ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 1, March 2018

6th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '18)

13th-14th March 2018

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

IOT Based Security System Based on Sensors Using Data Encryption Standard (DES)

Ragavendran.D[1], Saravanakumar.M[2], Sekar.D[3], Kushal.S[4] and Ashok kumar.M[5]

UG Scholar, Department of ECE, Adhiyamaan College of Engineering, Hosur, TN, India[1,2,3,4]

Associate Professor, Department of ECE, Adhiyamaan College of Engineering, Hosur, TN, India[5]

ABSTRACT: Security is the main concern of the world now days. Sensor based home/Industry security system are the high technology and methodical systems which connect wirelessly and ensure real time operation and indication of the threat to the house. The idea of comfortable living in home has changed since the past decade as digital, vision and wireless technologies are integrated into it. Now-a-days internet plays a major role in every area, so integrating sensors technology with an IOT environment could resolve the security issues of society to a great extent. The various drawbacks of existing technologies are cost and range. In this paper the design and implementation of sensor based security system with an IOT environment has been presented, which will resolve various security issues like unauthorized intruder entry, fire detection etc. Therefore continuous monitoring of the home/apartment is possible. The system is cost effective, reliable and has low power consumption.

KEYWORDS: PIC16F877A, Temperature Sensor, PIR sensor, Fire Sensor, IOT Module.

I. INTRODUCTION

The Internet of Things (IoT) being a promising technology of the future is expected to connect billions of devices. The increased number of communication is expected to generate mountains of data and the security of data can be a threat. The devices in the architecture are essentially smaller in size and low powered. Conventional encryption algorithms are generally computationally expensive due to their complexity and requires many rounds to encrypt, essentially wasting the constrained energy of the gadgets. Less complex algorithm, however, may compromise the desired integrity. In this paper we propose a lightweight encryption algorithm named as Data Encryption Standard (DES). It is a 64-bit block cipher and requires 64-bit key to encrypt the data.

II. PROPOSED SYSTEM

The whole system is categorized in two parts: hardware part which deals with various sensors and software part which deals with IOT (internet of things). The sensor subsystem consists of four different types of sensor used for security like fire sensor, Temperature and PIR sensor. The wireless sensor network data collecting node module is connected with PIC16F877A board. This system monitors the house/apartment, through detectors it detects accident/abnormal behavior or event when the monitored physical phenomena exceed a certain threshold. If the sensor value increased above threshold value the message will be updated in the website.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 1, March 2018

6th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '18)

13th-14th March 2018

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

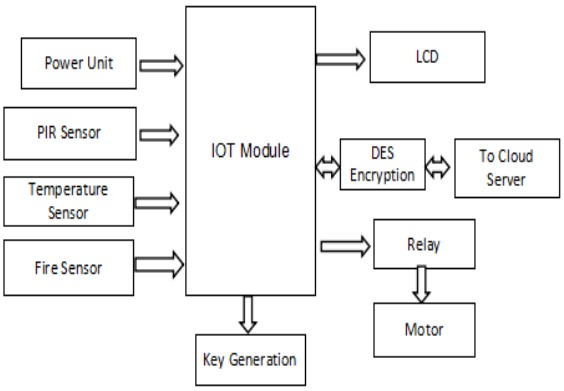

Fig 1: Block Diagram

III.COMPONENTS OF PROPOSED SYSTEM

1PIC16F877A

High-performance RISC CPU, Operating speed: DC - 20 MHz clock input DC - 200 ns instruction cycle, Up to 8K x 14 words of FLASH Program Memory, Up to 368 x 8 bytes of Data Memory (RAM) Up to 256 x 8 bytes of EEPROM data memory, Low-power, high-speed CMOS FLASH/EEPROM technology, In-Circuit Serial Programming (ICSP), Wide operating voltage range: 2.0V to 5.5V, Commercial and Industrial temperature ranges, Low-power consumption.

TEMPERATURE SENSOR

The LM35 is an integrated circuit sensor that can be used to measure temperature with an electrical output proportional to the temperature (in ^{o}C). You can measure temperature more accurately than a using a thermistor. The sensor circuitry is sealed and it should not be subject to oxidation. The LM35 generates a higher output voltage than thermocouples and may not require that the output voltage be amplified.

