SURE-H:A Secure IoT Enabled Smart Home System

Prem Brat Kumar[1], Avinash Kumar[2]
[1]Dept of Computer Science and Engineering
[2]Assistant Professor, Dept of Computer Science and Engineering
[1, 2] Atria Institute of Technology

Abstract- *In today Era IOT enable Smart home systems achieved great popularity in the last decades as they increase the comfort of life. Most smart home systems are controlled by android smartphones and microcontrollers. The demand for smart things is increasing day by day. The IoT (Internet of Things) is one of the major components that provides facility to digitalized the world with the help of various sensor and by using internet. In this work, we are going to develop smart home system that enable to protect our homes from theft or unwanted activities and parallelly saves power. Our thesis is based on exploiting the features of IoT that facilitates us to digitalized home to the smart home so that we can take care of our home from anywhere over the Internet when data are stored in the cloud.*

Keywords- IoT,Smart Home,Android smart phone, Home automation, Motion sensor.

I. INTRODUCTION

In today Era IoT structure has increased rapidly. By the same time, problems arise regarding burglary or theft anything from small home to the huge industries. Regular monitoring of people's habit, activities are required for the protection and management of the useful data in this work, we present an advanced IoT enabled smart house system that advanced the securities from theft and parallelly saves enormous power. It will use an Android application which provides multiple switching functionalities, where the electrical or electronic devices are monitored and controlled remotely to keep safe, the fire alarm and suppression system needs to be carefully managed, as do the door and physical security alarm systems With the uses of Internet, the demand for IoT structure has increased rapidly.[1] By the same time, problems arise regarding burglary or theft anything from small home to the huge industries. Regular monitoring of people's habit, activities are required for the protection and management of the useful data. The function of a building is to provide a work environment that keeps the efficient, and safe. Work areas need to be well little and kept at a moderate temperature. To keep workers safe, the fire alarm system and suppression system needs to be very carefully managed, as do the door and physical security alarm systems. While IoT enable systems for modern buildings are being deployed and improved for each of these functions, most of these systems currently run independently through each other and they rarely take into account. However, many buildings are beginning to locate sensors throughout the building to detect the condition. Motion sensors work great if everyone is moving around in a crowded room and can automatically shut the lights off when everyone has left, but what if a person in the room is out of sight of the sensor? It is a frustrating matter to be at the mercy of an unintelligent sensor on the wall that wants to turn off the lights on you. Similarly, sensors are often used to control the heating, ventilation, and air-conditioning (HVAC) system. Temperature sensors are spread throughout the building and they are used to influence the building management system's control of air flow into a room. In this work, we present an advanced IoT-enabled smart house system that advanced the securities from theft parallelly saves enormous power. It will use an Android application which provides multiple switching functionalities, where the electrical or electronic devices are monitored and controlled remotely. This system adds advantage by eliminating the use of traditional personal computers (PC) and its peripheral devices during execution.

II. LITERATURE SURVEY

A smart home refers to a convenient home setup where appliances and devices can be automatically controlled remotely from anywhere with an internet connection using a mobile or other networked device. Devices in a smart home are interconnected through the internet, allowing the user to control functions such as security access to the home, temperature, lighting, and a home theater remotely [1].

N. Sriskanthan [6] has implemented the Bluetooth model for home automation via PC. But Bluetooth has range limitation. Because of Bluetooth, U-V rays get extracted which harms the public life. Nowadays we have to check SAR value of the devices. But in this paper, he has not said anything about SAR-value.

Back in the 1980s, Japan, US and Europe have taken the ambition to develop more advanced home automation systems. The term home automation system was first used by the[4] Japanese companies like Hitachi and Matsushita who showed the interest in IoT enable home automation system. It

is comprised of major manufacturer companies and provided supports for the hardware and software required for the home automation system.[5]

Hasan [7] has developed a telephone and PIC remote-controlled device for controlling the devices. Pin check algorithm was used to implement the system where it was with cable network but not wireless communication. In cable network Speeds are slower than those you receive with wireless Internet, and the connection speed you receive often depends on how many people in your area are connected to the Internet at once. Using above model, we can't be able to monitor our home from outside the city. Remotely monitoring is not possible using this system.

Amul Jadhav [8] had used universal XML format to design automation system which can be easily ported to any other smart devices. The redundancy in syntax of **XML** causes higher storage and transportation cost when the volume of data is large. Embedded C is the best language used to do such operation. Using above method, we cannot get the proper security as it can easily be ported to any other mobile devices.

