AUTONOMIC SMART SENSOR INTERFACE FOR INDUSTRIAL AND HOME IN IOT ENVIRONMENT

Venkatesh Basavaraju[1], J. Madhan Kumar[2]
[1]*M.Tech student, Sri Venkateswara College of Engineering & Technology,*
[2]*Associate Professor, Sri Venkateswara College of Engineering & Technology,*
Chittoor,Andhra Pradesh, India

***Abstract*- The main aim of this project is to design and develop a security sensor interface device is essential for security sensor data collection of industrial/Home wireless security sensor networks (WSSN) in IOT environments. It consists of PIR sensor node deployed in the location as well as the doors/ windows of the shopping malls, railway station together with the zigbee modules which act as end devices that monitor continuously and send the security status of each location to the coordinator node connected to a PC/mobile which acts as the master. It sends/informs over sms to the concerned department in case of Un-authenticated person.**

***Index Terms*- IoT, Zigbee, Radio Frequency Identification, WSN, ARM Controller**

I. INTRODUCTION

Key technologies that drive the future of IoT are related to smart sensor technologies including WSN, nanotechnology, and miniaturization. Since IoT is associated with a large number of wireless sensor devices, it generates a huge number of data. Sensor data acquisition interface equipment is one of the key parts in IoT applications. Data collection is the essential application of WSN and more importantly it is the foundation of other advanced applications in IoT environment. IoT is a major drive to support service composition with various applications. Now days, IoT (Internet of Things) is a new revolution of the Internet and it provides a platform for communication between objects where objects can organize and manage themselves. Internet of Things (IoT) is the expansion of internet services because it allows daily life things to connect with user and operate remotely from anywhere. We can describe IoT in simple words, when the objects or things connected with each other using standard protocols and standard infrastructure so that they can communicate between each other and all these objects/things can be monitored and controlled by anywhere and anytime using internet. The IoT was began in the year 1998 and the term Internet of Things was first called by Kevin Ashton in 1999 [4]. The objective of IoT is Anything, Anyone, Anytime, Anyplace, Any service and any network. Fig.1 describes the coupling of two things suppose its C's and A's which may be reveals, people and things can be connected Anytime, Anyplace, with Anything and Anyone, ideally by using in Any path/network and Any service.

This implies addressing elements such as Convergence, Content, Collections (Repositories), Computing, Communication, and Connectivity in the context where there is seamless inter connection between people and things and/or between things and things so the A and C elements are present and tightly coupled [8].

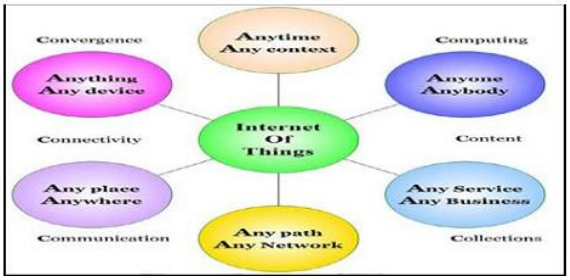

Figure. 1 Objectives of IoT

Following fig. 2 shows the methodology of IoT system or basic structure of IoT system.

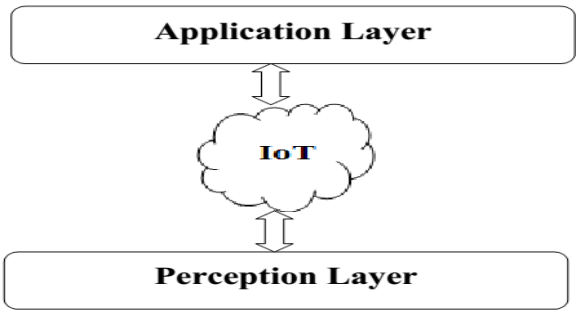

Figure. 2 Basic structure of IoT system

Fig. 2 consists of three layers: Perception Layer; main function of this layer is data acquisition interface and responsible for the integration and collaboration of various environments and collection of sensor data; Network Layer; this layer is nothing but the internet or IoT and provides interface between the Application layer and Perception Layer and application layer; Application Layer is smart system like Urban management, Green agriculture, industrial wireless sensor network or Industrial management, Environmental monitoring, Telemedicine, Intelligent transportation and smart homes etc.

II. RELATED WORKS

Radio Frequency Identification and Wireless Sensor Network are two important wireless technologies that have wide variety of applications and provide limitless future potentials. However, RFID and sensor networks almost are under development in parallel way. Integration of RFID and wireless sensor networks attracts little attention from research community. This paper first presents a brief introduction on RFID, and then investigates recent research works, new products/patents and applications that integrate RFID with sensor networks. Four types of integration are discussed. They are integrating tags with sensors, integrating tags with wireless sensor nodes, integrating readers with wireless sensor nodes and wireless devices, and mix of RFID and sensors. New challenges and future works are discussed in the end. RFID readers have relatively low range and are quite expensive, we envision that the first applications will not have RFID readers deployed ubiquitously. The applications which allow mobile readers to be attached to persons hands, cars or robots will be good candidates.

