Smart Door Locking System

Nishad N. Gupte
Department of Electronics Engineering,
Datta Meghe College of Engineering, Airoli

Mihir R. Shelar
Department of Electronics Engineering,
Datta Meghe College of Engineering, Airoli

Abstract

Today's world is a smart world we live in and Smart Phones have a major contribution in it. A smart phone is now a very common device that everyone carries with them all the time. Smart phones have enabled us to perform various tasks while using a single device. Considering this phenomenon we can exploit the idea of remote-controlling a door with the help of a smart phone.

Physical keys and a lock are the basic requirements for a door. However managing these keys has become cumbersome. To overcome this, we present a solution which is a smart and a secure way of remote-controlling the door using a smart phone.

1. Introduction

Using physical keys to lock or unlock the door is the most natural way and everyone is acquainted with it. The physical key is a well-tested and well-known technology, but it also has its flaws. There can only be one unique key for a lock. For different locks you have different keys. Furthermore, carrying a large number of keys is a burden and increases the chance of keys getting stolen, misplaced or lost.

Our goal is to design a solution for secure access control that can replace physical keys for accessing door. We propose a solution using digital keys on smart phones providing wireless and automatic unlocking via Bluetooth. The design will allow easy implementation and distribution of keys and the device will work autonomously. This will enhance the security and will eliminate the need of carrying physical keys.

2. Existing System and its limitations

The most commonly used system for locking and unlocking the door is a lock and a physical key. The entire process is a mechanical one. If the key is lost, misplaced or stolen, then the entire locking mechanism has to be replaced. This problem with the physical keys intensifies when it comes to big companies where employees are needed to carry several keys for different doors. Apart from the extra burden, all the keys add to become vulnerable to getting lost.

An alternative used for physical keys currently is RFID (Radio-Frequency Identification). There are RFID cards being used as pass keys. The RFID card reader unit is installed near the door. When the card is brought near the reader, it identifies the radio frequency of the card and thus verifies the key. Multiple cards can be paired with the device. But again they are vulnerable to theft or getting lost. It also does not solve the purpose of not carrying a key. To overcome all such problems we propose a solution using a smart phone as a replacement for existing systems.

3. Proposed System

To tackle the above issues, we propose to replace physical keys with digital keys that:

- can easily be distributed to users
- can only be used by the correct user
- can be restricted to a given time or date range
- can be specialized for each user so each key will be unique

We propose to use a smart phone equipped with Bluetooth. A smart phone has now become a very common commodity and everyone carries it along with them. It is as natural as carrying a physical key. Further, smart phones running on operating systems like Android are becoming increasingly open to third-party developers, while the hardware at the same time is getting more and more powerful. This makes smart phones a suitable platform for uses beyond making and receiving phone calls. Combined with the ability to perform short-range wireless communications via Bluetooth, the smart phone is a good candidate for the replacement of physical keys.

The user will be required to install the mobile application on the smart phone and the hardware will be installed on the door. Then, the following steps will be needed to carry out the process:

- Start the mobile application,
- Pair the mobile once with the door hardware via Bluetooth,

- Enter the pre-defined password in the mobile application to get access, or to create a new password.
- Get the access of the door by selecting Lock-Unlock option on the mobile.

If the password matches then only the system will give access to the door. If there is a mismatch then a warning will be given regarding incorrect password. On three consecutive incorrect inputs, the owner will be notified about the intrusion.

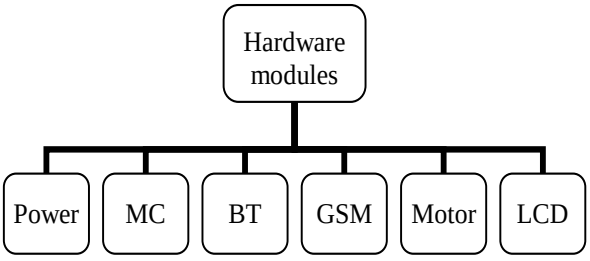
The range of the Bluetooth transmission is about 10 meters. If one has to get access to the door while being outside this range, it can be done via SMS. The GSM module will carry out the same functions as that of the Bluetooth module. In this case, the steps to be carried out are:

- Start the mobile application,
- Enter the pre-defined password and send it via SMS to the GSM module, to get access or to create a new password.
- Get the access of the door by selecting Lock-Unlock option on the mobile.

