EasyChair Preprint

№ 710

A Security Access Control of the Industrial Wireless Sensing System

Yun Sheng Yan, Hai-Feng Chang, Jun Tao and Yun-Ling Zhang

January 3, 2019

A Security Access Control of the Industrial Wireless Sensing System

Yun-Sheng Yan[1], Hai-Feng Chang[1], JunTao[2], Yun-Ling Zhang[2]

[1]Guangxi University of Science and Technology, Guangxi, China

[2]Anhui Institute of Information Technology, Anhui, China

simbayen@gxust.edu.cn, 1105307533@qq.com, taonian@126.com , 983146151@qq.com

Abstract Access sensing system can be roughly divided into two categories: one is traditional, mainly based on different structures of locks with a key or a set of buttons (or a dial) for combinational codes to unlock; another type is digitally scientific, mainly consisted of electronics constructed with electromagnetic induction mechanism of locks applying a barcode card, RFID, fingerprint (palm print) identification system, or radio remote control to unlock. This paper tries to adopt the Frequency Hopping Spread Spectrum (FHSS) transmission function through the Bluetooth and multi-authenticated encryption technology, along with the open operating system of the smartphone --- Android, to establish a secure and reliable control system, to improve the weakness of the old style access sensing system, and to enhance the security on the management of access sensing system.

1 Introduction

Access sensing system [1] can be roughly divided into two categories: one is traditional, mainly based on different structures of locks with a key, or a set of buttons, or a dial for combination codes to unlock; another type is digitally scientific, mainly consisted of electronics with electromagnetic induction mechanism of locks with a barcode card, RFID, fingerprint (or palm print) identification system, or radio remote control to unlock. However, some problems can happen while adopting those different approaches of access sensing system, including forgetting to bring the key, barcode card reading error, high cost for RFID and finger identification system, as well as the interference of radio remote control, etc. For these reasons, this study tried to improve the disadvantages and to reinforce the security [2] of access sensing system through the application of Android used on smartphone [3] with the Bluetooth [4] apparatus along with encryption technology.[5]

On the smartphone, this study chooses the cell phone models with Android working as the operating system mainly because Android is constructed on the

Kernel of Linux 2.6 and it uses Java programming language for system development, which is a portable computer language and can be executed on various system platforms. Not only Java is more popular on the design of the programming development, the most important factor lies on that Android provides more freedom for developers on writing applications due to its system structure of open source. Bluetooth is selected mainly because it employs Frequency-Hopping Spread Spectrum (FHSS) to transmit the signals in order to avoid the interference and being intercepted. Furthermore, Bluetooth requires multilayer encryption and authentication while building connections and transmitting, with which data can be better secured. In addition, each Bluetooth apparatus supports connections up to seven devices simultaneously, giving the system more flexibility in its application. Finally, the chips for Bluetooth are very common in the market, so they are easily available at a lower price.

The motivation of this paper focuses on improving previously mentioned disadvantages of traditional access sensing system and parts of the digital access sensing system. Based on the reasons above, a secure and protective access sensing system can be achieved by using the smartphone, which runs on Android system and is easily available, as well as the authentication and encryption technology of Bluetooth.

The rest parts of this paper are: chapter two demonstrates the methodology; chapter three describes the implementation procedures; chapter four indicates the experiment results; and chapter five concludes the research and proposes for future studies.

2 Related studies

2.1 Bluetooth

Bluetooth was initiated by Ericsson, one of the world largest cell phone companies, and followed by IBM, Nokia, Toshiba and Intel. Its primitive purpose was to replace IrDA and to increase the information transmitting efficiency between personal communicative devices, e.g.: PDA, mobile phone, laptop computer, printer, and so on, to form a personal area network (PAN) in a short distance. The Bluetooth standard is IEEE 802.15.1, which applies radio technology in transmission and the license-free band is reserved particularly for industrial, scientific and medical purposes, called ISM (Industrial Scientific Medical) band. The designated section for ISM band is 2.4GHz, and the communicative band between 2.402 ~ 2.435GHz is divided into 79 channels, and the bandwidth for each channel is 1MHz. It utilizes frequency-hopping spread spectrum (FHSS) scheme, with 1600 hops per second and the maximum range of the signal transmission reaches 100 meters in an environment of no obstacles.

