ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

High Level Security Authentication for ATM Machines Using Fingerprint

Ms.K.Abhilasha
M.Tech Student,
Malla Reddy Engineering College for Womens,
Maisammaguda, Secunderabad-500014.

Mrs.R.Bhanu
Assistant Professor,
Malla Reddy Engineering College for Womens,
Maisammaguda, Secunderabad-500014.

Abstract:

Automated teller machines (ATMs) are a part of most of our lives. The major appeal of these machines is convenience. ATMs allow customers access to get cash twenty-four hours a day. Customers access their bank accounts through a plastic bankcard. This card has a magnetic strip on the back containing a password and relevant account information. ATM technology has virtually remained the same over the last several decades, with a few minor changes like color touch-sensitive screens and voice-activated commands for the visually impaired. With so many machines available to account holders, it's no wonder that illegal users take advantage of this technology.

KEYWORDS:

ARM7,LCD,RS-232,RECTIFIER, TRANSFORMER ,REGULATOR,LPC2148.

I.INTRODUCTION:

ATM security system through biometric fingerprint technology and GSM is one of the innovative topics in the embedded systems industry. This project work is intended to introduce more security for the ATM's using biometric technology, which describes about design, development and fabrication of one demonstration unit of the project "High level Security Authentication for ATM's using Fingerprint". For providing security for the consumer accounts at the ATMs, fingerprint scanner and GSM modules are interfaced with the ATM machines with suitable software. In project work the ATM machine is designed using biometric equipment fingerprint scanner, GSM, EEPROM, etc along with the controller unit designed using ARM7. To introduce the subject of biometric ATM's and also to provide some historical context, this report explains about overview of ATM's.

Biometrics is automated methods of recognizing a person based on physiological or behavioral characteristics. Among the features measured are: face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The need for biometrics can be found in federal, state and local governments, in the military, and in commercial applications. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies.

1.1 Examples of Different Biometrics:

- Face
- Fingerprint
- Voice
- Palm print
- Hand Geometry
- Iris
- Retina Scan
- Voice
- DNA
- Signatures
- Gait
- Keystroke

These techniques of identification are preferred over traditional passwords and PIN-based techniques for various reasons:

•The person to be identified is required to be physically present at the time of identification.

•Identification based on biometric techniques obviates the need to remember a password or carry a token.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A biometric system essentially is a pattern recognition system that makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic." A biometric system can be either an identification system or a verification (authentication) system; both are defined below.

1.2 Identification and Verification:

•Identification: One to Many — A comparison of an individual's submitted biometric sample against the entire database of biometric reference templates to determine whether it matches any of the templates.
•Verification: One to One — A comparison of two sets of biometrics to determine if they are from the same individual.

Biometric authentication requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, the one captured during a login). This is a three-step process (Capture, Process, Enroll) followed by a Verification or Identification.

During Capture, raw biometric is captured by a sensing device, such as a fingerprint scanner or video camera; then, distinguishing characteristics are extracted from the raw biometric sample and converted into a processed biometric identifier record (biometric template). Next is enrollment, in which the processed sample (a mathematical representation of the template) is stored / registered in a storage medium for comparison during authentication. In many commercial applications, only the processed biometric sample is stored. The original biometric sample cannot be reconstructed from this identifier.

Fingerprint identification is one of the most well-known and publicized biometrics. Because of their uniqueness and consistency over time, fingerprints have been used for identification for over a century, more recently becoming capabilities. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration.

No two humans on earth have the same fingerprint. Even each finger for the same person has a different pattern. This even holds true for identical twins. Because of this fact, fingerprint authentication is an excellent way to differentiate users. Users are first required to scan a specific finger into a computer system. With that user's unique fingerprint on file, a wall mounted device can be deployed at any point that authentication is necessary. The user then applies his finger (the exact finger initially scanned) to the biometric reader. The system calculates a score based on the fingerprints on record and the currently scanned fingerprint. The system checks for similarities between the fingerprints and allows or denies access if the score is above or below a certain threshold. This technology can also be applied to palm prints as well.

