The Design and Implementation of a Low Cost and High Security Smart Home System Based on Wi-Fi and SSL Technologies

Chong-Yao Xu¹, Xin Zheng¹ and Xiao-Ming Xiong¹,²

¹ Guangdong University of Technology, School of Automation, No. 100 Waihuan Xi Road Guangzhou Higher Education Mega Center Panyu District, 510006 Guangzhou P.R China
² Guangzhou National Integrated Circuit Design Industrialization Center for Modern Service Industry

chongyaoxu@126.com, 18963983546@163.com, xmxiong@gdut.edu.cn

Abstract. With the development of Internet of Things (IoT) and the popularity of intelligent mobile terminals, smart home system has come into people’s vision. However, due to the high cost, complex installation and inconvenience, as well as network security issues, smart home system has not been popularized. In this paper, combined with Wi-Fi technology, Android system, cloud server and SSL security protocol, a new set of smart home system is designed, with low cost, easy operation, high security and stability. The system consists of Wi-Fi smart node (WSN), Android client and cloud server. In order to reduce system cost and complexity of the installation, each Wi-Fi transceiver, appliance control logic and data conversion in the WSN is setup by a single chip. In addition, all the data of the WSN can be uploaded to the server through the home router, without having to transit through the gateway. All the appliance status information and environmental information are preserved in the cloud server. Furthermore, to ensure the security of information, the Secure Sockets Layer (SSL) protocol is used in the WSN communication with the server. What’s more, to improve the comfort and simplify the operation, Android client is designed with room pattern to control home appliances more realistic, and more convenient.

1. Introduction
Recently, the Internet of Things (IoT) and intelligent hardware have shown explosive growth, and the intelligent terminals can be seen everywhere. On the one hand, home appliances can access to the Internet through the Wi-Fi, thus it can be accurately controlled and monitored by a mobile phone or a tablet, which greatly improve people’s living quality and ensure the safety of home [1-4]. On the other hand, as the IoT technology become more sophisticated, with the continuously decreasing cost and more convenient operation of smart home, the popularity of smart home system has become an inevitable trend.

1.1. Existing smart home technologies
As early as 1984, the United States had the world’s first smart home building. After decades of development, the smart home system has experienced quite a few great reforms. Reference [5] introduces a smart home system based on Java, all of the intelligent appliances are connected together
with physical means, and through a personal computer (PC) to realize the separate control, with providing a secure network interface. However, due to the complex installation of physical connections, and adding the personal PC and physical connections, the cost of system implementation is very expensive. Reference [6] proposed a smart home system based on Bluetooth (BT), each home appliances are equipped with a local BT sub-controller, which unified the data sending to the BT master controller. The scheme solves the problem of complex cable installation and connection, but it is constrained by the short distance of BT transmission, the limitation of the network and the lack of remote control. Reference [7-8] introduced a smart home system that controls appliances through global system for mobile communications (GSM) and general packet radio service (GPRS). The program is not subject to distance restrictions, and the user can control it through the mobile phone. However, because the user has to remember the control code of the appliance and the telephone number corresponding to each appliance, each appliance requires a GSM/GPRS module with high cost, and each module needs to install the Subscriber Identification Module (SIM) card separately. Reference [9] presented a kind of smart home system based on ZigBee network, which solves the limitation of the BT network. Because the ZigBee can’t directly access to the Internet or communicate with mobile phone, so in order to realize the remote control, it is necessary to design an embedded development board with Ethernet interface or Wi-Fi functions as a gateway, as a centralized controller achieving unified transfer of data. Reference [10] described a solution for controlling television through gestures, which means the television can be controlled by recognizing different gestures of the user. It consists of a set of ultrasonic sensor, a red/green/blue (RGB) camera, and a depth camera above the television. Combined with the recognition algorithm, it has unique advantages. The deficiency of the method is that it is susceptible to gestures accuracy and lighting. Besides, it’s easy to cause fatigue when the user repeatedly making gestures [9]. Reference [11] introduced a smart home control system based on the ZigBee wireless sensor networks and power line communications. Each electrical equipment in the system is equipped with a power line communication transceiver, which receives control information from management station by the power line to control appliances and to feedback the appliance status to the management system. Each room has multiple ZigBee sensor nodes and a power line communications (PLC) transceiver integrating a ZigBee coordinator which sends data to the management system after receiving the information of sensor node through the PLC transceiver. Compared with simple Zigbee system, the system can effectively improve the data accuracy of sensor nodes in a large amount of data (>200Kbytes/s), which has good innovation. In addition, many foreign researchers has proposed many power management systems of smart home [12-15], and reference [15-17] shows that intelligent residence can be more efficient than traditional residential power utilization.