For the strict requirement of this study on the security of the access sensing system, it's impossible to access to the controlled system from a long distance when trying to activate the access sensing system. Besides, packet delivery is only for the purpose of identity authentication and activation of the access sensing system, thus a too rapid transmission rate and a long distant range of transmission are not essential. To prevent the packet delivery from being interfered or intercepted, it requires a protective mechanism to insure the security. Because the access sensing system needs to go through authenticating authorized identities, it has to equips a functional network structure mode of low cost in construction, so as not to diminish the user's interest in using it, and that is the major goal of this study to design this access sensing system.

2.2 Network architecture

In the environment of Bluetooth, it's basically a one-on-one connection mode, but the connection can be constructed among 8 Bluetooth devices in the real application. A network mode like this is called Piconet, which includes a master device with 7 slave devices and each device can act as a master or slave device at any time. The two roles of them can be defined as:
Master: an initializing device for information exchange.
Slave: a device responding to the master device. The constructed architecture is shown as below Fig. 2.1.

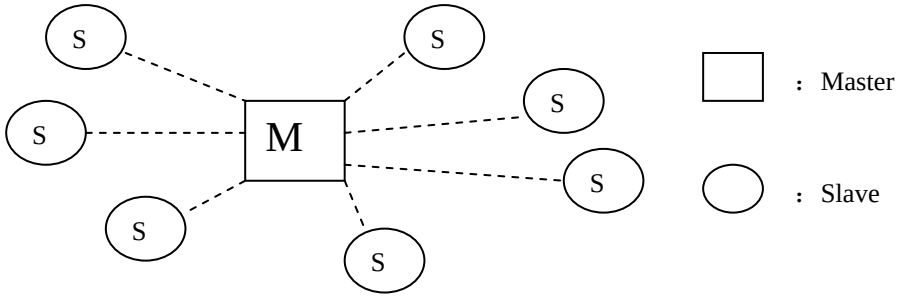

Figure 2.1 Bluetooth Piconet structure

2.3 Connection mode

When the Bluetooth stays in connection mode, there are several modes:

(1) Standby: In this mode, the Bluetooth itself is not functioning, no data-transmission and the radio is not activated; the purpose is to execute saving energy.

(2) Inquiry: This mode is a procedure prior to executing connection; the purpose is to explore all the applicable Bluetooth devices in the surrounding.

(3) Page: To establish the connection with each other, the master device is ordered by programming to call the other slave devices.

(4) Active: This is an ordinary working mode when transmitting data among the devices; in this mode, there are continuous signals of inquiry and paging executed by the devices.

(5) Hold: In this mode, the device stops supporting ACL connection transmission, but still supports SCO connection; the purpose is to spare the time slot of the physical channel for other usage, so as to increase the efficiency of the Bluetooth in the network.

(6) Sniff: In this mode, the slave device will be assigned to a previously defined time slot to search periodically for data string.

(7) Park: The main purpose of this mode is to execute a sleeping energy-saving mode; the device will wake up instantly at a specific notification.

The connection mode of the Bluetooth is shown as Fig. 2.2.

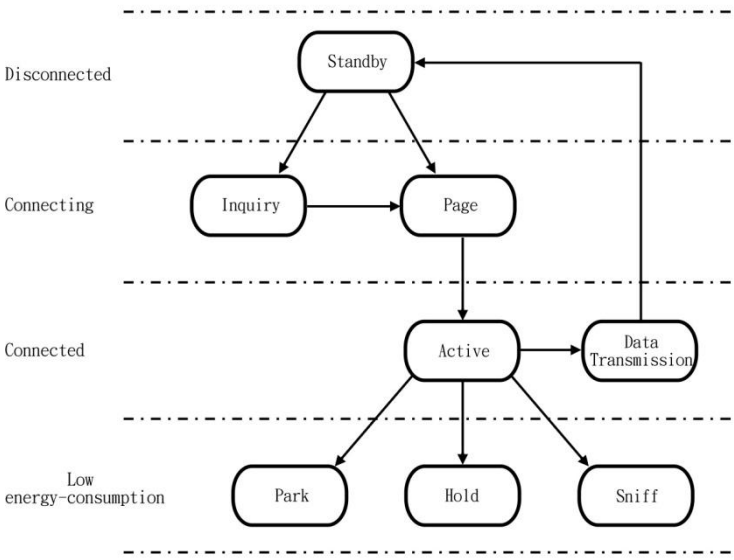

Figure 2.2 The connection mode of the Bluetooth

2.4 Security and encryption

Wireless transmission [6,7] is the key point in the development of the Bluetooth. But, wireless transmission comes with a big weakness, which is the radio interception in the air by anyone using related devices without being detected.

Therefore to ensure the confidentiality of wireless transmission is a vital issue in this paper.

