ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 8, August 2019

IoT and Finger Print Based Home Security Monitoring and Controlling System

Jaya Dewangan, Ajay Kushwaha

M. Tech Student, CSE, RCET, Bhilai, India

Associate Professor, CSE, RCET, Bhilai, India

ABSTRACT: One of the prominent application segments of Internet of Things framework is in the Security Sector. It is important to arrive at a unique low cost solution to prevent theft and ensure security to members of the home. The Internet of Things (IoT) Layered Architecture based design approach assists the system designer to conveniently differentiate the system component requirements distinctly at various layers. This paper highlights the model driven development process for Home Security System. It remarks the uses of customers end application such as Telegram to securely transmit information through layers of IoT architecture. This paper aims at providing a low-power, cost effective and unobtrusive IoT based home security system which assists in presence detection, identification and authentication of stranger. The proposed solution makes use of finger print sensor as capturing unit, Electric Door Strike as an actuator and arduino with ESP8266 as IoT infrastructure.

KEYWORDS: Internet of Things, Arduino, Home Security, Electric Door Strike, Doorbell.

I. INTRODUCTION

Along with the growth of the smart phone, a large number of embedded devices have been developed to provide various services. Especially, the smart home, smart city, smart health care and smart card services have been receiving the spotlight throughout the society in recent years. For this reason, various sensors, small embedded devices and home appliances have been studied and developed continuously through several companies, universities and research institutions. And then they have been gradually intellectualized in order to provide smart services to the users.

However, an increment phenomenon of user privacy data leakage and security vulnerability should not be overlooked in the IoT (Internet of Things) environment. A number of significant research needs, including security and privacy, for future IoT systems is described in and the general definitions for the main security aspects within the IoT domain. If the service infrastructure is designed without considering predictable security flaws, user privacy data leakage, social infrastructure paralysis, and economic losses as well as a risk of human life as severe cases can be occurred by the attacks of outsiders with malicious purpose.

To establish the service infrastructure that provides security features, it is necessary to define the appropriate security features required for each component that make up the service infrastructure. In addition, various services require a different security issue that is suitable for individual characteristics.

For example, data (e.g. user's privacy data) security is essential to the intelligent transportation service and intelligent medical service, while authentication scheme is more important in the case of smart city and intelligent farm services. Therefore, we should carefully scrutinize the security requirements and necessity for a specific IoT services.

In this paper we define the security requirements for the smart home service which is emerged as a hot item of major IT companies, and specifically describes a security feature for each component of smart home system in the IoT environment.

The rest of this paper is organized as follows. In Section II, we give some overview of the smart home system. Section III describes the security requirements of the smart home service. Section IV addresses the security functions for the components (smart home device, home gateway, and home server) that make up the smart home system. Finally, Section V concludes this paper with a summary and future works.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 8, August 2019

Bluetooth based home automation system using cell phones:
In Bluetooth based home automation system the home appliances are connected to the Arduino BT board at input output ports using relay. The program of Arduino BT board is based on high level interactive C language of microcontrollers; the connection is made via Bluetooth. The password protection is provided so only authorized user is allowed to access the appliances. The Bluetooth connection is established between Arduino BT board and phone for wireless communication. In this system the python script is used and it can install on any of the OS environment, it is portable. One circuit is designed and implemented for receiving the feedback from the phone, which indicate the status of the device.

Zigbee based home automation system using cell phones:
To monitor and control the home appliances the system is designed and implemented using Zigbee. The device performance is record and store by network coordinators.
For this the Wi-Fi network is used, which uses the four switch port standard wireless ADSL modern router. The network SSID and security Wi-Fi parameter are preconfigured. The message for security purpose first process by the virtual home algorithm and when it is declared safe it is re-encrypted and forward to the real network device of the home. Over Zigbee network, Zigbee controller sent messages to the end. The safety and security of all messages that are received by the virtual home algorithm. To reduce the expense of the system and the intrusiveness of respective installation of the system Zigbee communication is helpful.

GSM based home automation system using cell phones:
Because of the mobile phone and GSM technology, the GSM based home automation is lure to research. The SMS based home automation, GPRS based home automation and dual tone multi frequency (DTMF) based home automation, these options we considered mainly for communication in GSM.

In figure shows the logical diagram the work of A. It shows how the home sensors and devices interact with the home network and communicates through GSM and SIM (subscriber identity module). The system use transducer which convert machine function into electrical signals which goes into microcontroller. The sensors of system convert the physical qualities like sound, temperature and humidity into some other quantity like voltage. The microcontroller analysis all signal and convert them into command to understand by GSM module. Select appropriate communication method among SMS, GPRS and DTFC based on the command which received GSM module.

