the modules of LCD, Keypad, GSM and RFID are connected with the main chip. There are some modules consisted of the system as follows:

1) *RFID Module*: A basic RFID system consists of three components:
An antenna or coil
A transceiver (with decoder)
A transponder (RF tag) electronically programmed with unique information

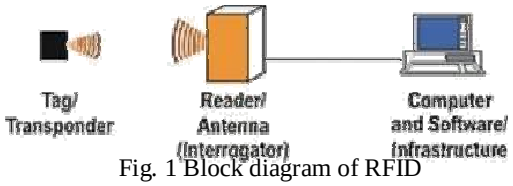


Fig. 1 Block diagram of RFID

The purpose of an RFID system is to enable data to be transmitted by a portable device, called a tag, which is read by an RFID reader and processed according to the needs of a particular application. The data transmitted by the tag may provide identification or location information. A typical RFID tag consists of a microchip attached to a radio antenna mounted on a substrate. The chip can store as much as 2 kilobytes of data.

2) *GSM Module:* GSM module is used to establish communication between a computer and a GSM system. Its Operation is Receiving and sending messages in a SIM. GSM is required to send an OTP (One Time Password). If OTP doesn't match then message will send on authorised mobile phone through GSM Module.The longest distance the GSM specification supports in practical use is 35 kilometres. Here the system is capable of controlling the devices by receiving control messages from an authorized mobile number.
3) *LCD Display:* A liquid crystal display is a thin, flat electronic visual display that uses the light modulating properties of light crystal (LCs). It is an output device. When we give the power supply then LCD is on & the coding which is in the microcontroller is display on the screen. After inserting card the instruction i.e. display on the screen of LCD. LCDs do not emit light directly. LCDs are more energy efficient and offer safer disposal than CRTs.
4) *Keypad:* A keypad *is* a set of buttons arranged in a block or "Pad" which usually bear digits & other symbol & usually a complete set of alphabetical letters. If it mostly contains numbers then it can also be called a numeric keypad. It is a input device, in our project we use 4*4 keypad layout. It is use for writing the password & the OTP number.
5) *GPS Module:* The Global Positioning System (GPS) is a space- based satellite navigation system that provides location and time information. It is maintained by United States government and is freely accessible to anyone with a GPS receiver.The GPS satellites rotate twice a day around the earth in a specific orbit. These satellites transmit signal information to earth. GPS is used to measure 2D position (latitude, longitude) and track movement.

The proposed block diagram of the ATM security system as shown below:

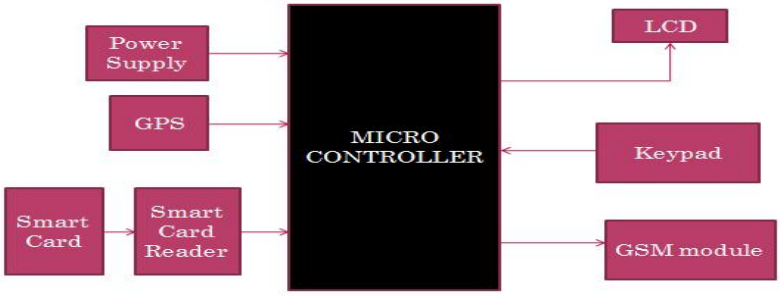


Fig. 2 Basic block diagram of ATM security system

B. Software Description

The embedded platform discussed above is programmed in C language with KeilµVision4.

µVision4 is an IDE (Integrated Development Environment) that helps you write, compile, and debug embedded programs. It encapsulates the following components:

A project manager.
A make facility.
Tool configuration.
Editor.
A powerful debugger.

The µVision simulator traps and reports illegal memory accesses. In addition to memory mapping, the simulator also provides support for the integrated peripherals of the various 8051 derivatives. The on-chip peripherals of the CPU you have selected are configured from the Device. After you have tested your application, it is required to create an Intel HEX file to download the software into an EPROM programmer or simulator. µVision creates HEX files with each build process when Create HEX files under Options for Target – Output is enabled. You may start your PROM programming utility after the make process when you specify the program under the option Run User Program #1. Target are all you need to start a new application. You may translate all source files and line the application with a click on the Build Target toolbar icon. When you build an application with syntax errors, µVision4 will display errors and warning messages in the Output Window

Build page. A double click on a message line opens the source file on the correct location in a µVision4 editor window. Once you have successfully generated your application you can start debugging. Start the debug mode of µVision4 with the Debug – Start/Stop Debug Session command. Depending on the Options for Target – Debug Configuration, µVision4 will load the application program and run the start-up code µVision saves the editor screen layout and restores the screen layout of the last debug session. If the program execution stops, µVision4 opens an editor window with the source text or shows CPU instructions in the disassembly window. The next executable statement is marked with a yellow arrow. During debugging, most editor features are still available.

