IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 73-79
www.iosrjournals.org

A Secure Biometrics and GSM –Based MSAP Using ATM Cards

R.Hari Prakash, D.Praveen,N.J.Arun Pandian, R.JeevanRaj
ECE Department, K.Ramakrishnan College of Technology
Tiruchirappalli, TamilNadu, India

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 using fingerprint. The first one is normal user fingerprint 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 unauthorized person use ATM check the fingerprint if it is not match message to the user using GSM. The user 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. And, also using fingerprint technology . In this technology for security purpose.*

Keywords: Fingerprint scanner ;IR Sensor; ADC ; GSM Modem ; 8051 Micro Controller ; LCD.

I. INTRODUCTION

The rapid development of the wireless communication networks and e-commerce applications, such as e-banking and transaction-oriented services, there is a growing demand to protect the user credentials privacy.In the recent couple of decades, more and more transactions for the mobile devices have been implemented on the Internet or wireless networks due to the portability property of mobile devices, such as laptops, smart cards and smart phones. Thus, the authentication protocols become the trusted components in a communication system. In order to protect the sensitive information against a malicious adversary, a variety of security services such as mutual authentication, user credentials privacy and SK-security need to be considered.We also consider the following two real-life scenarios for the smart card based authentication schemes in which the registered users may revoke and re-register with the same identity: (i) when unexpectedly the secret token of a legal user is revealed and(ii) if the smart card of a legal user is stolen or lost. Hence, the authentication schemes must support the user revocation and re-registration with the same identity. The user revocation and re-registration with the same identity may cause the user impersonation attack, when an authentication scheme distributes the static secret tokens. Therefore, designing an efficient approach to tackle the problem of user revocation while supporting a strong user untraced ability becomes a challenging problem. As a result, the user revocation and re-registration with the same identity is identified as fundamental security functionality for the smart card-based authentication schemes.

SK-security: An authentication scheme should guarantee the security of the session key, called the session key security (SK-security), in the following two cases: (i) The leakage of session key or session-specific temporary information will have no effects on the security of other sessions.(ii) The leakage of the crucial long-term secrets, suchas the private keys of users or servers, which areused across the multiple sessions, will not necessarilycompromise the secretinformation from all pastsessions, known as the perfect forward secrecy. ***User***

credentials privacy: It ensures that *A* cannot derive a user credentials, such as authentication parameter, user password and identity.

***Secure mutual authentication*:** It ensures that an authentication scheme must provide the secure mutual authentication with the presence of the shared secret credentials.

II. PROJECT DESCRIPTION

The existing system of the project are

- ✓ In the existing system of, we have taken the money from the ATM. Then, the server send the message to mobile phone.
- ✓ Unauthorized person also know the password.

- ✓ It is one way communication process.

The proposed system of the project are as follows:

- ✓ It is two way communication process.
- ✓ For security purpose fingerprint.
- ✓ If the password check simultaneously ATM and mobile. The message automatically send to the user. The user is give YES message only activated. otherwise deactivated account.

