International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 11 | Nov 2018 www.irjet.net p-ISSN: 2395-0072

Automatic Door Lock System using PIN on Android phone

Mr. Patil Bhushan S[1], Mr. Mahajan Vishal A[2], Mr. Suryawanshi Sagar A[3], Mr. Pawar Mayur B[4], Prof. Mr. U. R. Patole[5]

[1,2,3,4]*B.E Student, computer engineering, SVIT Nashik*
[5] *Assistant Professor, Dept. of Computer Engineering, SVIT Nashik, Maharashtra, India*

Abstract - *The growth of technology make smartphone can control the home appliances. An automated device can work more flexible and efficient, including the use in unlocking door. For busy family or busy people, it is not easy to get out of the seat only to reach the door for unlocking people that already have known and made appointment before. So, it is not only the open button from smartphone application that anyone can control, but also it is added an interface for speech command or pin which also can be useful as security. Android smartphone application is used for serial communication to the Bluetooth module which is connected in Arduino Board to unlock the door. Speech command enacted to the system is also tested the Bluetooth connectivity. The farthest range is 14 m to the controlled hardware system.*

Key Words: **Home automation/ Car automation, door automation system, door lock system/ car lock system, pin code, Android, Adriano.**

1. INTRODUCTION

The technology of keys and locks remained the same for the last century while everything else is evolving exponentially. So why not use current technologies and apply it with old ones to build something new and innovative. Around 4000 years ago, the concept of Locks and Keys were invented and until today, regardless of some minimal variation in security and sustainability locks are installed in doors stimulated mechanically by the right key. Recently, the Internet was enhanced, and everything was connected to it (phones, television, laptops, tablets, cars and so on). This was done because we wanted to make systems smarter in other term a more productive. Why not do the same thing with Locks? Enhancing the locks mechanism by connecting them to the internet, making them more robust and productive. Today, the number of mobile device users including smart phone users has rapidly been increasing worldwide, and various convenient and useful smart phone applications have been developed. Now smart phones are not only used to send and receive phone calls, send text messages and perform mobile banking operations, but they also are used to control various other devices in our real everyday lives. Through a mobile operating system and internal applications, we can remotely control a variety of external devices such as TVs, projectors, computers, cars, etc. People normally operate ordinary locks with keys or keyword locks such as a pin code. However, these locks have few drawbacks such as misplacing keys or forgetting passwords. Using smart phones, the remote lock can be easily managed. Furthermore, the proposed system has wide range of applications and can be used for various types of locks and systems, such as lockers, bicycles, cars, etc. Smart-Lock- System is a complete reinvention of the standard Key-Door lock, where all the digital keys are stored in a Digital Key chain kept on the owner as phone. Encrypted and secured Smart-Lock-System can be connected to the Internet via internet cable (UTP) or wirelessly (Wi-Fi).

question paper from this semantically labelled question bank.

1.1 Objective

1. The main objective is to design secure lock using the advance algorithm like AES.

2. Designing secured door lock to prevent unwanted access in the server room.

3. To Replace RFID based lock system with the smart phone.

4. To give the user hassle free access without compromising security.

5. This system gives notifications about access to user.

1.2 Literature survey

This section contains the Literature review and the theoretical deatils about the project.

Infrared Optical Wireless Communication for Smart Door Locks Using Smart phones With the recent rapid advancements in the Internet of Things (IoT), one of the applications being developed is that of smart door lock (SDL) systems. SDL are intended to over high security, easy access and easy sharing. Unlike existing SDL solutions that mostly use biometrics or crunched RF spectrum, we uniquely propose to use Infrared (IR) optical wireless signal (OWS) using IR light emitting diode (LED) of smart phones. We designed and developed a complete system of Android smart phone app including physical layer encoding, a cloud server and programmable hardware prototypes using Arduino as well as Raspberry Pi. Optlock includes multi-level security schemes including user registration, authentication and authorization using one-time-password (OTP). This extensive experiments show 100 accuracy with 1.33 kbps of average data rate is achieved up to 20 meters of distance between a smart phone and a lock. It allows convenient remote access, easy access control and sharing as well as high security.[1]

