Smart Phone Based Intrusion Detection System

Ogunrinola. O.B., Olalere, N. A., Nwosu E.U. & Alao, W.A.
Dept. of Industrial Maintenance Engineering
Yaba College of Technology
Yaba-Lagos. Nigeria
E-mail: imepapers@yahoo.com

ABSTRACT

The security of a state begins with home security. Deploying advanced technology in managing security challenges will go a long way in promoting the socio-economic development of a state because insecurity hinders business activities and discourages both local and foreign investors. The intrusion detection system presented in this paper consists of a sensor which detects human presence and sends equivalent electrical signal to a microcontroller which has been programmed to send AT command to a GSM modem whenever the data it received from the sensor exceeds a prescribed limit. The GSM modem was used to establish communication between the microcontroller and the mobile station. It sends SMS message to alert the home/office owner at the instant of intrusion using the GSM network. A buzzer was also incorporated into the system for local intrusion alarm. The system design involved both hard-wire of all the components as well as writing of computer programs to interface each of the sub-units with the microcontroller. The program was written in C language, while Keil µVision5 was used to create hex file (machine language) from the C code and ProgISP was used to load the hex file on to the chip. The device was test-run by deliberately allowing someone to move his hand across the sensor view field and an SMS message was immediately received on the assigned mobile phone.

KEYWORDS: Interfacing, AT command, PIR sensor, Serial port.

SMART-SMART-iSTEAMS Conference Proceedings Paper Citation Format
Ogunrinola. O.B., Olalere, N. A., Nwosu, E.U. & Alao, W.A. (2018): Smart Phone Based Intrusion Detection System. SMART-iSTEAMS Multidisciplinary Conference, February, 2018, Ogwuashi-uku, Delta State, Nigeria. Pp 201-210

1. INTRODUCTION

Intrusion is an event in which someone enters a place where he is not expected to be. It is a breach of security that is often done secretly with criminal intent. The intrusion detection system is a device designed to identify unauthorized entry into designated areas and notify the home or office owner through his mobile phone at the instant of intrusion. Depending on the user's choice, the alarm system incorporated in this device can be activated to create intrusion awareness for people within the vicinity and of course frighten the intruder. Intrusion detection is a research area that started gaining more attention in 1853 when the first electro-magnetic alarm system was invented (Terrance, 2012). Over the years, there had been various attempts to prevent intrusion but most of the developed techniques are being defeated by intruders who eventually accomplish their mission.

If intrusion cannot be absolutely prevented, developing and implementing a system that would alert the property owner at the instant of intrusion wherever he may be is definitely a step in the right direction.

A) Burglar Alarm System

The first electro-magnetic alarm system in the world was invented by a man called Augustus Russell Pope, an inventor from Summerville in Boston (Terrance, 2012). His invention was a battery-operated gadget that reacted to the closing of an electric circuit. Doors and windows were connected as independent units by a parallel circuit. If a door or window was opened and the electric circuit closed, the sudden flow of current caused one of the attached magnets in the system to vibrate. The electro-magnetic vibrations were transmitted to a hammer which then struck a brass bell (Terrance, 2012). The special feature of this invention was that the alarm could not be switched off by merely closing the windows or doors. However, a major hitch was that its output is local. To address this shortcoming, a central monitoring station for all the installed alarm systems was developed by Edwin Holmes (Terrance, 2012). He used weatherproof telegraph cables to connect his customers' alarm system to a central monitoring station. But the fact that cables had to be laid before the network can be established remains a weakness of this technology. In addition, false alarm is a general problem related to burglar alarm systems. The United States Department of Justice estimates that between 94% and 98% of all alarm calls to law enforcement are false alarms *(Rana, 2007).*