1.2. The characteristics and innovation of the system

The improvements and innovations of the proposed system are described as following:

1) All Wi-Fi Smart Nodes (WSNs) are accessed to the Internet through the router, and are directly controlled by mobile phone, without centralizing control of data transfer. It can reduce the complexity of installation and debugging, enhance the scalability, and decreases the cost drastically.

2) ESP8266, with high performance and low cost Wi-Fi solution, is used in the smart appliances node. It is a system on a chip (SOC) design, including an internal 32-bit embedded professor, a Wi-Fi transceiver, an analog-to-digital converter (ADC), input/output (I/O) controllers, serial transceivers and so on. There is no need to add other microcontroller unit (MCU), so it can improve the stability and reduce the cost of the system.

3) WSN module can be embedded with a Secure Sockets Layer (SSL) to encrypt the data, which can ensure the information security of remote control, and reduce the risk of system attacks.

4) The Application (APP) based on Android client is designed according to a pattern of room, and all appliances have a real simulation effect that improving the operability of the system.
Moreover, users can also add the intelligent Wi-Fi nodes to increase home appliances through APP which can increase the flexibility and extendibility of the smart home system.

2. System architecture
The smart home system mainly includes three parts: WSN, Cloud Server and APP Client. The system architecture is shown in figure 1. Each household application is equipped with a WSN which can access to the Internet through Wi-Fi network. A database is built on the cloud server to record status of home appliances, environment conditions and user’s habits. Users can control every home appliance or detect the environment when you login in the server at anywhere. The SSL security protocol is embedded in the WSN, which is used to encrypt data between cloud server and WSN with 1024 bit keys.

![System architecture overview](image)

**Figure 1.** System architecture overview

2.1. WSN
Wi-Fi technology is a popular wireless communication protocol, because of its high communication speed and easy operation, it has a wide range of applications. Now almost every smartphone has Wi-Fi configuration, and Wi-Fi hotspots (APs) are covered in the home, school, and every prosperous business district. In recent years, with the rapid development of the IoT technology, the cost of the Wi-Fi chip decreases gradually and the function is becoming stronger. It has the advantages such as strong versatility, high speed, simple operation and low cost, using Wi-Fi as the wireless solutions of smart home system. It should be noted that the retail price of Wi-Fi chip for this design is less than 0.88 USA dollar (USD), which is programmable and can be used as MCU.

In this design, each WSN is integrated with Wi-Fi functions, which can be accessed directly through the router to the cloud server. The socket, fluorescent lamp, TV and other appliances are connected to the same Wi-Fi network via WSN, so as to set up a home Wi-Fi network, users can access through the cloud server to control appliances and realize the environment situation in the home.

2.2. Cloud Server
Cloud server is also known as cloud computing server, which has three core elements: computing, network and storage. It is based on the cluster server technology. Cloud server is simple, efficient, safe and reliable. It has flexible and scalable processing capacity. It has four main features including high-
density, energy-saving, easy reorganization, and system optimization. Applying cloud server into the smart home system can bring more safety and stability to the smart home system.

The cloud server we used is a free Internet cloud platform offered by a third party companies. It mainly helps users set up the remote control of home appliances. When users need to control home appliances or learn the home situation, they only open the APP to login into the server and click on the control button of appliance, then the APP will automatically upload the information to the server which sends control commands to the corresponding home appliance and feedback control results to the client after the server receives the data.

