ISSN: 2664-9640

Design of Indoor Intelligent Security System Based on Internet of Things Cloud Platform

Liang Yu[1,*], Meiling Deng[1] and Shengli Yang[2]

[1]College of Computer, Guangdong University of Science and Technology, Dongguan 523083, China;

[2]School of Computer and Information, city college of Dongguan university of technology, Dongguan 523419, China.

Abstract

With the rise of smart homes, indoor intelligent security systems have emerged as an important subsystem of smart home systems[1]. The traditional indoor security system is mainly composed of a single video surveillance system or multiple security surveillance devices independently. There is no linkage control, only single-dimensional monitoring data can be provided, and the indoor security situation cannot be fully understood. In addition, the monitoring situation cannot be sensed in real time. Based on the existing problems of indoor security systems, The indoor intelligent security monitoring system based on the Internet of Things cloud platform[2] which is proposed in this paper. The Arduino development board is used to collect and sense the multi-dimensional data of the indoor environment in this system, and then it is connected to the IoT cloud platform through the ESP8266 WiFi communication protocol. The platform employs the open source MQTT protocol to realize the open decoupling of the application layer client to the space-time of data release of the perception layer . Moreover, the cloud platform architecture exploits the object model to describe the functions of the device in the cloud, and uses the triplet information of the device to bind and authenticate it to the physical device, which simplifies the design of the system. The indoor intelligent security system on the IoT cloud platform promotes the comprehensive convergence of data and remote security monitoring at any time and place, realizing the system's holographic perception, front-end and back-end linkage, and network-wide intelligence.

Keywords

Internet of Things cloud platform, MQTT protocol, Object model, Intelligent security, Arduino, Triplet information.

1. Introduction

The traditional indoor security system mainly consists of a single video surveillance system, focusing only on the collection of video data, but not the multi-dimensional and all-round protection of indoor security. At the same time, the original video acquisition + Internet transmission mode has been adopted for indoor security system, and can only be viewed through the mobile terminal or the terminal can perform playback monitoring, and the real-time monitoring cannot be realized, so that the monitoring effect is not satisfactory [3].The multi-dimensional object data sources are considered in this paper, including not only traditional video data, but also environmental data and spatio-temporal data. At the same time, the wireless network technology is exploited to transmit the underlying sensory data for the IoT cloud platform, which it is convenient for remote terminals and mobile to construct an intelligent security system, which will realize front-end linkage, holographic perception, and

ISSN: 2664-9640

network-wide intelligence. In terms of technology implementation, the traditional end-to-end control implementation method is breaked through, and utilizes the powerful equipment management and data analysis capabilities of the Internet of Things cloud platform to enable a large amount of real-time data to be effectively and reliably managed. Meanwhile, the object model development method based on the MQTT protocol of the Internet of Things cloud platform is used, which simplifies the development difficulty and reduces the development cost and maintenance cost [4].

2. The Overall Design of the System

The main modules of the security monitoring system is designed by including six security inspection modules, such as illegal intrusion monitoring, fire monitoring, leakage detection, toxic gas leakage monitoring, water leakage monitoring and video monitoring, to achieve comprehensive monitoring of indoor safety hazards, as shown in the figure. 1 is shown.

