International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Special Issue 31(September, 2015), PP. 84-89

DEVELOPMENT OF INDUSTRIAL INTRUSION DETECTION AND MONITORING USING INTERNET OF THINGS

P. Gokul Sai Sreeram[1], Chandra Mohan Reddy Sivappagari[2]

***Abstract*— The need for deployment of security systems rapidly increasing so as to curb illegal entry. Wildcat entry into an industry is a major problem that causes havoc situation. This paper presents development of industrial intrusion detection and monitoring system in an industry to monitor the intrusion of an unauthorized entry. This wall mounted system comprised of infrared sensor and ultra sonic sensor along with IP camera. The information collected from remote sensor nodes is sent to central monitoring station through Internet of Things (IoT) from remote node system. IR sensor along with ultra sonic sensor senses unauthorized intrusion with RFID reader which reads authorized tag, IP camera continuously records motion data through images and video. Through IoT, recorded data monitored in central station if intrusion verified through analyzing real time data an alert message is send to specified authority through SMS by GSM module attached to central system, even intruded area is alerted with a buzzer by sending acknowledge to particular IP address of remote node. This deployment provides integrity to more number of sensors, fast deployment and reduces cost. Fundamental approach is to enable high quality of service, effective and authentic data progression of data from wireless sensor networks.**

Keywords: IoT, WSN, intrusion detection, GSM module

I. INTRODUCTION

NOW a day's there are lot of increasing threats and unidentified entry are major concern for industries and large organizations. These industries protected by wired systems can be easily detached and can easily enter into premises. Those who has malicious intensions cannot be curbed as they expertise in such precautions for detaching wired systems by available cutting edge technologies. Therefore security threat arises so; intrusion detection mechanism is developed based on wireless sensor networks. The area which has to be protected is equipped with IR sensor and ultra sonic sensor they monitor the surroundings automatically. They generate alert immediately after intrusion as if unauthenticated person with no recognized RFID pass through [1], [2]. The information collected by the sensors is collectively passed to the monitoring station. This information is passed through IOT where it is monitored and reports alarm.

IoT has been emerged as most important in information and communication technology. It connects sensors, actuators and other different devices to internet to create a networked hardware for visualizing data any where [3]. IoT made easy of things by connecting to smart objects through internet connecting server systems remotely deployed through IP address of server system wirelessly and made significant changes in our daily life by interacting wirelessly to smart things [4], [5].

Various applications ranging from heath monitoring, air pollution monitoring, home automation, smart cities, and industrial security are developing through IoT. There is large scope for applications such as smart cities, smart environment, smart water, security emergencies, industrial control etc. Components of IoT include embedded devices and RFID reader, tags [6] and other authenticated components are rapidly emerging newer as to compatible to developing technologies. So, scope of doing embedded devices with IoT is maximizing.

Securing large industrial arenas through wired system now a days is quite difficult as that trespassers may cause damage to surrounding unnoticed by security. Such security issue will severely affect ongoing things in industry as this collaboration fails. In such wicked things include raw material throwing, intruder enter into premises by cutting fence etc. Conventional system have concerned flaws include if they are fenced they can be easily detached and can be intruded by intruder. There is possibility of human failure if it is monitored manually as it is difficult to monitor larger premises and sue to detecting error by human eyes can also leads to fail detection of intrusion. As the arena is larger it is impossible to monitor larger premises.

Restrictions of traditional methods can be surmounting through development of Real time intrusion detection systems which monitors arena continuously and prone to human errors. Transfer of data from affected area to central monitoring system which is transmitted by server node by this monitoring. Generation of automatic alert system and sending information of intrusion to concerned officer from server through intrusion detected at server.

Intrusion detection system is developed through using wireless sensor networks [8]. Data from server to central monitoring system is transmitted through data paths as shown in figure 1. Intrusion data detected from server is send through routers and reached to central monitoring system via hops included in system. Such systems lead to failure at node if

P. Gokul Sai Sreeram is with J.N.T.U.A College of Engineering, Pulivendula, 516390 INDIA (e-mail: saisreeram4011@gmail.com).