B) Video Surveillance System

The word “surveillance” comes from a French phrase for "watching over" - sur means "from above" and veiller means "to watch" (Minsky, Kurzweil, & Mann, 2013). In line with this study, surveillance can be described as the act of carefully watching an area for the purpose of protecting life and properties. When electronic means such as the closed-circuit television (CCTV) system is employed, it is referred to as video surveillance systems (Leighton & Martin, 2014). The first video surveillance system was designed by three German engineers and installed in Peenemünde, Germany, in 1942 (Bing, Yunhung, Guangwei, & Tian 2001). Video surveillance started out as 100-percent analog systems. The IP camera, also known as network camera, is a key driver in the network video revolution (Fredrik, 2009). With this system, videos from network cameras are continuously transported over an IP network via network switches and is recorded on a PC server with video management software installed. Obviously, deployment of video surveillance system in deterring crime is very effective. But a large percentage of homes and organizations in developing countries cannot benefit from this technology considering its acquisition/running costs.

C) Automatic Home Security System

This development was an attempt to ensure absolute security of a home. A system was designed to detect intrusion as well as to prevent possible incidences that could lead to fire outbreak in the home. Five different categories of sensors were utilized, each responsible for detecting either smoke, fire, gas leakage, or human body and then communicate with the microcontroller to trigger both local and remote alarm through the GSM modem. The introduction of many sensors made this design a bit complex. Two separate power supply sections were incorporated to prevent overheating of the LM 7085 voltage regulator (Prakash & Pradeep, 2013). These and more had negative impact on the cost of the product. Having a single system that can perform multiple tasks is a quite desirous and welcomed development but affordability especially by the 'lower class' should be given more attention because every individual deserves security of life properties. Therefore, it is necessary to design a system that proffers solution to the most pressing need of every individual. Such system should be flexible enough to accommodate future expansion of its functionality.

2. METHODOLOGY

The system consists of a PIR (Passive Infrared) sensor which detects human presence and sends corresponding data to a microcontroller. The microcontroller was programmed such that it sends command signal to a GSM modem whenever the data it received from the sensor exceeds a prescribed limit. Similar command signals are equally sent to a buzzer, if activated, for local alarm. An LCD (Liquid Crystal Display) unit was interfaced with the microcontroller to display on-going processes in the chip, following by interfacing of every other hardware. The GSM modem was used to establish communication between the microcontroller and the mobile station. It sends SMS message to alert the home/office owner at the instant of intrusion using the GSM network. Upon reception of such SMS alert on his mobile phone, the owner can quickly take appropriate action to prevent the intruder from achieving his mission. Provision for upgrading was also made to enhance capability of the system.

2.1 System Overview

The entire system is made up of an input section, a control section, an output section, and of course, a power supply section without which all other sections cannot function.

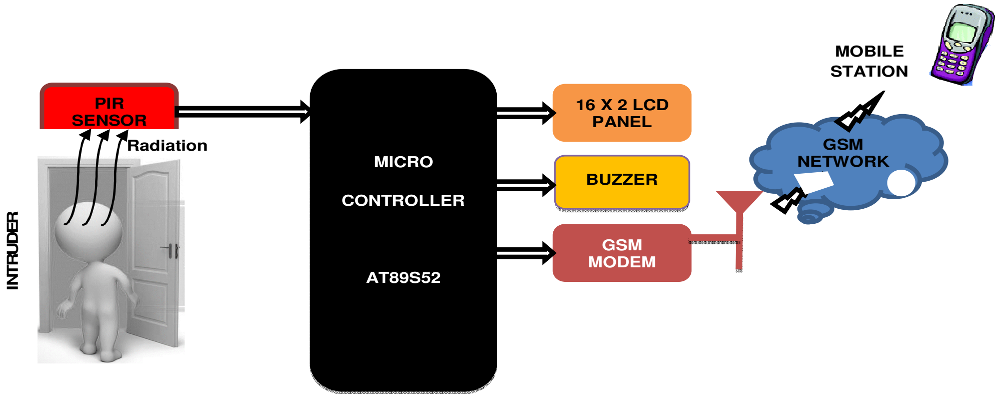


Figure 2.1: An Overview of Intrusion Detection System

2.2 LCD Interfacing with AT89S52 Microcontroller

Port 2 of the microcontroller was dedicated for programming the LCD, therefore the control lines of the LCD: E, R/W, and RS were connected to P2.5, P2.6, and P2.7 respectively. In this design, port 2 was taken as the control port. Similarly, port 0 of the microcontroller was assigned to the 8 data pins (D0 to D7) of the LCD module.