III. THE PROPOSED SYSTEM

To design SURE-H system, initially, the sensors are configured and attached to the ESP8266-12E module. This module is capable to accept instruction through an interfacing port. The ESP8266-12E module of the relay board is programmed with Arduino and then it is configured to receive and process a specific command transmitted over the Internet from user. The cloud server is configured based on a cloud service provider known as Blynk. Blynk provides end-to-end solution for IoT based application development. Finally, we design a smartphone app and connected with the ESP8266-12E module through a cloud service provider over the Internet.

The proposed automated smart home system consists of three main modules such as (i) the cloud server, (ii) the hardware interface module, and (iii) the software package or smartphone application.

Figure 1 shows the prototype model of the proposed system. User uses the Internet to login into the cloud server and control the home automation system. Low voltage switching relays are used to integrate devices with the ESP8266-12E [2] module for demonstrating the switching functionality. If server is connected to the Internet then remote users can access server using web-based application over the Internet.

SURE-H come up with following features.
i   automated switches for all home appliances capable to detect moving object
ii   generate password by combining user password and fingerprint

The SURE-H system works based on the stored cloud server data. We store the details of home appliances for each room into the server. Initially, it sends a request to the server and wait for the approval. As soon as it observes any motion object detect it sends an alarm with detail report against the incident. This alarm will trigger only when the new object observes. Figure 2 shows the flow of data of the SURE-H system.

IV. PROTOTYPE

In this section, we present Parameter estimation is really necessary to fit the system in real-time environment.
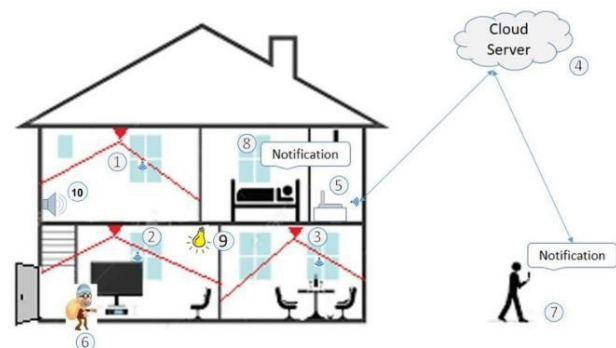
1.   Motion detector sensor
2.   Motion detector sensor
3.   Motion detector sensor
4.   Blynk cloud server
5.   Wi-Fi Internet gateway
6.   Thief
7.   User 1 getting notification
8.   User 2 getting notification
9.   Lights automatically turns on detection of the thief
10. An alarm is also raised on detection of the thief

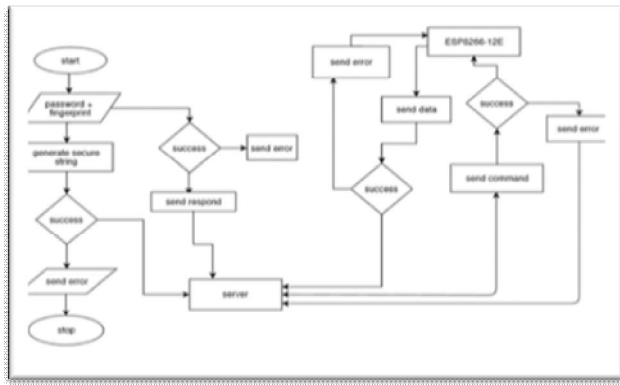Fig. 1. SURE-H: a prototype model of autonomous smart home system

Fig. 2. SURE-H: a dataflow diagram

Setup

To evaluate a system in real-time, it is really important to deploy the system in real environment. We setup and deploy modules in 30 different rooms for 60 days to observe the efficiency, which is designed based on an approximation model of power consumption for each room. During the period, we measure the efficiency of detection theft and power cost per room after each five alternative days. To estimate the total cost, we compute (i) the total hours consumes the power,t_h = (consumed time in seconds=60 seconds) (24 hours=day), (ii) the total hours in a months, t_m = (t_h number of days), (iii) the total watts consumed,t_w= t_m % of total watts bulbs or devices deployed.

the total cost, T_c = t_w rate per unit. SURE-H system follows two major steps to accomplish this task.

Step 1: Setting up ESP8266-12E relay board

After getting ESP8266-12E board, we write instructions that passes through Arduino. After that required relay board was connected to the GPIO pins and power cable with 220v-240v AC connection. The various home appliances are connected to the State Relay (SSR) switches. The AC is converted to DC with the help of AC to DC converter to pass current to the board.

Step 2: Operating ESP8266-12E with smartphone ESP8266-12E is attached with Internet through Wi-Fi or any other connectivity so that it can be accessed through cloud server. Through Arduino IDE ESP8266-12E, it is programmed and works in stand-alone mode. An Android or iOS application is installed in the user's smartphone which can connect to the same cloud server through either IP address of the server or domain name. Moreover, user should provide the password and fingerprint to login to the server. Finally, the user can monitor their home or office remotely from anywhere and anytime with low cost and save power consumption.