For example: creation of programme

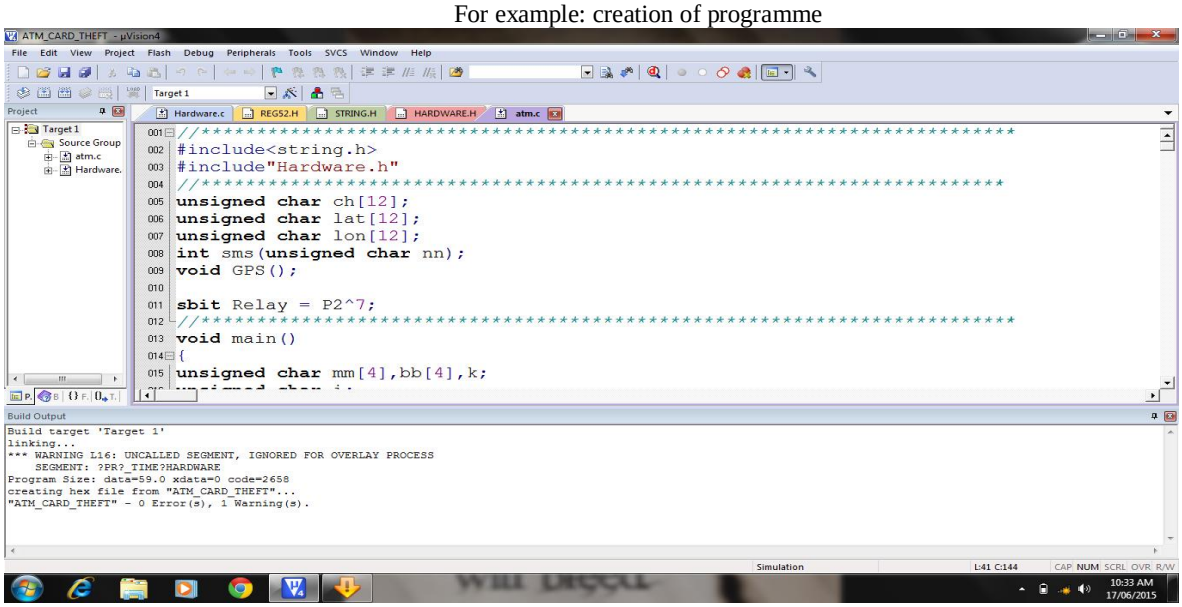


Fig. 3 Compiling programmed

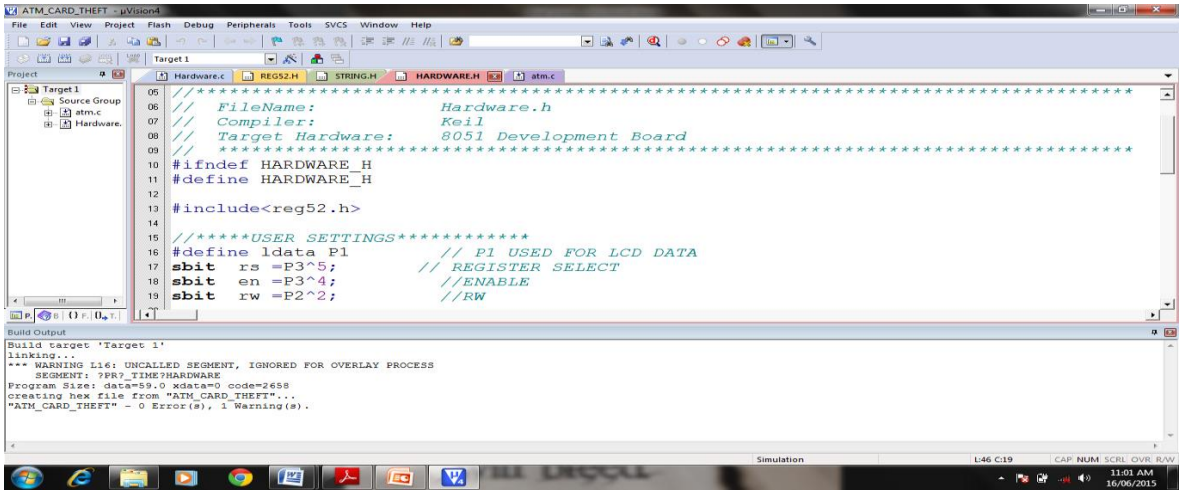


Fig. 4 Hex file

III. CONCLUSIONS

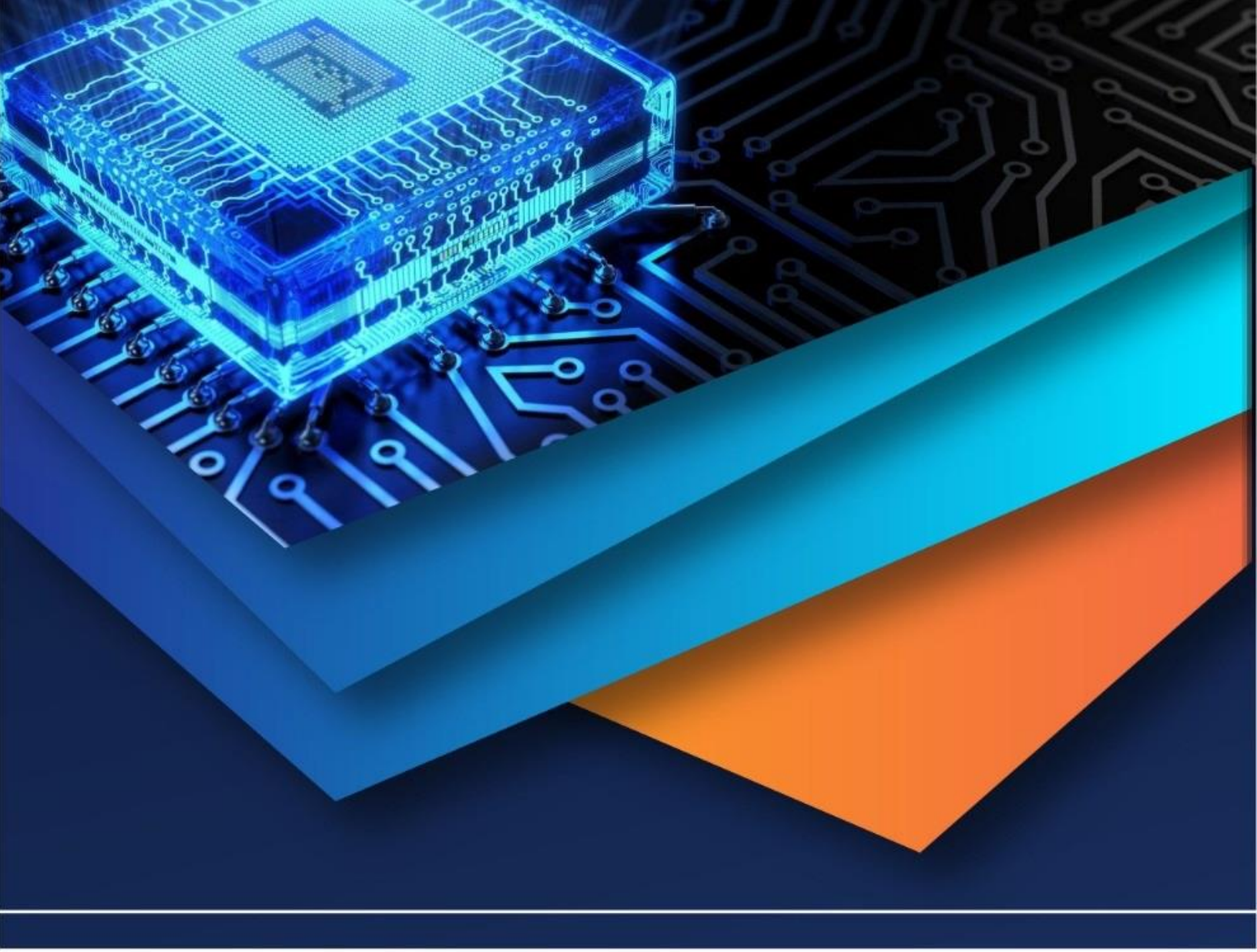
We have been able to develop a system to enhance the security features of the ATM for effective banking transaction for banks. This system of Authentication can also be used in various other application that offers related services in both security and integrity of data being handled. This system when fully deployed will definitely reduce the rate of fraudulent activities on the ATM machines such that only the registered owner of a card access to the bank account.