Each of the 8 data lines was connected to the corresponding pin of port 0 through a resistor network R5 used for pulling-up the port. This was done because port 0 of AT89S52 is an open drain and it will not work properly as an output port without external pull-up resistors.

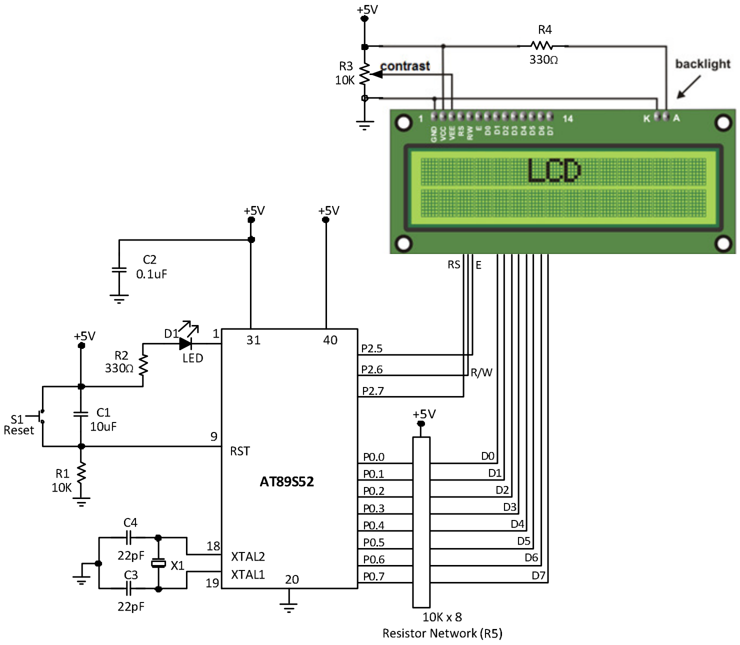


Figure 2.2: LCD – Microcontroller Interfacing

The backlight pins (A and K) of the LCD were connected across a 10kΩ potentiometer through a 330Ω current limiting resistor (R4) to power the backlight from a regulated 5V dc supply. Output of the potentiometer was then connected to the VEE pin so that the LCD contrast can be adjusted simply by rotating the potentiometer knob forward and backward. The VCC pin was connected to the +5V dc supply to power the LCD panel itself.

2.3 PIR Sensor Interfacing with AT89S52 Microcontroller

The sensor consists of three pins (Vcc, OUT, and GND) which were connected into the working circuit as shown below. The Vcc pin which corresponds to the drain terminal of the sensor was connected to the positive 5V dc supply. Output pin of the sensor, which represents the source terminal, was connected to port 3.5 (pin 15) of the microcontroller. Lastly, the GND pin was connected to the ground. The PIR sensor operates from 4.5 to 5V supply and the stand-by current is less than 60uA. When the sensor detects motion in its field of view, the output voltage will be 3.3V and status of the OUT pin is described as HIGH.