A Smart Lock System using Wi-Fi Security

In large apartment complexes, fraternities, or even for an owner having many keys for each and every apartment, car, or gate he owns, maintaining entry to authorized personnel only is a problem. Besides the costs involved in fabrication, duplication, and distribution of keys, there are security problems in case of lost keys. In this paper an innovative lock system prototype using todays technologies will be presented. The novelty of this prototype relies on the fact that using new technologies along with old ones will result in a smart and more efficient. We propose a smart digital door lock system for any lock system. A digital door lock system is any equipment that uses the digital information such as a secret code instead of the legacy key system. In our proposed system, a Central Control module is embedded in the door itself, this is required to prevent additional complications and more robust mechanism for the door as a whole. Technically, this system embeds itself in the Local Area Network of the house. This adds extra security layers and prevents access to the system only through the network. Furthermore, the biggest advantage of the proposed system over existing ones is that it can be easily installed with minimal requirement of infrastructures and planning.[2]

Arduino Uno

The Arduino Uno is a micro-controller board based on the ATmega328 (data sheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the micro-controller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started. The Uno dicers from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter[3]

Software Card Emulation in NFC-Enabled Mobile Phones: Great Advantage or Security Nightmare Software card emulation is a new approach to advance the interoperability of NFC with legacy contactless smart card systems. It has been rest introduced to NFC-enabled mobile phones by Research In Motion (RIM) on their BlackBerry platform. Software card emulation aims at opening and simplifying the complex and tightly controlled card emulation functionality. While this form of card emulation, that gets rid of the secure element (a device tightly controlled by the big players), is a great chance for development of innovative NFC applications, it potentially makes card emulation less secure and paves the way for interesting attack scenarios. This paper evaluates the advantages and disadvantages of software card emulation based on existing application scenarios and recent research results[4]

Secure and Anonymous Hybrid Encryption From Coding Theory

A Hybrid Encryption scheme is a cryptographic protocol that features both a publickey encryption scheme and a symmetric encryption scheme, the former with the task of encrypting a key for the latter, in charge of encrypting the actual body of the message. The rest component is therefore known as Key Encapsulation Mechanism (KEM) while the second is called Data Encapsulation Mechanism (DEM). Key feature is that the two parts are independent of one another. The framework was rest introduced in a seminal work by Cramer and Shoup, along with the corresponding notions of security and an example of a scheme based on the DDH assumptions.[5]

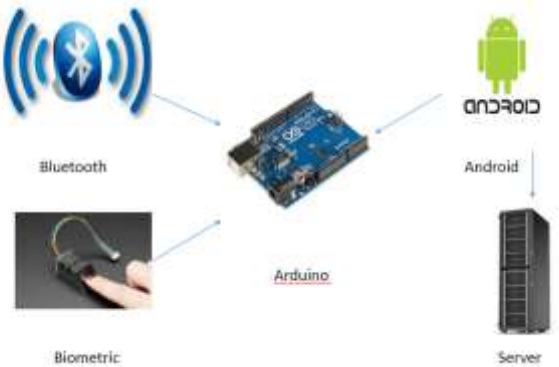
Designing an Access Control System

Electronic door locks have been a popular mechanism to enforce physical access security in the enterprise for close to four decades. It allows the maintenance staff to issue keys i.e. access cards, revoke them remotely and also control access to the specific sections of a building. For example, when employees unauthorized to access a sensitive section of the building use their cards to access it, the maintenance staff gets alerted with the identifying information of the miscreant, area being accessed, and the time at which the infraction happened. Such deployments needed heavy investments of infrastructure, software, and maintenance staff which drove up the deployment cost prohibiting their usage for regular home settings. The average costs for having electronic access control for each door can be as high as 5000[6]

Access Systems

The access control systems can be a highly secure solution for the enterprise but have not been affordable or suitable for home use. However, the revolution in the IoT coupled with the proliferation of smart phones and cloud based technologies spurs the recent adoption of SDL for home and other commercial use. The SDL are an attractive replacement to traditional door locks as they offer increased security and easy key sharing while offering ease of operation. The cost is not prohibitive for home usage, especially considering its benefits over a traditional door lock[7]

1.3 Architecture Diagram



1 Infrared Optical Wireless Communication for Smart Door Locks Using

Smart phones[1]

With the recent rapid advancements in the Internet of Things (IoT), one of the applications being developed is that of smart door lock (SDL) systems. SDL are intended to over high security, easy access and easy sharing. Unlike existing SDL solutions that mostly use biometrics or crunched RF spectrum, we uniquely propose to use Infrared (IR) optical wireless signal (OWS) using IR light emitting diode (LED) of smart phones. We designed and developed a complete system of Android smart phone app including physical layer encoding, a cloud server and programmable hardware prototypes using Arduino as well as Raspberry Pi. Optlock includes multi-level security schemes including user registration, authentication and authorization using one-time-password (OTP). This extensive experiments show 100 accuracy with 1.33 kbps of average data rate is achieved up to 20 meters of distance between a smart phone and a lock. It allows convenient remote access, easy access control and sharing as well as high security.

2 A Smart Lock System using Wi-Fi Security[2]

In large apartment complexes, fraternities, or even for an owner having many keys for each and every apartment, car, or gate he owns, maintaining entry to authorized personnel only is a problem. Besides the costs involved in fabrication, duplication, and distribution of keys, there are security problems in case of lost keys. In this paper an innovative lock system prototype using today's technologies will be presented. The novelty of this prototype relies on the fact that using new technologies along with old ones will result in a smart and more efficient. We propose a smart digital door lock system for any lock system. A digital door lock system is any equipment that uses the digital information such as a secret code instead of the legacy key system. In our proposed system, a Central Control module is embedded in the door itself, this is required to prevent additional complications and more robust mechanism for the door as a whole. Technically, this system embeds itself in the Local Area Network of the house. This adds extra security layers and prevents access to the system only through the network. Furthermore, the biggest advantage of the proposed system over existing ones is that it can be easily installed with minimal requirement of infrastructures and planning.

3 Arduino Uno[3]

The Arduino Uno is a micro-controller board based on the ATmega328 (data sheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the micro-controller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.

The Uno dicers from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter.

4 Software Card Emulation in NFC-enabled Mobile Phones: Great Advantage or Security Nightmare[4]

Software card emulation is a new approach to advance the interoperability of NFC with legacy contactless smartcard systems. It has been rest introduced to NFC-enabled mobile phones by Research In Motion (RIM) on their BlackBerry platform. Software card emulation aims at opening and simplifying the complex and tightly controlled card emulation functionality. While this form of card emulation, that gets rid of the secure element (a device tightly controlled by the big players), is a great chance for development of innovative NFC applications, it potentially makes card emulation less secure and paves the way for interesting attack scenarios. This paper evaluates the advantages and disadvantages of software card emulation based on existing application scenarios and recent research results.

5 Secure and Anonymous Hybrid Encryption from Coding Theory[5]

A Hybrid Encryption scheme is a cryptographic protocol that features both a public-key encryption scheme and a symmetric encryption scheme, the former with the task of encrypting a key for the latter, in charge of encrypting the actual body of the message. The rest component is therefore known as Key Encapsulation Mechanism (KEM) while the second is called Data Encapsulation Mechanism (DEM). Key feature is that the two parts are independent of one another. The framework was rest introduced in a seminal work by Cramer and Shoup, along with the corresponding notions of security and an example of a scheme based on the DDH assumptions.

6 Designing an access control system[6]

Electronic door locks have been a popular mechanism to enforce physical access security in the enterprise for close to four decades. It allows the maintenance staff to issue keys i.e. access cards, revoke them remotely and also control access to the specific sections of a building. For example, when employees unauthorized to access a sensitive section of the building use their cards to access it, the maintenance staff gets alerted with the identifying information of the miscreant, area being accessed, and the time at which the infraction happened. Such deployments needed heavy investments of infrastructure, software, and maintenance staff which drove up the deployment cost prohibiting their usage for regular home settings. The average costs for having electronic access control for each door can be as high as 5000:

7 Access systems[7]

The access control systems can be a highly secure solution for the enterprise but have not been affordable or suitable for home use. However, the revolution in the IoT coupled with the proliferation of smart phones and cloud based technologies spurs the recent adoption of SDL for home and other commercial use. The SDL are an attractive replacement to traditional door locks as they offer increased security, and easy key sharing while offering ease of operation. The cost is not prohibitive for home usage, especially considering its benefits over a traditional door lock.