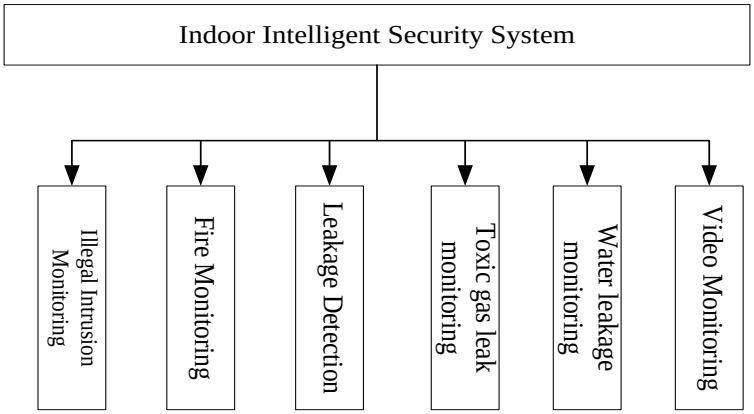

Figure 1. The composition of the indoor intelligent security system

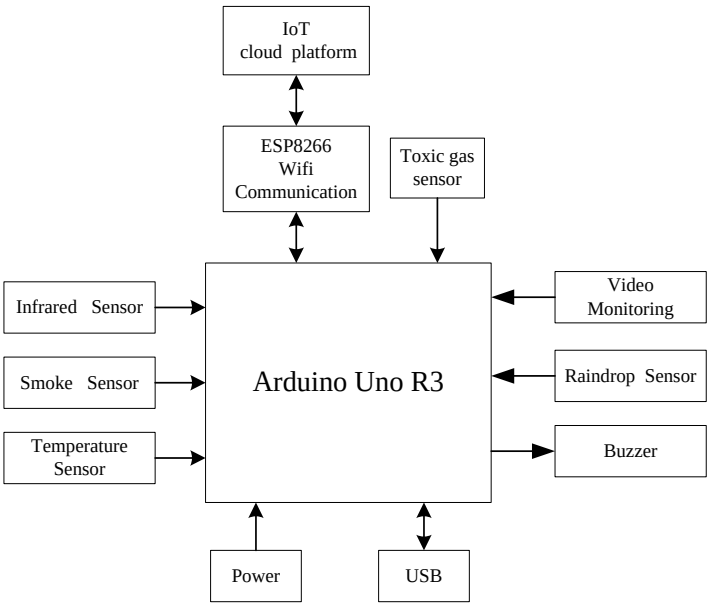

Figure 2. Overall design block diagram of system control

The indoor intelligent security control system uses the Arduino Uno R3 development board as the core, using infrared human body sensing sensors on the window sill to monitor illegal

ISSN: 2664-9640

intrusion; smoke sensors and temperature sensors are employed to collect environmental data, coordinate control to monitor the occurrence of fire [5]; Use the leakage detector to check whether the voltage of the live line and the neutral line are equal. If not, the leakage of the household circuit will occur, and the leakage circuit breaker will be automatically disconnected to protect the circuit; The flammable gas sensor is used to detect the concentration of toxic gas in the kitchen [6]; the water leakage detection line of the liquid conductive detection method is exploited for water leakage monitoring of the bathroom and the balcony; and the indoor scene is equipped with video monitoring to improve the quality of intelligent security. In addition, the system employs the USB interface to download the program, the buzzer to perform local alarms [7], and the ESP8266 Wifi module to wirelessly connect to the IoT cloud platform, enabling data to be updated to the cloud in the real time, making it easy for users to view online or offline [8]. The overall design block diagram of the system control is shown in Figure 2.

2.1. System Hardware Circuit Design

The system's microcontroller is exploited by the Arduino Uno R3, which its possesses an ATmega328P-based microcontroller board with a 16MHz crystal clock, 14 digital input/output pins (6 of which can be used as PWM outputs) [9], 6 analog input interfaces A0~A5, 5V-12V input voltage; 5V DC voltage and 3.3V DC voltage output; support ICSP download and USB download two ways, support TX/RX serial communication mode [10]. In general, the system only needs to connect to the computer through the USB data cable to provide power, program download and data communication. It is powerful, inexpensive, and very easy to use. The minimum system of the microcontroller Arduino Uno R3 is shown in Figure 3:

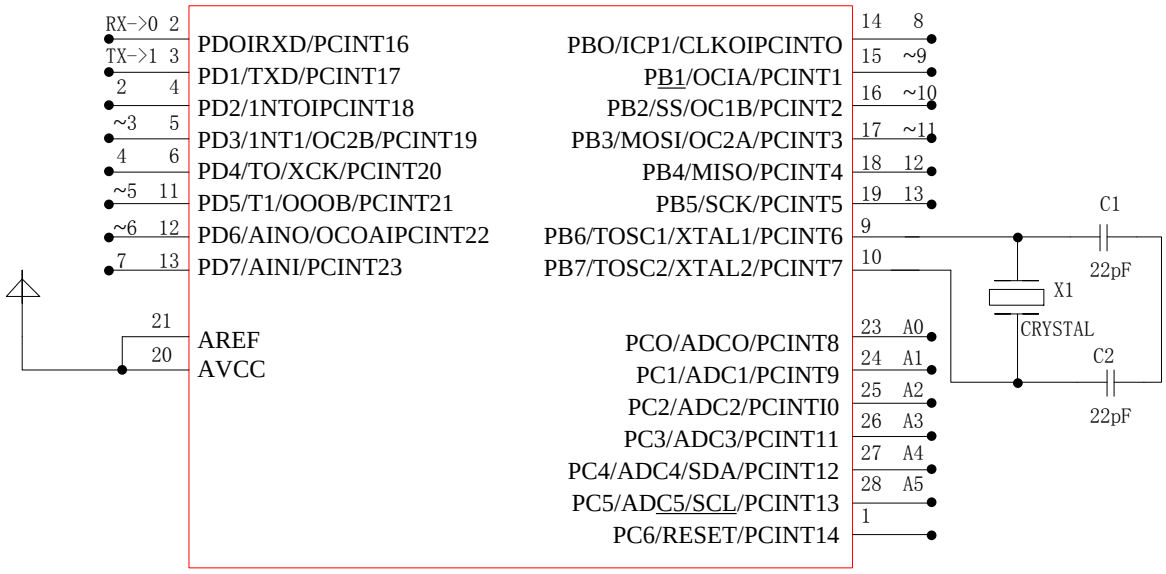

Figure 3. Microsystem Arduino Uno R3 minimum system

1. Design of illegal intrusion monitoring circuit

The system's illegal intrusion monitoring mainly involves of two aspects. The first aspect is the access control system. Since the family now has relatively safe fingerprint identification or password lock access control system, illegal intrusion is difficult. On the other hand, in fact, it is easy to invade the window at present. In this paper, infrared sensors are installed on the window sill of the home to detect whether there are strangers invading, not only can detect illegal intrusion, but also prevent children from climbing the window. The infrared sensor is adopted the integrated module U5/GH-718. The specific circuit diagram is shown in Figure 4.

ISSN: 2664-9640

Once an object is approached, a high level is detected at the PD3 end, and an alarm device is triggered. When no one is intrusion, the delay outputs a low level [11].

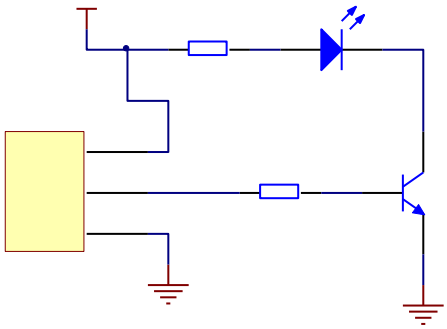

Figure 4. Infrared detection circuit

2. Fire monitoring circuit design

Indoor fire monitoring mainly consists of a smoke alarm module and a temperature acquisition module. The smoke detection module combined with the temperature acquisition module can more accurately determine whether a fire has occurred to avoid malfunction. Since the temperature is a large inertia and large hysteresis control object, the smoke sensor U2 module can first detect the ambient smoke concentration and input it to the controller analog input pin A3 to compare the collected value with the set threshold. When it is greater than the threshold, the buzzer sounds, and the IoT cloud platform connected to the wifi is forwarded to the mobile terminal for alarm; and when the collected value falls below the set threshold, and the temperature detection value is the digital temperature sensor DS1820 When the DQ pin is lower than the set value, the alarm is released to prevent the fire from re-igniting. Therefore, the system uses a combination of the two to ensure fire monitoring, the circuit diagram of which is designed as shown in Figures 5 and 6.