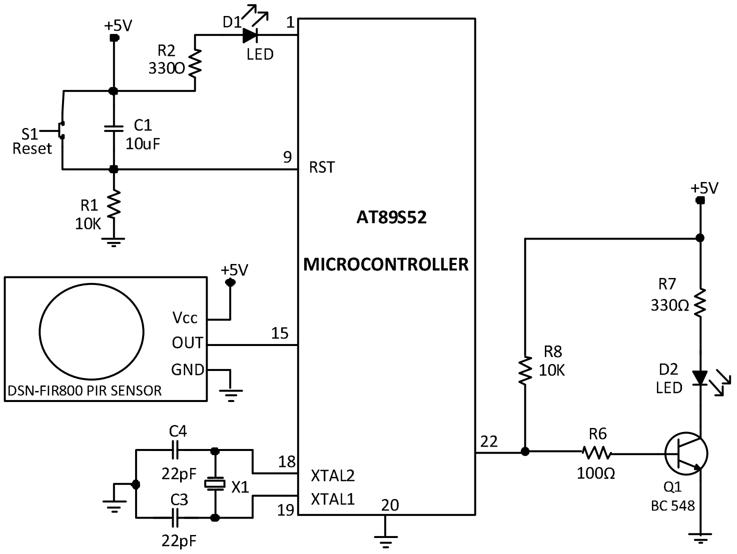


Figure 2.3: PIR Sensor – Microcontroller Interfacing

On the other hand, when motion is not detected, the output voltage will be 0V and status of the OUT pin is described as LOW. The AT89S52 microcontroller considers any voltage between 2 and 5V at its port pin as HIGH and any voltage between 0 to 0.8V as LOW. Since the output of the PIR sensor module has only two stages (HIGH and LOW), it was directly interfaced to the microcontroller. The microcontroller reads the status of the PIR sensor output and switch ON the LED (D2) when the output voltage is HIGH, while the LED remains OFF if otherwise.

2.4 GSM Modem Interfacing with AT89S52 Microcontroller

The GSM modem used in our design has RXD and TXD (with GND) pins on board, which indicates that it is capable of working at TTL (Transistor-Transistor Logic) logic. A GSM modem requires a wired connection at one end and wireless at the other. Therefore, the RXD of the GSM modem was connected to TXD (pin 11) of the microcontroller, while TXD of the modem was connected to RXD (pin 10) of the microcontroller such that the RXD and TXD were used for the receiving and transmitting data continuously. To communicate with the GSM modem, AT commands are required. Therefore, after the connection, we wrote a program to send AT commands from the microcontroller to the modem since the GSM module only understands **AT commands** and can respond accordingly.