The security mechanism of Bluetooth is divided into three parts: key management, encryption and authentication. In each Bluetooth device, four mechanisms are applied to protect the security of the link layer:

(1) Bluetooth Device Address (BD_ADDR): each Bluetooth device owns a unique address of 48 bits, regulated by the IEEE standard, when it is manufactured.

(2) Private Authentication Key: a random value generated with 128 bits in length, which is used for authentication.

(3) Private Encryption Key: a value with a length between 8 bits and 128 bits used for encryption.

(4) RAND: a random value in 128-bit length created by the Bluetooth device itself.

In the encryption engine of the Bluetooth, a random value is generated for initialization, and after that, four inputs are added into the encryption engine:

(1) A number for executing encryption or decryption.

(2) The address of the master device.

(3) The time slot in the master clock.

(4) A secret key shared between two devices.

In the Bluetooth network, the master device address and the time slot of the master clock keep each other informed, and the application of the keys makes the encryption more diversified. During the process of authentication, the master device that executes authentication requires more than just a key from the slave device, because the key can be intercepted in the midway easily, instead the master device creates a random value and send it to the slave device, and requests the slave device to use it as a key to be encrypted, and then the encrypted number is sent back to be authenticated. Meanwhile, the master device can use the returned random value as a key to be encrypted again and sends the encrypted random number to the slave device to be compared. If the encrypted random number matches, it indicates that the two devices both possess a same key, thus both identities are confirmed.

SAFER+ (Secure and Fast Encryption Routine) Algorithm [8, 9] is applied by the Bluetooth in the encryption mechanism to create keys. SAFER, presented by the Swiss Federal Institute of Technology and the American Cylink Corporation in 1993, is an algorithm using block cipher with a length of 64 bits. Later on, it evolves into SAFER+ converting a 128-bit text into a 128-bit cipher. The encryption keeps repeating, at least 6 times, and at most 10 times. The processes for encryption and decryption are different, and that makes it unique from other algorithms. Only byte-based computing needs to be operated. This design focuses on the application on smart cards, to avoid the limitation of calculating ability.[10, 11,12]

2.5 Authentication

The Bluetooth authentication mechanism is a process to verify the key shared by the devices. The process can be executed at any time. In the process of authentication, the master device transmits a random number, after that, both devices use the random number, the slave device address (BD-ADDR) and the current link key as inputs to create a response (SRES); the slave device will transmit a response to the master device for comparison, if it matches, then, it passes the authentication. The process of authentication is shown in Fig. 2.5.

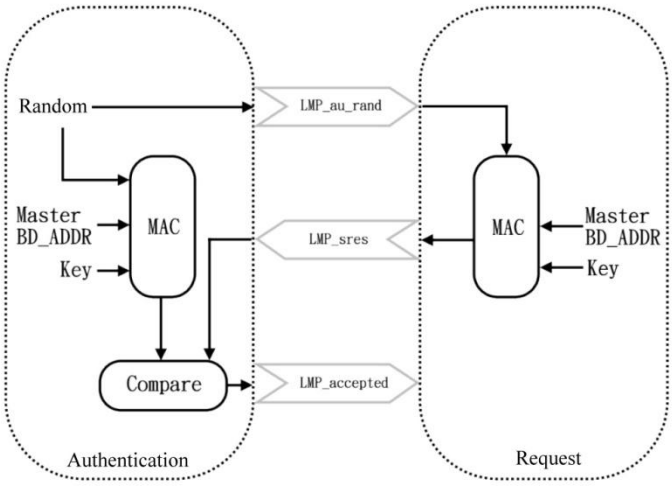

Figure 2.3The authentication process of the Bluetooth encryption engine

The process of authentication generally is operated before connection and encryption. But in Bluetooth, it can be completed independently outside the encryption process. This purpose is to verify if the communication has begun with the authenticated device.

The process combining authentication and the link key is called pairing. In the application, pairing can be replaced by the security information of the higher layer, which is called bonding. After pairing, another authentication may be processed and the link key will be used as a shared secret key.

3 System design and implementation

Current various digital access sensing systems authenticate identity through the user's physical objects (e.g., fingerprint, RFID card), therefore a physical corresponding access control device needs to be established outdoor. Common access sensing systems are shown in Fig. 3.1.

Fingerprint	RFID
	1. 

Figure 3.1 Common access sensing systems

An access control device established outdoor is vulnerable to get damaged. To prevent the information security issue from happening, the design of this paper establishes the receiver of the access control device inside the house. By sending radio signals through a Bluetooth device to the receiver of the access sensing system indoor for authentication, this method can avoid the physical access control device from being destructed.