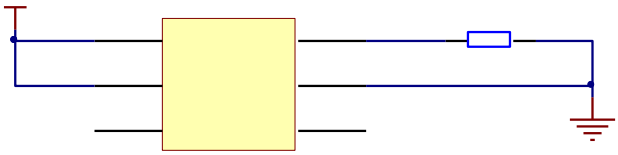

Figure 5. Smoke acquisition circuit

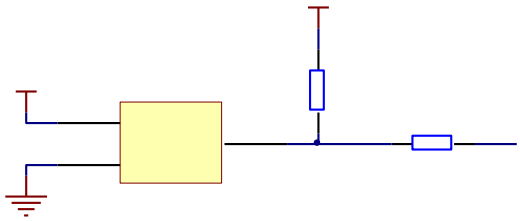

Figure 6. Temperature detection circuit

3. Design of toxic gas leakage monitoring circuit

At present, the kitchen generally exploits natural gas or liquefied petroleum gas as an energy source for cooking, and sometimes it may accidentally forget to close the valve or the child's

ISSN: 2664-9640

malfunction causes the flammable gas to leak. These leaking gases are generally easily poisoned by inhalation, and these gases are prone to explosion when mixed with a certain amount of air. Therefore, flammable gas leakage is very dangerous and is an important part of the indoor security system [12]. The system employs the tin dioxide natural gas detection sensor MQ-2 to monitor the indoor toxic gas concentration in real time, and connects the analog monitoring pin PB0 to the analog input pin A1 of the microcontroller. The circuit schematic is shown in Figure 7.When the air is clean, the conductivity in the gas sensitive material is low, the conductivity is poor, and the input voltage of the A1 interface is low. If there is a large amount of natural gas or other flammable toxic vapor in the working environment, the conductivity in the gas sensitive material in the sensor will increase with the increasing concentration of the gas in the environment, so that the input voltage of the A1 interface becomes high.

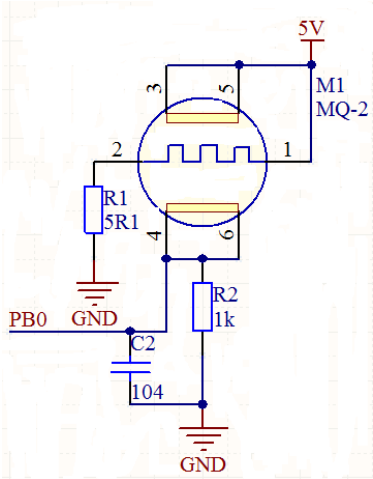

Figure 7. Natural gas detection circuit

4. Security alarm circuit design

The system's security alarm functions mainly include buzzer alarms and remote alarms using the wifi connection cloud platform. The latter uses the software data triggering method to remind the remote terminal, while the indoor local uses the buzzer alarm prompt information, and can also be remotely cleared by the Internet of Things cloud platform to eliminate the alarm. The specific buzzer alarm circuit is shown in Figure 8. Use a digital output GPIO port PD2 of the microprocessor Arduino Uno R3 to connect the triode to drive the amplification control buzzer to work.