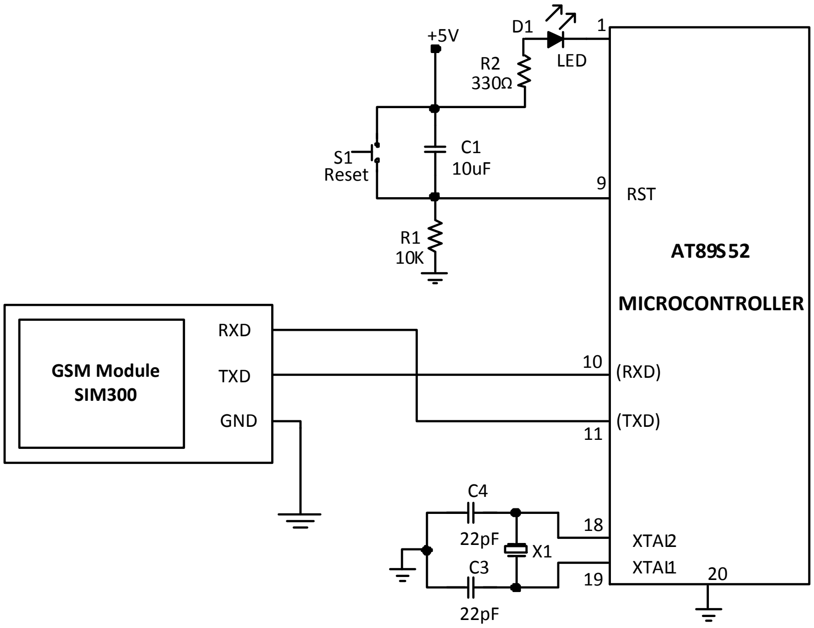


Figure 2.4: GSM Modem – Microcontroller Interfacing

2.5 LED Interfacing with AT89S52 Microcontroller

The cathode lead of the LED was connected directly to pin 1 of port 1 (P1.0) with a 330Ω current limiting resistor at the anode lead. The LED is said to be forward-biased because the input voltage is connected to the positive terminal. With this connection, the LED runs on the negative logic such that when the pin output is 0, it behaves like ground and the LED will glow as current flows towards the pin due to its lower potential. Contrarily, when the pin output is 1, the LED will be tuned OFF. This connection was done because the pin output may not provide enough power to glow the LED.

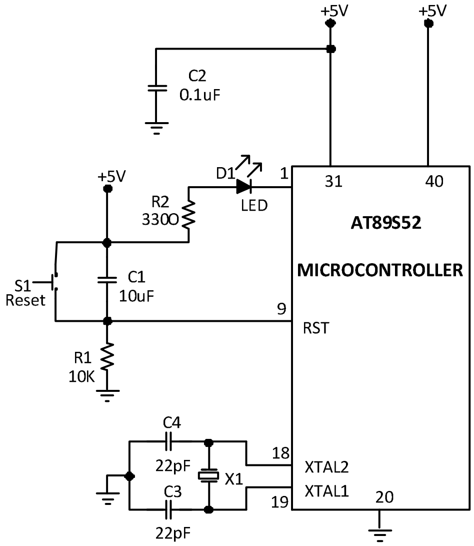


Figure 2.5: LED – Microcontroller Interfacing

The microcontroller was connected to external crystal oscillator of 11.0592MHz frequency using pin 19 and 18 (XTAL1 and XTAL2). This oscillator is used to generate clock pulses, and clock pulse is used as a means of timing calculation, which is mandatory to synchronize all the events. Although AT89S52 has an on-chip oscillator, it requires an external clock to run it. Because the **quartz** is a resonant oscillator circuit, two capacitors (C3, C4) of the same value (22pf) were connected to oscillate the crystal for generating a clock signal of the desired frequency. The crystal pins were then connected to the ground through these capacitors. Resistor R1, capacitor C1 and push button switch S1 form the reset circuit. It resets the microcontroller when connected to HIGH. A 10kΩ resistor and 10uF Capacitor were used in the reset circuitry to which the RST pin (pin 9) was connected. Capacitor C2 is just a decoupling capacitor.

3. RESULT AND DISCUSSION

The complete unit was provided with a 9V dc supply through an ac-dc adaptor plugged into a 230V ac outlet. However, this is not the actual voltage that is applied to the hardware. An internal voltage regulator (LM7805) was used to achieve the desired 5V regulated dc voltage which is the operating voltage of our microcontroller, sensor, GSM modem, etc. A 9V battery can equally be used as the external power supply.

With availability of the power supply, the intrusion detection system was test-run as follows:

Step 1: A registered SIM card (07031328860) was inserted into the GSM modem for sending intrusion alert.

Step 2: The device was switched ON using the SPST (Single Pole Single Throw) switch by a side of the casing.

Step 3: To initialize the modem, the red momentary switch on the device was pressed down until a confirmation message 'MODEM OK' was displayed on the LCD. This process took about ten seconds.

Step 4: To validate the SIM card where intrusion alert should be directed to, the text message 'PRG08058484851E' was sent to 07031328860 from a mobile phone with a registered SIM card (08058484851). This setting implies that the SIM card number 08058484851 will receive SMS message from 07031328860 whenever intrusion is detected.

Step 5: To initialize the microcontroller, the text message 'MAON' was sent to 07031328860 from the same mobile phone with SIM card 08058484851 and a confirmation message 'DEVICE ACTIVATED' was received.