2.3. App Client
As technology evolves, mobile phones, Pad and other portable intelligent terminals become more pervasive, almost everyone will take at least one intelligent terminal. Intelligent mobile terminal is selected as the control terminal of smart home system, which can not only reduce the complexity of the system, improve the flexibility of control and ease of operation, but also greatly reduce the cost of the system. Android system, as one of the three major mobile operating systems, it is favored by customers and mobile phone manufacturers for its completely free, open source code, plentiful application software features. Therefore, in this paper, a control software based on Android platform is designed for realizing the function of all kinds of control. The software has a warm interface, a reasonable layout, powerful functions and can be expanded flexibly.

3. System implementation
The photograph of the proposed smart home system is shown in figure 2. The realization of the design of the WSN mainly consists of Wi-Fi smart socket, Infrared Radiation (IR) learning module, CO2 sensor, harmful gas (CO) monitoring module. Router is used as AP to launch wireless signal to build home Wi-Fi network. When WSNs are connected to the router, using the mobile phone to login to server, the system will work properly.

![Figure 2. System implementation](image)

3.1. WSN hardware design
In this system, we designed four WSNs to comprise a simple smart home system, including smart socket, IR learning module, CO2 sensor module and harmful gas (CO) monitoring module. The detailed information will be introduced as following.
1) CO2 sensor module: This module is composed of CO2 concentration sensor and Wi-Fi module, as shown in figure 3 (a). Wi-Fi module read the data a sensor every ten minutes via the serial port, and feedback to the server, then enter into the low power mode with only 12uA current consumption. Ten minutes later, the Wi-Fi module will automatically wake up and read the next data.

2) Harmful gas (CO) monitoring module: figure 3 (b) illustrates the printed circuit boards (PCBs) used in the system debugging, this module is mainly responsible for monitoring the indoor CO concentration. Wi-Fi module adopts the Modbus protocol to communicate with the sensor through the serial port, query data each one minute, and upload the result to the server, presently enter the low power state. When the concentration of CO exceeds the standard, the module will send an emergency notification to the mobile phone through the server to remind the user.

3) Smart socket: Smart socket products is shown as in figure 3 (c). It is mainly ideal for receiving and transmitting control information through the Wi-Fi chip. In addition, the S8050 low cost transistor is used to driver relays, so it can achieve on and off of the relay. Then the 220V socket can be controlled to handle the appliances work or not.

4) IR learning module: This module is shown as in figure 3 (d), which is mainly used for controlling air conditioner, television and other IR equipment. It has a universal IR receiver and a MCU with Cortex-M3 kernel. The MCU can learn the encoding of all kinds of IR controllers through calculating the elapsed time of high and low voltage of IR encoding. In addition, there are IR emitters in 8 directions to transmit the corresponding signal to control appliances according to the control information sent from the mobile phone.

3.2. Embedded software design
The embedded software designed by this system refers to the internal control program of Wi-Fi chip. The program is mainly responsible for the connection of Wi-Fi network, work mode settings, Wi-Fi data transmission and reception, IO port control, serial data dispatch, AD data acquisition and so on.

WSN will start automatically in Station+AP mode, and try to connect Wi-Fi according to the last recorded information, WSN switches from Station+AP mode to Station mode after successful Wi-Fi connection, if it is not connected in a minute, we can access the Wi-Fi wireless network from WSN itself by mobile phone, and configure Wi-Fi network information (SSID and password) which WSN needs through the APP. Besides, it will automatically connect to the cloud server and enter the suspended state after successful Wi-Fi connection. If the WSN is the sensor node, it will automatically report to the server. The flow chart of the program is shown in figure 4.

3.3. APP design
In this system, an application program based on Android (APP) is designed for home appliances control. In order to facilitate the operation, Android client is designed in room pattern to control home appliances, such as drawing and graphical interface, each appliance has its corresponding graphical
interface, as shown in figure 5. Simultaneously, the APP also supports to increase home appliances against actual conditions.

3.4. Control protocol
Control protocol is shown in figure 6. According to the user's requirement, there are 12 bytes control information in the system, the first 2 bytes is fixed for two hexadecimal number—0xA5, 0x5A, followed by 4 bytes of user ID, 1 byte random number, 1 byte room code, 1 byte command code and 2 bytes CRC check code. After the server receives the control information, firstly it returns instructions to confirm the information, and then controls the home appliances, finally it feedback the current status of home appliances and environmental information to the client.