3.1 Receiver of the access sensing system program

This paper chooses to use Bluetooth receiver with USB for the hardware device to authenticate identities, because it equips a capability of connecting to smartphone for authentication, excludes unnecessary complicated multimedia functions and is easily available on the market. A Bluetooth receiver with USB is shown in Fig. 3.2.

Figure 3.2 Bluetooth receiver with USB

This paper based on Visual Basic designs a program to authenticate and to control the access sensing system. The procedure of creating an authentication code is shown in Fig. 3.3.

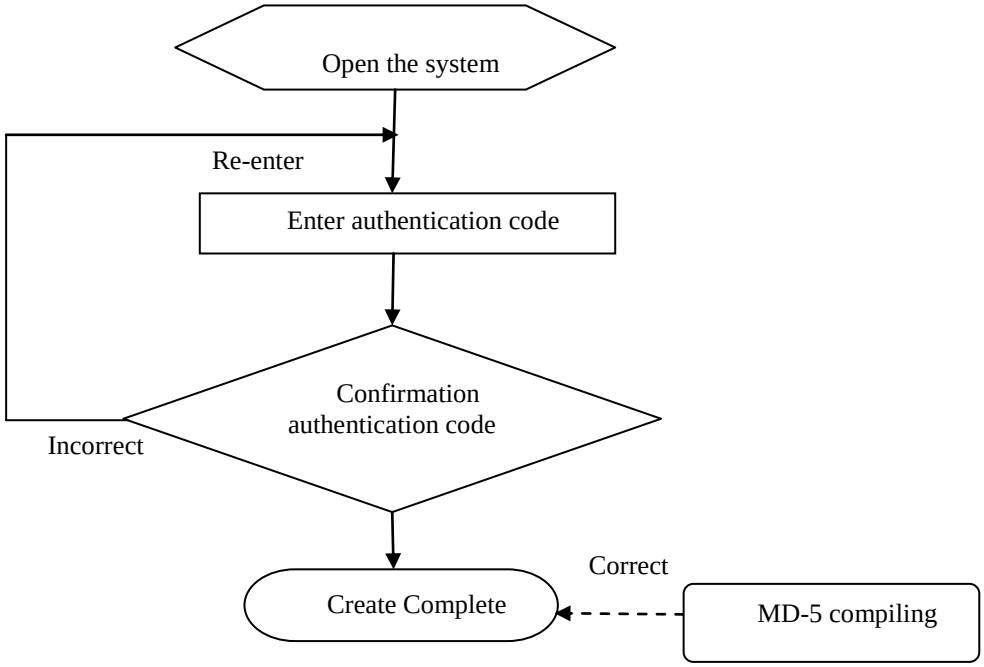

Figure 3.3 Procedure of creating an authentication code

The system picture is shown in Fig.3.4.

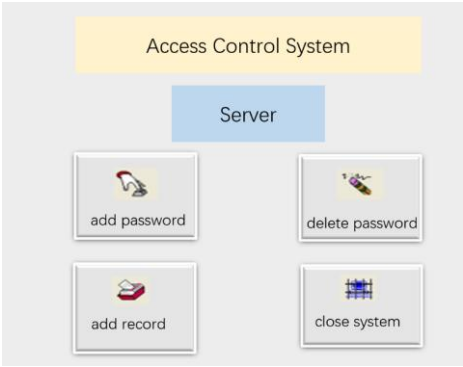

Figure 3.4 Picture of the system

Before operating the access sensing system of this paper, the manager has to set up an authentication code through the procedure of creating a new authentication code in the server program. The authentication code accepts English, numbers and

signs. After the code is entered and the Enter key is clicked, the system will display the code that is just input and a code after MD5 algorithm [7] for comparison and authentication. If an error appears, user can close the window and enter the input again. If the code is correct, then choose the “Enter” key and the system will save the code that is just entered in the system and finish the procedure of creating a new authentication code. The picture of creating a new code for the system is shown in Figs. 3.5 and 3.6.

Figure 3.5 Creating a new code of the server

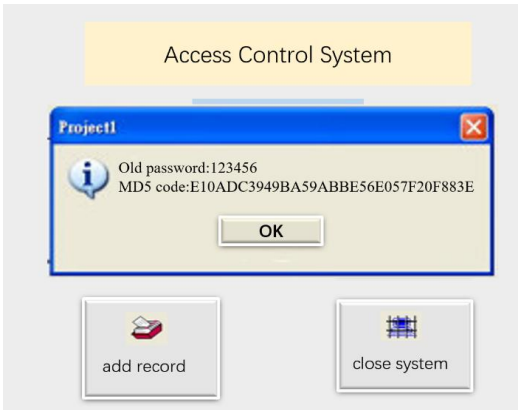

Figure 3.6 Confirmation for the new created code of the server

This paper is in experimental period and only one log-in code can be set up. Meanwhile, based on security principle, user has to delete the previous data in order to create a new code if the code needs to be changed. The picture of deleting a code is shown in Fig. 3.7.