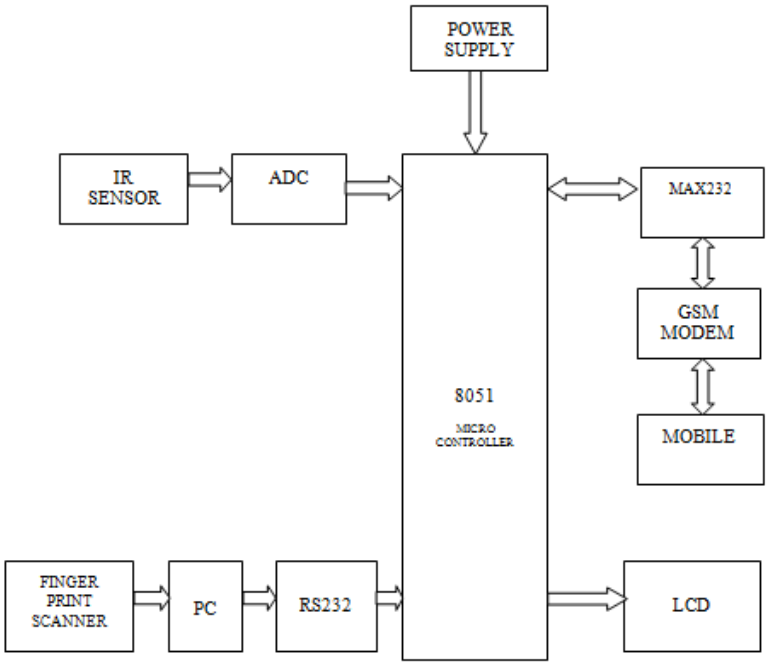


Fig1-Block diagram

POWER SUPPLY:

Power supply is a reference to a source of electrical power. A device or system that supplies electrical or other types of energy to an output load or group of loads is called a power supply unit or PSU. The term is most commonly applied to electrical energy supplies, less often to mechanical ones, and rarely to others.

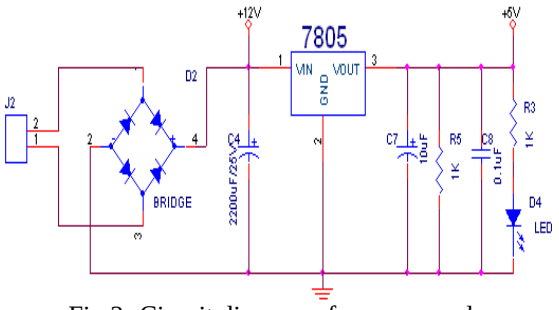


Fig 2- Circuit diagram of power supply

A 230v, 50Hz Single phase AC power supply is given to a step down transformer to get 12v supply. This voltage is converted to DC voltage using a Bridge Rectifier. The converted pulsating DC voltage is filtered by a 2200uf capacitor and then given to 7805 voltage regulator to obtain constant 5v supply. This 5v supply is given to all the components in the circuit. A RC time constant circuit is added to discharge all the capacitors quickly. To ensure the power supply a LED is connected for indication purpose.

Voltage Regulator:

Fig 3- voltage regulator

The features of voltage regulator are
(i) Output Current up to 1A
(ii) Output Voltages of 5, 6, 8, 9, 10, 12, 15, 18, 24V
(iii)Thermal Overload Protection
(iv) Short Circuit Protection
(v) Output Transistor Safe Operating Area Protection

The KA78XX/KA78XXA series of three-terminal positive regulator are available in the TO-220/D-PAK package and with several fixed output voltages, making them useful in a wide range of applications. Each type employs internal current limiting, thermal shut down and safe operating area protection, making it essentially indestructible. If adequate heat sinking is provided, they can deliver over 1A output current. Although designed primarily as fixed voltage regulators, these devices can be used with external components to obtain adjustable voltages and currents.

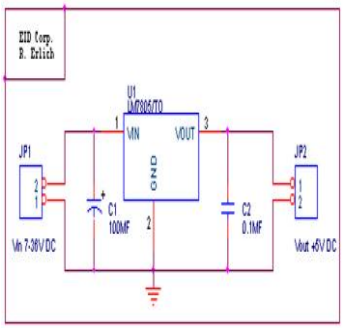


Fig 4- Circuit diagram of voltage regulator

The hardware components used in our project are Microcontroller, GSM modem, ADC unit, finger print module, IR ATM reader, LCD, Personal computer, Power supply. The software components used in our project are Embedded C programming and keil programmer.

