



## AUTOMATIC VIDEO SURVILLANCE FOR THEFT DETECTION IN ATM MACHINES: AN ENHANCED APPROACH

J.RANJITHMARIYAL<sup>1</sup>, M.NANDHINI<sup>2</sup>, P.JAYASREE<sup>2</sup>, T.MUTHULAKSHMI<sup>2</sup>

<sup>1</sup>Assistant professor, Department of Electronics and communication Engineering

<sup>2</sup>Student, Department of Electronics and Communication Engineering [sabnandhini@gmail.com](mailto:sabnandhini@gmail.com)

Idhaya Engineering College for women villupuram ,Tamilnadu

**Abstract**— This paper presents an automated Teller Machine (ATM) surveillance system which is a smart system based on embedded technology and incorporates various sensors to continuously monitor its surroundings for suspicious activities like physical attack, fraud and theft that might jeopardize the ATM and people nearby. Also discussed is the security and safety measures that can be implemented to prevent such raids by proper surveillance. This paper analyses the different forms of physical attacks on ATM's and discusses the methods that are used to detect the foray, commence proactive measures and tipoff officials through GSM network. We also discuss about the implementation of the sensors and the other supporting hardware that are being used to deploy this system. This paper mainly deals with implementation of OTP password and RFID tag in order to prevent in the ATM machine. The proposed system thus heightens the security of ATM.

**Keywords**—Automated Teller Machine (ATM), Global System for Mobile Communication (GSM), Microcontroller, Personal Identification Number (PIN), temperature sensor, vibration sensor, RFID tag.

### I.INTRODUCTION:

ATMs are predominantly used all over the world. Maintaining the security of an ATM fleet is one of the most technically challenging areas [1][2][3]. To ensure the most effective protection against these types of threats, must implement a comprehensive, security program that includes hardware, software[4] and services designed to protect against all breaches today and in the future. However, the safety of any money transaction is always a concern, no matter how many technologies are developed to protect the transaction. The idea of this project is to develop the prevention of theft of the ATM card and to control the usage of the ATM card by unauthorized person. Conditional security is provided with protocol data unit. The additional feature of this project is that no transaction can be done without the knowledge of the respective card holder for the cause that NFC transactions are being implemented.

### II.EXISTING METHOD:

Researchers provide several ways to protect the ATM System. In Existing Method used vision based surveillance security system. In this manner detect the unusual event by CCTV camera located in ATM environment[1]. In this existing



method use Image Processing Technique for detect the unusual event. Process of this method detects the movement in ATM room and monitoring the usual and unusual events[2][3]. For differentiate the events it does not use any classifier.

### **III.DISADVANTAGES**

Vision based Surveillance system is too difficult to detect the unusual event, because they are not used classifier. This method is unreliable, because camera was broken total security system become fail.Event detection process is very slow and need memory consumption.

### **IV.PROPOSED SYSTEM**

This project deals with the design and implementation of NFC based secure transaction system in ATM machines. This system consists of two modules, the transmitter and the receiver module in order to provide high end security for the ATM card users and the service providers. The password for transaction is send to the cardholder's mobile phone with the help of NFC technology, which is an added advantage. This increases the high usage of smart cards with radio frequency communication between the target devices.

Whenever the transaction has to be done, the RFID card is inserted inside the ATM machine and NFC devices are made to interact with some of the legacy systems. Granting that both RFID and NFC device is found to be accurate, a message is received to the mobile phone of the rightful proprietor with a pin number of four digits. In case of password being correct it moves on to the next level of money transaction, asking for the money withdrawal. Scenario like, the password is found to be defective, next in order of time, the passage out will be locked.

The temperature and vibration are used to provide the additional security to the

ATM. If theft people damage the ATM means vibration sensor will use to find out the vibration and give the alert signal to the micro controller. Microcontroller automatically locks the shutter.When the machine damaged by robbers i.e., they can be damage the machine chassis using welding machine in some time. In this case we will detect the uncertain level of temperature in machine (during the welding machine used) and alert the environment.

### **RFID TAG**

RFID or Radio Frequency Identification is a technology where information stored on a microchip can be read remotely, without physical contact using energy in the RF spectrum. An RFID[5] system consists of a reader, or interrogator, which emits an RF signal via an antenna. The microchip receives the energy via an attached antenna (termed an RFID tag) and varies the electromagnetic response its antenna in such a way that information can be transferred to the reader.