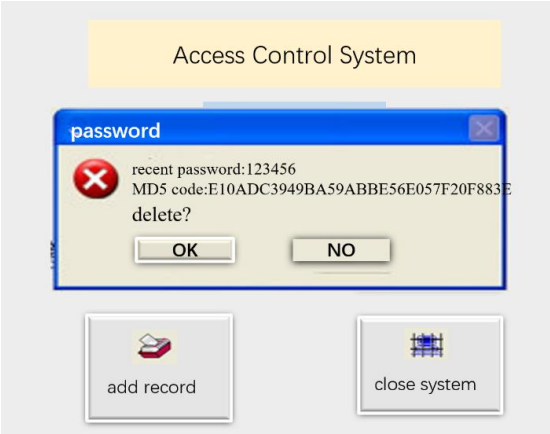

Figure 3.7 deleting a code of the server

Prior to the connection and interaction between the smartphone and the server, both of them have to complete pairing. Because the Bluetooth operation mode is based on that the device initiates connection is called the client and the other device that offers service is called the server, so this system has set the smartphone as a client to connect the server. In executing paring, the manager needs to open the device name of the Bluetooth server for initiating service discovery protocol, allowing the smartphone to find the server. Then the server will request a 4-digit input in order to create a link key. After the input is entered and sent, a request for entering a code will appear on the smartphone during pairing. Pairing will be finished after entering the same code as the server. Both the server and the client will keep records of the pairing data. So, no need to run pairing again after that. When completing a successful pairing, close the device name to avoid being detected.

While the access sensing system is running the program, the server will compare the authentication code sent by the smartphone with the code saved on the previous newly created code procedure. This paper demonstrates the authentication diagram with the following pseudo code.

3.2 Client of the access sensing system program

When accepted message after authentication has been received, the access sensing system program transmits signals through RS-232 interface to the magnetic lock on the door to shut down power supply, thus the door is open. As for the authentication code transmitted by the smartphone, this paper designs an APP tool, called “Key to the Access Control”. The picture of input the authentication code of the client APP is shown in Fig. 3.8.

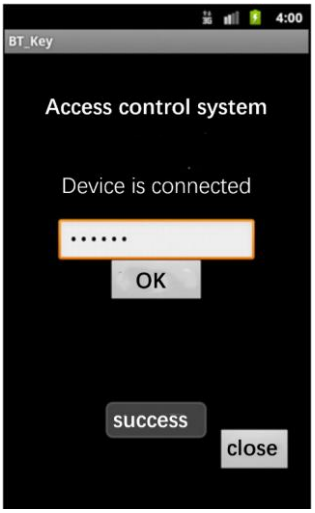

Figure 3.8 Input the authentication code of the client APP

On the design of the program code for the client, because Android itself supports encryption mode, this paper designing the program of "Key to the Access Control" calls for the encryption library of MD5 from the main program. It shows as below:

import java.security.MessageDigest

After clicking the Enter key, the program will transmit the text to MD5 compiler to be compiled. By means of Bluetooth system, the compiled text is transmitted to the server for data authentication. The program code of the design is shown as below:

```
1.  public String encryptmd5(String str) {
2.          char[] a = str.toCharArray();
3.          for (int i = 0; i < a.length; i++)
4.          {
5.                  a[i] = (char) (a[i] ^ 'l');
6.          }
7.          String s = new String(a);
8.          return s;
9.      }
10.             public String MD5(String str)
11.     {
12.         MessageDigest md5 = null;
13.         try
14.         {
15.             md5 = MessageDigest.getInstance("MD5");
16.          } catch(Exception e)
```

```
17.     {
18.        e.printStackTrace();
19.        return "";
20.      }
21.     char[] charArray = str.toCharArray();
22.     byte[] byteArray = new byte[charArray.length];
23.     for(int i = 0; i < charArray.length; i++)
24.     {
25.        byteArray[i] = (byte)charArray[i];
26.      }
27.     byte[] md5Bytes = md5.digest(byteArray);
28.     StringBuffer hexValue = new StringBuffer();
29.     for( int i = 0; i < md5Bytes.length; i++)
30.     {
31.        int val = ((int)md5Bytes[i])&0xff;
32.        if(val < 16)
33.        {
34.           hexValue.append("0");
35.         }
36.        hexValue.append(Integer.toHexString(val));
37.      }
38.     return hexValue.toString();
```

The following is the code description of the program code above:

Line 1 & 2, define “a” as a string variable, and set “a” as an array.

