ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 6, June 2017

Design and Implementation of Security Based Automatic Teller Machine against Intruders

[1] Niranjan L, [2] Sushma S,[3] Shreekanth R, [4] Santhoshilakshmi G S
[1] Department of Electronics and Communication, R R Institute of Technology , Chikkabanavara, Bangalore.

Abstract **- This paper explores The Idea of Designing and Implementation of Security Based ATM against intruder are born with the observation in our real-life incidents happening around us. This paper deals with prevention of intruder from robbery and to overcome the drawback found in existing technology in our society. Whenever an intruder tries to attack a citizen in the ATM unit, the citizen used the panic button which is places next to the keyboard which sends the SMS to the concerned bank manager and the nearest police station and alarm goes on. And whenever the intruder tries to steal the ATM money box in the ATM unit metal detector senses this which is placed near by the ATM money box and sends the SMS to the concerned bank manager and nearby police station and alarm goes on. There by locking down the ATM with the magnetic door lock present at the top of the ATM door till the police attends the place.**

Key words: ATM, Security, Panic Button, Metal Detector, GSM Module.

I. INTRODUCTION

A new system designed to prevent of intruders from robbery and to overcome the drawback found in existing technology in our society. There are many draw back present in the existing system which is more vulnerable to thefts in the ATM machines. Here we propose a system which will overcome all these drawbacks which will help both citizens and the public servants to stop such type of events occurring in future. The system is placed in the automated teller machine which is not visible to users nor the robbers. The system is equipped with GSM module, panic button, metal detector. The GSM is used to send the SMS to the bank manager and the nearby police station regarding the event. The panic button helps the citizen to activate the alarm, the metal detector is used if the robbers is taken place in the night if the teller machine is removed from the place, all these events may happened due to advance technologies which are present which helps the robber to steal the money, as soon the machine is opened the sensor senses this event and send the information to the bank manager and the nearest police station along with this it will lock down the ATM door by using the magnetic lock which makes the robber more confusion and try not to steal the money. By this method, we can avoid most of the robberies in our nation.

II. DESCRIPTION

This project is designed for the two purposes. Whenever an intruder tries to attack a citizen in the ATM unit, the citizen has to press the panic button which is placed next to the keyboard which sends the SMS to the concerned bank manager and the nearest police station and alarm goes on.

This system also incorporates with a money theft box placed inside the ATM unit whenever an intruder tries to steal the money in the ATM money box the metal detector which is placed at a 1cm away from the ATM money box senses this and the information to the concerned Bank manager and the nearby police station and the alarm goes on. There by locking down the ATM with the magnetic door lock present at the top of the ATM door till the police attends to the place.

This system uses Microcontroller based embedded system to process real time data from the panic button. The return of the concerned person must deactivate the locking system and the alarm system by entering the security key which is place at the entrance of the ATM and after the confirmation of the password the system allows the police to enter the ATM. This will prevent the robbery and the person involving in robbery can be easily caught. The

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 6, June 2017

password for the police and the bank manager is of the length of 5 Digits and the master code is of 10 Digits and it is an efficient hacking prevention from Brute Force and it's not easy for an intruder to break the lock unless you keep the code simple. The input is taken from a 4×3 Keypad and Display the user input on a 2×16 LCD. The user has two options either he/she can use its own 5-digit code or use the default 5-digit code. If user has to do setup his own code, then he has to enter the 5-digit code and press '#'. After this the controller, will ask for 10 Digit master password which is pre-programmed in the controller. Entering master lock, user can enter the new 5-digit code for the lock and press '#' to save it. Keypad has 12 keys (4×3) starting from 1,2,3,4,5,6,7,8,9,*,0,# numeric keys are used for entering numbers. '*' is used as the Cancel key and '#' is used as the Enter key.

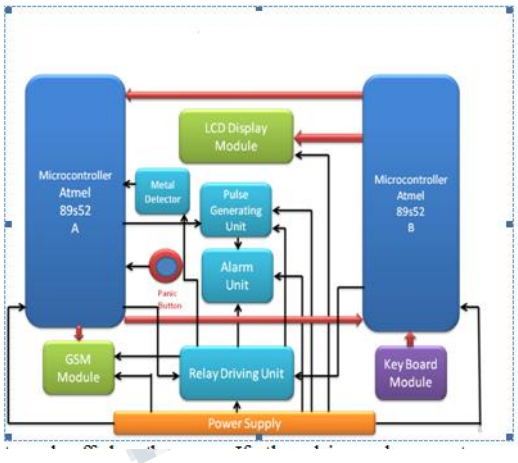

Fig. 1: Block diagram

III. WORKING

There are three conditions to be met in the above said system

1. Whenever the citizen enters the ATM unit he does his normal transaction and leaves.

2. Whenever an intruder attacks the citizen in the ATM unit the citizen should press the panic button which is places next to the keyboard the microcontroller detects this and activate the relay driving unit which intern activate the pulse generating unit which is an inbuilt IC 555 Astable multi vibrator which generates an high pulse which intern activates the alarm unit at the same time the relay activate the GSM Module which sends the message to the concerned bank manager nearby police station within 3seconds by using IC 555 Monostable multi vibrator.

