Development of the IoT module using MQTT Protocol and AES

Jr-Hung Guo *
Department of Electrical Engineering, National Yunlin University of Science & Technology
123 University Road, Section 3,Douliou, Yunlin 64002 , Taiwan, R.O.C †

Lin Tzu Yuan
Department of Electrical Engineering, National Yunlin University of Science & Technology
123 University Road, Section 3,Douliou, Yunlin 64002 , Taiwan, R.O.C

Kuo-Hsien Hsia
College of Future National Yunlin University of Science and Technology
123 University Road, Section 3,Douliou, Yunlin 64002 , Taiwan, R.O.C
E-mail: jrhung@yuntech.edu.tw, m10812021@yuntech.edu.tw, khhsia@yuntech.edu.tw

(leave space here should be 4 lines between *www.university_name.edu* and **Abstract***)*

Abstract

The efficiency and safety of the Internet of Things (IoT) have always been the focus of the development of IoT devices. Because the chips used in IoT devices generally have poor computing power, they cannot transmit data quickly and in large amounts, and use more complex security algorithms. Therefore, this thesis is to develop an IoT module with STM32 chip as the main controller. This module uses MQ Telemetry Transport (MQTT)[1] Protocol and AES encryption technology, and this IoT module can be operated directly with a browser. MQTT is a communication protocol for the Internet of Things, which was developed by IBM and Eurotech, and officially became an OASIS international standard in 2014. The purpose of development is to send and receive processing messages under narrow bandwidth and low energy consumption conditions. To ensure the security of IoT communications, we use AES encryption technology. Through this design, the communication of the entire IoT module is more efficient and safe. Finally, we applied this IoT module to the home security system, and the overall efficiency and safety have been verified. In the future, we will continue to improve related software and hardware so that this IoT module can be used in different fields.

Keywords: *Internet of Things (IoT), MQ Telemetry Transport (MQTT), AES, Home Security System.*

1. Introduction

The devices of the IoT have been widely used in our living environment, and these devices have brought many conveniences to our lives. However, the efficiency and safety of these devices are still very hot topics. In previous studies such as Parkhomenko, Anzhelika, et al. [2], the efficiency and safety of Smart House Systems have been studied. It concluded that the safety of Smart House Systems still needs to be strengthened. AHMAD, Farhan, et al. [3] researched the safety of VANET (Vehicular Ad-hoc NET) Because VANET has a great relationship with people's life and property safety, how to ensure the safety of communication and information is

.

very important. MENEGHELLO, Francesca, et al. [4] researched the security issues of the Internet of Things and proposed related solutions. NAIK, Nitin. [5] compares and analyzes the efficiency and security of several commonly used IoT communication protocols such as MQTT, CoAP, AMQP and HTTP.

From previous research, we can find that the communication efficiency and security of IoT are still important research topics. Therefore, this article uses the STM32 chip to develop an IoT module and uses the MQTT protocol as the entire system communication protocol. MQTT is a communication protocol invented in 1999 by Dr. Andy Stanford-Clark of IBM and Dr. Arlen Nipper of Arcom (renamed Eurotech) [6]. This protocol was originally designed to allow IoT devices to effectively transmit messages even with limited bandwidth and computing power. And this agreement also became an international standard of OASIS (Organization Advancement Structured Information Standards) in 2014. Although this standard is designed for communication between IoT devices, large network service providers such as Facebook Messenger[7] and Amazon Iot[8] also use the MQTT protocol. It can be seen that the MQTT protocol is still one of the important protocols for network communication and IoT systems. Therefore, we chose MQTT as the main communication protocol of the Internet of Things system in this paper.

In this paper, we have also modified the MQTT protocol, so that the original MQTT protocol, which can only be transmitted in one direction and cannot be operated, becomes a system that allows users to operate. Punctuation marks are used at the end of equations as if they appeared directly in the text. In order to ensure the security of the entire system, we have also adopted AES to ensure the security of the communication and data of the entire system.

Through the integration of MQTT and AES, and the IoT module developed in this paper using STM32 chips, the relevant software and hardware of this paper can provide a safe and efficient system. And used in different fields.

2. System Architecture

MQTT is a communication protocol invented in 1999 by Dr. Andy Stanford-Clark of IBM and Dr. Arlen Nipper of Arcom (renamed Eurotech). They were in order to provide a lightweight and reliable binary communication protocol between the oil pipeline sensor and the artificial satellite under the premise of the narrow network bandwidth and small power loss. MQTT originally stood for Message Queueing Telemetry Transport. This kind of expression is no longer used. MQTT is MQTT, not an abbreviation of other words.

Because the message content of the MQTT protocol is very streamlined, it is very suitable for IoT devices with limited processor resources and network bandwidth. Many MQTT libraries have been developed for Arduino control boards (C/C++), JavaScript (Node.js, Espruino control boards), Python, etc. There is also an open source MQTT server, which makes it very easy to develop the MQTT IoT and the communication between machines (Machine-to-Machine, M2M).

The advantage of MQTT is that it is a lightweight protocol. Since it is a protocol designed for the Internet of Things, the network bandwidth it requires is very low. And the required hardware resources are also low. It is very suitable for IoT environments with low power consumption and limited network bandwidth. Such as smart appliances or medical devices.

MQTT uses the Publish/Subscribe mechanism for messaging, which contains 4 main elements, Publisher, Subscriber, Topic, and Broker. Among them, the IoT module is the Publisher, and the information that the IoT module needs to send out is the Topic. And these information Topics will not be sent directly to the demand-side Subscriber, but sent through the Broker. So the Publisher and the Subscriber are not directly connected. But because of this, the information and communication security of the entire IoT system must be controlled through a Broker.

At present, most Brokers have SSL (Secure Sockets Layer) encryption mechanism when transmitting data, but SSL is too complicated for IoT devices. Therefore, this paper uses AES (Advanced Encryption Standard) technology to ensure the security of all communication and data in the communication of the IoT module and the communication of the Broker.

Finally, we also modified the MQTT architecture. Because the original MQTT architecture Subscriber can only simply respond to whether it has received a Topic from the Publisher. But in the application of the IoTs system, in many cases, the Subscriber needs to send messages or control the Publisher. Therefore, the revised MQTT architecture of this paper is shown in Fig. 1.

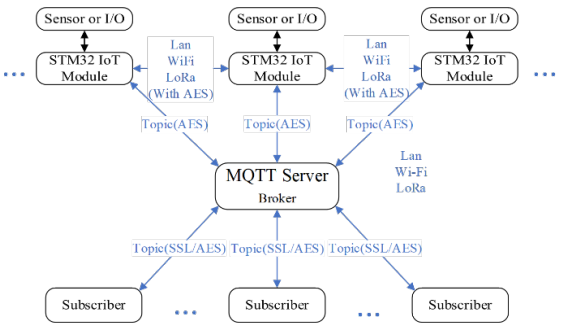


Fig. 1. The Revised MQTT Architecture Diagram of This Paper.

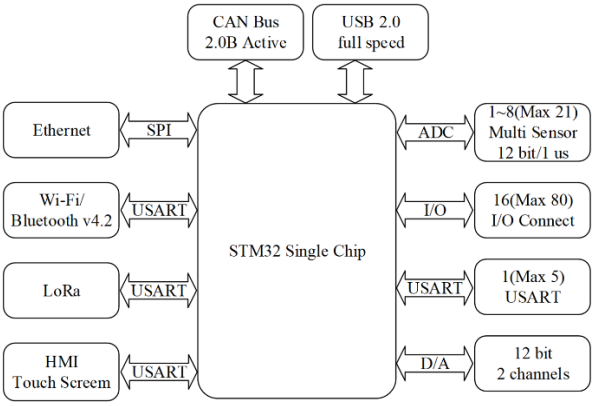


Fig. 2. Base on STM32 Chip IoT Module Block Diagram.

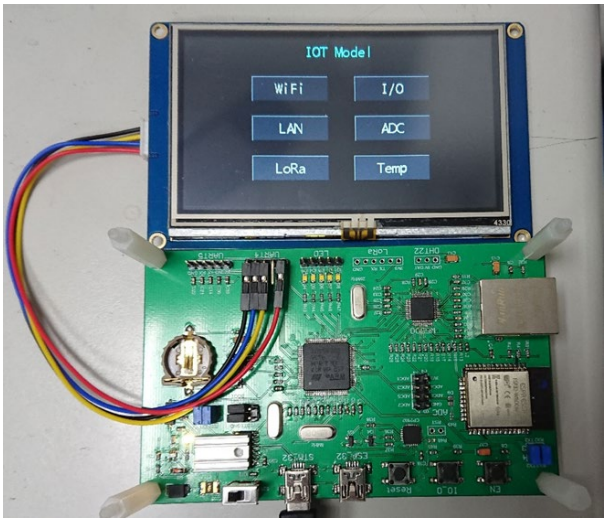
2.1. *Hardware Architecture*

The IoT module developed in this paper uses a 32-bit STM32 series microcontroller. This series of microcontrollers are designed based on ARM Cortex™-M. Mainly to provide MCU users with new development freedom. It integrates high performance, real-time functions, digital signal processing, low power consumption and low voltage operation. At the same time, it is highly integrated and easy to develop. For the IoT module developed in this paper, the microcontroller we chose is STM32F103VET6. It is an integration CPU, RAM, ROM, a variety of I/O ports (including display drive circuit, PWM, analog multiplexer, A/D converter, etc.) and interrupt system, timer/counter and other functions constitute a microcomputer system. Because of its better stability and low price, this paper chooses this chip as the main controller of the IoT module.

In the communication interface part, the IoT module developed in this paper can connect to Wi-Fi, Ethernet, and USART (Universal synchronous/asynchronous receiver transmitter), LoRa (Long Range) etc. for the communication interface. Moreover, this IoT module adopts a modular design, so you can choose to use different communication modules according to different needs. And in order to ensure the security of data and communication, we use AES encryption technology in this IoT module. Let this IoT module provide secure data communication and transmission. The block diagram of this IoT module is shown in Fig. 2.

3. Experimental Results

We use STM32 chip as the main controller of the IoT module developed in this paper. This module adopts modular design, so most of the communication interface can be replaced according to needs. And we also add a touch LCD to this IoT module. When necessary, we don't need to connect with the host, and directly operate through the touch LCD. In addition, we also added the function of Web Server to this IoT module. Allow users to directly use the browser to control this IoT module. But for the sake of security, the MQTT setting still has to be set through the Broker. Through this design, the IoT module we developed is both convenient and safe. Fig. 3 shows the browser interface of the IoT module developed by us, and the screen of the entity with the touch LCD and the IoT module connected with the browser.



(a)IoT Module.

(b)IoT Module Browser and LCD Screen.

Fig. 3. STM32 chip IoT Module and Screen.

3.1. *MQTT Broker System and Experiment Results.*

In the MQTT Broker, we use Visual Studio 2017 C# to develop our system. The picture of this system is shown in Fig. 4. In this system, users can define the map of the environment and the related attributes of the IoT module. And the I/O or A/D related parameters of which IoT module the Topic corresponds to. In addition, this system also provides an automatic search function. The system can automatically search for a Ethernet or Wi-Fi was the IoT devices having MQTT function. After searching, it will automatically name the I/O or A/D on the device based on the IP. This simplifies the user naming operation, and the system management of MQTT Topics will be more efficient. The rules for this automatic Topics naming are as follows:

Topic Rule:

INDEX,I/O Type,I/O Locate,IP, PORT

Table 1. Topic Rule Description

Field	Description
INDEX	After the IP of the IoT module is found, the sequence of saving it into the system.
I/O Type	I/O category, such as I/O, A/D, D/A, etc.
I/O Locate	I/O Type corresponds to the physical location of the IoT module.
IP	IoT module IP
PORT	The communication port used by the IoT module.

