International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org Volume 3 Issue 5‖ May 2014 ‖ PP.22-26

Design of Highly Secured Automatic Teller Machine System by Using Aadhaar Card and Fingerprint

[1,] Mr Abhijeet S. Kale, [2,] Prof. Sunpreet Kaur Nanda
[1]*M.E 2nd year,* [2,] *Professor*
[1, 2,] *Dept. of Electronics and Telecommunication PRPCET, Amravati Maharashtra, India*

ABSTRACT: *The main objective of this system is to develop an embedded system, which is used for ATM security applications. In these systems, Bankers will collect the customer finger prints, Aadhaar cards and mobile number while opening the accounts then customer only access ATM machine.Security measures at banks can play a critical, contributory role in preventing attacks on customers. These measures are of paramount importance when considering vulnerabilities and causation in civil litigation. Banks must meet certain standards in order to ensure a safe and secure banking environment for their customers. Existing ATM systems use magnetic card reader. The customer is identifying by inserting an ATM card with magnetic card that contain unique information such as card number and some security parameters. By entering a personal identification number, the customer is authenticated first then can access bank account in order to make cash withdraw or other services provided by the bank. Cases of card fraud are another problem once the user's bank card is missing and the password is stolen, or simply steal a customer's card& PIN the criminal will draw all cash in very short time, which will being tremendous financial losses in customer, this type of fraud has spread globally. So to rectify this issue we are implementing this system using ARMCONTROLLER on "BIOMETRICS" and "AADHAAR CARD" in order to improve authentication of customer using ATM machine and confidence in the banking sector.*

KEYWORDS: *ARM 7, Fingerprint module, Aadhaar card scanner, GSM module.*

I. INTRODUCTION

Automated teller machine is a mechanical device that has its roots embedded in the accounts and records of a banking institution. In the real world, today people are concerned about their safety, for their valuable things. Old concepts and devices are getting modified as per requirement of people. Crime at ATM's has become a nationwide issue that faces not only customers, but also bank operators. In day to day life we need to seek new security system. So we develop to provide the maximum level security system. Money transactions play an important role in the nature of trade. Enormously growing banking technology has changed the way banking activities are dealt with. Security measures at banks can play a critical, contributory role in preventing attacks on customers. These measures are of paramount importance when considering vulnerabilities &causation in civil litigation and banks must meet certain standards in order to ensure a safe and secure banking environment for their customers. An ATM is a mechanical system that has its roots embedded in the accounts and records of a banking institution. Today, Credit cards & ATM are used for this purpose, the authentication of these transactions are totally unsecure. Existing system of ATM client authentication there is a magnetic card reader, client using the ATM require Bank card and password which provide customers with the convenient banknote withdraw and other services. A newer high-tech method of operating sometimes called card cloning to entangle the installation of a magnetic card reader over the ATM's card slot & the use of a wireless surveillance camera to keep the user's Personal Identification Number. Real Card data are then cloned into a duplicate card & the criminal attempts to cash withdrawal. To overcome this piracy in money transactions, I proposed the idea using fingerprints & AADHAARCARD along with GSM modem for authentication of customers. Biometrics and Aadhaar card can be defined as a measurable physiological and behavioral characteristic that can be subsequently compared & captured with another instance at the time of verification. These technologies are a secure way of authentication because data of both technologies are unique, cannot be shared, cannot be copied and cannot be overlooked. GSM is used for sending a message to higher authorities when fingerprint and Aadhaar card recognition false also type wrong password. Our project secures the money along with minimum risk factor. Continue with it, it gives a master password for the use of long Businesses chain with the use of it; we can use one ATM on a large scale with more security.

II. OBJECTIVE

[1] To research scope of biometric authentication techniques in ATMs.
[2] Fingerprint recognition: The masters' fingerprint information was used as the standards of identification. It must certify the feature of the human fingerprint before using ATM system.
[3] Remote authentication: System can compare current client's fingerprint & Aadhaar card information with remote data server.
[4] To generate module this helps for simple operation of ATMs with full proof secure authentication.