3. Whenever an intruder tries to steal the money in the ATM money box the metal detector which is an inductive proximate sensor of 12mm detect this and activate the microcontroller which intern activates the relay and alarm goes on and message is sent to the concerned bank manager and nearby police station. There by locking down the ATM with the magnetic door lock present at the top of the ATM door till the police attends to the place.

IV. DEACTIVATING OF THE ALARM AND THE OPENING OF MAGNETIC METALIC DOOR

After receiving the message the concerned bank manager must arrive at the place and to deactivate the locking system and the alarm system by entering the security key which is place at the entrance of the ATM and after the confirmation of the password the system allows the police to enter into the ATM. This will prevent the robbery and the person involving in robbery can be easily caught. The password for the

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 6, June 2017

police and the bank manager is of the length of 5 Digits and the master code is of 10 Digits and it is an efficient hacking prevention from Brute Force and it's not easy for an intruder to break the lock unless you keep the code simple. The input is taken from a 4×3 Keypad and Display the user input on a 2×16 LCD. The user has two options either he/she can use its own 5 digit code or use the default 5 digit code. If user has to do setup his own code, then he has to enter the 5 digit code and press '#'. After this the controller, will ask for 10 Digit master password which is preprogramed in the controller. Entering master lock, user can enter the new 5 digit code for the lock and press '#' to save it. Keypad has 12 keys (4×3) starting from 1,2,3,4,5,6,7,8,9,*,0,# numeric keys are used for entering numbers. '*' is used as the Cancel key and '#' is used as the Enter key.

V. HARDWARE SETUP

A. Hardware Requirement

- Microcontroller 89s52.
- Serial port interface cable.
- LCD display (16x2).
- Power supply.
- GSM Modem.
- Keypad.
- Panic Button.
- Metal detector

B. Software Requirement

- Embedded C.
- PROCEUS.
- Keil C.

VI. DESCRIPTION OF EACH COMPONENTS

1. Panic button

A panic alarm is frequently but not always controlled by a concealed panic alarm button. These buttons can be connected to a monitoring center or locally via a silent alarm or an audible bell/siren. The alarm can be used to request emergency assistance from local security, police or emergency services. Some systems can also activate closed-circuit television to record or assess the event. Many panic alarm buttons lock on when pressed, and require a key to reset them.

2.GSM Modem

A GSM modem is a wireless modem that works with a GSM wireless network. A wireless modem behaves like a dial-up modem. The main difference between them is that a dial-up modem sends and receives data through a fixed telephone line while a wireless modem sends and receives data through radio waves.

2.1 AT Commands to GSM

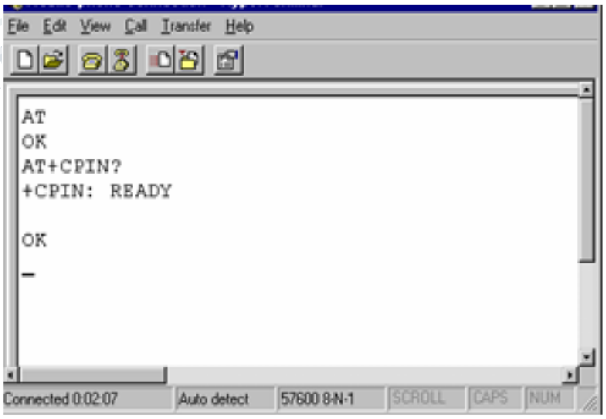

Fig. 2: Response from the GSM modem

The GSM modem is used to send the SMS to the concerned bank manager and to nearest Police station

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 6, June 2017

when an intruder tries to attack a citizen in the ATM unit which is stored in the SIM is invoked and sent [8]. The collision is detected by the vibration sensor which is calibrated to detect the collision of the vehicle [9]. This information is sent to the microcontroller there by invoking the commands for the GSM modem to send the SMS.

Fig. 3: Connectivity of GSM modem

GSM modem is connected via a serial cable, i.e. RS-232 where the information is send as the Commands followed by the AT of the microcontroller and to the Rx pin of the GSM microcontroller and to Tx pin of microcontroller.

