WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Security Locking System Using Arduino and Android Application

Ephraim Asher Akash Mills[1]*, Manojkumar . R*[2]*, Prabin singh*[3]*, E.R. Ramesh*[4]

[1]Department of Information Security and Digital Forensics, Dr.MG.R.Educational and Research Institute,Chennai 600095, Tamilnadu, India. 181621101008.eaakashmills@gmail.com

[2]Department of Information Security and Digital Forensics, Dr.MG.R.Educational and Research Institute,Chennai 600095, Tamilnadu, India. manojkumarthenpair@gmail.com

[3]Department of Information Security and Digital Forensics, Dr.MG.R.Educational and Research Institute,Chennai 600095, Tamilnadu, India. India.181621101024.prabinsingh.d@gmail.com

[4]Center of Excellencein Digital Forensics,Chennai-600096,Tamilnadu, India.rameshvani@gmail.com

ABSTRACT

This project deals with unlocking a door lock using biometric fingerprint authentication. Usually this process takes place using a single fingerprint sensor end-point on the door lock to scan fingerprints for authentication. This project is to make the authentication of fingerprints to be remotely carried over by a mobile application using the biometric authentication facilities provided by the different available mobile operating system and communicate to the lock through Bluetooth, after which another authentication process using cryptography is done using the data communicated by the mobile application on the lock using Arduino UNO. This paper has the potential to increase the security in certain aspects to the previously in use fingerprint authentication standards. With the increase in demand for the use of biometric authentication , nowadays pretty much all mobile vendors have an inbuilt biometric sensor and all operating systems have an biometric authentication mode of operation,(i.e) how to authenticate biometrics within the device. Using this feature and some cryptography we can authenticate the fingerprints on a mobile device and communicate through Bluetooth rather than using a single sensor endpoint for all authentication purposes. The mobile application associated with this paper can be integrated with any service requiring biometric authentication remotely with a little more subjective work according to the service.

1. INTRODUCTION:

This paper aims to authenticate fingerprints to unlock a door lock remotely using Bluetooth. This method uses the fingerprint authentication and fingerprint sensor found on pretty much all mobile device today. All the authenticate workflow happens within the mobile device. This method may help to improve the security posture of the already existing fingerprint authentications systems. The mobile application used in this paper can standalone be used to authenticate fingerprints for other remote service with a some tweaks with regards with service requesting the authentication. It can be used to authenticate fingerprints to unlock doors, or authenticate fingerprint for banking application and such.

2. EXISTING SYSTEM:

A system electrically identical to this one exist. The fingerprint authentication also happens inside a mobile application. The system authenticates fingerprints registered on only a single device. After authentication the application sends a Boolean response through a hc-05 bluetooth module to the Arduino UNO connected to a door lock through a servo motor.

3. PROPOSED SYSTEM:

The proposed system for this paper carries out the authentication process differently, by incorporating cryptography aiming to increase the security of the existing system. The proposed system in this paper uses multiple devices to authenticate fingerprints. After authentication of the fingerprints the proposed method unlike the existing system send a encrypted message of information about the fingerprint ,which changes with each device. The encrypted message is used in the verification of registered saved fingerprints in the Arduino UNO . The proposed design aims for an improved security posture device wise as well as data wise.

4.REQUIREMENTS:

- Mobile device with fingerprint scanner
- Bluetooth mobile application
- Arduino UNO
- HC-05
- Servo Motor
- Door lock

5.WORKFLOW:

For a user to authenticate his fingerprint with the door lock, the user is required to register his fingerprint with door lock first. During registration the authenticator id , a unique tag for fingerprints to be identified in that particular mobile device is used in the cryptography operation used to authenticate the fingerprint .After registration a user use the registered fingerprint to open and close the door lock.

A basic workflow to authenticate a fingerprint is as follows:

1. The user opens the app.
2. The user places the registered fingerprint in the application when prompted.
3. On successful authentication the application encrypts authenticator id a special identifier to identify the print template in that particular device.
4. The authenticator id is used in a cryptography function in the arduino to authenticate the fingerprint by the arduino.

Application Workflow:

1. When the application is opened it searches for Bluetooth door by scan nearby devices.
2. If the door is in connecting range the application connects automatically to the device.
3. After pressing the open button application prompts you to place your fingerprint on the sensor.
4. If the fingerprint is enrolled on the mobile device , a successful authentication callback is received on which it encrypts and send the send the authenticator id for the scanned fingerprint.
5. If the sent ID successfully decrypts the encrypted message in the arduino the door lock opens and the ui show a button to close the door, which locks the door.

Arduino Workflow:

1. The arduino waits for incoming connections using the HC-05 module.
2. After successful connection the arduino waits for the encrypted authenticator id from the mobile application.
3. The ID is used in decryption of device id which are stored in arduino encrypted using the authenticator id belong to that device during registration.
4. If decrypted message is equal to the current device id the arduino commands the servo motor to open the door lock.
5. Therefore the authenticator id acts as key to encrypted device id, it emulates the characteristic of a key in a literal lock and key.

6.SECURITY:

The improved aspects security wise in this proposed systems will be :

- The fingerprint templates is not stored on an external device instead it stays inside the mobile device while the id mapping the template in the specific device is used in a cryptographical function to decrypt and check if the coonected device id and the decrypted message are the same.
- Unlike the existing system ,cryptography is used to strengthen the authentication mode of operation between the lock and the application . The existing system could easily be compromised by a malicious actor as he just has to send a Boolean value to the lock mimicking the device id of the allowed id.

7.CONCLUSION:

This paper aims to improve the security and integrity of Bluetooth fingerprint authentication. Tieing up the authenticator ids with its device name in the cryptographical function acts as a key for a particular lock. Adding basic cryptography tightens the security aspects so much ,further research into the fingerprint facilities in mobile device and cryptography may lead to a more security tighter methods to authenticate fingerprints.