A wireless smart sensor platform targeted for instrumentation and predictive maintenance systems is presented. The generic smart sensor platform with "plugand-play" capability supports hardware interface, payload and communications needs of multiple inertial and position sensors, and actuators, using a RF link for communications, in a point-to-point topology. The design also provides means to update operating and monitoring parameters as well as sensor/RF link specific firmware modules " over-the-air". Sample implementations for industrial applications and system performance are discussed. In this project has used on Zigbee. This cost is too high and the WSN are controlled by remote access.

III. PROPOSED SCHEME

The proposed work includes the collection of data from various sensors well like IR proximity sensor, PIR Sensor. The signals of the sensors undergo signal conditioning to convert the signals from analog to digital. The microcontroller used belongs to LPC 2148 family. It processes the data and displays the parameters on the LCD as well as provides it to the GSM module.

A. Sensor: A sensor is a device used for the detection of changes in quantities and it provides a corresponding output, generally as an electrical or optical signal.

1).IR proximity sensor: This sensor is used to detect the objects and obstacles.

- This sensor keep on transmitting modulated intared light and when any object comes near it will detect by monitoring the reflected light from the object.
- Digital low output on detecting objects in front. We are using this sensor in door locks bank lockers.
- If anyone inserts the key it will detect the key and send the SMS to particular person.

2). PIR Sensor:(Passive Infrared –sensor): This sensor is a pyroelectric device that detects motion by measuring changes in the infared levels emitted by surrounding objects.

- This motion can be detected by checking for a high signal on a I/O pin. It provides an optimised circuit that will detect motion up to 6 meters away and can be used in burglar alarms and access control systems.

- Power it up and wait 1-2 seconds for the sensor to get a snapshot of the room.
- If anything moves after that period, the 'alarm' pin will go low.
- If any person is entered in to the room the sensor will detect only human bodies.
- The out will gives to controller. Controller will send the SMS to particular person.

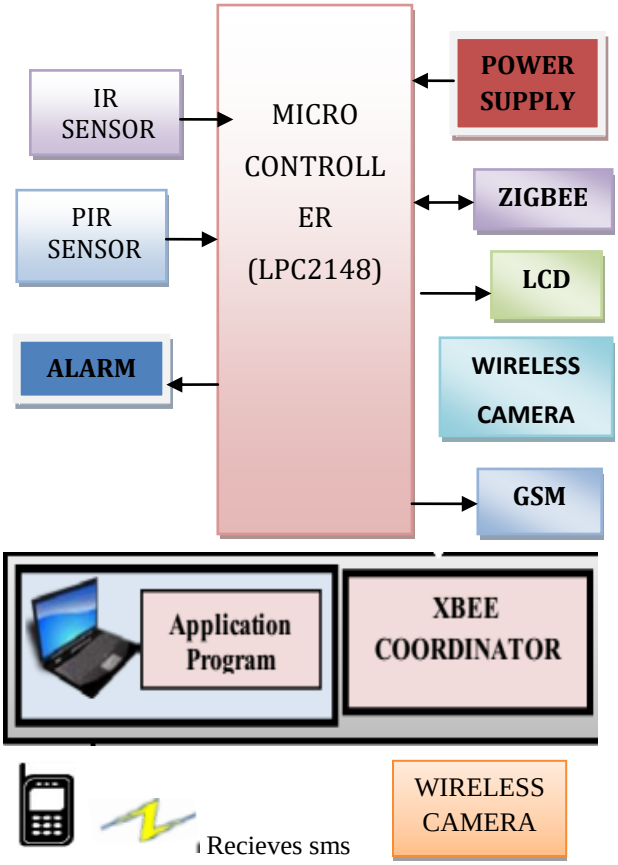

Figure.3. Block diagram of system

B. LPC 2148 Microcontroller: This is a 32-bit ARM7-TDMI-S microcontroller with 32kB of on-chip static RAM and 512 KB of on-chip flash memory. It has 128-bit wide interface/accelerator that permits 60MHz of operation. Also it has In-System Programming using on-chip boot loader software, 400ms of full chip erase and 256 B of programming in 1ms. For interfacing of sensors, it has 10-bit ADC with 8 analog inputs and a conversion time as low as 2.44µs per channel. CPU operating voltage is 3V to 3.6V so that the proposed system requires only lower power consumption as the same mentioned before. The Architecture is based on RISC principles and its simplicity yields in a high instruction throughput and real-time interrupt response form a small and cost effective processor core. It also has another architectural approach such as 16-bit Thumb instruction along with 32-bit ARM instruction set which will enhance the code density in restricted memory conditions while recurring most of the ARM's performance.

C. ZIGBEE™ Networks: ZigBee™ networks are basically based on IEEE 802.15.4standard, which specifies the MAC [33, 34] and physical layers for low rate wireless personal area networks (LR-WPAN). The schematic diagram for XBEE Pro series1 is given below in fig 4.