B. Results and discussion

The Arduino script monitors the difference in IR (infrared) signal of the motion sensor, if there is any interference in IR signals then the motion flag is set, triggering the buzzer and switching on the light. When the motion is detected, sensor data will trigger out and it will send a notification to Android or iOS application installed in the user's smartphone and connected email account. It will then report any intrusion inside the surveillance area and make the user aware of the situation in every 5 second. Figure 3 demonstrates the app activity for a single room.

The smart home system was fully functional and the user interface is updated to reflect the current status when the appliances are switched on. The SURE-H system is tested

VI. SYSTEM ARCHITECTURE
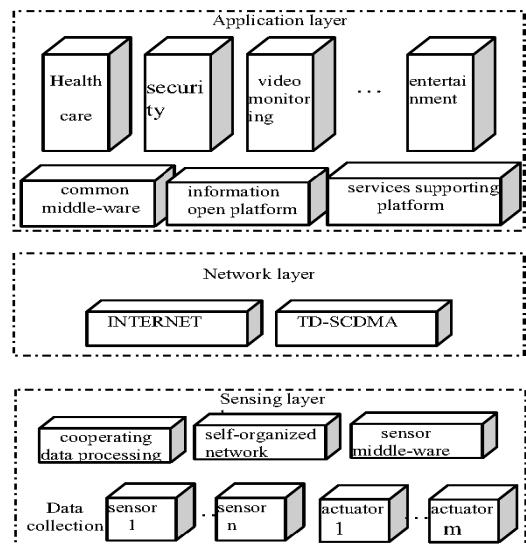
The protocol comprises of three layers, where in the sensing layer performs the operations of co- operating data processing enabling self-organized Network and sensor middleware to perform specific activities. The data assembly is done by the aid of sensors and actuators. The network layer embraces internet which is basically a global computer network used for communications of sensors present in the application over the human beings as a bridge. TD-CDMA a telephone standard for wireless network operators who want to make headway from 2G to 3G or 4G. The application layer incorporates common middleware and open platform for information coverage and service supporting platform to encompass venture of healthcare applications, video monitoring, security and entertainment.

VII. CONCLUSION AND FUTURE WORKS

This paper gives basic idea how we can advance home appliances by computer technology using Internet. The main objective of this project is to help people to control their home remotely. It reduced the human effort for security basic and makes of life easier and comfortable in the way that we can do our daily work without and pressure and tension of home security. It provides security and saves energy. As we are accessing devices by website, we can access it even if we are far away from home where the Wi-Fi is available. We can monitor our home from anywhere we want. It will be controlled remotely based on user authorization. This system has been designed in such a way that it can fulfill the needs of the user that reduces manual effort, save power and need security. Any android device can be used to monitor the smart home to detect any unusual act. It has several features include low cost, minimum time, highly scalable, and needs minimum infrastructures.

SURE-H can be extended to the large-scale environment such as offices and companies. It can also add additional features such incorporating camera, call alerts and live video streaming for future reference and analysis.

VIII. ACKNOWLEDGEMENT

REFERENCE

[1] D. Choi, S. Seo, Y. Oh, and Y. Kang, "Two-Factor Fuzzy Commitment for Unmanned IoT Devices Security," IEEE Internet of Things Journal,vol. 6, no. 1, pp. 335–348, Feb 2019.

[2] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, Network Traffic Anomaly Detection and Prevention – Concept Techniques, and Tools, 1st ed., ser. Compute Communications and Networks Series. Springer International Germany, 2017.

[3] R. Petrolo, V. Loscri, and N. Mitton, "Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms," Trans. Emerg. Telecommun. Technol., vol. 28, no. 1, pp. 1–12, 2015.

[4] M. Kumar and R. Singh, "Home appliance controlling using zigbee on atmega128 hardware platform," International Journal of Research in Engineering and Technology, vol. 3, no. 7, pp. 469–472, 2014

[5] C. Jose and R. Malekian, "Smart home automation security: A literature review," Smart Computing Review, vol. 5, no. 4, pp. 269–285,2015.

[6] N. Sriskanthan and Tan Karand. "Bluetooth Based Home Automation System". Journal of Microprocessors and Microsystems, Vol. 26, pp.281-289, 2002

[7] E. Yavuz, B. Hasan, I. Serkan and K. Duygu. "Safe and Secure PIC Based Remote Control Application for Intelligent Home". International Journal of Computer Science and Network Security, Vol. 7, No. 5, May 2007.