Line 3 ~ 9, execute string “a” length loop, and include the string into the array. After that, define a string “s”, and re-define “a” into the string “s”.

Line 10, start to read MD5 string library.

Line 12, first of all, clear the message.

Line 13 ~ 20, define “md5” variable as an empty value, and make sure to escape the undergoing encryption when an exceptional situation is encountered.

Line 21 & 22, define string array and character array, and put the previous defined array into the program.

Line 23 ~ 26, by means of a loop, put the character array, word by word, into the bit array to execute encryption.

Line 27, define “md5Byte” variable as a bit array, and put the value of the previous bit array into it. Then, wait for conversion.

Line 28 ~ 35, define “hexValue” variable for encryption, and start encrypting the value of md5Byte. At the end, take the last 16 characters, and add 0 if it is less than 16 characters.

Line 36, execute converting procedure.

Line 38, resume the value to its original value before conversion, and keep going converting the next character.

Fig. 3.9 shows the authentication diagram of the system.

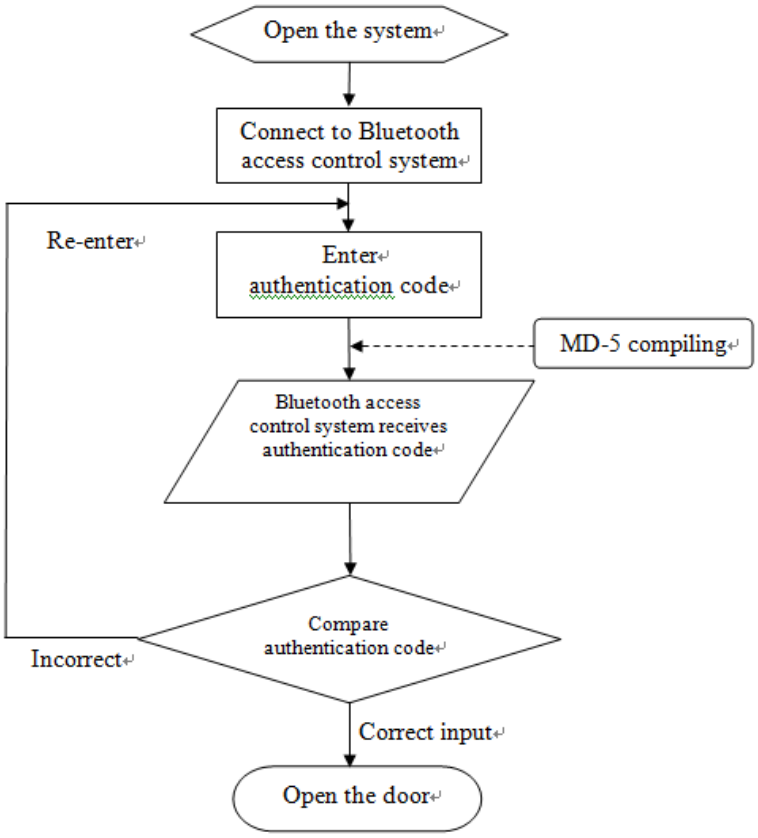

Figure 3.9 Authentication diagram of the system

The manager can install the APP "Key to the Access Control" on any smartphones that run on Android 2.3.3. Before operation, the smartphone needs to contact the Bluetooth receiver, which is connected to the server through USB, requesting for ID authentication for the first time. While comparing the ID, the Bluetooth master will request the Bluetooth slave to input the link key for authentication. After the authentication is completed, disable the Service Discovery Application function to avoid being illegally detected. Afterward, when using the APP "Key to the Access Control", the manager has to make a connection between the smartphone and the Bluetooth receiver on the server. A connected message will display on the APP system screen after they both successfully connected. Input the authentication code and select "Enter". The system will use MD5 algorithm to recompile the authentication code, and the recompiled code will be transmitted to the access sensing system in the server for authentication. If the authentication is correct, the system will transmit an "Open" message to the IC card, and then the IC card will drive to open the magnetic lock controlled by the access sensing system.

The IC card is shown in Fig. 3.10.