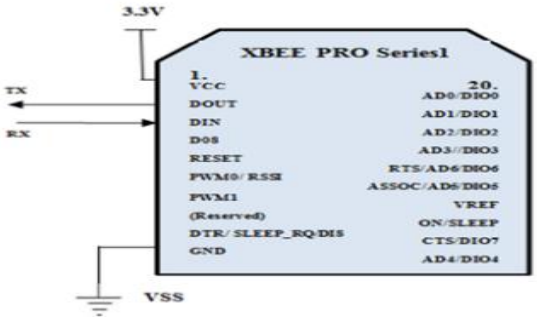

Figure 4: Schematic diagram for XBEE

D. Global system for mobile communication (GSM) : GSM is a digital mobile telephone system that is widely used in Europe and other parts of the world. GSM Time Division Multiple Access (TDMA) is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and CDMA) and operates in the 900 MHz, 1800 MHz, or 1900 MHz frequency bands.

It is composed of following information:

1. An international mobile subscriber identity (IMSI), that uniquely identifies a subscriber within GSM.
2. A secret subscriber authentication key (Ki).
3. A cryptographic algorithm A3, which provide security functions for authenticating the SIM.
4. Temporary network related data: temporary mobile subscriber identity (TMSI), Location Area Identity (LAI) and Kc.

E. The Surveyance System (Remote PC, buzzer and cameras)

The Surveyance system is basically the event monitoring and capturing system. Our Surveyance

system consists of a remote PC that is connected to a coordinator XBEE via USB Serial cable. Each sensor node (PIR) sends the regular security status reports to the coordinator which analyses them carefully. Surveillance Wireless camera receiver is connected to the PC via USB. It has a database that contains the record of all the information/images captured. Whenever an intrusion is detected by the sensors, the security status is set to 1/A (no intrusion security status is 0/N) and the data is send to the coordinator which confirms the intrusion, generates an alarm using the buzzer connected to the end device from where the intrusion report has been received and sends SMS to the owner and local police station via GSM modem. Thus, it helps in detecting as well as localizing the intruder. Also, the camera is used to capture all the pictures and videos during intrusion. This can be shown in figure 3.

IV. SIMULATION RESULTS

Figure 5 shows terminal window in which we can watch update status of sensor at monitoring section which is placed at remote area.

- Also total experimental setup shown below consists of embedded unit along with wireless camera mounted on stepper motor that rotates clockwise and anticlockwise to capture images and video when the Human had detected .
- It wirelessly transmits image/video to remote host/PC where wireless receiver grabs image.

Figure 5 .Experimental Setup

V. CONCLUSION

The use of Zigbee makes it a low cost, low power scheme which gives it an edge over the traditional schemes that use Bluetooth or Wi-Fi for communication. When there is no human in front of the PIR sensor then if he try to open any unauthorized doors or lockers it will monitored by AV camera and treated him as unauthenticated. As GSM SIM-900 module has been embedded to the system so that it messages can be send to the owner's/police mobile regarding the security status in case of intrusion.

REFERENCES

[1] A. R. Al-Ali and M. Al-Rousan, "Java-based home automation system",IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 498-504, 2004

[2] N. Sriskanthan, F. Tan and A. arande, "Bluetooth based home automation system", Microprocessors and Microsystems, Vo l. 26, no. 6, pp. 281-289, 2002

[3] H. Ardam and I. Coskun, "A remote controller for home and office appliances by telephone", IEEE Transactions on Consumer Electronics, vol. 44, no. 4, pp. 1291-1297, 1998

[4] Dr. V. Bhuvaneswari, Dr. R Porkodi, "The Internet of Things (IoT) Applications and Communication Enabling Technology Standards: An Overview", International Conference on Intelligent Computing Applications, 2014, pp. 324-329.

[5] W. He, G. Yan, and L. Xu, "Developing vehicular data cloud services in the IoT environment," IEEE Trans. Ind. Informat., vol. 10, no. 2, pp. 1587–1595, 2014.

[6] Bharani M., Elango S., Ramesh S.M., and Preetilatha R., "An Embedded System Based Monitoring System For Industries By interfacing Sensors With ATmega Microcontroller" International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 3, Issue 11, November 2014, pp. 1472-1474.

[7] GauravTiwari, RiyazKazi,"Realization of the Functions of Autonomic Smart Sensor Interface for Industrial in IOT Environment", International Journal of Advanced Research in Computer Science and Software Engineering, (IJARCSSE) Volume 5, Issue 1, January 2015, pp. 878-883.

[8] S. Pandikumar and R.S. Vetrivel," Internet of Things Based Architecture of Web and Smart Home Interface Using GSM", International Journal of Innovative Research in Science, Engineering and Technology(IJIRSET), Volume 3, Special Issue 3 , March 2014, pp. 1721-1727.

BIODATA

Author

Venkatesh Basavaraju presently pursuing his M.Tech in Embedded Systems from Sri Venkateswara College of Engineering & Technology (SVCET) ,Chittoor,Andhra Pradesh , India.

Co-Author

J.Madhan Kumar received M.Tech. Presently working as Associate Professor, in Sri Venkateswara College of Engineering & Technology, Chittoor, Andhra Pradesh, India.