International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

Smart Door Locking System using IoT

Karthik A Patil[1], Niteen Vittalkar[2], Pavan Hiremath[3], Manoj A Murthy[4]

[1-4]*Student, School of Computing and Information Technology, REVA University, Bengaluru, India*

Abstract - *Conceptual Security has consistently been a significant worry to the general public either in the family units or the workplace condition. There are different methodologies set up to address these issues. This venture is proposed to build up a savvy locking framework utilizing the Internet of Things. Utilizing conventional keyed locks is basic since the start of humankind, anyway there is a high risk of keys being lost or getting into inappropriate hands. Subsequently, many individuals prefer biometric locks over traditional keyed locks to improve the security of their homes or workplaces. In contrast to the conventional lock, a cutting-edge biometric lock requires no key to bolt or open the door and instead uses a biometric sensor. Our project is an Arduino nano based adaptable working device that provides physical security utilizing the biometric sensor which is available in a smartphone.*

Key Words: Arduino Nano, Biometric Sensor, framework, smartphone, savvy.

1. INTRODUCTION

Every living being wishes to be safe whether it is a safety related to his belongings or safety of his own precious life. We have been taking several measures in order to attain it to live a worry-free life. In this project we propose a smart locking system which is designed to work based on the Internet of Things to prevent unauthorized access and trespassing. Normally the common targets where unauthorized access takes place are Banks, Financial organization, Government offices and organization, and shops. Such activities are performed with an intention of stealing money, or any important documents for personal gain. The main aim of our project is to provide a useful and a feasible solution to many of such issues.

Fingerprint acknowledgment is one of the most secure systems in light of the fact that a fingerprint of one individual never coordinates with the others. Hence, unapproved access can be restricted by arranging a lock that stores the fingerprints of at least one approved individual and opens the lock when a match is found. Bio-measurements approval ends up being perhaps the best attribute considering the fact that the skin on our palms and soles shows a stream like case of edges on each fingerprint which is uncommon and invariable. This makes fingerprint a novel ID for every individual. With this idea, a plan and a model of fingerprint based entryway lock framework has been presented in this paper.

Tech-savvy locks are made utilizing biometric sensors, therefore the expense of those locks is exorbitant. So, we have structured a low-cost biometric lock. As smart phones with fingerprint sensors are common, we are going to utilize this sensor to make a model of biometric lock.

There are several advantages of the biometric lock. Firstly, it is secure, unapproved individuals won't have any probability of accessing the framework. Besides, there is no requirement for a key. The main thing which will be required is a smartphone phone with the required hardware and software.

2.IMPLEMENTATION

Our project helps in building an economical and a low-budget biometric lock using the fingerprint sensor available in a smartphone. The first step is to create a program using Arduino IDE and uploading it into a microcontroller, in this case it is Arduino Nano. This program sets up a communication link between the nano board and a smartphone via Bluetooth. This communication link helps the microcontroller in executing the commands sent by the smartphone.

The first step in developing the program is to create a string variable which stores the unique device ID for lock, and then the servo library is added. The basic idea behind the working of door lock lies in the ID sent by the Android phone by means of the developed app. To receive the data sent by the phone we use Bluetooth module HC-05 with a default baud rate of 9600. It is connected to the Arduino nano board (Microcontroller) at the same baud rate (Refer fig 1).

```
#include <Servo.h>
String reads;


Servo myservo;

void setup() {
  Serial.begin(9600);
  myservo.attach(9);
  // put your setup code here, to run once:

}
```

Fig -1: Arduino Code Setting servo

The next step is to create a loop function that stores the device ID sent via Bluetooth. This is stored in "reads" string. Then, an 'if condition' is used for verifying the device ID sent by the Bluetooth. When the fingerprint of an user is scanned by the smartphone, it first authenticates with the one present in the application. After the successful authentication, the application sends the device ID to the Arduino Nano board. In the event that this ID matches with the one set in Arduino, at that point the servo motor moves the lock to open position. In the event that the Bluetooth reads an inappropriate fingerprint, at that point it naturally turns the servo motor to lock position. There is no movement if it is already in 'lock' position. (Refer Fig 2).

```
void loop() {
  while (Serial.available()==0);
reads=Serial.readStringUntil('\n');

   if (reads== "adrfjhlnm")
   {
  myservo.write(0);
  }
   if (reads== "wrong")
   {
  myservo.write(79);

}}
```

Fig -2: Arduino Code Checking Device ID.

The required android application can be made in two different ways. It can be baked using Android Studio or using Kodular. In our project we have made use of Kodular since it is easy to use and spares us from writing lengthy codes. The kodluar website can be opened using any web browser.