III. REVIEW OF LITERATURE

Mr. Wang et al. Expresses his view like that now a day ATM with magnetic strip authenticated only by inserting password on the ATM machine. But according to today's scenario, cases of fraud are another problem. So they provided fingerprint for more security. Now a days we are directing towards the pile of new powerful, intelligent, auto rated system, which will give us easy to do the work smoothly, Thus systems are not dependent on human support, one of these 'ATM SECURITY SYSTEM' which we have evolved [1].Mr. Aru et al. Suggests that Today, ATM systems use PIN & access card for identity verification. The recent advance in biometric identification techniques, retina scanning, including fingerprinting, and facial recognition has made a great effort to rescue the unsafe situation at the ATM. This research investigated the development of a scheme that integrates facial recognition technology into the verification process used in ATMs. An ATM system that is reliable in providing more security by using facial recognition is proposed. The development of such a scheme would help to protect clients & financial institutions alike from intruders and identity thieves. This paper concentrates on an ATM security system that would combine a physical access card, a Personal Identification Number, & electronic facial recognition that will go as far as withholding the fraudster's card. Nevertheless, it's obvious that man's biometric features cannot be replicated, this proposal will go a long way to solve the problem of Account safety making it possible for the actual account owner alone have access to his accounts. The combined biometric features approach is to serve the purpose both the identification and authentication that card and PIN do [2].

What is Identification Authentication?

Identification is the process by which the identity of a user is established, authentication is the process by which a service confirms the claim of a user to use a specific identity by the use of credentials. Biometrics is very reliable for authentication. The difference is between a system that looks at a hand geometry and says "this is Doctor Hunk" (identification) versus a man'swho says "I, Doctor Hunk, present my hand to prove who I am? And the system confirms this hand matches Doctor Hunk"s template (authentication). Biometric authentication is feasible today.

What is biometric authentication?

Biometrics is biological authentications, based on some physical characteristics of the human body. The list of biometric authentication technologies is still growing. There are two categories of biometric identifiers include physiological and behavioral characteristics. Physiological characteristics are related to the shape of the body, and include but are not limited to: fingerprint, face recognition, DNA, palm print, hand geometry, iris recognition (which has largely replaced retina). Behavioral characteristics are related to the behavior of a person, including but not limited to: typing rhythm, gait, digital signature and voice. More traditional means of access control include token-based identification systems, such as driver's license or passport, and knowledge-based identification systems, such as password or Personal Identification Number (PIN) [3].

IV. METHODOLOGY

The design of entire system consisted of two part which are hardware and software. The hardware is designed by the rules of embedded system, and the steps of software consisted of three parts. The more details are shown as follows.

A. Hardware Design

The LQFP64 chip is used as the core of entire hardware. Furthermore, the modules of LCD, keyboard, alarm, fingerprint recognition are connected with the main chip (LQFP64).

There are some modules consisted of the system as follows:

- Fingerprint module: Fingerprint processing includes two parts: fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1: N). When enrolling, user needs to enter the finger two times. The system will process the two time finger images, generate a template of the finger based on processing

results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, system will compare the live finger with specific template designated in the Module; for 1:N matching, or searching, system will search the whole finger library for the matching finger. In both circumstances, system will return the matching result, success or failure.

- LCD Display: A liquid crystal display (LCD) is a thin, flat panel used for electronically to display information such as text, images, and moving pictures. Its uses include monitors for computers, televisions, instrument panels, and other devices ranging from aircraft cockpit displays, to every-day consumer devices such as clocks, watches, calculators. Among its major features are their lightweight constructions. Its low electrical power consumption enables it to be used in battery-powered electronic equipment. It is an electronically-modulated optical device made up of any number of pixels filled with liquid crystals and arrayed in front of a light source (backlight) or reflector to produce images in color or monochrome.
- GSM: This GSM modem is a highly flexible plug and play quad band GSM modem for direct and easy integration to RS232. Supports features like Voice, Data/Fax, SMS,GPRS and integrated TCP/IP stack.