Step 6: Someone was then allowed to deliberately move his hand across the PIR sensor view field and an SMS message was immediately received on the mobile phone with SIM card 08058484851.

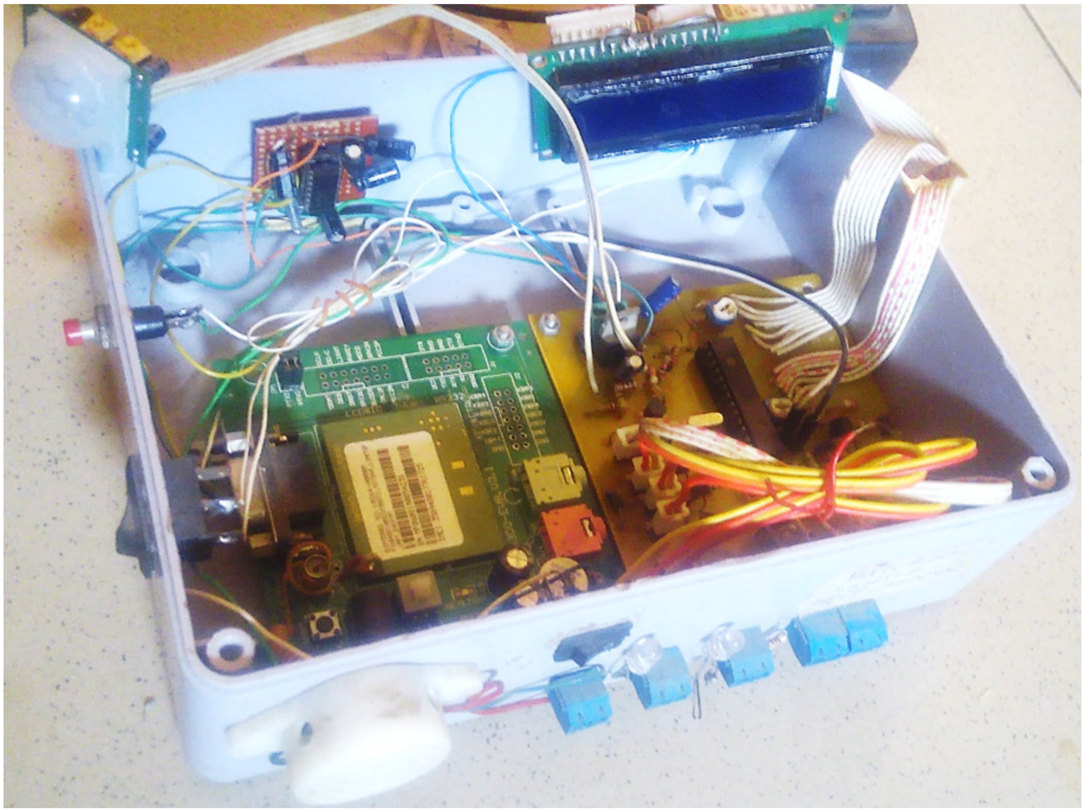
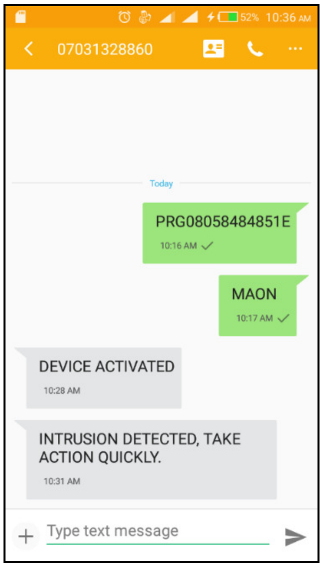