Microcontroller:

A microcontroller (also microcontroller unit, MCU or µC) is a small computer on a single integrated circuit consisting of a relatively simple CPU combined with support functions such as a crystal oscillator, timers, watchdog timer, serial and analog I/O etc. either Program memory in the form of NOR flash or OTP ROM is also often included on chip, as well as a typically small amount of RAM. Microcontrollers are designed for small or dedicated applications.
The features of the micro controller are as follows:
(i) Compatible with MCS-51Ô Products
(ii) 4 Kbytes of In-System Reprogrammable
(iii) Fully Static Operation: 0 Hz to 24 MHz
(iv) Three-Level Program Memory Lock
(v) 128 x 8-Bit Internal RAM
(vi) 32 Programmable I/O Lines

(vii) Two 16-Bit Timer/Counters
(viii) Six Interrupt Sources
(ix) Programmable Serial Channel
(x) Low Power Idle and Power Down Modes

GSM:

GSM (Global System for Mobile communications: originally from *Group Special Mobile*) is the most popular standard for mobile phones in the world. Its promoter, the GSM Association, estimates that 80% of the global mobile market uses the standard. GSM is used by over 3 billion people across more than 212 countries and territories. Its ubiquity makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world. GSM differs from its predecessors in that both signaling and speech channels are digital, and thus is considered a *second generation* (2G) mobile phone system. This has also meant that data communication was easy to build into the system. GSM EDGE is a 3G version of the protocol.

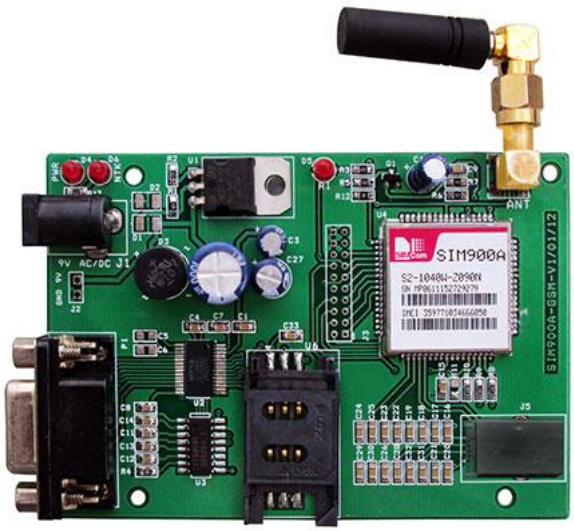


Fig 5- GSM

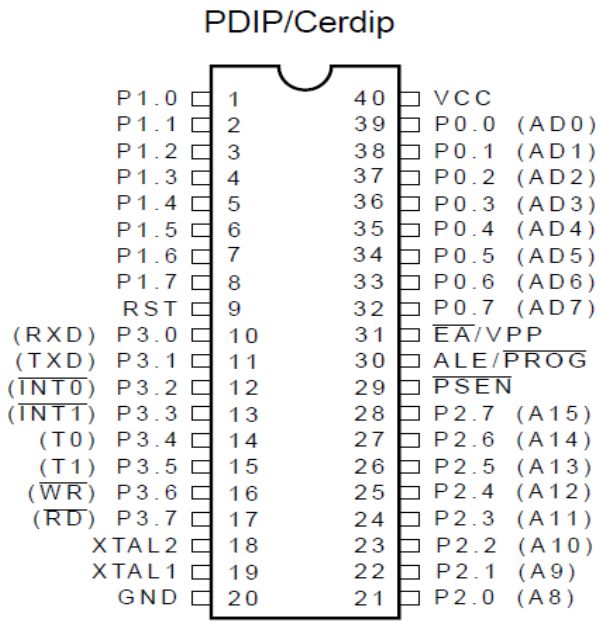


Fig 6 – PIN diagram

The AT89C51 is a low-power, high-performance CMOS 8-bit microcomputer with 4Kbytes of Flash Programmable and Erasable Read Only Memory (PEROM). The device is manufactured using Atmel's high density nonvolatile memory technology and is compatible with the industry standard MCS-51Ô instruction set and pin out. The on-chip Flash allows the program memory to be reprogrammed in-system or by a conventional nonvolatile memory programmer. By combining a versatile 8-bit CPU With Flash on a monolithic chip, the Atmel AT89C51 is a powerful microcomputer which provides a highly flexible and cost effective solution to many embedded control applications. ***Finger print scanner :***Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. Fingerprint Scanner uses advanced CMOS sensor technology and precise optical system to deliver a high quality fingerprint image. It can capture an almost undistorted fingerprint image and is good for any fingerprint recognition application. It is much more reliable and robust compared to any semiconductor-type fingerprint