S. Chandra Mohan Reddy, is with J.N.T.U.A College of Engineering, Pulivendula, 516390 INDIA (e-mail: cmr.ece@jntua.ac.in).

routers are displaced and heavy procedure is adopted as many number of hardware equipments have to be embedded such as routers, node systems and central security detection system. There exist time delays as all are processed through single router. As data transmitted through dual radio communication channel intrusion is not detected if either of two networks. Even power emissions are more through transmission through RF channels through IEEE 802.15.4 ZigBee.

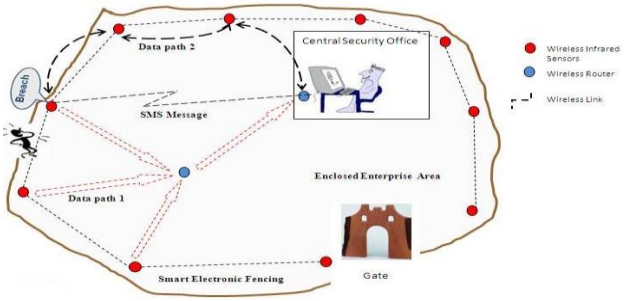

Fig 1: WSN intrusion detection system

The rest of paper is organized as Section II proposed system architecture and different sensors and RFID interfacing to arduino of proposed system is given. Section III provides system architecture more in detail and approach for IoT for proposed system. Finally section IV provides implementation and results of proposed intrusion detection in various cases and detailed approach connecting database to web interface.

II. PROPOSED INTRUSION DETECTION SYSTEM

This wireless intrusion system consists of different sensors to detect intrusion this include Infra Red sensor, Passive IR sensor, Ultra sonic sensor and RFID reader as shown in fig 2. RFID detects for authentication person detection through reading RFID tags of authorized persons who are part of industry. IP camera takes a snapshot when intrusion occurs. These are monitored by system through Aurdino board which is connected to system through cable. Overall this information is monitored in central monitoring station (client) through IoT.

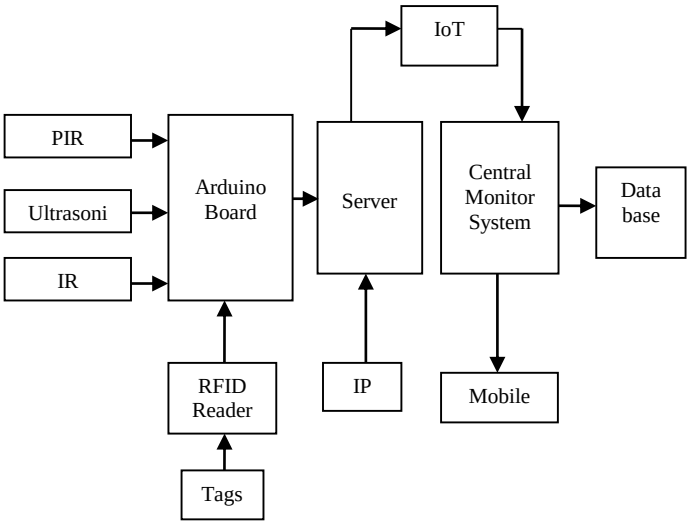

Fig 2: Block diagram of proposed intrusion detection system

A. Arduino board

Aurdino is open source development platform for building devices which can interface through the physical world. Arduino IDE operates on windows, Linux etc. Arduino IDE is done in C++, C languages and cross-platform of java performed for server architecture. This uses pulse width modulation technique to process data into microcontroller. The arduino board consists of ATmega328 microcontroller which consists of 40 pins of which 14 digital and 6 are analog.

External hardware is interfaced into its pins through digitalRead() function of particular digital pin included in 14 pins where 6 pins are PWM. It reads sensors data which is embedded and also connected to RFID reader which reads RFID tags data and process data through USB cable to the system to monitor data. The monitored data is serially processed to server through UART TTL communication port.