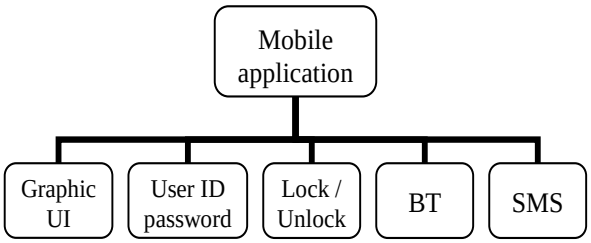
If the password matches then only the system will give access to the door. If there is a mismatch then a warning will be given regarding incorrect password. On three consecutive incorrect inputs, the owner will be notified about the intrusion and the owner will get information about the number trying to intrude. One SMS will be sent to the owner revealing the intruder's number. This security aspect of the system makes it favourable for its use in high security areas. Banks can employ this system for its lockers.

4. System overview and architecture

The entire system consists of an Embedded System and the Mobile Application. The different sub-modules in the embedded system can be understood from the following block diagram:



The different blocks of the mobile application are:



The hardware device will be an Embedded System consisting of different modules. The micro-controller from the 8051 family will be the core of the system. The Bluetooth modem and the GSM module will be interfaced to the microcontroller.

The working of different modules will be:

A. **Microcontroller**

The Microcontroller from the 8051 family will be the core of the device. It is responsible for all the execution and process management. The microcontroller will monitor all the modules and peripherals interfaced to it. The password verification will take place in the microcontroller.

The microcontroller code will be written in Embedded C and will be burned or programmed into the code memory.

This unit will require +5V DC for its proper operation.

B. **Bluetooth modem**

The Bluetooth modem will communicate with both, the microcontroller and the smart phone. Thus it will act as the mediator between the user and the embedded system. It will fetch the password from the mobile and forward it to the microcontroller. It has built-in protocol for serial communication i.e. Serial Port Profile. It has a limited range of around 10 meters.

This unit will require +3.3V DC supply.

C. **GSM module**

The GSM module will do the same function as that of the Bluetooth modem. It will fetch the password sent via SMS and will forward it to the microcontroller. Its RS232 port will be used to communicate with the microcontroller. Upon intrusion detection this unit will notify the user with a SMS containing the information of the intruder i.e. the mobile number which is used to intrude.

This unit will require +12V DC for its operation.

D. **DC Motor Driver**

This unit is nothing but H-Bridge driver encapsulated in a single IC. Here we will

use L293D IC for DC motor driving. It can drive up to 4 DC motors in unidirectional mode and 2 DC motors in bidirectional mode. It can sink up to 600mA per Channel.
The job of this unit is to drive the connected motors in the desired direction when the microcontroller sends a signal to their respective channels.
This unit requires +12V DC for its proper operation.

E. **DC Motor**

The motors used will be of 30 RPM. They are used to perform the locking and unlocking actions. They will be driven through the motor driver IC and the motors used will be bidirectional.
The motors will require +12V DC for its operation.

F. **LCD**

The Liquid Crystal Display which we will use is a 16x2 characters LCD. The LCD will display the status of the system and all the system generated messages. It will provide an interactive user interface.
It will require +3.3V DC supply for its operation.

G. **Power Supply**

The power supply unit will be made up of transformer, rectifier, filter and regulator. The regulator will be used for variable power supply. The rectifier used will be a bridge rectifier to convert a 230V AC into DC. This unit will supply the various voltage requirements of each unit.