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

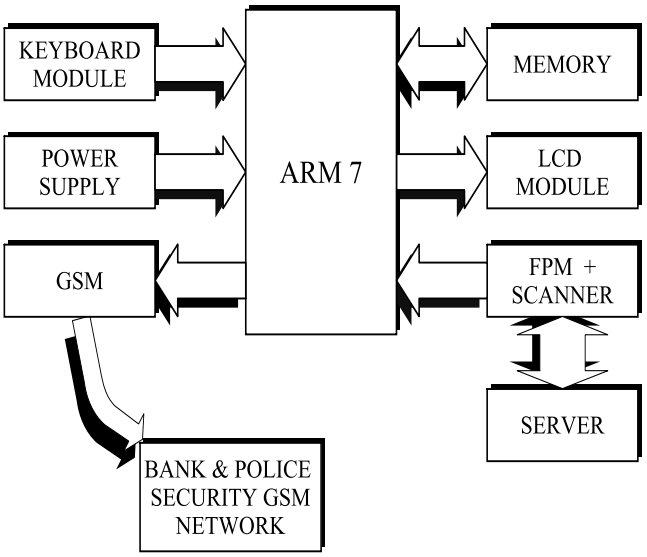

Figure 1: Basic block diagram of ATM security system

B. Software Design:

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

Keil µVision4: The LPC2148 is programmed with KeilµVision4. It is a window-based software platform that combines a robust and modern editor with a project manager and make facility tool for development. It integrates all the tools to develop embedded applications including a C/C++ compiler, macro assembler, linker/locator, and a HEX file generator. µVision helps expedite the development process of embedded applications by providing the IDE (Integrated Development Environment). KEIL is used to create source files; automatically compile, link and covert using options set with an easy to use user interface and finally simulate or perform debugging on the hardware with access to C variables and memory. Unless we have to use the tolls on the command line, the choice is clear. This IDE i.e. KEIL Greatly simplifies the process of creating and testing an embedded application. The user of KEIL centers on projects. A project is a list of all the source files required to build a single application, all the tool options which specify exactly how to build the application, and if required how the application should be simulated. A project is exactly the binary code required for the application. Because of the high degree of flexibility required from the tools, there are many options that can be set to configure the tools to operate in a specific and desired manner. It would be very tedious to have to set these options up every time the application is being built; therefore they are stored in a project file. Loading the project file into KEIL informs KEIL which source files are required, where they are, and how to configure the

tools in the correct way. KEIL can then execute each tool with the correct options. Source files are added to the project and the tool options are set as required.

How to create project file:

[1] Create a New Project File with the µVision menu command Project --- New Project. Select a microcontroller from the Device Database™. Use the MCB214x Board to develop code for many of the LPC214x's family of devices.

[2] Select file – add new project file by inserting header file, Right-clicking a group in the Project Window, then save as with ".c" extension and selecting add Files to Group from the context menu.

[3] Add your own Source Code to the project using the µVision editor by selecting Add Files to Group from the context menu.

[4] Then build a programme that shows compiling the programme. After compiling the programme select for generating HEX file.

For example: creation of UART programme.