3. LCD Module

It is very important to keep a track of almost all the automated and semiautomatic device, and the LCD (liquid crystal display) screen used as a display module which is 16x2 LCD very commonly used. This modules are replacing seven segments and other multi segments LED for this purpose. The reason for using this module is they are economical, easy programmable, have no limitation of displaying special and even custom characters, animations and so on. LCD can be easily interfaced with a microcontroller to display a message or status of device.

4. Inductive proximity sensor

Inductive proximity sensors operate under the electrical principle of inductance. Inductance is a phenomenon where a fluctuating current, which by definition has a magnetic component, induces an all electromotive force (emf) in a target object. To amplify a device's inductance effect, a sensor manufacturer twists wire into a tight coil and runs a current through it. An inductive proximity sensors has four components. The coil, oscillator, detection circuits and output circuit. The oscillator generates a fluctuating magnetic field the of a doughnut around the winding of the coil that locates in the device's sensing face. When a metal

object moves into the inductive proximity sensor's field of detection, Eddy circuits build upon the metallic object, magnetically push back, and finally reduce the inductive sensors, own oscillations field. The sensors detection circuit monitors the oscillator strength and triggers an output from the output circuitry when the oscillator becomes reduced to a sufficient level. As seem in Fig. 5 and Fig. 6, the port 0 which specifies the triggering of the alarm and activating the pulse generator. Here a relay is connected to change over the condition of the panic button. In this situation, the relay directly connected to the microcontroller, metal detector, pulse generator, GSM module [10]. The P1 is used to LCD display. P3 is used for the displaying the information for the alarm.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 6, June 2017

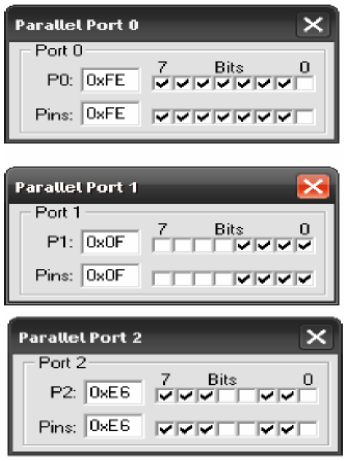

Fig. 4: Working of proximity sensor

Fig. 5. Proximity sensor

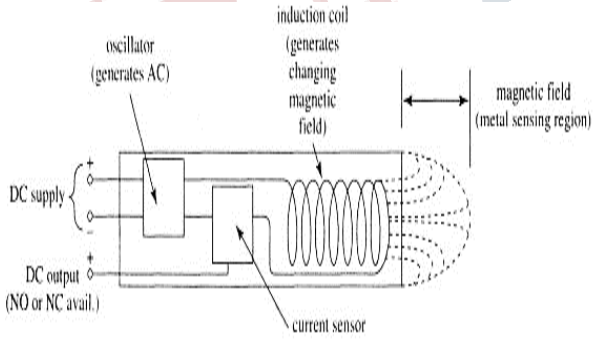

Fig. 6. Proximity sensor

The proximity sensor and the port which the sensor is connected is shown in the figure 4 and figure 5, the sensor output is fed to the port 2

IV. EXPECTED RESULTS

A. Normal Transaction

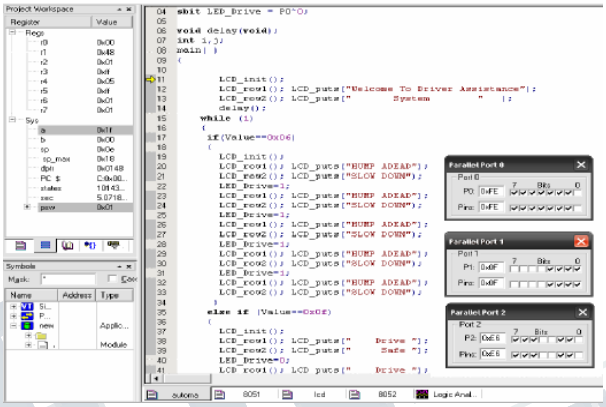

Fig. 7: Simulation of Normal transaction.

B. Real time Situation

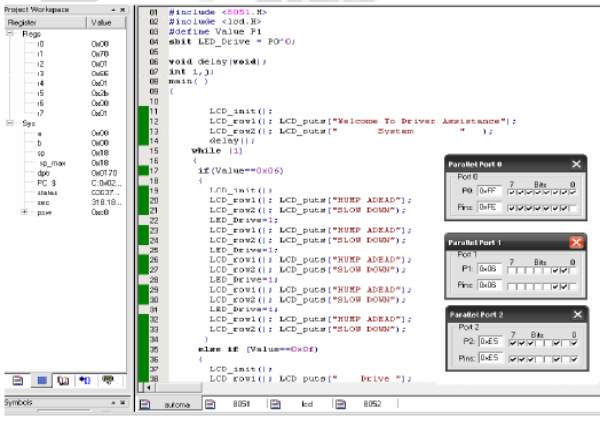

Fig. 8: Simulation when intruder enters.