H. **Mobile Application**

The mobile application will have a user friendly interface. It will be developed for smart phones based on Android as well as Java. For Bluetooth communication, the device and the mobile are needed to be paired once. The user will have to input the password in the application and then select the Lock/Unlock option as desired.

5. Features

The prominent features of the above proposed system are:

- Password protected access
- Eliminates the need to carry a key or any extra remote, as the user's phone is used
- The entire process requires virtually no time
- Bluetooth based short range communication with no interference due to another Bluetooth media
- Intrusion alert via SMS with details of intruder
- Customizable keys for each user
- The application software can be installed on any smart phone
- Real time monitoring of the system status

6. Technology and Programming languages

The various Technologies and Programming languages that are going to be used in the above proposed system are:

For embedded system:

- 8051 family based microcontroller
- Embedded C Keil compiler
- Eagle software for PCB designing
- Flash Magic for burning the code

For mobile system:

- Serial Communication Protocol (SPP)
- Android SDK for application development & programming
- J2ME and J3ME based mobile programming
- MIDlet programming

7. Application and Future scope

The above proposed system can have a large number of applications due to its practicality and its security aspect. Some of them are:

- Can be used for doors at Home and Offices
- Can be used for Industrial doors
- Can be used for high security Bank vault doors
- And practically any place where remote controlling is required

For future scope, the device can be paired with a CCTV module to enhance the security. Additional Face Recognition can be installed.

8. Conclusion

The proposed system allows remote access to lock or unlock the door without physical user interaction. The system fulfils the requirements of supporting autonomous locking device and easy key distribution compared to physical keys. The system has minimum requirements for hardware and supports customization of keys. The intrusion alert enhances the security of the system. The prototype built shows that the design consumes minimal power and the locking/unlocking of the door happens in 4 seconds on an average. Thus the system proposed is feasible.

9. References

A. Embedded Books & Websites

[1] Myke Predko, *Programming and Customizing the 8051 Microcontroller*, Edition 1999, Tata McGraw-Hill, Page: 157-167.

[2] Muhammad Ali Mazidi, Janice Gillispie Mazidi, *8051 Microcontroller and Embedded Systems*, Prentice-Hall, Page: 183-193, 236, 243.

[3] Dogan Ibrahim, *Microcontroller Projects in C for the 8051*, Newnes, Page: 29-161.

[4] Kenneth J. Ayala, *The 8051 Microcontroller Architecture, Programming and Applications*, West Publishing Company, Page: 131-197.

[5] Michael J. Pont *Embedded C*, Edition 2002, Addison Wesley, Page: 57-87, 217.

[6] www.beyondlogic.org
[7] www.discovercircuits.com
[8] www.electronicsforu.com

B. Electronics Books & Websites

[1] Ramakant A. Gayakwad, *Op-Amps and Linear Integrated Circuits*, 4th Edition, Prentice-Hall, Page: 342, 417, 455.

[2] Robert L. Boylestad, Louis Nashelsky, *Electronic Devices and Circuit Theory*, 10th Edition, Prentice-Hall, Page: 342, 417, 455.

[3] R. P. Jain, *Digital Electronics*, Tata McGraw-Hill.

[4] www.electronic-circuits-diagrams.com
[5] www.circuitstoday.com
[6] www.circuitlake.com

C. Software Books & Websites

[1] Brian W. Kernighan, Dennis M. Ritchie, *The C programming Language*, First Edition 1988, Prentice-Hall, ISBN 0-13-110370-9.

[2] Sing Li and Jonathan Knudsen, *Beginning J2ME: from Novice to Professional*, Third Edition 2005, Prentice-Hall, ISBN (pbk): 1-59059-479-7.

[3] www.learn-android.com

D. Other Books & Websites

[1] *"Using Mobile as Digital Key for Home Doors"*, Published in July 2010, ISBN 978-1-4244-7475-2

[2] www.alldatasheets.com
[3] www.wikipedia.org
[4] www.keil.com
[5] www.hobbyprojects.com