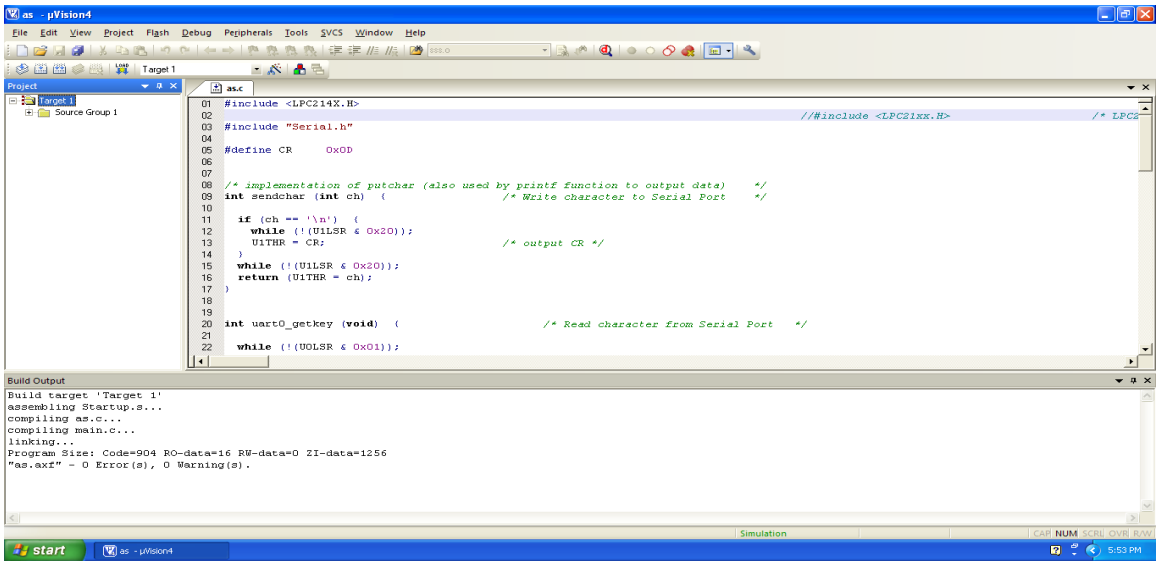

Figure 2: Compiling programmed of UART

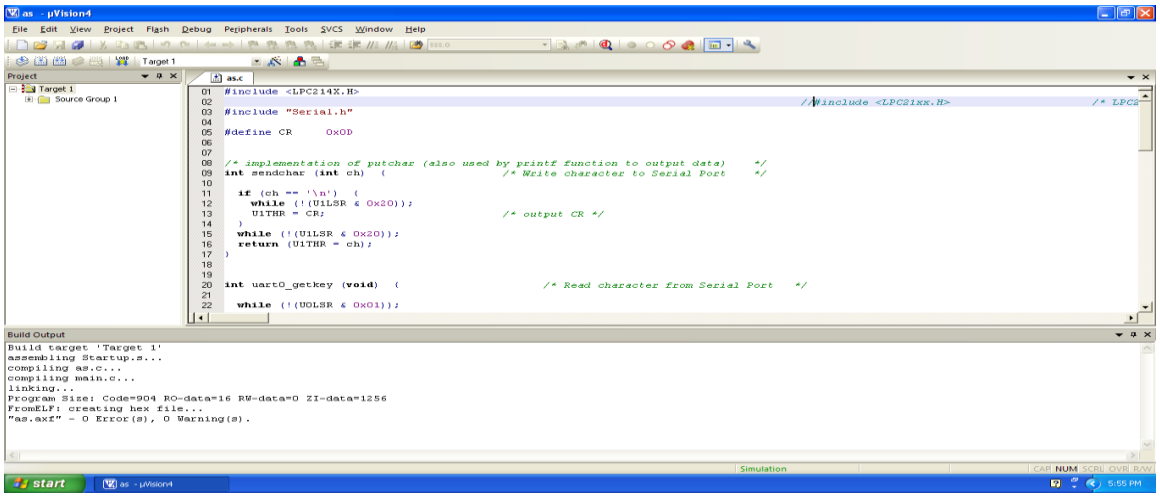

Figure 3: Hex file of UART

V. CONCLUSION

We have been able to develop a fingerprint mechanism and Aadhaar card mechanism as a biometric measure to enhance the security features of the ATM for effective banking transaction for banks. The prototype of the developed application has been found promising on the account of its sensitivity to the recognition of the customers' finger print & Aadhaar card recognition as contained in the database. 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. An embedded fingerprint biometric authentication scheme for ATM banking systems is proposed in this paper along with AADHAARCARD authentication for more security; also included in this paper. Finally, conclusions are drawn out after observing the AADHAR CARD &Fingerprint Biometric Authentication scheme results.

REFERENCES

[1] 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

[2] 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

[3] Laudon Kenneth, Traver Carol Guercio, E-Commerce (2005), Second Edition , pp. 237-239, Pearson Education (Singapore), Pvt. Ltd.

[4] 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

[5] 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: 2231-1963*Vol. 4, Issue 2, pp. 456-463

[6] 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

[7] 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

[8] 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

[9] **[9]** 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