Smart Security System in Homes using Simple Internet of Things Enabler

P.Anitha [1], A.Jayakumar[2]

[1]UG Scholar, Department of ECE, IFET College of Engineering, Villupuram
[2]Associate Professor, Department of ECE, IFET College of Engineering, Villupuram.

---***---

ABSTRACT: *This paper explains various security issues in the existing home automation systems and proposes the use of logic based security algorithms to improve home security. The work classifies natural access points to a home as primary and secondary access points depending on their use. Logic based sensing is implemented by identifying normal user behavior at these access points and requesting user verification when necessary. User position is also considered when various access points changed states. Moreover, the algorithm also verifies the legitimacy of a fire alarm by measuring the change in temperature, humidity and carbon monoxide levels, thus defending against manipulative attackers. The experiment conducted in this paper used a combination of sensors, microcontrollers communication to identify user behavior at various access points and implement the logical sensing algorithm . The proposed logical sensing algorithm was successfully implemented for a month in a studio apartment. During the course of the experiment the algorithm was able to detect all the state changes of the primary and secondary access points and also successfully verified user identity 55 times generating 14 warnings and 5 alarms.*

1. INTRODUCTION

Researchers have been experimenting and improving the concept of smart home since the late 1970s. As technology advanced with time, electronic devices and internet became more popular and affordable, so the concept of home automation and people‟s expectation from a smart home has changed dramatically[1]. Modern smart home is a sophisticated combination of various Ubiquitous Computing Devices and Wireless Sensor/Actor Networks . All these new user expectations, complicated electronics and unpredictable user behavior brought new security challenges to the home automation front[2]. The concept of home automation security has also evolved with time, sensors and actuators were integrated into the home to detect, alert and prevent intrusions. In the past, an average home had to deal with common slash and grab criminals, while a modern home has to deal with sophisticated and tech savvy attackers who know how to find vulnerabilities and manipulate the security devices to gain access or cause distress to the inhabitants[3].This is extremely challenging and complex, given the unpredictable nature of human behavior and home being occupied by guests and other trusted people. Identifying access points to a home and regulating access to them is the next logical step towards securing a home[4]. This paper proposes that, normal user behavior at access points to a home adhere to a set of predictable behaviors.

2.LITERATURE SURVEY

Design and implementation of intelligent home control systems based on active sensor networks.

The ubiquitous home network has gained wide-spread attentions due to its seamless integration into everyday life. This innovative system transparently unifies various home appliances, smart sensors/actuators and wireless communication technologies. The ubiquitous home network gradually forms a complex system to process various tasks. Developing this trend, we suggest a new intelligent home control system based on a wireless sensor/actuator network (we call it as an "Active sensor network"). The proposed intelligent home control system divides and assigns various home network tasks to appropriate components. It can integrate diversified physical sensing information and control various consumer home devices, with the support of active sensor networks having both sensor and actuator components. We develop a new routing protocol LQIR (Link Quality Indicator based Routing) to improve the performance of our active sensor networks. This paper introduces the proposed home control system's design that provides intelligent services for users. We demonstrate its implementation using a real test bed.

3. EXISTING SYSTEM

The existing design of home security systems typically monitors only the property and lacks physical control aspects of house itself. Also the term security is not well ensured and undefined because there is a time delay between alarm system going on and actual arrival of security personnel. No ways to detect un-even condition in industry. Manual intervention required for monitoring. CCTV used which only monitor but no Alert generation. Alert and their appropriate actions not present manually. Time consuming approach to detect and generate Alert Manually.

4. PROPOSED SYSTEM

Every user who is experienced in the existing system may think of a system that may add more flexibility and run with some common applications such as android. This work is designed in such a way to avoid the disadvantages of the existing system. The proposed system supports more elasticity, comfort capacity and safety.The main objectives is to design and to execute an cost effective and open source home automation system that's capable of leading most of the home and sustain the house automation system. The predictable system contains a great elasticity by using wireless reliable technology to interconnecting various modules to the server of home automation system. This in turn reduces the deployment cost; will add to the flexibility of advancement, and system reconfiguration..

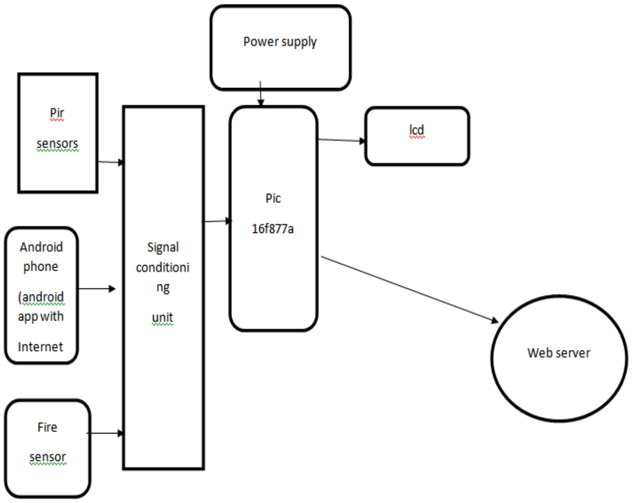
Power supply
Pir sensors
lcd
Pic 16f877a
Android phone (android app with Internet
Signal conditioni ng unit
Web server
Fire sensor

Fig: 5. Block Diagram

The projected system can make use of wireless LAN(Local space Network) connections between various sensor, hardware modules and server, and various communication protocols between users and server. The Infrared sensor (IR) is a low cost infrared object detection unit that we can be applied at home using IR LED's. It gets trigged when light is detected. When the sensor is sensed it sends a signal to microcontroller. creating web server in personal computer, tablet or we can create an app in mobile

5.1 PRINCIPLE OF PIR FUNCTION

A passive infrared sensor (PIR sensor) is an electronic sensor that measures infrared (IR) radiation being emitted from objects in its field of view. They are most often used in PIR-based motion detectors.