Figure 4. Program flow chart
Figure 5. APP control interface

Figure 6. Control protocol

①→Start flag, two bytes, fixed to 0xA5, 0x5A;
②→Instruction random code, one byte, to ensure that this section of the instructions correspond with the server response information;
3. User ID, four bytes, user unique certification;
4. Room information, one byte, indicates which room the home appliance is controlled by this instruction;
5. Appliance information, one byte, the only representation of a home appliance;
6. Control instruction, one byte, controls the operation of home appliances. For example: light switch, TV channel selection, air conditioning temperature switch, etc.;
7. CRC check, two bytes, verifies whether the transmitted information error, etc..

3.5. SSL security encryption
SSL encryption technology is one of the most securely and widely used network encryption technology. It is between the TCP/IP and many application protocols, providing security support for data communication. The SSL encryption certificate is implanted in the WSN node, so as to construct a secure channel between the WSN and the server to carry out data transmission. Owing to a vast amount of memory required for the SSL function (under SSL cache settings for the 8KB, SSL function requires at least 22KB space [18], and available to users of RAM is about 50KB [19], SSL). To set whether to open the SSL function via the macro definition before compilation, thus ensuring the flexibility of application.

The implementation method of the WSN as the SSL Client is described as following. SSL security encryption using the Software Development Kit (SDK) provided from ESP8266 chip manufacturers. Firstly, apply to Espressif Systems for a certificate synthesis script. Secondly, put it in the same directory as the CA certificate. Thirdly, run certificate synthesis script in lubuntu system so that the certificate will be made into a BIN file. Finally, download the BIN file into the specified location [18].

Certification process is as follows:
I. WSN initiates TCP connection, then read the CA certificate in the Flash, and load it into the corresponding SSL_CTX structure.
II. ESP8266 launches TLS handshake, get the certificate issued by SSL server, and verify CA certificate supported by WSN, if successful, completing the verification, otherwise disconnected.

4. Cost analysis
Because the system is directly connected to the router by WSN and accessed to the Internet without a centralized controller, so it can greatly reduce the cost of the system. Specifically, WSN adopts a single chip solution, the work of Wi-Fi communications and home appliances control are finished by a low cost chip. In this section, the Wi-Fi smart socket is considered as an example to analyze the market advantage of the system. The smart socket mainly composed of Wi-Fi module, relay, driving transistor, 3.3V voltage regulator chip, and the cost list is shown in the following table 1:

| Component        | Price (USD $) |
|------------------|---------------|
| Wi-Fi chip       | 0.88          |
| 32M SPI Flash    | 0.07          |
| S8050 triode     | 0.01          |
| Relay            | 0.18          |
| ASM1117-3.3V     | 0.03          |
| PCB board        | 0.29          |
| Power module     | 0.59          |
| Total            | 2.05          |
5. Test result

5.1. Wi-Fi socket
Wi-Fi socket is one of the most frequently used devices in smart home system. It can realize the control of household appliances such as fluorescent lamp, electric fan, water heater, curtain, etc. By repeating testing, the Wi-Fi socket can flexibly turn on and off the light through the APP. Figure 7 shows this working process. Considering the time-delay of relay, the light will be turned on after operating APP about 500ms later.

![Figure 7. Light control](image1)

![Figure 8. TV control](image2)

5.2. TV control
The intelligent IR learning module is also tested in this paper. Firstly, the self-learning method is used to learn the IR coding for remote controlling TV set in the IR module, and then the different keys are numbered. When a key is pressed, the mobile phone will send the corresponding number through the Wi-Fi network to the IR learning module which sends the corresponding IR signal after received the information, so it can realize the control of the TV.

Figure 8 shows a video screenshot of controlling TV by APP and IR learning module. The results of practical tests proves that it is easy to achieve all the functions of the remote control, including “program +”, “program –”, “silent”, “channel switch” and so on. In figure 8, “a” is the mobile phone control terminal; “b” is the remote control; “c” is the IR learning module.