semiconductor-type fingerprint sensor

Fig7- Finger print sensor

IR sensor :

The circuit required to make an IR Sensor consists of two parts ; the emitter circuit and the receiver circuit.The emitter is simply an IR LED (Light Emitting Diode) and the detector is simply an IR Photodiode which is sensitive to IR light of the same wavelength as that emitted by the IR LED.When IR light falls on the photodiode , its resistance and correspondingly,its output voltage ,change in proportion to the magnitude of the magnitude of the IR light received.This is the underlying principle of working of the IR sensor.There is an obstacle ,the green indicator light on the circuit board.Detection distance is 2-30cm,detection angle 35',comparator chip-LM393,3mm screw holes for mounting.We have already discussed how a light sensor works.IR Sensor work by using a specific light sensor to detect a select light wavelength in the Infra-Red (IR) spectrum.By using an large jump in the intensity, which we already know can be detected using a threshold.LED which produces light at the same wavelength as what the sensor is looking for, you can look at the intensity of the received light. When an object is close to the sensor, the light from the LED bounces off the object and into the light sensor. This results in a large jump in the intensity, which we already know can be detected using a threshold. Infrared energy is emitted or absorbed by molecules when they change their rotational-vibrational movements. Infrared energy excites vibrational modes in a molecule through a change in the dipole moment, making it a useful frequency range for study of these energy states for molecules of the proper symmetry. Infrared spectroscopy examines absorption and transmission of photons in the infrared energy range. Infrared radiation is used in industrial, scientific, and medical applications. Night-vision devices using active near-infrared illumination allow people or animals to be observed without the observer being detected. Infrared astronomy uses sensor-equipped telescopes to penetrate dusty regions of space, such as molecular clouds; detect objects such as planets, and to view highly red-shifted objects from the early days of the universe. Infrared thermal-imaging cameras are used to detect heat loss in insulated systems, to observe changing blood flow in the skin, and to detect overheating of electrical apparatus.Thermal-infrared imaging is used extensively for military and civilian purposes. Military applications include target acquisition, surveillance, night vision, homing and tracking. Humans at normal body temperature radiate chiefly at wavelengths around 10μm (micrometers). Non-military uses include thermal efficiency analysis, environmental monitoring, industrial facility inspections, remote temperature sensing, short-ranged wireless communication, spectroscopy, and weather forecasting.

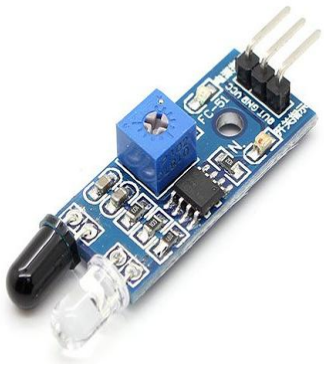
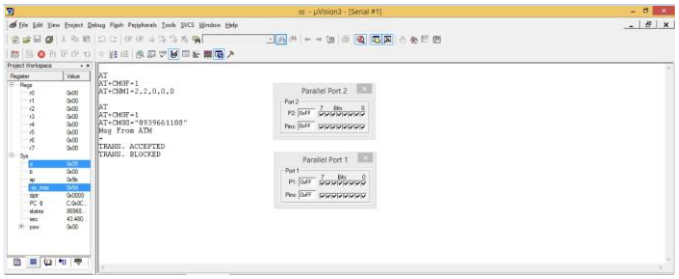