B. Interfacing arduino with IR sensor

Arduino board is interfaced with Infrared sensor by connecting its pins to +5v Vcc and another pin to gnd which delivers power supply to sensor through arduino and middle pin of IR sensor is connected to A1 pin of arduino ATmega microcontroller. Connected A1 pin is analog pin ATmega board so it reads only analog data and output is from pin 13. Range of IR sensor works is <10 feet. It radiates IR light when intrusion detected IR radiance is reflects back. Photo diode depicted in IR sensor senses these reflected light and different analog readings are done these are ranged between 0-1023 values according to input and corresponding readings are taken by arduino board.

C. Interfacing Arduino with PIR sensor

Passive IR sensor is interfaced to arduino board connecting power with 5v and gnd with gnd of ATmega controller. This gives power supply to PIR sensor. The central pin is given to analog pin A1 of arduino board. PIR senses radiation from intruder and reads the reading as per the Radiation received. This reading is written to arduino board through A1 pin and output through pin 13. This is read in terms of analog values where the value is further digitally analyzed by ADC converter embedded in arduino board. Normally detection range is <15 feet.

D. Interfacing Arduino with Ultra Sonic sensor

Ultra sonic sensor is interfaced to arduino board connecting first and last pin to Vcc and GND. Other pins are trigger and Echo pins. This ultrasonic module sends ultrasonic waves. If intrusion arrives waves hit it and are reflected back to board. Echo signal received and arduino measuring distance based on time of received signal. This is done by giving trigger pin and echo pin to pin 7 and 8 of arduino and trigger pin is made output and echo is made input.

E. Interfacing Arduino with RFID

RFID reader is connected to arduino by connecting 5v to 5v pin of arduino board and ground to gnd pin. It makes power supply to RFID which emits electromagnetic field. The received data is outputted serially. Both RFID tag and reader are provided with 125 KHz clock frequency. When RFID tag comes near to reader electromagnetic induction takes between coils in reader and tag and chip in tag gets activated and sends data to reader. RFID tag is in general 12 byte code. RFID reader has two possible outputs which transmit serial data to arduino. They are TTL and RS232 companionable outputs. TTL attuned is directly connected to arduino. RS232 companionable o/p is first converted to TTL using converter. Using this RFID data can be encrypted arduino through TTL.

F. Experimental Setup

The aurdino board given below in figure equipped with sensors and is mounted in wall where ever to be monitored. This sensors senses data and read them into aurdino board. Whenever RFID Tag is read by RFID reader data from sensors not considered as they are authenticated. The data from aurdino is converted in to ASCII form to be read by node system. Through IoT entire data is transmitted to central monitoring station.

G. Server Architecture

Java language is used to implement node and for serial communication library uses RxTxComm. Node performs certain functions firstly it receives and controls the functions of sensor node. Secondly it shows data collected by different sensors in sensor node and display them. Finally it process request from Client as well as smart phone application to transmit data received from sensor node and sends data to them. First two tasks are done without internet in real time as they are connected through serial cable but final task certainly require internet to process to central monitoring room which is done through standby mode. As third task affect performance of remaining tasks so that it is processed through separate thread. Node receives data and process to central monitoring system is done by cross platform of java application performed through eclipse and entire data is processed to server through full duplex i.e. even node receives commands to be performed directly by central monitoring station.

H. Client Architecture

Intrusion detection can be recognized from here as from remote node and inform authorized authorities of intrusion entry into the premises. Here firstly messages from node system are received which shows data by sensors. Thereafter from monitoring system it is detected whether unauthorized entry is done or not by seeing RFID number. If sensor data shows maximum levels without proper RFID number intrusion is detected and there by switching on IP camera embedded at node system to visualize locality whether it is human or by moisture. The images of surroundings are taken and viewed through IP camera. Finally it sends alert system to concerned officer and also sends alarm to node system in view of intrusion detected. From central monitoring room alarm is set in intruded area through IoT.

I. Flow Chart for Intrusion Detection system

The flow chart for the procedure for detection and monitoring the intrusion is shown in Fig.3.