Finally, we apply the IoT module developed in this paper and the MQTT system to home security. We connect the IoT module to the temperature and humidity sensor and integrate it with the MQTT system we developed. The result is shown in Fig. 5.

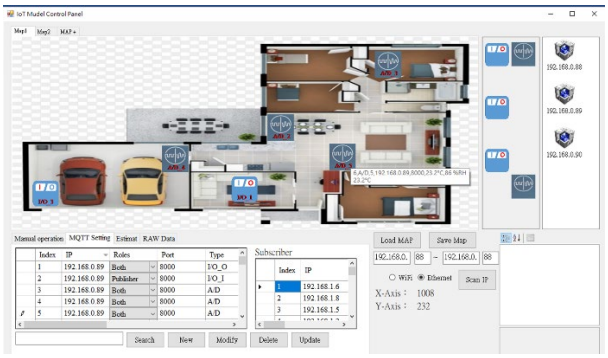


Fig. 4. MQTT Broker Software System with MQTT Topic Names Sample.

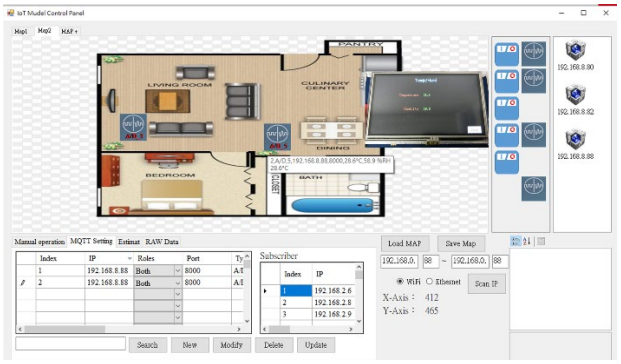


Fig. 5. MQTT Broker System with IoT Module.

4. Conclusions

This paper uses STM32 chip to develop a multi-functional IoT module, and uses MQTT protocol to develop an application system. Finally, the software and hardware are integrated and applied to the home security system. The performance and condition of the entire operation are very good. At present, we put the MQTT management interface and the user's operation interface together. Although this design has its convenience, there may be doubts in practical application and safety. Therefore, in the future, we will separate the management interface from the user's operating interface, and convert this system to a web. I believe that the overall ease of use and safety can be improved. In the future, we will continue to add artificial intelligence and more sensor functions. In addition to being used in home security, this system can also be used in different fields such as smart cities and Industry 4.0.

5. References

1. http://public.dhe.ibm.com/software/dw/webservices/ws-mqtt/mqtt-v3r1.html,2020/12/01
2. Parkhomenko, A., Tulenkov, A., Sokolyanskii, A., Zalyubovskiy, Y., Parkhomenko, A., & Stepanenko, A. (2018, March). The application of the remote lab for studying the issues of Smart House systems power efficiency, safety and cybersecurity. In International conference on Remote engineering and virtual instrumentation (pp. 395-402). Springer, Cham.
3. AHMAD, Farhan, et al. A comparative analysis of trust models for safety applications in IoT-enabled vehicular networks. In: 2019 Wireless Days (WD). IEEE, 2019. p. 1-8.
4. MENEGHELLO, Francesca, et al. IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet of Things Journal, 2019, 6.5: pp. 8182-8201.
5. NAIK, Nitin. Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In: 2017 IEEE international systems engineering symposium (ISSE). IEEE, 2017. p. 1-7.
6. http://www.steves-internet-guide.com/mqtt/,2020/12/01
7. https://www.facebook.com/notes/facebook-engineering/building-facebook-messenger/10150259350998920,2020/12/01
8. https://aws.amazon.com/tw/blogs/aws/aws-iot-cloud-services-for-connected-devices/,2020/12/01