1.3 Block Diagram:

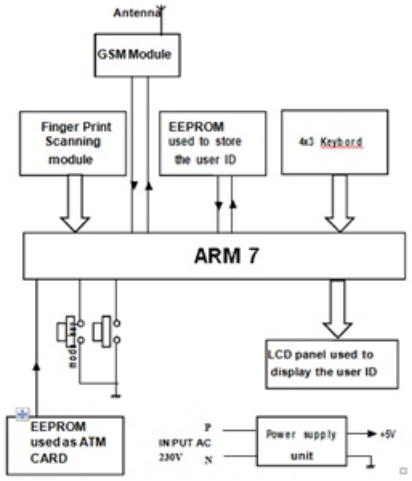

Fig 1.3 Block Diagram

II.LITERATURE SURVEY:

Because biometrics-based authentication offers several advantages over other authentication methods, there has been a significant surge in the use of biometrics for user authentication in recent years. In this paper the existing security of the ATM (Automated Teller Machine) system has been improved by integrating the fingerprint of the user into the bank's database as to further authenticate it. This was achieved by modelling and building an ATM simulator that will mimic a typical ATM system. The end result is an enhanced biometric authenticated ATM system that ensures greater security and increased customer's confidence in the banking sector.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

2.1Existing System:

Previously the existing ATM system authenticates transactions via the card and PIN-based system. Thereafter, it grants access to bank customers to several services such as cash withdrawal and deposits, account to account transfers, balance enquiry, top-up purchases and utility bills payment. The ATM system compares the PIN entered against the stored authorization PIN for every ATM users. If there is a match, the system authenticates the user and grants access to all the services available via the ATM. If there is a mismatch on the other hand, the user authentication process fails and the user is given two more opportunities to enter a correct PIN. If an incorrect PIN is entered for the third time, the card gets blocked and retained by the ATM. An instance of cash withdrawal on the existing ATM system is depicted.

2.2Proposed system:

Here the proposed system is dependant on the biometrics i.e. fingerprint. In future it will be very easy to implement because each person has his own fingerprints with the permanent uniqueness. The system will provide many advantages such as, we do not forget our fingers, Users respect them, fraudsters are afraid of them, Protects privacy. Fingerprints do not change over time, Fingerprints stop unauthorized access, and all fingers are unique, which allows each person to have ten easy uses of identifiers, Base of all world-wide identification.

III.MODULES:

3.1ARM7 CONTROLLER:

A silicon chip that contains a CPU. In the world of personal computers, the terms microprocessor and CPU are used interchangeably. At the heart of all personal computers and most workstations sits a microprocessor. Microprocessors also control the logic of almost all digital devices, from clock radios to fuel-injection systems for automobiles.

Three basic characteristics differentiate microprocessors

» Instruction set: The set of instructions that the microprocessor can execute.
» Bandwidth : The number of bits processed in a single instruction.
» Clock speed : Given in megahertz (MHz), the clock speed determines how many instructions per second the processor can execute.

The LPC2148 microcontroller is based on a 16-bit/32-bit ARM7TDMI-S CPU with real-time emulation and embedded trace support, that combine microcontroller with embedded high speed flash memory ranging from 32 kB to 512 kB. A 128-bit wide memory interface and a unique accelerator architecture enable 32-bit code execution at the maximum clock rate. For critical code size applications, the alternative 16-bit Thumb mode reduces code by more than 30 % with minimal performance penalty. Due to their tiny size and low power consumption, LPC2141/42/44/46/48 are ideal for applications where miniaturization is a key requirement, such as access control and point-of-sale.

3.1.1CIRCUIT DIAGRAM:

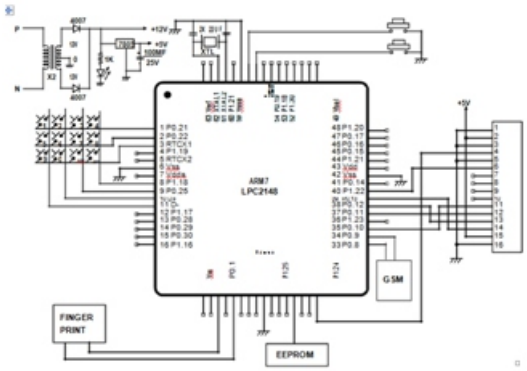

Fig3.1.1 circuit diagram.