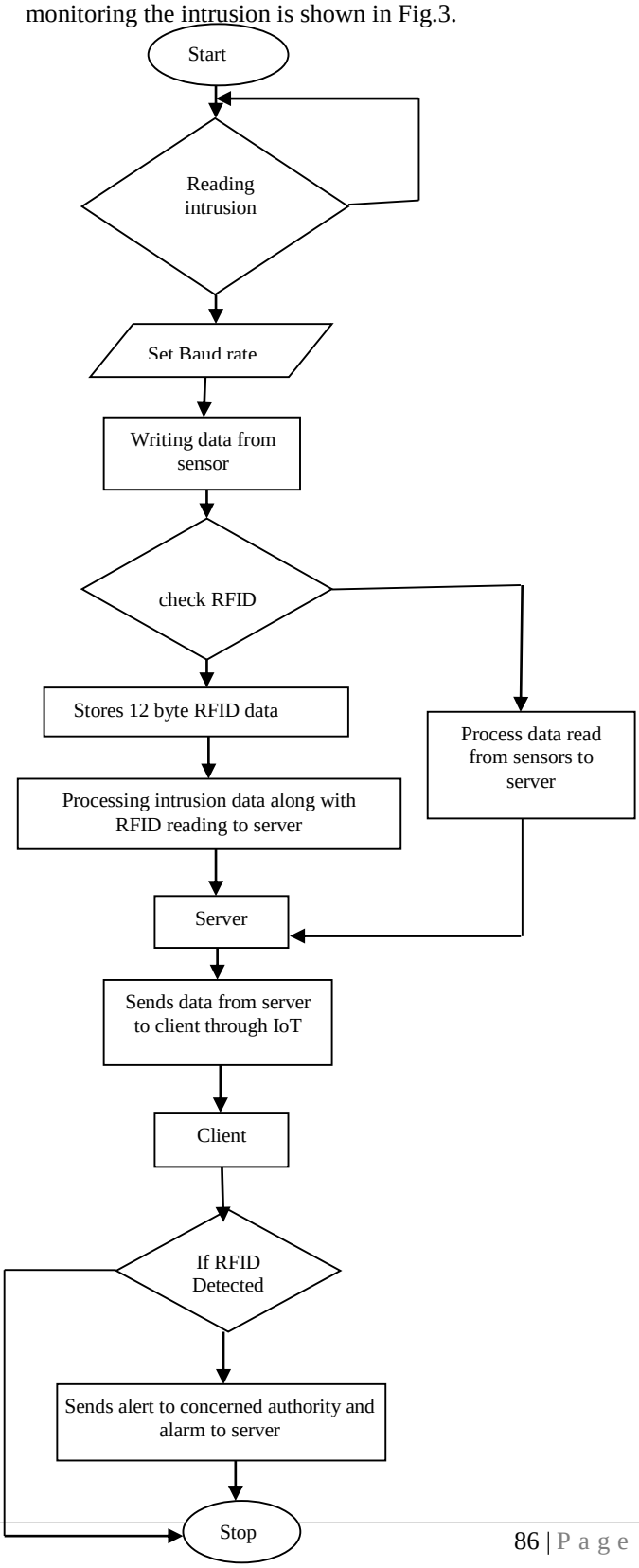

Fig 3: Flow chart of overall intrusion detected system.

III. IMPLEMENTATION AND RESULTS

This intrusion detection system includes certain stages for proposed system implementation. Node system (server) that is embedded with sensors is provided with ATMega328 for CPU. Development language used in kit is C Language and through usb2.0 information is transmitted to CPU. Node system uses java for transmission purpose and for serial communication RxTxComm.jar file is used. D-link camera is used as IP camera.

Case1: Authenticated RFID Detection

The figure 4 shows that it is node system IP is 192.168.1.143. Here the figure showed detected RFID which is authenticated so that if sensors show data even though it is as intrusion detected where it is authenticated person. The entire data is transferred to client there it checked whether intrusion is by authorized or by other.