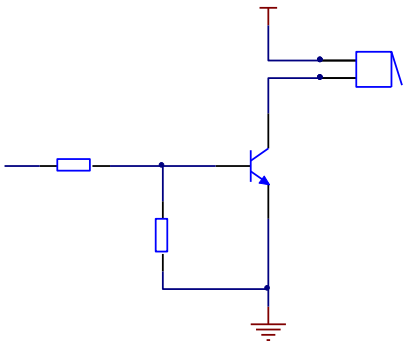

Figure 8. Buzzer alarm circuit

5. ESP8266 wireless communication module design

ISSN: 2664-9640

ESP8266 is a wifi module that implements the wireless communication connection IoT cloud platform. It exploits the serial port TXD/RXD interface of the microprocessor Arduino Uno R3 to connect the serial port to WIFI communication mode of the ESP8266 module. The system applies the standard 2.4GHz operating frequency band, IEEE802.11b/g/n protocol [13], and employs the AT command to configure it into transparent transmission mode. The circuit diagram of the ESP826 WIFi module is shown in Figure 9.

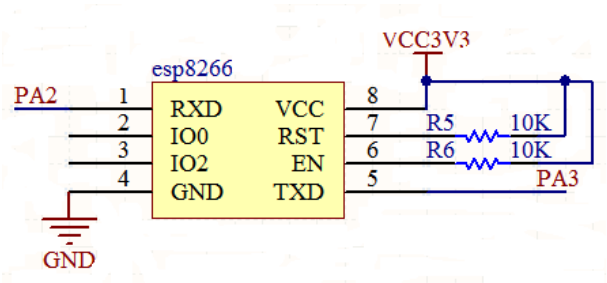

Figure 9. ESP8266 wireless communication module

2.2. System Software Design

The main process of system design includes two parts, namely the initial design of the system and the logic design of the control function of the system. The initialization design of the system includes serial port initialization, GPIO port initialization, sensor initialization and cloud connection initialization, all of which are implemented in the setup() function, and the program is executed only once; the control logic design of the system includes various types of data acquisition and sensing, logic control, data cloud and cloud command control, all of which are implemented in the loop() function, this part can be repeatedly executed, continuously monitor the multi-dimensional data in the room, and then transmit it to the IoT cloud platform for viewing and control. Finally, the indoor environment can be remotely monitored by the mobile device at any time and any place. The main flow chart of the system is shown in Figure 10:

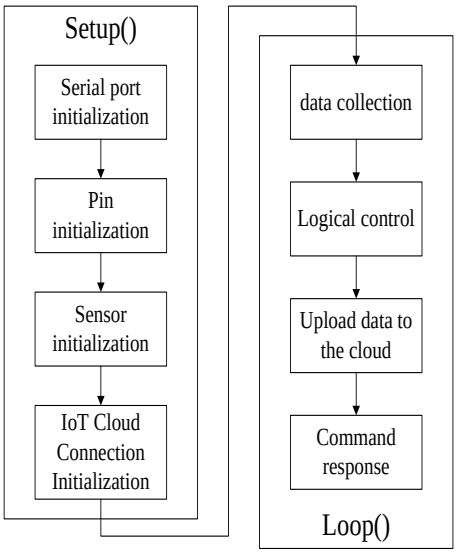

Figure 10. Mainstream diagram of the system

1. Workflow of combustible gas leakage monitoring and fire monitoring

The more complex indoor security module in the system is flammable gas leakage monitoring and fire monitoring. The specific monitoring process design is shown in Figure 11. When a flammable gas concentration reading or a smoke concentration reading are detected more than

ISSN: 2664-9640

400 ppm, it indicatesthat a flammable gas leak or fire has occurred in the room. At this point, the fan is turned on to realize gas circulation, prevent explosion, and the buzzer alarms, and sends the relevant real-time information in the room to the Internet of Things cloud platform. People can check the indoor situation through the cloud platform or the mobile terminal to know whether the indoor flammable gas leakage or the fire situation is serious, determine whether we have an alarm, and can also mute the buzzer alarm. When the flammable gas concentration reading is less than 150 ppm and the temperature reading is less than 30 C, it indicates that the room is already in a safe state, and the exhaust fan and the buzzer are turned off at this time.

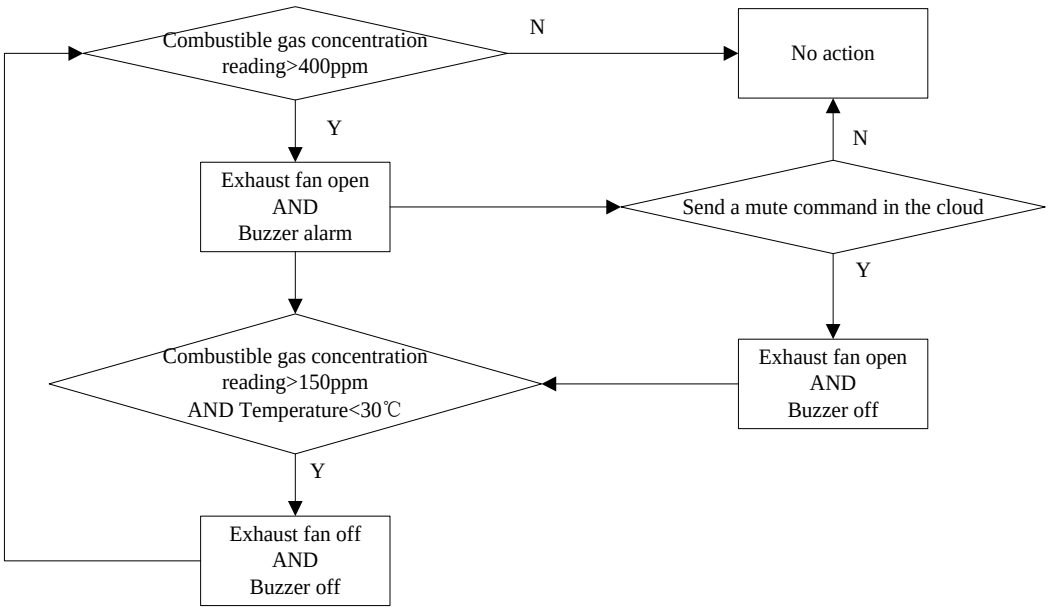

Figure 11. Combustible gas leakage monitoring and fire monitoring

2. Workflow of buzzer automatic alarm and elimination

The buzzer alarm control logic of the system is shown in Figure 12, in which a buzzer alarm is triggered when a flammable gas leaks and fires or illegally invades. The alarm sound can be cancelled by the cloud or automatically when the indoor environment returns to normal. The indoor environment returns to normal, including various sensor readings and no illegal intrusion detected.