Wi-Fi based home automation system using cell phones:
Wi-Fi based home automation system mainly consist three modules, the server, the hardware interface module, and the software package. The figure shows the system model layout. Wi-Fi technology is used by server, and hardware Interface module to communicate with each other. The same technology uses to login to the server web based application. The server is connected to the internet, so remote users can access server web based application through the internet using compatible web browser. Software of the latest home automation system is split to server application software, and Microcontroller (Arduino) firmware. The Arduino software, built using C language, using IDE comes with the microcontroller itself. Arduino software is culpable for gathering events from connected sensors, then applies action to actuators and pre- programmed in the server. Another job is to report the and record the history in the server DB. The server application software package for the proposed home automation system is a web based application built using asp.net. The server application software can be accessed from internal network or from internet if the server has real IP on the internet using any internet navigator supports asp.net technology. Server application software is culpable of, maintain the whole home automation system, setup, configuration. Server use database to keep log of home automation system components, we choose to use XML files to save system log.

Home automation using RF module:
The important goal of Home Automation System is to build a home automation system using a RF controlled remote. Now technology is accelerating so homes are also getting smarter. Modern homes are deliberately relocating from current l switches to centralized control system, containing RF controlled switches. Today traditional wall switches situated in various parts of the home makes it laborious t for the end user to go near them to control and operate. Even further it turns into more problematic for the old persons or physically handicapped people to do so. Home

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 8, August 2019

Automation using remote implements an easier solution with RF technology.
In order to accomplish this, a RF remote is combined to the microcontroller on transmitter side that sends ON/OFF signals to the receiver where devices are connected. By operating the stated remote switch on the transmitter, the loads can be turned ON/OFF globally using wireless technology.

Home automation using Android ADK:
The devices of home are associated to the ADK and the Connection is established between the Android device and ADK. The devices of house are link to the input/output
Ports of the board (EMBEDDED SYSTEM) and their current situation will have passed to the ADK. The microcontroller board (Arduino ADK) is based on the ATmega2560. It has a USB host connection to associate with Android based phones, and that is based on the MAX3421e IC. The two important features of Android Open Accessory Protocol 2.0(AOAP) are as follows:
It has audio output that is from the Android device to the component and it also support for the component serves as one or more Human Interface Devices (HID) to the Android device. This paper depends upon Android and Arduino platform in which both are FOSS(Free Open Source Software). Including motion sensors for safety systems will detect an unauthorized action and it will automatically notice the user through cell phone or the security system.

Cloud Based home automation system:
Home Automation using cloud based system focuses on design and implementation of home gateway to collect data about data from home appliances and then send to the cloud-based data server to get store on Hadoop Distributed File System, it is process using Map Reduce and use to implement a monitoring tasks to Remote user Presently home Automation System is persistently developing its resilience by assimilating the current characteristics which gratify the rising interest of the people. This paper presents the design and development of home automation system that use the cloud computing as service. The current system consists of three important units: the first part is cloud server, handle and controls the data and information of client and users and the status of devices the hardware interface module is the second part which implement the relevant connection to the actuators and sensing devices which give the physical service. Last part is Home Server, which construct the hardware device and gives the user interface. This paper focus to build the web services using cloud which is need for security and storage and availability of the data. The current system is cost efficient, reliable and comfortable which also gives a secured home automation system for entire family.

Raspberry pi home automation with wireless sensors using smart phone
Home Automation System has been developed with Raspberry Pi by reading the algorithm and subject of E- mail. Raspberry Pi guarantees to be an efficient platform for implementation powerful, and economic smart home automation. Home automation using Raspberry pi is better than any other home automation methods in several ways. For example, DTMF (dual tone multi-frequency) using home automation, the call tariff is a big demerit, which is not the problem in their proposed method. In Home Automation using web server, the design of web server and the memory space required is dismiss by this method, because it just uses the already established web server service given by G-mail. LEDs were used to identify the switching action. This System is efficient and flexible interactive.
Sending Commands to the Raspberry Pi
The script running on server side of our laptop or on a web server receives the input commands from the user and appropriately sends it to the client (Raspberry Pi). In this, we will be using those input commands to turn a light ON/OFF. When we give the command to turn ON a light by the server side script, the data and information gets relayed to the Raspberry Pi and its GPIO pin will turns ON a relay. The system can send current updates to the server to detect whether the light is ON/OFF.
Using PIR motion sensor we can send the data signal to the Raspberry Pi, we just run a script which can reads the sensor by a GPIO pin and transmit the data to overall system through the IoT platform. This can then be look by the IoT console.