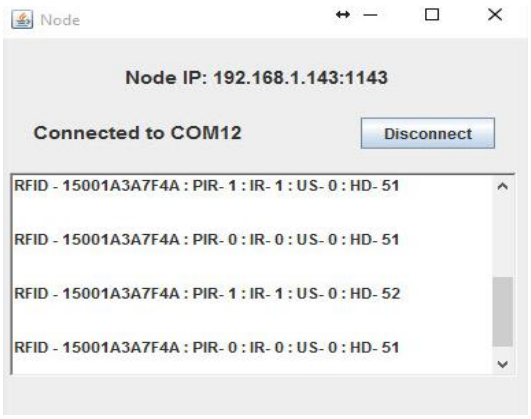

Fig 4: Server system showing for authorized RFID

The monitor system checks entire data received as shown in fig 5 and then sensor reading communicated through internet based java protocol. RFID is verified by person in central monitoring room. Detection is by authenticated person so, client system don't send any signal to higher officials of reporting about an intrusion.

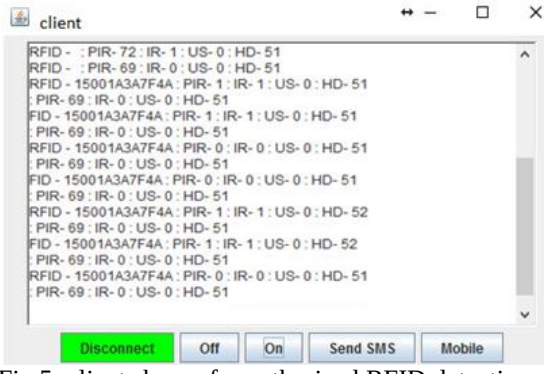

Fig 5: client shown for authorized RFID detection

Case2: Unauthorized detection

In this case RFID does not detected at server end and proceedings are done and this information is transmitted from server to client. The figure 6 shows an intrusion detected on IP 192.168.1.143. As the sensors showing some reading this is not confirmed here itself and passed on to the monitoring room for detection and this done by internet based java protocol in physical layer of TCP/IP.

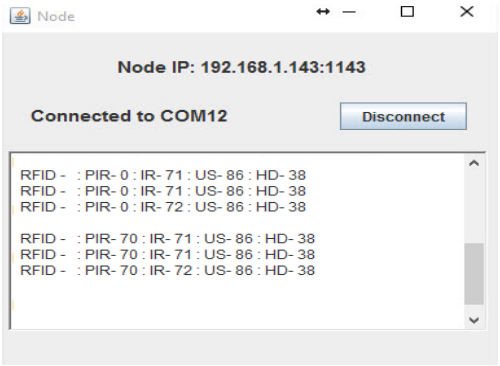

Fig 6: Server system showing intrusion detection.

Figure 7 shows intrusion detection in central monitoring room. As all sensors shows reading and there is clear indication of intrusion detected and to confirm the detection at that particular node. IP camera is used for this purpose. So IP camera is turned on from server room to detect surroundings of intruded area.

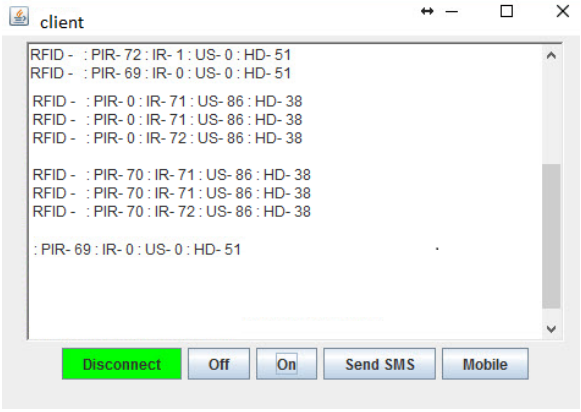

Fig 7: Intrusion detection in client room

The figure 8 confirms intrusion at node 192.168.1.143 and message is send from central monitoring room to concerned authority and this server room is also embedded with alert system such that it sends signal on to node system of IP 192.168.1.143. So that node system is alerted confirming that intrusion is detected. Alert system is executed.

Fig 8: Image by IP camera detected at server room

Message is send to officer or higher official through GSM module connected to central monitoring room and even application is developed in mobile to investigate progress of system and can be controlled from mobile application as it can send alert system to particular node directly.

From mobile node is as shown in fig 9 informed with intrusion and alert system is done by on signal and data received to node and alert system is operated.