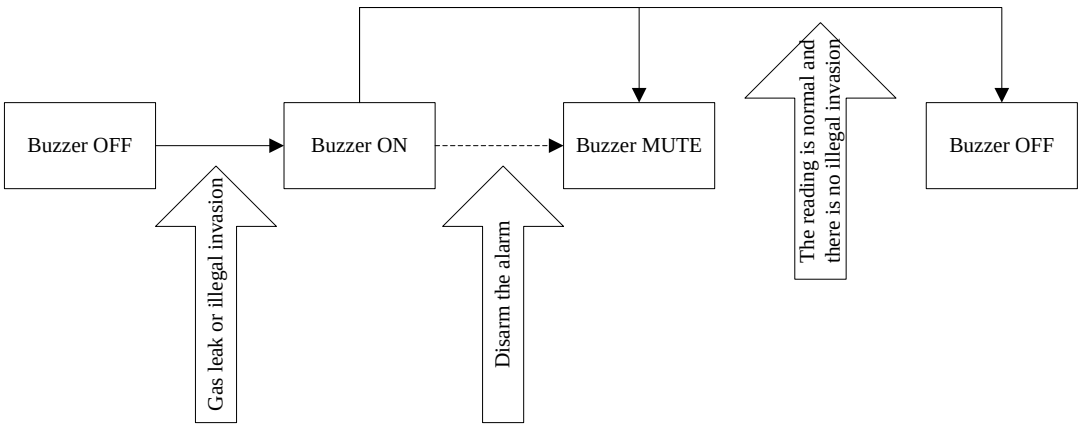

Figure 12. Buzzer switching logic

ISSN: 2664-9640

3. Design and connection of IOT cloud platform

The system employs the Alibaba Internet of Things cloud platform, which its asynchronous communication mode is the PUB / SUB, and controls and manages the interconnection method of the physical device and the application layer through the open source-based MQTT connection control. The MQTT protocol treats physical devices as publishers, the cloud platform accomplishes for a proxy server, and the PC and mobile terminal of the application layer as subscribers, where the publisher publishes messages and the proxy server forwards the subscribed messages to the subscriber client. At the same time, the subscriber client can also control the perception layer hardware devices through the IoT cloud platform. The framework of the MQTT protocol is shown in Figure 13. The proxy publish / subscribe model used by it implements the decoupling of publishers and subscribers in time and space.

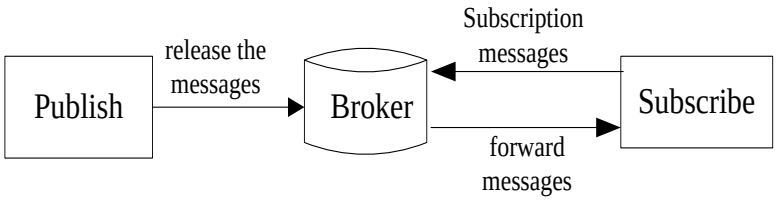

Figure 13. MQTT protocol framework

The design process of the Alibaba IoT cloud platform requires four steps:

(1) Create a product

(2) Add product features

(3) Create and add devices

(4) Binding of physical device and logical device

Create a logical device through the IoT cloud platform, where the product is a collection of devices and a group of devices with the same function. Each product can be added by the thousands of devices. The cloud platform assigns a globally unique product number ProductKey to each product, assigns a unique device number DeviceName to the devices in each product, and an authentication certificate DeviceSecret for the purpose of binding the logical device to the physical device. This is the triplet information for the device. In addition, the function of the system can be added in two ways. One is to directly import the object model written in the JSON format into the equipment group, and the other is to manually set the function.

The added device in the system is in an inactive state, and the triplet information of the device is required to authenticate the binding of the physical device to the logical device in the cloud. The Alibaba Cloud module of the standard MQTTQ protocol integrates the link kit SDK component (acting as middleware in the MQTT connection), which makes it easier to implement Ardunio device code and logical device binding operations. The ESP8266 wifi communication chip is be used in the system does not integrate the link kit SDK component. Therefore, the system can only use the more complex and reliable open source MQTT protocol autonomous access method. The specific device binding access method is shown in Figure 14.

The open-source MQTT protocol access method of the system possesses MQTT-TCP connection communication. The system exploits the triplet information of the device module as the authentication key, uses the device information as the corresponding plaintext, and uses the HmacSHA1 signature algorithm to encrypt and generate the hash key corresponding to the plaintext of the device as the authentication binding of the physical device.