IV. ACKNOWLEDGMENT

I would like to express our sincere gratitude towards Prof. Vijay Wadhankar of the Department of Electronics & Communication Engineering, Rashtrasanth Tukduji Maharaj Nagpur University India(MS) for guiding me throughout this paper research and providing me eclectically the resources needed for me to make this paper possible. Without his help and guidance I cannot bring the theories into practice.

REFERENCES

[1] Mr Abhijeet S. Kale, 2, Prof. Sunpreet Kaur Nanda" Design of Highly Secured Automatic Teller Machine System by Using Aadhaar Card and Fingerprint" www.ijesi.org Volume 3 Issue 5‖ May 2014 ‖ PP.22-26
[2] Srivatsan Sridharan1, Gorthy Ravi Kiran2, Sridhar Jammalamadaka3" Improvising Authenticity and Security of Automated Teller Machine Services" IJCSMC, Vol. 3, Issue. 2, February 2014, pg.666 – 674
[3] Mr. John Mashurano1, Mr. Wang liqiang2, "ATM Systems Authentication Based On Fingerprint Using ARM Cortex-M3" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 3, March - 2013 ISSN: 2278-0181 1 www.ijert.org IJERTIJERT
[4] Aru, Okereke Eze, Ihekweaba Gozie "Facial Verification Technology for Use In ATM Transactions "American Journal of Engineering Research (AJER)e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-02, Issue-05, pp-188-193 www.ajer.us
[5] Laudon Kenneth, Traver Carol Guercio, E-Commerce (2005), Second Edition , pp. 237-239, Pearson Education (Singapore), Pvt. Ltd.
[6] Ibidapo, O. Akinyemi, Zaccheous O. Omogbadegun, and Olufemi M. Oyelami, "Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria E-Banking System" International Journal of Electrical & Computer Sciences IJECS-IJENS Vol:10 No:06
[7] M. Subha and S. Vanithaasri "A study on authenticated admittance of ATM clients using biometrics based cryptosystem" International Journal of Advances in Engineering & Technology, Sept 2012. ©IJAET ISSN: 2231-1963Vol. 4, Issue 2, pp. 456-463
[8] Lasisi, H.; Ajisafe, A.A., "Development of stripe biometric based fingerprint authentications systems in Automated Teller Machines," Advances in Computational Tools for Engineering Applications (ACTEA), 2012 2nd International Conference on , vol., no., pp.172,175, 12-15 Dec. 2012 doi: 10.1109/ICTEA.2012.6462860
[9] Patiyoot, D.; Shepherd, S.J., "Security issues for wireless ATM network," Universal Personal Communications, 1998. ICUP'98. IEEE 1998 International Conference on, vol.2, no., 5-9 Oct 1998 doi: 10.1109/ICUPC.1998.733713
[10] Bharath E, Dhananjaya K M, Anoop C.N, Raghavendra B V "Automated Teller Machine (ATM) Banking a User friendly"ISSN : 2230-9519 (Online) | ISSN : 2231-2463 (Print) IJMBS Vol. 2, Issue 4, Oct - Dec 2012
[11] Jain, A.K.; Ross, A.; Prabhakar, S., "An introduction to biometric recognition," Circuits and Systems for Video Technology, IEEE Transactions on, Vol. 14, no. 1, pp. 4,20, Jan. 2004 doi: 10.1109/TCSVT.2003.818349
[12]]. G. Mujtaba, "Adaptive Automated Teller Machine Part-II", International Conference on Information and Communication Technologies, pp. 1 – 6, 2011.
[13] G. Mujtaba, "Adaptive Automated Teller Machine Part-I", International Conference on Information and Communication Technologies, 2010.
[14] A.S. Adams, and K. A. Thieben, "Automatic teller machines and the older population", Applied Ergonomics, Vol. 22, pp. 85 -90, 11991.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY