MANTECH Publications

Journal of Android iOS Development and Testing
Volume 7, Issue 2, May-August 2022

# *Using an Android Application to Perform Password-Protected Remote Door Unlocking and Entry*

***Akansha Saxsena[1], Rahul Choudhary[2], Alok Tiwari[3]***

*Assistant Professor[1], Student[2,3]*

*Department of Computer Science Engineering*

*Guru Premsukh Memorial College of Engineering*

***Corresponding Author's Email: -****rahulchoudhary8545@gmail.com*

***Abstract***

*The main goal of this article is to use an android application to open a hotel room door using a password entered through the android application device. The use of a smart card is required to open and close the hotel room door. The hotel room door is opened and closed using an Android application. The owner may connect an Android application device to the system through Wi-Fi, which is then linked to a microcontroller-controlled door that can be opened and closed by inputting the password. Any Android-powered smartphone or tablet may perform remote control using a touch-screen GUI (Graphical User Interface). This article is based on the Android application, which sends data through Wi-Fi. Another Wi-Fi device is attached at the receiving end and feeds information to the microcontroller. The supplied data (the user's password) matches the password stored in the microcontroller, and the microcontroller then begins a mechanism to unlock the door through a motor driver interface. The integration of Wi-Fi and Android technologies will provide timeliness, security, and the abolition of smart cards.*

***Keywords:*** *- Android Application, Password-Protected, Remote Door Unlocking, Wi-Fi*

## INTRODUCTION

The technology creates a secure door opening mechanism in which the door only unlocks when a security staff opens it by inputting the correct password into an android application. The authorised

employees must be present within Wi-Fi range of the door but do not need to manually lock or unlock the door. However, he must be linked to a Wi-Fi router, which provides some protection by restricting the wireless devices that may connect to it through MAC address. To unlock/lock the door, he just enters the correct password into his Android application.

The command transmitting feature is provided via an Android app. For this aim, the programme has an interactive, user-friendly graphical user interface (GUI). The Android application may be used from any smartphone running Android OS and sends and receives commands through Wi-Fi. When orders are delivered via the android smartphone, a signal receiver (LAN CONTROLLER) is utilised to receive them. These instructions are subsequently sent to the ARM11 PROCESSOR. The PROCESSOR executes these actions and then counts the password to ensure its accuracy. If the correct password is entered, the instruction to open the door is sent. A little buzzer sounds if the password is entered incorrectly. This is a handy notion in situations when security has to open gates often or operate a door from a vehicle without having to step out. Also, if the person is inside the bedroom and someone knocks on the main door, it may be unlocked with the use of video surveillance in mobile for the correct person.

**KEY LOCKING SYSTEM**

Mechanical locks are the most prevalent techniques for controlling access to doors and security containers. They can be located in (and guard the entrances to) the great majority of homes, commercial companies, educational institutions, and government sites, and they frequently act as the principal deterrent to entry and theft. Locks are significant in their own right, but their design and function have also affected how people think about security in general. Much of the terminology and philosophy of computer security and cryptology is derived from analogies that invoke mechanical locks mitting. The concept of a "key" as a little secret that permits access or operation, the idea that system security should be constructed to rely only on key secrecy, and even the term "intruder" for attackers may all be traced back to analogies that predate computers and current cryptography.

Conversely, the philosophy and practise of computer security and cryptology may significantly influence the design of

mechanical locks. Many parts of mechanical locks, for example, might be analysed and designed using formal ideas of computing complexity and other resources necessary to attack a system. However, these approaches have not been widely adopted by locksmiths or lock designers in general. Computer security experts, for their part, are frequently remarkably unskeptical when it comes to analysing promises of physical security.

**SMART CARD ENTRY SYSTEM**

A smart card is similar to a "electronic wallet." Consider the power of a computer, the speed and security of electronic data, and the ability to transport that data anywhere on the planet. Consider a computer so compact that it fits within a plastic card, similar to the credit card you keep in your wallet. Smart card technology has been around for well over two decades. Since its debut to the market, its primary application has been for the payphone system.

Smart card usage has increased as card manufacturing costs have fallen. In May 1996, a consortium of firms led by Microsoft, Hewlett-Packard, and Schlumberger created a PC/SC workgroup with the goal of integrating smart cards with personal computers (PC). This workgroup is primarily concerned with developing common smart card and PC interface standards for smart card and PC software manufacturers. Many interface standards and hierarchies are already in place. Some of these prototype goods are now commercially accessible.

The security needs of smart cards in personal communication systems are twofold: authentication and information protection. The security benefits of using smart cards in security systems are explored. A smart card is required to fulfil three basic activities. 1) To interact with a host device. 2) To save information. 3) Additionally, data received by and stored on the card must be processed.

**ANDROID APPLICATION SECURITY SYSTEM**

In this case, an Android phone is used to open a room door via Wi-Fi connectivity. This door-opening system is more complex, and it offers the user with security in a variety of ways, including: By utilising the MAC address of the Android devices to limit the number of mobiles that may connect to it. It also offers security by providing users with a login id and its matching password; these information are saved in the database of the related door

circuit, and if they match, the user can login.

### A) OPERATING MODULES

It has three operating modules. And they are as follows,

- Reception Part [PC & Wi-Fi modem]
- Door Circuit [Raspberry Pi, Motor driver, Motor]
- Android Mobile [Door Opener application]

See figure 1

### RECEPTION MODULE

This module includes a PC for monitoring the database and a Wi-Fi modem which transmits and receives data between mobile and door circuit. The accessibility to database is limited/controlled by password such that on higher personnel can login for viewing details. See Figure 2

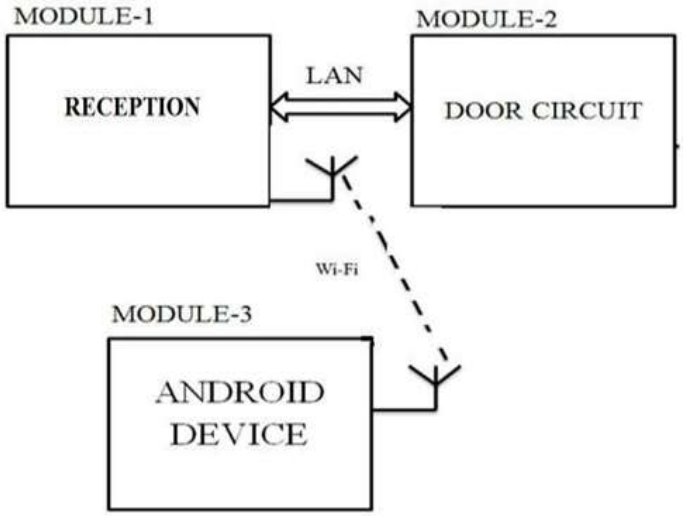



***Fig.1. Operation Modules***

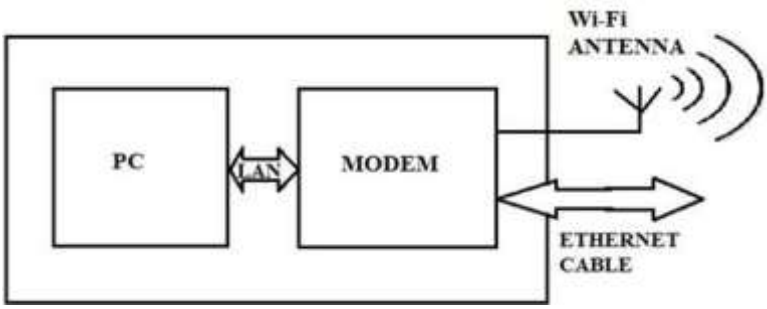



***Fig.2. Reception module***

#### a) PC

The PC is used for displaying all process that are being carried. It need to be ready with all necessary software supports. It requires following softwares installed :
1)phpmyadmin-for loging into the database of server. 2)filezilla-for making changes in the app at administrator level.

**b) MODEM**

Here I have used TD-W8951 ND modem for transmitting and receiving purposes. The TD-W8951ND connects to an Ethernet LAN or computers via standard Ethernet ports. The ADSL connection is made using ordinary telephone line with standard connectors. Multiple workstations can be networked and connected to the Internet using a single Wide Area Network (WAN) interface and single global IP address. The advanced security enhancements, IP/MAC Filter, Application Filter and URL Filter can help to protect network from potentially devastating intrusions by malicious agents from the outside of the network. As soon as the guest enters in to the hotel his/her MAC Address of the device must be got and it must be registered to the Wi-Fi device and then he must be provided with the SSID & password for that id so that he can get connected to the Wi-Fi of the hotel. Then he can install the DOOR OPENER application in his android mobile by logging in to the server. Then he can login in to the corresponding room by getting the user name and password from reception. As soon as he gets the user name and password from reception he can move to corresponding room entrance door.

**2. DOOR CIRCUIT**

In this module there are three components. As soon as commands are received from the mobile through LAN cable to this module, these commands are sent to LAN controller chip of the pi board then it being verified and decoded by the processor. Then the commands are sent to driver circuit for processing the required action and the motor is being driven in either clockwise or anticlockwise as per requirement for locking or unlocking the door.

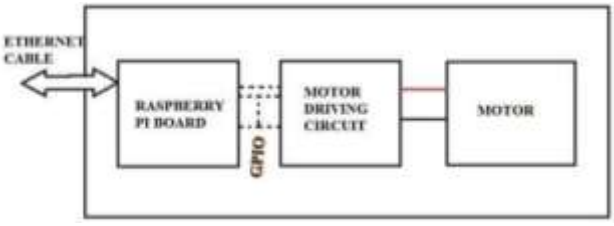
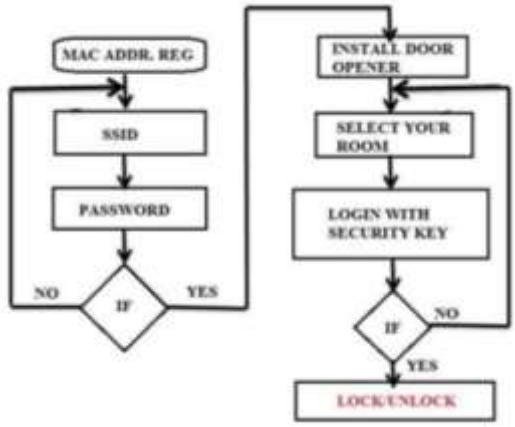



***Fig.3. Door circuit***

When the guest reaches the corresponding room he can login in to DOOR OPENER by entering the username and password that is provided by the receptionist. If there are many users for the same room then all will be provided with different user name and password, so that as each user logins for opening/closing the room door he will be registered at the database with the time and date of login and logout.

The below flow chart explains the process that is being carried out.




**RASPBERRY PI**

The Raspberry Pi is a credit-card sized general purpose Linux computer designed and manufactured by the Raspberry Pi Foundation, a non-profit organization dedicated to making computers and programming instruction as accessible as possible to the widest number of people. Although the original mission of the Raspberry Pi was to get inexpensive computers with programming capabilities into the hands of students, the Pi has been embraced by a diverse audience. Tinkers, programmers, and DIYers across the globe have adopted the tiny platform ranging from recreating retro arcade cabinets to controlling robots to setting up cheap but powerful home media devices.

The Pi features a system on a chip setup built around the Broadcom BCM2835 processor (a tiny but fairly powerful mobile processor commonly used in cellphones) that includes a CPU, GPU, audio/video processing, and other functionality all on a low-power chip. Although the Pi is an amazing little device. The Raspberry Pi is not an outright replacement for desktop computer or laptop. It cannot run Windows on it (its ARM-based processor doesnot support x86/x64 code), although it can run many distributions of Linux including distributions with desktop environments, web browsers, and other elements. The Raspberry Pi is, however, an astoundingly versatile device that packs a lot of hardware into a very inexpensive body and is perfect for hobby electronics, setting up an inexpensive computer for coding/programming lessons and experiments, etc.

## CONCLUSION

In this research, a clearly developing awareness of people's general security demands has been established in society. Furthermore, as the availability of mobile technology such as smart phones grows, mobile apps will have a unique chance to address security in novel ways. Aside from design concerns, the dynamic nature of the mobile application industry leads in the frequent introduction of new applications. Throughout the development of DOOR OPENER, rivals with similar goods in the field arose, emphasising the need of product uniqueness if being the first to market is not possible. There are currently hundreds of programmes seeking to solve the issue of enhancing user demands, even in a somewhat peripheral sector such as security applications.

Thus, using my approach, it should be possible to unlock the doors remotely using Android phones. This is a handy notion in situations when security has to open gates often or operate a door from a vehicle without having to step out. Also, if the individual is inside the bedroom and someone knocks on the main door, it may be unlocked using video surveillance in mobile for the correct person. This system may be improved further to do video surveillance of persons at the door as well as automatic door opening.

## REFERENCES

1. Siquan Hu, Yu Fu,School of Computer and Communication Engineering University of Science and Technology Beijing, Chundong She, Hui Yao, Ruijie Networks Co., Ltd, “Enabling Zigbee Communications in Android Devices”, published in Proceedings of the 2012 2nd International Conference on Computer and Information Application (ICCIA 2012).

2. Kuan J.H. , Chang J. , Ho J. ,” A development of information protection system using system engineering and RFID technolog”, published in International Conference on System Science and Engineering (ICSSE), IEEE 2010.

3. Ushie James Ogri, Donatus Enang Bassey Okwong, Akaiso Etim, Department of Physics, University of Calabar, “DESIGN AND CONSTRUCTION OF DOOR LOCKING SECURITY SYSTEM USING GSM”, published in International Journal Of

Engineering And Computer Science ISSN:2319-7242,Volume 2 Issue 7 (July 2013), Page No. 2235-2257.

4. Xi Li, Tiyan Shen, Jinjie Zhang, Changmin Shi, “A Spatial Technology Approach to Campus Security, Networking, Sensing and Control”, 2008, published in ICNSC 2008.

5. M. SATHISH KUMAR & S. NAGARAJ, Sri Venkateswara College of Engineering, R.V.S Nagar, Chittor, “THE CAMPUS SECURITY TRACKING SYSTEM BASED ON RFID AND ZIGBEE NETWORK”, published in International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), ISSN No. 2248-9738 (Print), Vol-2, Iss-3,4, 2012.

6. Jin-Shyan Lee; Yu-Wei Su; Chung-Chou Shen, “A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi”, published in Industrial Electronics Society, 2007. IECON 2007.

7. Vivek Kumar Sehgal, Nitin , Durg Singh Chauhan, ACM, “Embedded Controller Based Smart Card Access”, published in Proceedings of the World Congress on Engineering and Computer Science WCECS 2008, October 22 - 24, 2008, San Francisco, USA. 68