The following components must be added in the layout whilst making the app:

1. Bluetooth Clint
2. Fingerprint
3. List View
4. Image Button

Further, all the code blocks are combined together. Now that the app is baked, the .apk is extracted and then installed on a smartphone. (Refer Fig 3).

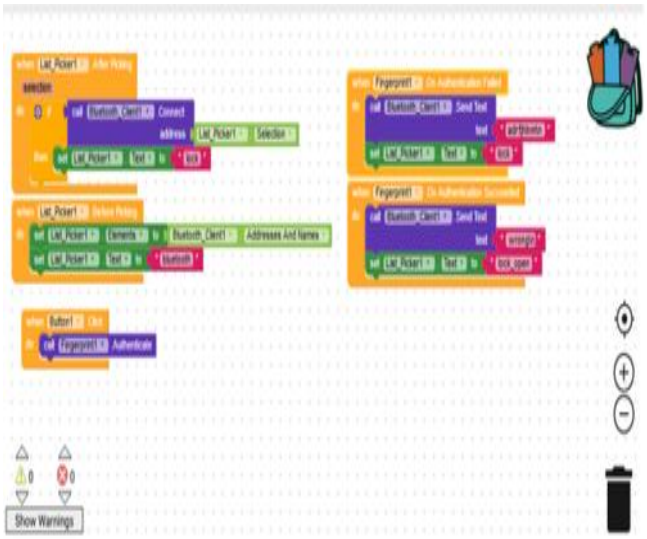

Fig -3: Code Blocks.

After the installation of the application in a smartphone and the code uploaded into the smartphone. The following components are connected and soldered together.

Pins	Components
Rx	Bluetooth Tx
Tx	Bluetooth Rx
5V	Bluetooth 5V
GND	Bluetooth GND
GND	Servo Motor GND
Pin 9	Servo Motor Signal Wire

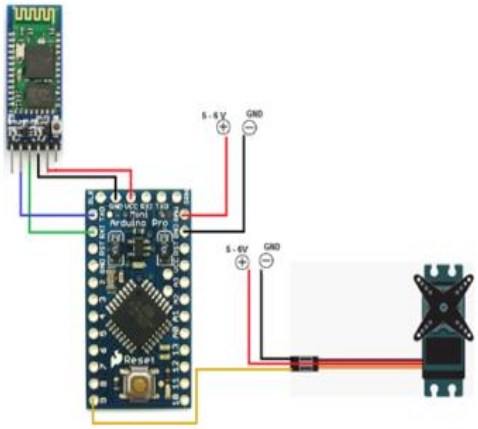

Fig -4: Connection

The next step is to prepare a physical lock for the biometric locking system. The following steps are followed to achieve this:

1. An already opened or a broken lock should be used. (Refer fig 5).
2. The moving shaft of the servo motor is attached to the lever of the lock for movement.
3. The last step is to place all the electronic components within the framework of the lock and then it is covered. (Refer fig 6).

Fig -5: Broken Lock.

Fig -6: Servo attached to lever.

Next, the lock is powered using a battery of 5-9V. Furthermore, the Bluetooth of the smartphone is turned on and is paired with the Bluetooth module connected to the Arduino board. On opening the application, the Bluetooth icon turn into lock icon. (Refer fig 7).

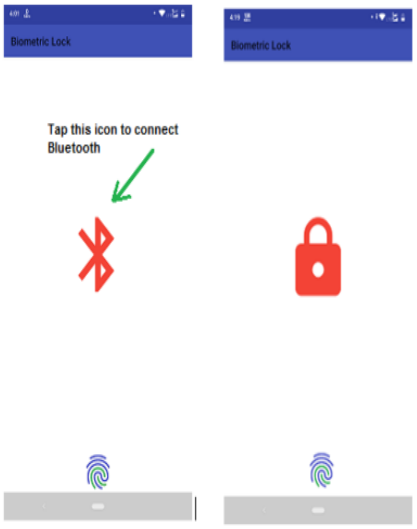

Fig -7: Layout within the app.

On touching the fingerprint symbol, a message box requesting to unlock with fingerprint pops up. Next touch the fingerprint sensor on the smartphone. In the event that it matches with the fingerprint set in the smartphone, at that point it turns the lock to 'on position' and simultaneously the lock symbol changes into unlocked icon. (Refer Fig 8).