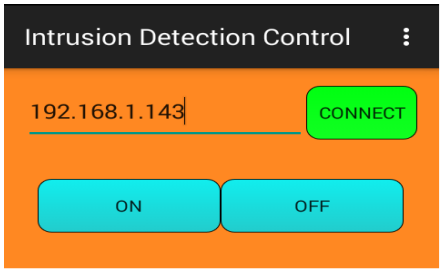

Fig 9: Mobile application for intrusion detection

The client system measures at different node so that intrusion is measured at different node and database is created as shown in fig 10 for different node entry from surroundings for detection of intrusion time and message sent to particular authority and node at which intrusion had take place.

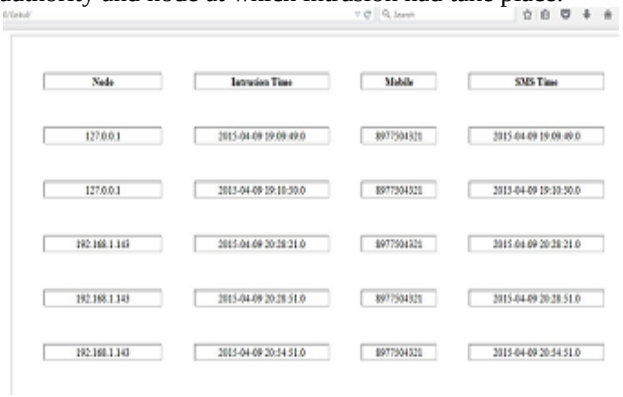

Fig 10: Database for intrusion detection system

IV. CONCLUSION

Implementation of system for intrusion system shows clear data and intrusion detection area corresponding to node system. It clearly determines intrusion time and place and extra provided alert system works better compared to traditional system as wiring. This system works on real time for intrusion detection. Sensors embedded in node system works effectively to determine intrusion and with IP Camera surroundings are measured in case of intrusion. This system further reduced complications of traditional system such as wire trenching and cutting by intruders and this system provides information at real time so by surroundings can be monitored from central monitoring room which is distantly located. As security is significant this system paves way to solve intrusion problems. Larger areas can be monitored remotely through this developed system slashing problems aroused by human monitoring. Overcoming short outs of these system innovative roots are developed in near future.

REFERENCES

[1] S. Roy, Anurag D, and S. Bandyopadhyay, "Testbed implementation of a pollution monitoring system using wireless sensor network for the protection of public spaces," International *Journal of Business Data Communications and Networking*, vol. 5,no. 4, Oct-Dec, 2009.

[2] Prashant Kharat and Jayashree Kharat, "Wireless Sensor Network: A Conceptual Framework", *International Journal of Electronics and Electrical Engineering Vol. 2, No. 2, June, 2014.*

[3] E. Welbourne, *et al.*, "Building the Internet of Things Using RFID: The RFID Ecosystem Experience," *IEEE Internet Computing* vol.13, no.3, pp.48 55, Jun. 2009.

[4] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart objects as building blocks for the Internet of things," *IEEE Internet Computing,*vol.14, no.1, pp.44-51, Feb. 2010.

[5] S. Tozlu, M. Senel, W. Mao, and A. Keshavarzian, "Wi-Fi enabled sensors for internet of things: A practical approach," *IEEE Communications Magazine,* vol.50, no.6, pp.134-143, Jun. 2012.

[6] S.-Y. Lee, L.-H. Wang, and Q. Fang, "A Low-Power RFID Integrated Circuits for Intelligent Healthcare Systems," *IEEE Transactions on Information Technology in Biomedicine,* vol.14, no.6, pp.1387-1396, Nov. 2010.

[7] S. Roy, S. Bandyopadhyay, M. Das, S. Batabyal, and S. Pal, "Real time traffic congestion detection and management using active RFID and GSM technology," presented at the 2010 International Conference on Intelligent Transport Systems Telecommunications, Kyoto, Japan, 9-11 November 2010.

[8] Sumitro Ghatak and sagar Bose "Intelligent Wall Mounted Wireless Fencing System using Wireless Sensor Actuator Network," 2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014, Coimbatore