Fig:5.1. Pir Sensor

5.2 LCD DISPLAY

Liquid Crystal Display is the material, which have the molecular structure and flows like a liquid. LCD module is a low power device. Properties of the molecular structure are associated with the solid structure. The power requirement for LCD is in the order of microwatts. LCD's are subjected to chemical degradation, so it is operated at the temperature range from 0 to 60 degree Celsius and the lifetime is short. Classification of LCD:

1.Dynamic-scattering LCDs
2.Field-effect LCDs

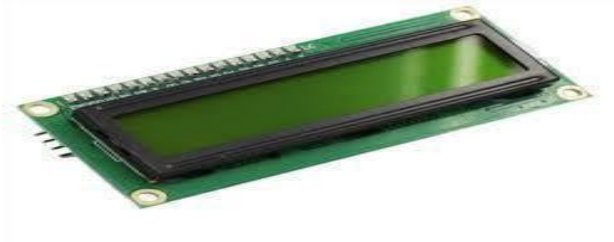

Fig:5.2. 16×2 LCD Display

5.3. MQ6 GAS

Toxic and harmful gases like methane, carbon monoxide may be present in the surfaces of underground coal mines. During working hour, due digging or blasting of coal, methane or other harmful gas can explode and cause dangerous accidents. It is difficult to stop the emission of such harmful gases, but we can save the lives of coal worker by evacuating them, if such accidents occur. So it is important to detect these gases during digging of coal. Different sensors like MQ4, MQ5, TGS2611 etc. can be used to detect methane in underground coal mines.

Fig :7.5.1. MQ-4 Sensor and MQ-4 Module

5.4. TEMPERATURE SENSOR

Suitable temperature is one of the most important condition inside underground mines. It is important for coal mine worker to have proper temperature to work safely and effectively inside the mines. During working hour due to drilling or blasting inside mines, new surfaces are get opened up which may cause increase or decrease in temperature, so it is very much important to monitor temperature inside the mines. Lots of technologies have been developed for temperature measurement .Thermocouple, RTD, Thermistor, LM series sensors etc. Can be used to measure the temperature changes inside the mines.

5.5 MICROCONTROLLER

A microcontroller is an integrated circuit or a chip with a processor and other support devices like program memory, data memory, I/O ports, serial communication interface etc. integrated together. Unlike a microprocessor (ex: Intel 8051), a microcontroller does not require any external interfacing of support devices. Microcontroller differs from a microprocessor in many ways. First and the most important is its functionality. In order for a microprocessor to be used, other components such as memory, or components for receiving and sending data must be added to it. In short that microprocessor is the very heart of the computer. On the other hand, microcontroller is designed to be all of that in one.

6. CONCLUSION:

Nowadays, a real demand to make homes smarter in order to face challenges - i.e., waste management, traffic congestion, etc. - caused by the population growth. In this context, one key role is played by the Internet of Things and its data streams that can be converted into relevant information used to address the above issues. According with this vision, the number of Iota solutions is, nowadays, increasing, but on the other hand those initiatives are standalone and based on different protocols and standards. This paper deals with this problematic issues, by introducing an abstract virtualized layer that operates across multiple Iota architectures and platforms. This layer represents the end-point services by which it is possible to monitor, visualize, and control all the operations.

REFERENCES

[1] C. Suh and Y.-B. Ko, “Design and implementation of intelligent home control systems based on active sensor networks,” IEEE Transactions on Consumer Electronics, vol. 54, no. 3, pp. 1177–1184, 2008.

[2] B. Fouladi, S. Ghanoun, “Security Evaluation of the Z-Wave Wireless Protocol,” Black hat USA, Aug. 2013.

[3] Wenye Wang, Zhuo Lu, “Cyber security in the Smart Grid: Survey and challenges,” Computer Networks, Volume 57, Issue 5, Pages 1344-1371, April 2013.

[4] N. Komninos, E. Philippou and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," in IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1933-1954, Fourthquarter 2014.

[5] C. Karlof, D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures”, Ad Hoc Networks, vol. 1, pp. 293–315, 2003.

[6] Y. Hu, A. Perrig, D. Johnson, “Wormhole attacks in wireless networks”, IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 370–380, Feb. 2006.

[7] Y. Mo and B. Sinopoli, "Secure control against replay attacks," 2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, pp. 911-918, 2009.

[8] D. Deadman, “Forecasting residential burglary,” International Journal of Forecasting, vol. 19, no. 4, pp. 567–578, 2003.

[9] UNODC, “International Burglary, Car Theft and Housebreaking Statistics,” United Nations Office on Drugs and Crime (UNODC), Technical Report, 2015.

[10] A.C Jose, R. Malekian, N. Ye, "Improving Home Automation Security; Integrating Device Fingerprinting Into Smart Home", IEEE Access, vol. 4, October 2016.

[11] A.C Jose, R. Malekian, “Smart Home Automation Security: A Literature Review”, Smart Computing Review, Vol. 5, No. 4, pp. 269-285, August 31, 2015.

[12] Jonghwa Choi, Dongkyoo Shin and Dongil Shin, "Research and implementation of the context-aware middleware for controlling home appliances," IEEE Transactions on Consumer Electronics, vol. 51, no. 1, pp. 301-306, Feb. 2005.

[13] British Broadcasting Corporation (BBC) - Andrew Silke, "Webcams taken over by hackers, charity warns", [Online]. Available: http://www.bbc.com/news/uk-22967622