Fig 8-IR Sensor

LCD:

A **liquid-crystal display** (**LCD**) is a flat-panel display or other electronic visual display that uses the light modulating properties of liquid crystals. Liquid crystals do not emit light directly. LCDs are available to display arbitrary images (as in a general-purpose computer display) or fixed images with low information content, which can be displayed or hidden, such as preset words, digits, and 7-segment displays as in a digital clock. They use the same basic technology, except that arbitrary images are made up of a large number of small pixels, while other displays have larger elements. LCDs are used in a wide range of applications including computer monitors, televisions, instrument panels, aircraft cockpit displays, and signage. They are common in consumer devices such as DVD players, gaming devices, clocks, watches, calculators, and telephones, and have replaced cathode ray tube (CRT) displays in nearly all applications. They are available in a wider range of screen sizes than CRT and plasma displays, and since they do not use phosphors, they do not suffer image burn-in. LCDs are, however, susceptible to image persistence. The LCD screen is more energy-efficient and can be disposed of more safely than a CRT. Its low electrical power consumption enables it to be used in battery-powered electronic equipment more efficiently than CRTs. It is an electronically modulated optical device made up of any number of segments controlling a layer of liquid crystals and arrayed in front of a light source (backlight) or reflector to produce images in color or monochrome. Liquid crystals were first discovered in 1888.[3] By 2008, annual sales of televisions with LCD screens exceeded sales of CRT units worldwide, and the CRT became obsolete for most purposes. Before an electric field is applied, the orientation of the liquid-crystal molecules is determined by the alignment at the surfaces of electrodes. In a twisted nematic (TN) device, the surface alignment directions at the two electrodes are perpendicular to each other, and so the molecules arrange themselves in a helical structure, or twist. This induces the rotation of the polarization of the incident light, and the device appears gray. If the applied voltage is large enough, the liquid crystal molecules in the center of the layer are almost completely untwisted and the polarization of the incident light is not rotated as it passes through the liquid crystal layer. This light will then be mainly polarized perpendicular to the second filter, and thus be blocked and the pixel will appear black. By controlling the voltage applied across the liquid crystal layer in each pixel, light can be allowed to pass through in varying amounts thus constituting different levels of gray.

III. RESULT



IV. CONCLUSION

This paper presents a novel architecture that can be used as a means of interaction between mobile phone, ATM machine and a Banking application for the purpose of withdrawing cash. The proposed design; the secure M-cash withdrawal allows the use of mobile phones as a tool of interaction and provide flexibility through a robust identity management architecture. The first part of the architecture is the process of being implemented and all the process involved has been analyzed and justified where possible. The Secure M cash has examined the possibility of making use of similar approaches/techniques (RFID and NFC) for other applications and already there are some applications that have adapted this strategy. The Secure M-Cash Withdrawal architecture has been defined, it will form as a foundation for future work within this area which includes implementing a PC based simulation of the architecture and implementing the system

REFERENCES

[1] Jain, R. Bolle, and S. Pankati, "*Biometrics: personal identification in networked society*", Kluwer Academic Publishers, 1998.
[2] J. Chirillo and S. Blaul, "*Implementing Biometric Security*",Wiley & Sons, 2003.
[3] S. Hoque, M.C. Fairhurst, F. Deravi, W.G.J. Howells, "*On the Feasibility of Generating Biometric Encryption Keys"* IEE Electronics Letters, 41(6), 309-311, 2005.
[4] Cellan-Jones, R., *London starts digital cash trial* in Technology correspondent, BBC News Online,
[5] http://news.bbc.co.uk/1/hi/technology/7117213.stm. 2007: UK.
[6] Blythe, P.T. *Improving public transport ticketing through smart cards*. in Proceedings of the Institution of Civil Engineers: Municipal Engineer. 2004.
[7] New Barclaycard is touch-and-pay in BBC News, http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6945991.stm. 2007.