8. A Wireless Controlled Digital Car Lock For Smart Transportation

In current era the Internet of Things (IoT) is becoming an important part of our daily life. It is employed in a variety of applications like smart buildings, intelligent transport systems, smart grid, etc. The aim of this project is to contribute to the evolution of Internet of Things (IoT) application in intelligent transportation systems. The focus is to develop a smartphone based wireless controlled car lock demonstrator for education. Indeed, the recent technological evolution has revolutionized the use of smartphones in our lives. The idea is to allow a group of authorized people to share a lot of cars. Whenever an authorized person requires a car, a request is firstly submitted via internet to a server based utility. On the availability of a car the request is granted and vice versa. In the case of an authorization, a digital code is sent to the smartphone of the person who has originated the car request. In order to convey the digital code, received on the smartphone, to the front end embedded controller a customized Android-based application is devised. It is developed by using the MIT inventor app. This application is installed on the smartphone and it is linked to the front-end embedded controller based digital car lock via the Bluetooth interface. The intended code, to lock or unlock the car, is sent by the concerned person by using this application. The command is transmitted to the front-end embedded controller via the Bluetooth port. After recognition, the received command is executed by the front-end module and a flag is returned to the smartphone-based soft application. The concerned car status with time and date is also recorded in the application platform and is updated on the cloud. It allows accessing this information globally and at any time with a passcode. A system prototype is implemented and tested. Experimental results have confirmed a proper system operation.3

ALGORITHM

AES Algorithm (Advanced Encryption Standard):

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plain text).
3. Add the initial round key to the starting state array.
4. Perform nine round of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the final data (ciphertext).
7. For decryption reverse the above steps.

Pin Authentication Algorithm

1. Initialize 4 digit pin code in the android application
2. Send the pin data via the Bluetooth
3. Receive the pin data in the arduino microcontroller
4. Check the protocol, if the first input character is #, the data is true for system
5. If not, no nothing
6. If true continue check, the next flag must be 1 to indicate the use of pin authentication
7. Then continue check, if next flag serial setting is 1, it is the command to set/update the pin code, then update the received 4digit pin code in the next serial data as a saved pin in the EEPROM
8. If the next flag serial setting is 0, it is the command protocol to open the door.
9. Do the authentication, if the 4 received digit pin is exactly same with the 4 digits pin saved, the relay turn HIGH to control solenoid to open the door
10. if not, shows the warning in the android application

CONCLUSIONS

The Smart-Lock-System will open the door leading to a wide range of innovations in the world of lock systems wherever they may be. With its ease of installation and use, minimum complexity, wide applicability options, and strong feasibility, SLS guarantees a huge aspiring step forward into a better future lock system. All of the above can't be considered authentic or even possible without considerately taking into account one of the most vital aspects to the innovation: security. Therefore, after examining the detailed evaluation and explanation of this phase, the project really tackles the security concerns to eliminate any worries which might cause a threat to the systems success and prosperity.

REFERENCES

[1] Kaustubh Dhondge Kaushik Ayinala Baek-Young Choi Sejun Song, "Infrared Optical Wireless Communication for Smart Door Locks Using Smart phones", 12th International Conference on Mobile Ad-Hoc and Sensor Networks, 2016.

[2] Abdallah Kassem and Sami El Murr, "A Smart Lock System using Wi-Fi Security", 3rd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA) 2016.

[3] 'Uno Revision 3",

http://arduino.cc/en/Main/arduinoBoardUno, 2016.

[4] M. Roland, "Software card emulation in nfc-enabled mobile phones: great advantage or security nightmare", in Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use, 2012.

[5] Edoardo Persichetti,"Secure and Anonymous Hybrid Encryption from Coding Theory", Springer-Verlag Berlin Heidelberg 2013.

[6] B. Rhodes, "Designing an access control system", https://ipvm.com/reports/designing- an-access-control-system", 2015.

[7] "Access systems",

https://www.security.honeywell.com/me/documents/Access Systems 2011.pdf, 2011.

AUTHORS

Mr. Patil Bhushan S.

B.E Student, computer engineering, SVIT Nashik.

Mr. Mahajan Vishal A.

B.E Student, computer engineering, SVIT Nashik.

Mr. Suryawanshi Sagar A.

B.E Student, computer engineering, SVIT Nashik.

Mr. Pawar Mayur B.

B.E Student, computer engineering, SVIT Nashik.

Prof. Mr. U. R. Patole

Assistant Professor, Dept. of Computer Engineering, SVIT Nashik, Maharashtra, India