An RFID reader combines the functions of radio transmitter, receiver and data interface. The transmitter activates the tag, the receiver reads the tag's response and the interface passes information along to a computer or other equipment.[5][6]

### **WORKING PRINCIPLE**

The diagram below describes the fundamental working of all RFID[6] systems. The transponder or tag can be either active of passive tag. It reacts to the signals from the reader or writer or interrogator which in turn conveys signals to the computer.

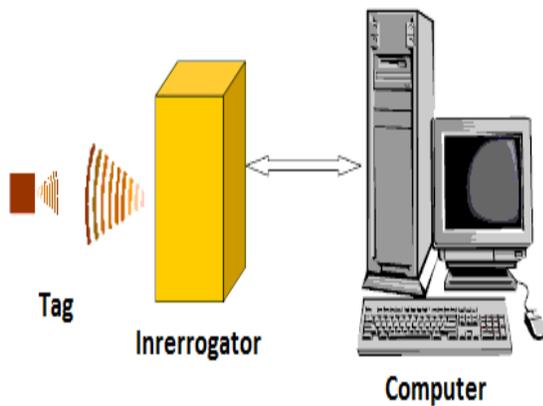


Figure: Fundamental working of RFID

## GSM MODEM

GSM is a mobile communication modem; it stands for global system for mobile communication (GSM). The idea of GSM was developed at Bell Laboratories in 1970. It is widely used mobile communication system in the world. GSM is an open and digital cellular technology used for transmitting mobile voice and data services operates at the 850MHz, 900MHz, 1800MHz and 1900MHz frequency bands.[7]. [10] discussed about a system, GSM based AMR has low infrastructure cost and it reduces man power. The system is fully automatic, hence the probability of error is reduced. The data is highly secured and it not only solve the problem of traditional meter reading system but also provides additional features such as power disconnection, reconnection and the concept of power management.



Figure:SIM900 GSM

## GSM ARCHITECTURE

A GSM network consists of the following components:

### A Mobile Station:

It is the mobile phone which consists of the transceiver, the display and the processor and is controlled by a SIM card operating over the network.

### Base Station Subsystem:

It acts as an interface between the mobile station and the network subsystem. It consists of the Base Transceiver Station which contains the radio transceivers and handles the protocols for communication[7] with mobiles. It also consists of the Base Station Controller which controls the Base Transceiver station and acts as a interface between the mobile station and mobile switching centre.

**Network Subsystem:** It provides the basic network connection to the mobile stations. The basic part of the Network Subsystem is the Mobile Service Switching Centre which provides access to different networks like ISDN, PSTN etc. It also consists of the Home Location Register and the Visitor Location Register which provides the call routing and roaming capabilities of GSM. It also contains the Equipment Identity Register which maintains an account of all the mobile equipments wherein each mobile is identified by its own IMEI number. IMEI stands for International Mobile Equipment Identity.

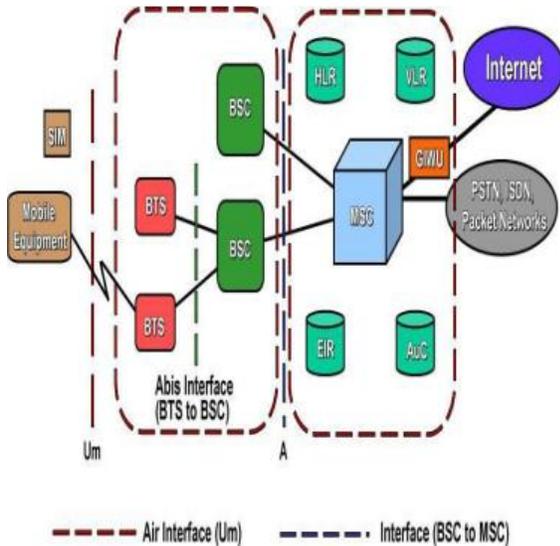


Figure: GSM architecture

### TEMPERATURE SENSOR:

In the temperature functional module we developed, we use the LM34 series of temperature sensors. The LM34 series are precision integrated-circuit temperature sensors, whose output voltage is linearly proportional to the Fahrenheit temperature. The LM34 thus has an advantage over linear temperature sensors[8] calibrated in degrees Kelvin, as the user is not required to subtract a large constant voltage from its output to obtain convenient Fahrenheit scaling.