3.2 GSM TECHNOLOGY:

GSM is known as Global System for Mobile Communication. A technology developed in 1985 by a French company known as Group Special Mobile. Cellular radio provides mobile telephone service by employing a network of cell sites distributed over a wide range. A cell site contains a radio transceiver and a base station controller, which manages, sends, and receives traffic from the mobiles in its geographical area to a cellular phone switch. It also employs a tower and its antennas, and provides a link to the distant cellular switch called a mobile telecommunication switching office. This MTSO places calls from land based telephones to the wireless customers, switches calls between cells as mobile travel across cell boundaries, and authenticates wireless customers before they make calls.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

GSM calls are either based on data or voice. Voice calls use audio codes called half-rate, full-rate and enhanced full-rate. Data calls can turn the cell phone into a modem operating at 9600 bps. It uses digital technology and time division multiple access transmission methods. GSM technology is continually evolving having made great leaps forward in the past 10 years. It is facing an even greater evolution in the years ahead.

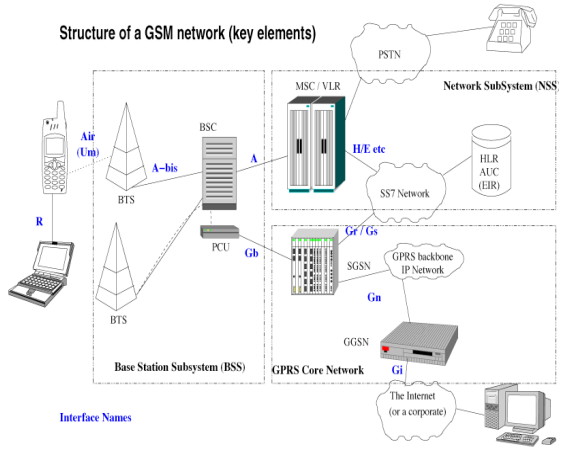

Fig 3.2 GSM structure

3.3 LCD :

LCD displays are dominating LED displays, because these displays can display alphabets, numbers and some kind of special symbols, where as LED's (seven segment display) can display only numbers. These LCD displays are very useful for displaying user information and communication. LCD displays are available in various formats. Most common are 2 x 16, is that two lines with 16 alphanumeric characters. Other formats are 3x16, 2x40, 3x40 etc; In recent years LCD is finding widespread use replacing LED's, because of the ability to display numbers, characters, and graphics. Another advantage is, because of its compactness and ease of programming for characters and graphics, more information in the form of text message or graphics can be displayed. Generally, the LCD modules have an 8-bit interface, besides the 8-bit data bus; the interface has a few other control lines. The 8-bit data bus is connected to port '0' and the control lines are connected to port '2'. The default data transfer between the LCD module and an external device is 8-bits, however it is possible to communicate with the LCD module using only four of the 8-data lines. The R/W line is connected to ground and hence the processor cannot read any status information from the LCD module, but can only write data to the LCD.The LCD panel used in this project work is having 14 pins. The function of each pin description with table is provided in the next page.

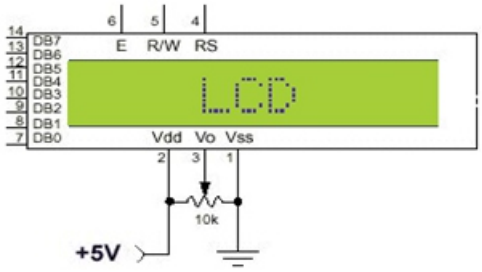

Fig 3.3 LCD panel

3.4 POWER SUPPLY:

The power supplies are designed to convert high voltage AC mains electricity to a suitable low voltage supply for electronics circuits and other devices. A RPS (Regulated Power Supply) is the Power Supply with Rectification, Filtering and Regulation being done on the AC mains to get a Regulated power supply for Microcontroller and for the other devices being interfaced to it. For example a 5V regulated power supply system as shown below:

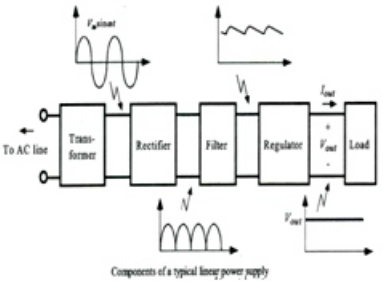

Fig 3.4 Power supply of 5v

IV.RESULT

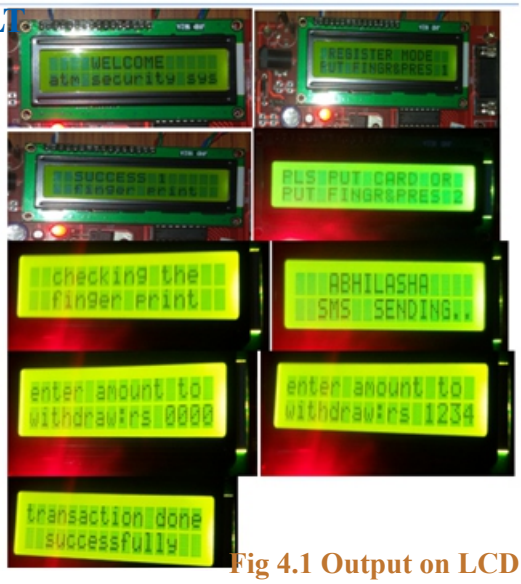

Fig 4.1 Output on LCD

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

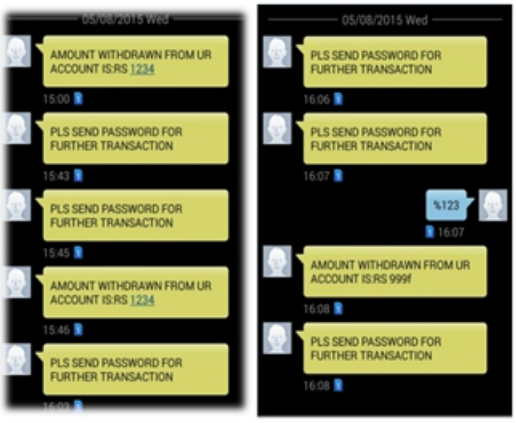

Fig 4.2 Output in Mobile

V.CONCLUSION:

The increased need of privacy and security in our daily life has given birth to this new area of science. These devices are here and are present around us everywhere in the society and are here to stay for a long time to come. Indeed, it will be interesting to watch the future impact that they will have on our day-to-day lives.The project work "High level security authentication for ATM'S using Fingerprint" is designed and developed successfully. For the demonstration purpose, a prototype module is constructed; and the results are found to be satisfactory. Since it is a prototype module, a simple module is constructed, which can be used for many applications like highly confidential area or where high level security is required. In this project we have explained why security is important in an Ambient Intelligent environment. In order to achieve Trust and Security not only cryptographic algorithms are needed but also secure methods for generation and storage of secret keys. By constriction of such security devices the cards, keys, etc can be made tamper proof and avoid them from destruction by the anti social elements or the unofficial persons. Moreover the applications of this finger print scanner are plenty generally categorized for the security purposes.

VI.FUTURESCOPE:

In this project we are using fingerprint module as mode of authentication. This project is depending on the biometrics i.e. fingerprint. In future it will be very easy to implement because each person has his own fingerprints with the permanent uniqueness.

The system will provide many advantages such as, we do not forget our fingers, Users respect them, fraudsters are afraid of them, Protects privacy. Fingerprints do not change over time, Fingerprints stop unauthorized access, and all fingers are unique, which allows each person to have ten easy uses of identifiers, Base of all world-wide identification.In future systems using biometric will be preferred as method to provide security and authentication this will eliminate forgery and fraud in many organizations.

VII.REFERENCES:

1.Linear Integrated Circuits – By: D. Roy Choudhury, Shail Jain

2.Digital Electronics. By JOSEPH J.CARR

3.Practical transistor circuit design and analysis - By: GERALD E. WILLIAMS

4.Digital Principles and Applications By ALBERT PAUL MALVINO AND DONALD P. LEACH

5.The concepts and Features of Micro-controllers - By: Raj Kamal

6.The 8051 Micro-controller Architecture, programming & Applications - By: Kenneth J. Ayala

7.Programming and Customizing the 8051 Micro-controller - By: Myke Predko

8.http://www.wvshare.com/datasheet_html/ LPC2148-PDF.html

9.Michael j. point "EMBEDDED C" Pearson education limited 2002

10.http://en.wikipedia.org/wiki/GSM