6. Conclusion
A smart home system solution with the properties of low cost, high security and reliability is introduced in this paper. Four kinds of WSN are developed. All WSN nodes can be connected directly to the Wi-Fi system, and access to the server via the SSL security protocol. At the same time, the APP based on the Android is designed for WSN controlling. Each WSN can work independently, and the user can control the nodes directly through the mobile phone without a centralized controller, which avoid the complication of system installation and commissioning process. And due to the low cost of the system, it has great market value and competitive advantage.

References
[1] Kim T, Lee H, and Chung Y 2010 Advanced universal remote controller for home automation and security. IEEE Trans. Consum. Electron., 56(4) 2537-42.
[2] Pavithra D and Balakrishnan R 2015 IoT based monitoring and control system for home automation. Communication Technologies (GCCT), 2015 Global Conf. on. IEEE (India: Kanya Kumari District) pp 169-173.
[3] Wenbo Y, Quanyu W, et al 2015 Smart home implementation based on internet and Wi-Fi technology. Control Conf. (CCC), 2015 34th Chinese. IEEE (Hangzhou: Zhejiang University) pp 9072-77.
[4] Yun J, Ahn I Y, Sung N M and Kim J 2015 A device software platform for consumer
electronics based on the Internet of Things. *IEEE Trans. Consum. Electron.*, 61(4) 564-571.

[5] Al-Ali A R, Al-Rousan M 2004 Java-based home automation system. *IEEE Trans. Consum. Electron.*, 50(2) 498-504.

[6] Sriskanthan N, Tan F, Karande A. 2002 Bluetooth based home automation system. *IEEE Trans. Consum. Electron.*, 26(6) 281-289.

[7] ElKamchouchi H, ElShafee A. 2012 Design and prototype implementation of SMS based home automation system. *Electronics Design, Systems and Applications (ICEDSA), 2012 IEEE Int. Conf. on. IEEE* (Malaysia: Kuala Lumpur) pp 162-167.

[8] Wei L, Wei L, et al 2013 Design and Implement on Smart Home System. *Intelligent Systems Design and Engineering Applications (ISDEA), 2013 4th Int. Conf. on. IEEE* (China: Zhangjiajie) pp 229-231.

[9] Gill K, Yang S H, Yao F, and Lu X 2009 A zigbee-based home automation system. *IEEE Trans. Consum. Electron.*, 55(2) 422-430.

[10] Lian S, Hu W and Wang K 2014 Automatic user state recognition for hand gesture based low-cost television control system. *IEEE Trans. Consum. Electron.*, 60(1) 107-115.

[11] Li M and Lin H J 2015 Design and implementation of smart home control systems based on wireless sensor networks and power line communications. *IEEE Trans. Ind. Electron.* 62(7) 4430-42.

[12] Byun J, Hong I, Lee B and Park S 2013 Intelligent household LED lighting system considering energy efficiency and user satisfaction. *IEEE Trans. Consum. Electron.*, 59(1) 70-76.

[13] Han D M and Lim J H 2010 Design and implementation of smart home energy management systems based on zigbee. *IEEE Trans. Consum. Electron.*, 56(3) 1417-25.

[14] Han J, Choi C S, Park W K and Lee I 2014 Smart home energy management system including renewable energy based on ZigBee and PLC. *IEEE Trans. Consum. Electron.*, 60(2) 198-202.

[15] Han D M and Lim J H 2010 Smart home energy management system using IEEE 802.15. 4 and zigbee. *IEEE Trans. Consum. Electron.*, 56(3) 1403-10.

[16] Missaoui R, Joumaa H, Ploix S and Bacha S 2014 Managing energy smart homes according to energy prices: analysis of a building energy management system. *Energy and Buildings*, 71 155-167.

[17] Molitor C, Benigni A, et al 2013 Multiphysics test bed for renewable energy systems in smart homes. *IEEE Trans. Ind. Electron.*, 60(3) 1235-48.

[18] Espressif Systems IOT Team 2015 ESP8266 SDK SSL User Manual CN v1.1 http://bbs.espressif.com/.

[19] Espressif Systems IOT Team 2015 ESP8266 Datasheet CN v4.4 http://bbs.espressif.com/.