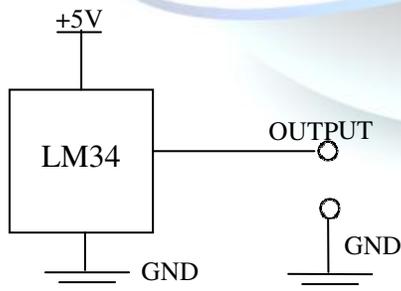


Figure: LM34 temperature sensor

### VIBRATION SENSOR:

It works on electromechanical principle vibration velocity sensors operate in accordance with the electrodynamic principle and are used for measuring the bearing absolute vibration based on the

piezoelectric effect. Change in resistance due to the force acting on it and convert it into 4 - 20 mA. They are measuring differences in oscillation, so they probably want a -12 and +12 swing with 0 as the base line we have piezoelectric sensor which detects the vibration created on the surface. We can also use shock sensor to detect vibrations.

### PIC16F877A MICROCONTROLLER

PIC microcontroller is the smallest microcontrollers that can be programmed to carry out a huge range of tasks. These microcontrollers are found in many electronic devices such as phones, computer control systems, alarm systems, systems.

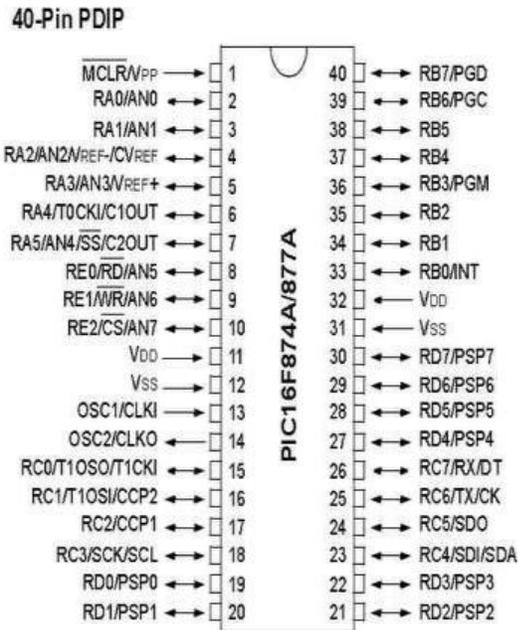
Every PIC microcontroller architecture consists of some registers and stack where registers function as Random Access Memory (RAM) and stack saves the return addresses. The main features of PIC microcontrollers are RAM, flash memory, Timers/Counters, EEPROM, I/O Ports, USART, CCP (Capture/Compare/PWM module), SSP, Comparator, ADC (analog to digital converter), PSP (parallel slave port), LCD and ICSP. The 8-bit PIC microcontroller is classified into four types on the basis of internal architecture such as Base Line PIC, Mid Range PIC, Enhanced Mid Range PIC and PIC18[9].

### ARCHITECTURE OF PIC MICROCONTROLLER

The PIC microcontroller architecture comprises of CPU, I/O ports, memory organization/D converter, timers/counters, interrupts, serial communication, and oscillator and CCP module. The four features that you might make you use a 16F887 instead of a 16F877 (A) are