In the Real-Time when intruder enters in the ATM unit the output of each port is described in Fig. 7 and Fig. 8, the port 0 which specifies the triggering of the

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 6, June 2017

alarm and activating buzzer. Here a relay is connected to change of high and low of the signal in the pulse generator. In this situation the relay connected via a series of resistors Connected to the electromagnetic switch. Fig. 8, the port 0 which specifies the triggering of the alarm and activating buzzer. Here a relay is connected to change of high and low of the signal in the pulse generator. In this situation the relay connected via a series of resistors Connected to the electromagnetic switch.

The increased need of privacy and security in our daily life has given birth to this new concept of designing and implementation of security based ATM using GSM panic button and metal detector against intruder.

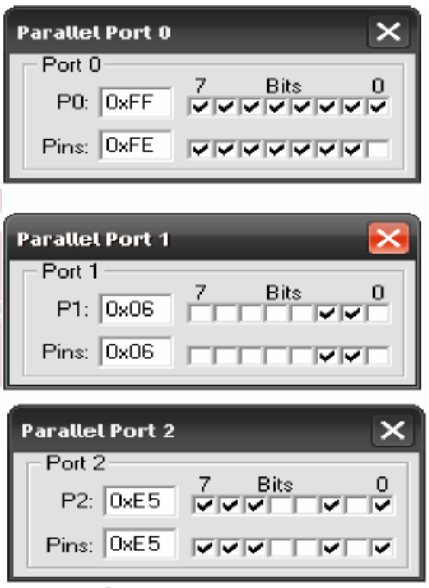

Fig. 9: Simulation Result for message.

As we can see here the port 0 is activated at the pin P0.0 where the relay is activated and the connection is through the resistor depend on the zone which is near its vicinity. The port 1 is the value for the alarm i.e. when intruder attacks the citizen in the ATM unit in our project, which is of 0x06h and the corresponding output on the display is via port 2 which displays in the form of message to the concerned bank manager and the nearby polices station.

V. ADVANTAGES

1. Cheaper and more reliable.
2. Time consumption is reduced in installations.
3. Good at Network Security.
4. Intruders can be easily caught.
5. Crimes can be controlled in the ATM.

VI. CONCLUSION

The proposed method overcomes the limitations that exists in other methods and provides a secured and safe environment that saves the hard-earned money of the user. The user will not be harmed and robbery from the intruder can be controlled and the criminals can be easily caught via mobile SMS after code verification and when forced can block the account's transaction with PII and even if the stranger tries trial and error, maximum of 3 times PII will function and gets blocked for 24 hrs. This provides two tier security. In future this method will be experimented using a biometric system to check the fingerprint and a SMS gateway has to be connected to send a verification code which should be updated in Database too. The efficiency of proposed algorithm will measured using performance

REFERENCES

[1] The ATM Forum Technical Committee, 'ATM Security Framework 1.0', AF-SEC-0096.000, February 1998.

[2] The ATM Forum TechnicalCommittee,'ATM Security Specification 1.0', ATM-SEC-0100.001, February 1999.

[3] Lyndon G. Pierson, Edward L. Witzke, Sandia National Laboratories, Mark O. Bean, and Gerry J. Trombley, National Security Agency, 'Context-Agile Encryptio for High Speed Communication Networks', Computer Communication Review, ISSN 0146-4233, Volume 29, Number 1, pages 35-49, January 1999.

[4] Which?, "Fraud victims struggle toget money back," June 2009. [Online]. Available: http:// www.which.co.uk /news /2009/06/fraudnt victims-struggle-to-get-money-back-179150.jsp

[5] S. Drimer and S. J. Murdoch, "Keep your enemies close: Distance bounding against smartcard relay attacks," in USENIX Security Symposium,August2007.

[6] S. Drimer, S. J. Murdoch, and R. Anderson, "Thinking inside the box: system-level failures of tamper proofing," inIEEE Symposium on Security and Privacy (Oakland), May2008, pp. 281–295. [Online]. Available: http:// www. cl. Cam . ac . uk / ~sd410/ papers /per attacks.pdf.

[7] Schwiderski-Grosche and H. Knospe. Securem-commerce. 2004.

[8] D. V. Thanh. Security issues in mobile e-commerce.mFirst International Conference on Electronic Commerce and Web Technologies, pages 467 { 476, 2000.

[9] Wishart and Neville. Micro-payment systems and their application to mobile networks. 2006.

[10] Biswas S., Bardhan Roy A., Ghosh K. And Dey N.,"A Biometric Authentication Based Secured ATM Banking System", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012