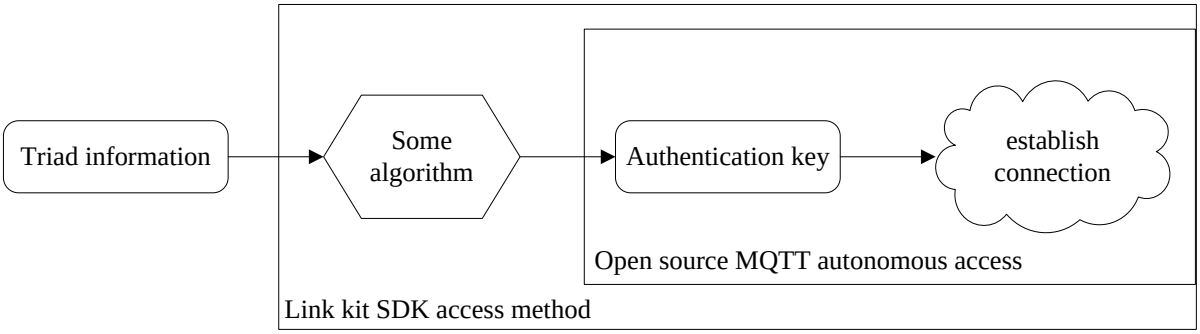

Figure 14. Binding of physical device and logical device

The system designs and builds the Internet of Things cloud platform according to requirements, and can monitor the monitoring status of indoor security equipment in the cloud in the real time, which providing a method for people to remotely and intelligently monitor the indoor security situation at home anytime, anywhere. At the same time, we can also allow our mobile terminal to connect to the Internet of Things cloud platform to remotely monitor indoor security through the HTTP protocol.

3. Conclusion

This article introduces an indoor intelligent security monitoring system based on the Internet of Things cloud platform, which realizes multi-dimensional and multi-angle remote monitoring and alarming of the home environment. The system employs an Arduino microcontroller to collect and control various sensor information, and then transmits it to the IoT cloud platform through the WIFI communication protocol. The IoT cloud platform uses the open source MQTT protocol framework to take charge of autonomous access to the device, use a simplified material model to describe the function of the device, and use the device's triplet information to bind and authenticate the physical device. It enables people to understand the home security situation anytime, anywhere through the cloud, and realize comprehensive monitoring of indoor security issues such as illegal intrusion, fire, electricity leakage, toxic gas leakage, and water leakage.

References

[1] Lanfanf Liu. Construction of Integrated Energy Efficiency Management System Based on Smart Home [C]. Proceedings of the 2016 Electric Power Industry Information Conference.(2016),9,24, Tianjin, China.

[2] Wenjun Luo. Home security monitoring system based on WeChat public platform [D]. Nanjing Normal University, China, 2015. p. 10-16.

[3] Sabaliauskaite, G.,Mathur, A.P.. Design of Intelligent Checkers to Enhance the Security and Safety of Cyber Physical Systems[C]. Computer Software and Applications Conference Workshops (COMPSACW), 2014 IEEE 38th International, 2014.

[4] Zhang, Yuanyi,Zhang, Ying. An Embedded-technology-based Security Monitoring System Design of Intelligent Building [J]. Sensors & Transducers, 156(9),2013.

[5] Su Liu. Design of fire smoke alarm in museum[J].modern electronic technology,Vol.40,No.23,p.104-108.(2017)

[6] Jinkun Guo, Dongxing Pei. Home fire detection and alarm system [J]. Digital Technology and Application, NO.11,p.122.(2014)

[7] Qinlu Huang,Xinglong Yu,Xu Ran,Xin Sun. Design of Intelligent Pedestrian Flow Detection and Security Alarm System based on Ethernet[C]. International Conference on Computer Science and Application Engineering (CSAE 2017), 2017.

ISSN: 2664-9640

[8] Welong Zhu,Xing Qin, Hong Dai, Gantao Lu. Design and Implementation of Socket-based Android Chat System [J]. Industrial control computer, Vol.29,No.03,p. 48-49+52.(2016)

[9] Yong Guo,Xiaoping Yu. Comprehensive design of electronic system. Peking University Press,(2007).

[10] Wei Huang,Zhong Wang,Weijun Yang,Xin Wang. Program download circuit failure of CH340T module and its solution [J]. Microcontroller and Embedded System Application, Vol.17,No.09,p. 43-45.(2017)

[11] Zhiqiang Li. Working principle and application of MW M2W transmitter carrier alarm [J]. Western radio and television, No.19,p. 235-236.(2018)

[12] Wenhai Zhang. Design of Smart Home Security System Based on Internet of Things [D]. Xidian University, 2015. p.30-31.

[13] Chuanfu Zhang,Ao Hu. Must read for new mobile communication business development. People's Posts and Telecommunications Publishing House, (2005).