### 16F877A PIN DIAGRAM



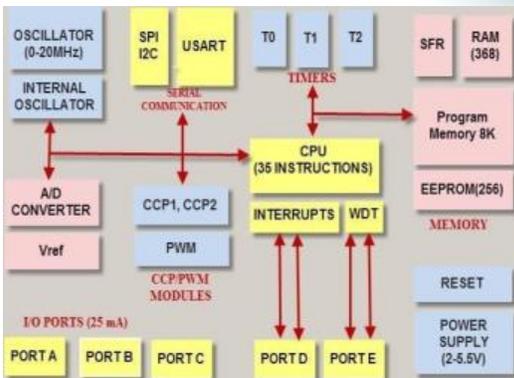
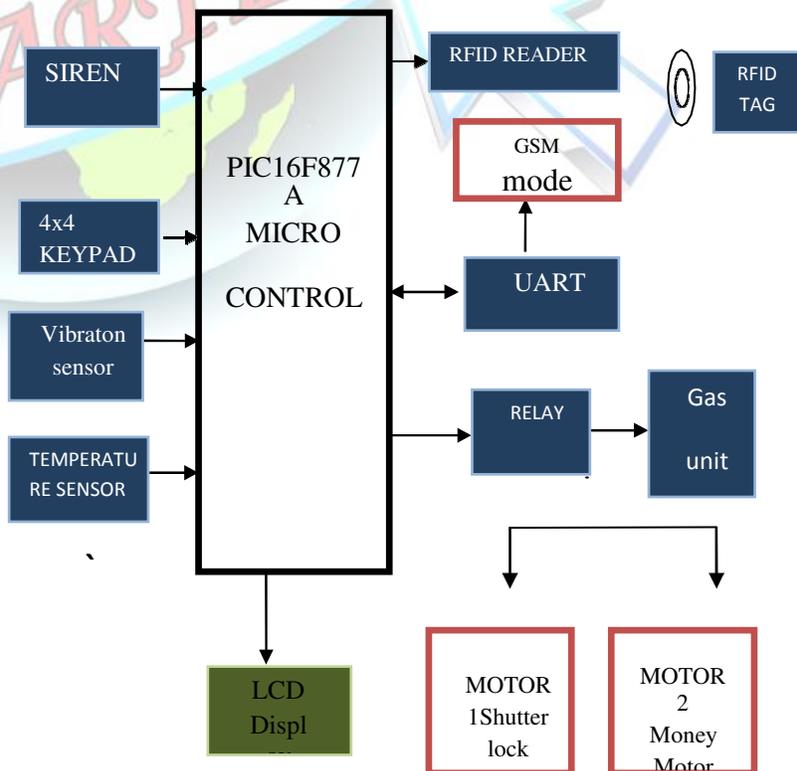
PORT-A	RA-0 to RA-5	6 bit wide
PORT-B	RB-0 to RB-7	8 bit wide
PORT-C	RC-0 to RC-7	8 bit wide
PORT-D	RD-0 to RD-7	8 bit wide
PORT-E	RE-0 to RE-2	3 bit wide

### INPUT/OUTPUT PORTS

PIC16F877 has 5 basic input/output ports. They are usually denoted by PORT A (R A), PORT B (RB), PORT C (RC), PORT D (RD), and PORT E (RE). These ports are used for input/ output interfacing. In this controller, PORT A is only 6 bits wide (RA-0 to RA-7), PORT B , PORT C,PORT D are only 8 bits wide (RB-0 to RB-7,RC-0 to RC-7,RD-0 to RD-7), "PORT E" has only 3 bit wide (RE-0 to RE-7).

All these ports are bi-directional. The direction of the port is controlled by using TRIS(X) registers (TRIS A used to set the direction of PORT-A, TRIS B used to set the direction for PORT-B, etc.). Setting a TRIS(X) bit '1' will set the corresponding PORT(X) bit as input. Clearing a TRIS(X) bit '0' will set the corresponding PORT(X) bit as output.

### BLOCK DIAGRAM





## V. BLOCK EXPLANATION

This project deals with the design and implementation of NFC based secure transaction system in ATM machines. This system consists of two modules, the transmitter and the receiver module in order to provide high end security for the ATM card users and the service providers. The password for transaction is sent to the cardholder's mobile phone with the help of NFC technology, which is an added advantage. This increases the high usage of smart cards with radio frequency communication between the target devices.

Whenever the transaction has to be done, the RFID card is inserted inside the ATM machine and NFC devices are made to interact with some of the legacy systems. Granting that both RFID and NFC device is found to be accurate, a message is received to the mobile phone of the rightful proprietor with a pin number of four digits. In case of password being correct it moves on to the next level of money transaction, asking for the money withdrawal. Scenario like, the password is found to be defective, next in order of time, the passage out will be locked.

The temperature and vibration are used to provide the additional security to the ATM. If theft people damage the ATM means vibration sensor will use to find out the vibration and give the alert signal to the micro controller. Microcontroller automatically locks the shutter.

When the machine damaged by robbers i.e., they can be damage the machine chassis using welding machine in some time. In this case we will detect the uncertain level of temperature in machine (during the welding machine used) and alert the environment.

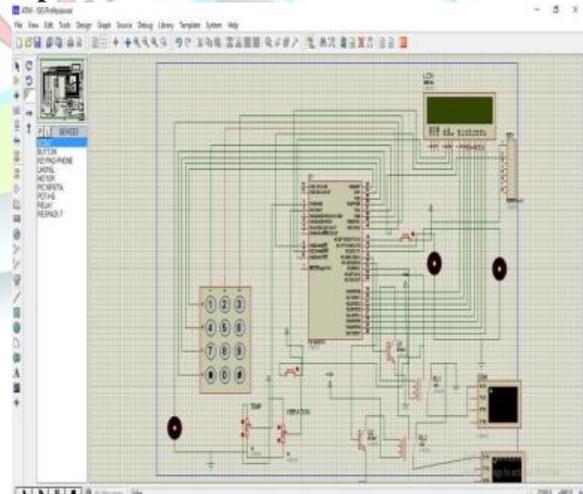
## One Time Password (OTP) Implementation

A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password based authentication.