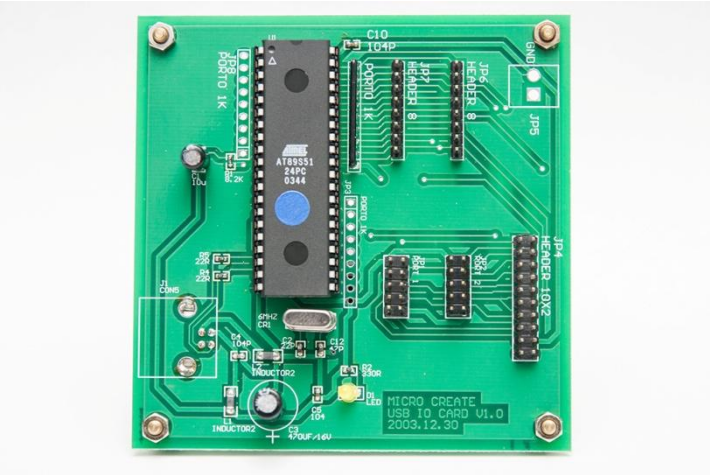

Figure 3.10 IC card

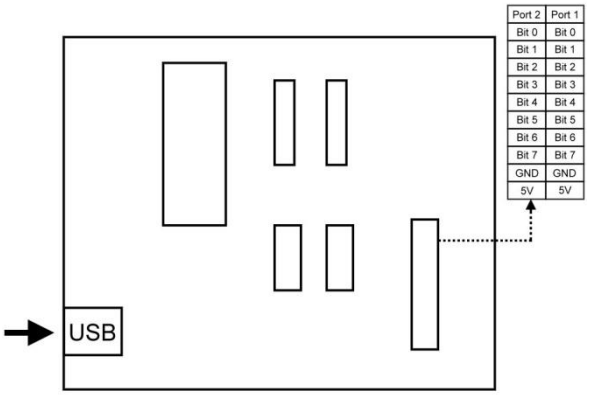

Figure 3.11 Diagram of the IC card

As shown in Fig. 3.12, the smartphone transmits an authentication code to the access sensing system in the server for authentication. If the comparison is correct, the server transmits a command to terminate power supply through the USB module on the system, and then to the IC card. The control chip on the IC card will transmit signals to the contacts of Bit 0 and GND on Port1. And the command will be relayed to the Solid State Relay (SSR) to execute cutting off the power, thus the magnetic lock controlled by the access sensing system will be opened. Fig. 3.12 of the completed system.

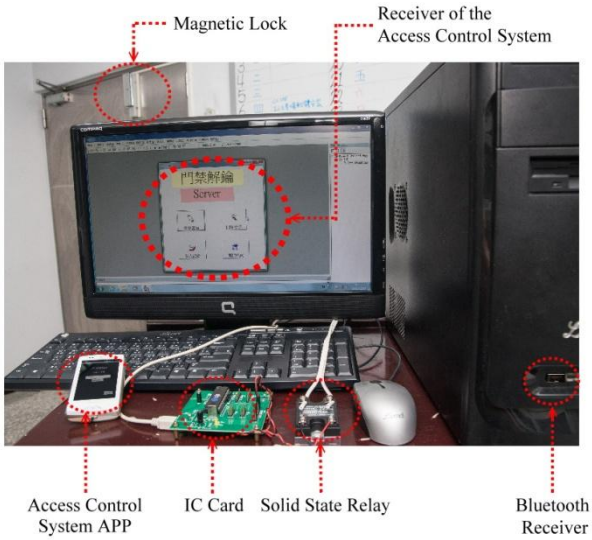

Figure 3.12 Completed system

4 Experiment results

4.1 The System architecture

The system hardware designed by this paper utilized USB Bluetooth receiver, which was easily available, and the system was installed on an over five-year functional personal computer as a server for the purpose of authentication. By using the built-in RS-232 on the computer main board, the system transmitted a control message to the magnetic lock to unlock the door, shown in Fig. 4.1.

Figure 4.1 Magnetic lock

4.2 Experiment results

On the experimental execution, this paper first completed ID authentication between the two devices, the smartphone and the server. After that, the Service Discovery Application of the Bluetooth connected to the server was disabled to avoid the relative data being detected. The first security gate had been built. Then, an authentication code: mytest was created through the new created authentication code procedure. After MD5 Algorithm, the recompiled code became a long and irregular integral number: 1jPGCyu5B$zAcKkxrJvOOumFyDKOuaD1, which was saved in the server waiting to be compared. The second security gate had been built.