Figure 3.1: Internal View of the Designed Model



07031328860

PRG08058484851E
10:16 AM

MAON
10:17 AM

DEVICE ACTIVATED
10:28 AM

INTRUSION DETECTED, TAKE ACTION QUICKLY.
10:31 AM

Figure 3.2: Screenshot of the SMS Messages during Testing

4. CONCLUSION AND RECOMMENDATION

The security of a state begins with home security which means every home owner is a stakeholder in security matters and must therefore play an important role in ensuring adequate security of personal properties among which life is not an exception. If security issue is not tackled at the home level, all efforts of the government in this direction cannot yield meaningfully. In addition, the financial benefits associated with this device outweighs its installation and maintenance costs. If your home or workplace is protected from intrusion, theft incidence that might require you to make a claim from your insurance company is less likely to occur. Hence you would be entitled to a reduced rate on your insurance policy, while you only pay the regular tariff for SMS message whenever intrusion is detected. Our design incorporated easily accessible unused ports through which extra sensors, alarms or any other desired output devices can be connected.

This approach makes the system flexible enough to accommodate future expansion of its functionality. Also, this intrusion detection system does not encroach on the privacy of innocent individual in the neighbourhood unlike the video surveillance system. When installing this system, the sensor is usually placed some distance away from the entire unit with some wires connecting them. In situation where it is difficult to completely hide such wires, breaking into the home or establishment only requires a pair of wire cutters. An intruder can easily sabotage the security system by cutting the wires connecting the sensor to the microcontroller. Although slightly expensive, the use of a wireless sensor will be a fantastic solution to this limitation of our design.

Since it has no wires that could be cut-off by the burglar. It rather uses radio waves for communication with the microcontroller which of course has distance limit. Introducing a wireless sensor will also make it easier and faster to set-up and dismantle the system. Repositioning the sensor into another area of the home or office will be done easily due to lack of wires. In addition, having no wires makes hiding the sensor a lot easier. A wireless sensor is independent of power supply to the entire system. It uses a separate battery which expands the system reliability. When more sensors (gas leakage, smoke or fire sensors) are added to the unit for different purposes, it is recommended to use a programmable buzzer. This type of buzzer allows you to give voice instructions along with a warning signal or a unique tone if multiple warning devices are used in the same area. It also allows you to program up to 30 seconds of MP3 file via USB from your computer. With the flexibility of programming your own sounds, you are no longer required to listen to the standard alarm tones and can quickly know what an alarm is signaling.

REFERENCES:

[1] Bing Z, Yunhung G, Guangwei Z, & Tian T. (2001) Home Video Security Surveillance. Info-Tech & Infonet Proceedings, ICII 2001-Beijing. International Conference, vol. 3, pp. 202-208.
[2] Fredrik N. (2009). Understanding Modern Video Surveillance Systems. Auerbach Publications, New York.
[3] Kapil S. (2015). Portable Security System with Panic Switch including Local and Remote Alarm. International Journal of Engineering Sciences & Research Technology.
[4] Kumar V, & Svensson J. (2015). Promoting Social Change and Democracy through Information Technology. IGI Global Book Series. pp. 75.
[5] Leighton W, & Martin M. (2014). The Effect of CCTV on Public Safety.
[6] Microchip Technology, AT89S52 Data Sheet, 2001. Retrieved from http://mouser.com/ ProductDetail/Microchip-Technology.../AT89S52-24PC/?qs.
[7] Minsky M, Kurzweil R, & Mann S. (2013). The Society of Intelligent Veillance. Proceedings of the IEEE ISTAS 2013, Toronto, Ontario, Canada, pp. 13–17.
[8] Prakash K, & Pradeep K. (2013). Arduino Based Wireless Intrusion Detection using IR Sensor and GSM. International Journal of Computer Science and Mobile Computing, Vol. 2, Issue 5.
[9] Rana S. (2007). False Burglar Alarms. 2nd Edition, US Department of Justice.
[10] Terrance H. (2012). History of the Home Burglar Alarm System. Retrieved from http://prezi.com/qnhvolcb44b6/history-of-the-home-burglar-alarm-system.