A number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has (such as a small key ring fob device with the OTP calculator built into it, or a smartcard or specific cell phone) as well as something a person knows.

A major advantage is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker.

VI. Here is a screenshot of the data coming from the sensor, when the sensor is pressed





## VII. Experimental work Hardware development of this project for ATM security system



### CONCLUSION:

The implementation Automatic video surveillance for the theft detection by using smart of sensors and GSM/GPRS modem took advantages of the stability and reliability of sensor characteristics. The security features were enhanced largely for protection of ATM's when compared to previous systems. The whole system will be built on the technology of embedded system which makes the system more safe, reliable and easy to use. Therefore the proposed surveillance system here utilizes the latest technology like smart sensors and GSM/GPRS modem which as a system has a very good endurance in the long run, which makes it ideal for protecting the ATM. Thus this system will be able to thwart physical attacks on the ATM and alerts necessary people to take action at any time and save people from lot of hardships involved in the ATM attacks.

### FUTURE WORK

Security plays a vital role in all fields and in various applications. The existing computer security systems used at various places like banking, passport, credit cards, smart cards, PIN (Personal Identification Number), access control and network security are using username and passwords for person identification. In distributed system like ATM (Automated Teller Machine) the

security is a main issue. The security level has been grown from providing PIN to Smart Card to Biometrics. Even though the security has been increased at the same time fraudulent activities have been grown to equal level. In the existing approaches different biometric technologies, multibiometrics, multimodal biometrics and two tier security is introduced in ATM to provide higher level of security. The proposed work is to enhance the security using brain fingerprinting technology which acts as an uncrackable password. A brain computer interaction has been developed to record the brain signal through Digital Electroencephalography. Brain fingerprinting is a technique used to find the unique brain-wave pattern generated by brain when a person encounters a familiar stimulus

### REFERENCES

- [1] ATmega328 datasheet, [www.atmel.com](http://www.atmel.com)
- [2] FSR – Force Sensitive Resistor datasheet, [www.interlinkelectronics.com/FSR402.php](http://www.interlinkelectronics.com/FSR402.php)
- [3] PIR – Passive Infrared Sensor, [www.parallax.com](http://www.parallax.com)
- [4] ADXL335 3-axis accelerometer datasheet, [www.analog.com](http://www.analog.com)
- [5] R. Weinstein, "RFID: A Technical Overview and Its Application to the Enterprise," IT Professional, vol. 7, no. 3, pp. 27 - 33, May - June 2005.
- [6] ASPIAN, Privacy Rights Clearinghouse, ACLU, EFF, EPIC, Junk busters, Meyda Online, and Privacy Activism, RFID position statement of consumer privacy and civil liberties organizations <http://www.privacyrights.org/ar/RFIDposition.htm>, 2003



Univ. of Technol. & Educ, Tianjin, China,  
Li Jie ; Li Guang-Hui

[7]SIM900 GSM/GPRS module datasheet,  
[www.simcom.us](http://www.simcom.us)

[8] For “vibration detection sensor”  
<http://www.alarmscctv.com/detectionprodint6.html>

[9]microcontroller”[http://www.societyofrobots.com/microcontroller\\_tutorial.shtml](http://www.societyofrobots.com/microcontroller_tutorial.shtml)

[10] Christo Ananth, G.Poncelina, M.Poolammal, S.Priyanka, M.Rakshana, Praghash.K., “GSM Based AMR”, International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1, Issue 4, July 2015, pp:26-28

[11] B. Klinder, ATM Security Guidelines, <http://atm.techtarget.com/articles/atmsecurity.htm>, November 200 I.

[12] Sivakumar T.1, Gajjala Askok2, k. Sai Venuprathap3” Design and Implementation of Security Based ATM theft Monitoring system” International Journal of Engineering Inventions e-ISSN: 2278-7461, p-ISSN: 2319-6491 Volume 3, Issue 1 (August 2013) PP: 01-07

[13] Vivek V. Jog, Rohan Arora, Darshan Jain, Badal Bhat” Theft Prevention ATM Model using Dormant Monitoring for Transactions” Proceedings of 2013 IEEE Conference on Information and Communication Technologies (ICT 2013).

[14] 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.