FIRE SENSOR

A fire sensor detector is a sensor designed to detect and respond to the presence of a flame or fire. It also can detect ordinary light source in the range of a wavelength 760nm-1100 nm. The detection distance is up to 100 cm. The Flame sensor can output digital or analog signal. It can be used as a flame alarm or in fire fighting robots.

PIR SENSOR

PIR is a PYROELECTRIC (“Passive”) INFRARED SENSOR. It is based on infrared technology, automatic control module, high sensitivity, high reliability, ultra-low-voltage operating mode, widely used in various auto-sensing electrical equipment, especially for battery-powered automatic controlled products. Clothing and accessories, goods for children, electronics, furniture, pet supplies, sport and fitness, jewelry, health and beauty, home and decor, office products and some others.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 1, March 2018

6th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '18)

13th-14th March 2018

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

RELAY WORKING

When a current flows through the coil, the resulting magnetic field attracts an armature that is mechanically linked to a moving contact. The movement either makes or breaks a connection with a fixed contact.

LCD DISPLAY

We have used 16*2 LCD Display.

IOT MODULE

Internet of Things (IoT) is an environment in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT board featured with SIM900 GPRS modem to activate internet connection also equipped with a controller to process all input UART data to GPRS based online data. Data may be updated to a specific site or a social network by which the user can able to access the data.

IOT SECTION

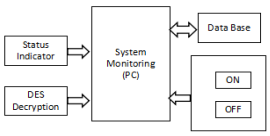

Fig 2: Block Diagram

IV. WORKING

In this project we have used network Security is one of the important concepts in data security as the data to be uploaded should be made secure. To make data secure, there exist number of algorithms like AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm) etc. These techniques of making the data secure come under Cryptography. Involving internet of Things (IoT) in Cryptography is an emerging domain. IoT can be defined as controlling things located at any part of the world via Internet. So, IoT involves data security i.e. Cryptography. Here, in this project we discuss how data can be made secure for IoT using Data Encryption Standard (DES).

ADVANTAGES

The advantages of this system are Secure data transmission, involving IoT, low cost, to control at any part of the world via internet.

V. RESULT

The increased number of communication is expected to generate mountains of data and the security of data can be a threat.The system we designed is categorized in two parts: hardware part which deals with various sensors and software part which deals with IOT (internet of things). The main process that we undergo in order to get the result is the agents that are placed to transmit the data to the server will be a secured in terms of transmission of data by encrypting the data which Is to be transmitted to the server and the data will be decrypted when it gets transmitted and in case if any hazard situation takes place in the environment of the agents location the output activities will be

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 1, March 2018

6th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '18)

13th-14th March 2018

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

done depending on the type of agents and machanism installed in the location. Presenting the message received from the agents after decrypting and taking the required action based on the received data.

VI. CONCLUSION

This paper tells about the design and implementation of Internet of Things connects heterogeneous devices together through the medium of internet in order to exchange important information. IoT has made human life simpler and comfortable by gradually changing technologies and applications as per peoples' standards. Medical, governance, education, industry, production, transportation etc. fields are using IoT at its best. Various challenges of IoT restrict the growth and progress. Security and Privacy are the biggest challenges against the IoT in the recent era. Security concerns sometimes confuse user whether to use IoT or not. Existing security framework supports and restricts security attacks and flaws in IoT at certain extent. Few important improvements like; monitoring of security threats from the initial points, Authentication of alleged devices, Identification of unauthorized devices, Some security provision planning, etc. are extremely needed to make IoT secure and reliable

REFERENCES

[1] BG. Kortuem, F. Kawsar, V. Sundramoorthy, and D. Fitton, "Smart objects as building blocks for the internet of things," IEEE Internet Computing, vol. 14, no. 1, pp. 44–51, 2010.
[2] R. Yang and M. W. Newman, "Learning from a learning thermostat: Lessons for intelligent systems for the home," in Proceedings of the 2013 AC International Joint Conference on Pervasive and Ubiquitous Computing, ser. UbiComp '13. New York, NY, USA: ACM, 2013, pp. 93–102.
[3] R. Li, T. Song, N. Capurso, J. Yu, and X. Cheng, "Iot applications on secure smart shopping," in to appear in International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI) 2016, 2016.