Wireless Home Automation system using IoT
This system uses mobiles or computers to control basic home control and function automatically through internet from anywhere around the world globally, an automated home is sometimes called a smart home. It is meant to save the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 8, August 2019

electric power and human energy. The proposed system is a distributed home automation system, consists of server i.e. Wi-Fi module, sensors. Server controls and monitors the various sensors, and can be easily configured to handle more hardware interface module (sensors). The Arduino board, with built in Wi-Fi module acts as web server. Automation System can be accessed from the web browser of any local PC using server IP, or remotely from any PC or mobile handheld device connected to the internet with appropriate web browser through server real IP (internet IP). Wi-Fi technology is selected to be the network infrastructure that connects server and the sensors. Wi-Fi is chosen to improve system security (by using secure Wi-Fi connection), and to increase system mobility and scalability.

II. COMPARISON

Serial no.	System	Communication Interface	Controller	User Interface	Applications	Merits
1	Wi-Fi based using Arduino microcontroller through IOT	Wi-Fi	Arduino	Web Application and android App	Temperature and motion detection, monitoring and controlling appliances	Low cost, Secure, Remotely controlled
2	Smart Task Scheduling Based using Arduino and Android	Wired X10 and Wireless Zig bee	Arduino	Android Application	Energy Management and task scheduling with power and cost	Energy-efficient and Highly scalable
3	Web service and android app Based using Raspberry pi	Web server and interface card	Raspberry pi	Android application	Controlling shutter of window	Autonomous, and Quite scalable
4	Cloud Based Using Hadoop System	Cloud based data server uses Hadoop technology	Home gateway and router	Smart device	Monitoring and Controlling Home Appliances	Effectively manage Semi structured and unstructured data, Reduce computational burden of smart devices
5	Cloud Based Using Zig Bee Microcontroller	Zig bee wireless Network	Smart Socket	PC or Android Phone	entrance control management, monitoring the power consumption, temperature and humidity	Convenience, safety, and Power-saving
6	Wireless Sensors Based with mobile Technology	cloud-based data server	PCB circuits	Mobile Application	monitor the home conditions and power consumption of appliance	Low power consumption And system cost efficiency.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 8, August 2019

7	Android based using Arduino	Micro Web Server	Arduino Mega 2560 and the Arduino Ethernet shield	Android App	Light switches, Temperature, Humidity sensors, Intrusion detection, Smoke/Gas sensor	Feasibility and Effectiveness
8	Konnex-Bus based using raspberry pi	SIP Provider	Raspberry pi and Konnex Bus	Mobile App	Lights Control, Temperature Monitoring	Performance improved, energy-consumption could be Reduced.
9	Bluetooth Based using Arduino	Bluetooth	Arduino	Python supported mobile	Controlling	Secured and Low cost
10	GSM Based Using Arduino	SMS	Arduino	Smartphone App	Control appliances	Simplicity

III. SMART HOME SYSTEM

In general, smart home system can be configured as shown in Figure 1. As shown in Figure 1, smart home system consists of largely three components, home server, home gateway, and smart home devices. First, the home server provides storage, integration and distribution function of the information collected from various media in the home as a kind of computer device.

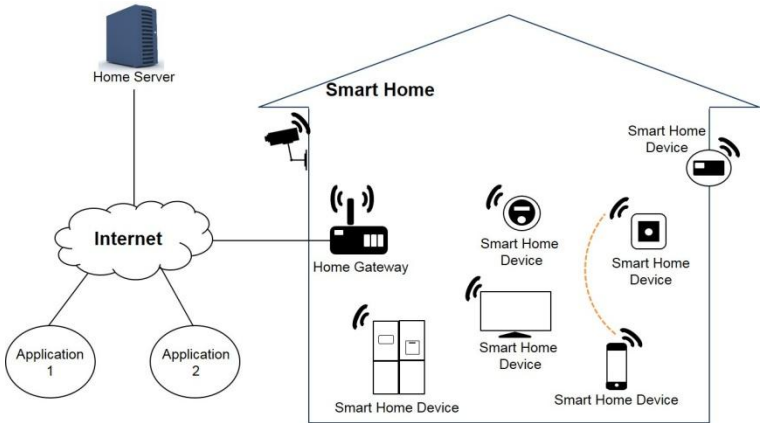

Figure1. Smart Home System

Next, the home gateway performs a relay function, or interconnects function between the subscriber access network and a wired/wireless home network. Finally, smart home devices can intelligently provide the information exchange function between the devices, and external internet access function [7].