Before executing authentication, this paper made a connection between the smartphone and the server through a Bluetooth receiver. After the authentication code was entered and the "Enter" key was clicked, the data was converted and compiled with the Bluetooth Frequency-Hopping Spread Spectrum (FHSS) technology, which transmitted the compiled signals of the authentication code in a hopping frequency of 1600 times per second to avoid the data being intercepted. The third security gate had been built. At the same time, with the Bluetooth technology itself possessing unique original security designs which included a variety of keys and algorithm mechanisms, the fourth security gate had been built. After comparing with common access sensing systems, this paper concluded the advantages and the disadvantages of the traditional, digital and the Bluetooth access sensing systems as below.

Table 4.1 Traditional, digital and Bluetooth access sensing systems compare list

	Traditional (Keys)	Digital (fingerprint)	Bluetooth
Lost	Rebuild a new key	None	Use another Android smartphone to install the APP again
Destructed	Easily	Easily	Constructed indoor; safe and unharmed
Interfered	None	By dust and dirt	With FHSS transmitting technology, little interfered
Security	None	Personal fingerprint; high security	Multi signal encryption technology; high security
Cost	Low	High	Medium

5 Conclusions

This paper in the experimental period not only improved the disadvantages of forgetting to bring the keys in the traditional access sensing system, reading abnormally in the barcode reading access sensing system, the high cost of RFID and fingerprint identification system, and being interfered in the radio remote controlled access sensing system, but also actually achieved the goal of protection by using the Bluetooth access sensing system. In considering of the convenience of the establishment and the cost, this Bluetooth Access Sensing system allowed tight budget units to easily set up a secure and efficient access sensing system in the computer servers room. In the current executing process, it was discovered that the only problem of using this type of digital electric access sensing system lied on the dependence on the usage of electricity. Whenever the power supply was terminated, this would cause the access sensing system failed to work and everybody could get in and out easily without obstacles. Under this circumstance, the Bluetooth access sensing system of this paper needed to go with an Uninterruptible Power Supply (UPS) to maintain the power required by the system, in order to insure the security management. In the future, because this access sensing system based on temporarily research purpose using only one authentication code, it would require different authentication codes for different managers in the future applications, in order to keep records of access and exit and to fulfill the experimental requirement of joint management by a group of managers.

References

1 Il-Kyu Hwang and Jin-Wook Baek. Wireless Access Monitoring and Control System based on Digital Door Lock[J]. IEEE Transaction on Consumer Electronics, 2007:53(4),1724-1730.

2 PekkaKanerva.Anonymous Authorization in Networked Systems: An Implementation of Physical Access Control System[D]. Department of Computer Science and Engineering.

3 Graham Kirby. Integrating Bluetooth Technology into Mobile Products.Intel Techno;ogy Journal Q2,2000:1-7.

4 http://www.Bluetooth.org,Bluetooth SIG

5 J.L. Massey, "SAFER K-64: A byte-oriented block ciphering algorithm," in Proceedings of 1st Workshop on Fast Software Encryption." pp. 1-17, Springer-Verlag, 1993.

6 M. Agiwal, A. Roy, and N. Saxena, "Next generation 5g wireless networks: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1617–1655, 2016.

7 GPP TR 38.900 v2.0.0, Channel model for frequency spectrum above 6 GHz, 3rd Generation Partnership Project, Technical Specification Group Radio Access Network, Technical Report,2016.

8 J.L. Massey, G.H. Khachatrian, and M. K. Kuregian, "SAFER+," First Advanced Encryption Standard Candidate Conference, August 20-22, 1998.

9 Lu, Y., W. Meier and S. Vaudenay. "The Conditional Correlation Attack. A Practical Attack on Bluetooth Encryption." Crypto'05, Santa Barbara, Aug 05, 14-18. Bernstein D.J. Cache-timing attacks on AES, 2005

10 JunTao, YangShen. "A distributed heuristic multicast algorithm based on QoS implemented by SDN." 2017 3rd IEEE International Conference on Computer and Communications (ICCC)[C] 2017(1):23-29

11 Mahmoudi S A, Belarbi M A. Towards a Smart Selection of Cloud Resources for Multimedia Big Data Computing[C]//3rd NESUS Winter School and PhD Symposium on Data Science and Heterogeneous computing. 2018.

12 ZF Mao, YM Jiang, GY Min,SP Leng, XL jin, K Yang. "Mobile social networks: Design requirements, architecture, and state-of-the-art technology," Computer Communications,vol. 100,Mar. 2017,pp. 1-19. https://doi.org/10.1016/j.comcom.2016.11.006