IV. SECURITY REQUIREMENTS OF THE SMART HOME SERVICE

Components constituting the smart home system are likely to be exposed highly to a variety of threats from inside or outside because most of them have internet connectivity, unlike the existing home network environment.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 8, August 2019

To cope with the security threats such as malware infections, unauthorized user access, important information disclosure, we should apply the security functions according to the component specific characteristics of a smart home system.

Table shows the security requirements that are required to provide a secure and trustworthy smart home service. As seen in Table 1 below, we classify the security requirements based on the integrity, confidentiality, availability viewpoint and describe the details.

Security requirements summarized in assume some limitations. First, smart home devices (e.g., smart phone, etc.) that can be connected to the internet via a mobile communication network are limited within the case connected to the internet via the home gateway. Also, the security functions of the home server and the home gateway can be performed by any one of the two objects, and it is possible to implement home gateway and home server as a single device in accordance with the system implementation method.

V. SECURITY FUNCTIONS FOR THE SMART HOME SYSTEM COMPONENTS

Security functions for the smart home system components (i.e. home server, home gateway, and smart home device). The security functions described in are the basic security functions to be preferentially applied in the smart home system.

Additionally, we do not consider network security functions and the security features related to a specific service, and also a remote service environment in this paper.

In case of data communication between devices as well as sending data to the outside, the transferring data should be converted into cipher text form. That is, the data confidentiality should be provided.

And, we recommend using hardware security module to enhance security of device which has a specification capable of providing a security feature by mounting a hardware security module. For example, device identification information can be managed securely by using the hardware security module.

To set a strong password, it is preferable to use a password of more than 8 figures composed of numbers, letters, and special characters. In addition, we recommend using a more secure algorithm than 128 bit encryption algorithm to enhance security.

Low capacity smart home devices (e.g., tiny sensors and actuators, etc.) and a home server can use the access control function and mutual authentication function provided by the home gateway.

In consideration of the device specification, the critical data (user's privacy data, key information, and access control/ authentication data, etc.) should be stored securely using a hardware security module.

Besides, data integrity should be provided to prevent data from being changed.

To defend cyber attacks including hacking from the outside, the firmware integrity verification feature should be provided. Also, we recommend the integrity verification function having fast execution speed and ease of implementation for a low capacity smart device.

In case secure software update, verification of the software update file and software update server should be provided.

According to the respective characteristics and specifications of the device, we should grant a different security level for each device. And also, suitable security functions such as access control, authentication and encryption algorithm which are applicable to each security level should be provided as a security policy setting function.

VI. CONCLUSIONS AND FUTURE WORKS

Since a user privacy data leakage, social infrastructure paralysis, and economic losses as well as a risk of human life can be occurred in the IoT environment, we have defined the security requirements for the smart home service which is emerged as a hot item of major IT companies.

In this paper, we specifically proposed the smart home system security requirements reflecting the IoT environmental characteristics. And, the security functions of the components that make up the smart home system was classified and defined according to confidentiality, integrity, and availability.

However, since we consider only the basic security functions for the smart home system, we will analyze additional security functions which are against the security vulnerabilities and the security flaws caused by device to device

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 8, August 2019

infection as a future work.

In addition, network security functions and the security features related to a specific service (i.e., smart metering service, smart health service, etc.), and also a remote service in the smart home will be defined in the near future.

REFERENCES

[1]J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things: A vision, architectural element, and future directions," ELSEVIER, Future Gener. Computet. Syst., vol. 29, issue 7, February 2013, pp. 16451660

[2]M. Newlin Rajkumar, C. Chatrapathi, and V. Venkatesakumar, "Internet of Things: A vision, technical issues, applications and security," IPASJ International Journal of Computer Science, vol. 2, issue 8, August 2014, pp. 2027.

[3]John A. Stankovic, "Research Directions for the Internet of Things," IEEE INTERNET OF THINGS JOURNAL, vol. 1, no. 1, February 2014, pp. 39.

[4]T. Heer, O. GarciaMorchon, R. Hummen, S. Keoh, S. Kumar, and K. Wehrle, "Security Challenges in the IPbased Internet of Things," Wireless Personal Communications Journal, vol. 61, issue 3, September 2011, pp. 527542.

[5]S. Sicari, A. Rizzardi, L.A. Grieco, and L.A. Grieco, "Security, privacy and trust in Internet of Things: The road ahead," ELSEVIER, Computer Networks, vol. 76, January 2015, pp. 146–164

[6]A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah, "A systemic approach for IoT security," IEEE International Conference on Distributed Computing in Sensor Systems, May 2013, pp. 351355.

[7]ITUT X.1111, 'Framework of security technologies for home network', February 2007.