SOFTWARE	HARDWARE
Kodular	Bluetooth HC 05
Arduino IDE	Broken Lock
	Arduino Nano
	Servo motor
	Wires-10 cm
	Battery 5-6 V

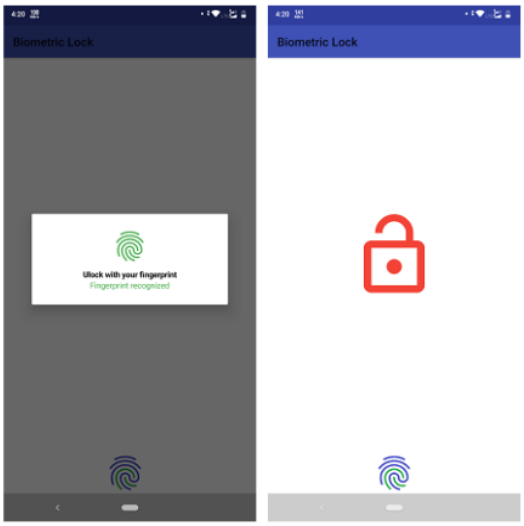

Fig -8: App after asking to touch Fingerprint sensor.

If the fingerprint scanned doesn't match with the one already stored, then the lock moves back to locking position. (Refer Fig 9).

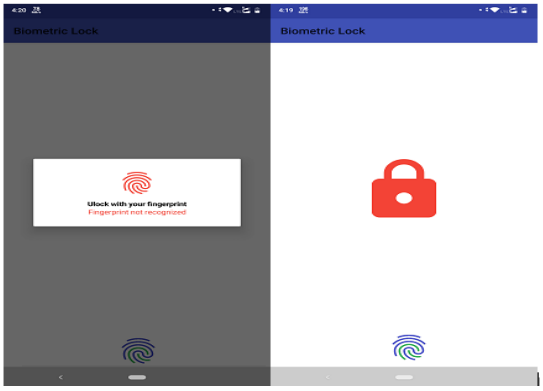

Fig -9: When the fingerprint doesn't match.

3.REQUIREMENTS

1. Arduino Nano: Is a microcontroller.

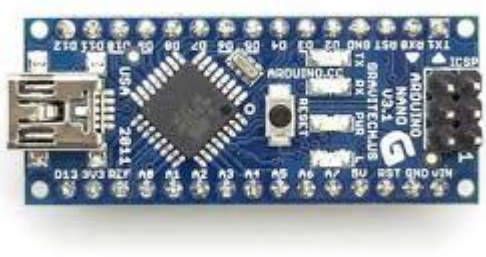

Fig -10: Arduino Nano.

2. Bluetooth HC-05: HC-05 module is an easy to use Bluetooth SPP (Serial Port Protocol) module.

Fig -11: Bluetooth HC-05.

3. Servo Motor: Motors are used for locking and unlocking the door.

Fig -12: Servo Motor.

4. USES

4.1 Security

The conventional lock and key based framework have a lot of vulnerabilities. The significant one among them is the way that the key can be effortlessly duplicated. This might result in an unwanted intrusion by a stranger at any point of time. Fingerprint of each person is unique; with the usage of a biometric lock it is nearly impossible for someone to break into your private property.

4.2 No risk of misplacing

Whilst using traditional locks there is always a moment of time where we might have misplaced our keys or we might not have enough time to search for them, in such situations there is no other solution than breaking the lock or getting a new pair of keys. This can be avoided using our biometric lock which is hassle free and very handy.

4.3 Cost-Effective

The cost estimation for our proposed project is very economical and in fact very negligible. No sophisticated instruments are being used in here, all the components required are easily available in the market.

4.4 Usability

In this biometric locking system, all we need to do is to scan our fingerprint using the fingerprint sensor readily available in a smartphone, with no added tools. This makes the process quite hassle free and quick.

4.5 In-accessible

A conventional lock can be picked or broken into. A card-based entry system can be hacked into or the card can be misplaced. These are not entirely fool-proof. Since fingerprint of each person is unique, which is the only criteria required to get access, the security provided here is quite reassuring.

5. CONCLUSION

Fingerprint lock have gained tremendous benefits compared to conventional key door locks, combination door locks, keyless keypad lock or card reader door locks. Thus, thumbprint door locks surpass security protection, convenience, and speed. Fingerprint reader scanning is the most mature and tested type of biometric technology. Recent studies on biometrics have shown that compared to the hand method, fingerprint is more accurate and cost-effective. The duplication of biometric fingerprint technology is virtually impossible, only one in one billionth of a chance. Biometric security guarantees a positive method of user identification with something that cannot be lost, replicated or stolen. This system is very cost-effective and easy to install and is designed under different modes which makes it useful. The Smart locking system has great potential. It will allow users to forget about their traditional key and to use only their mobile device to get access to the needed area. The system will be developed in the future to provide more extensions and to be as mobile as possible.

ACKNOWLEDGMENT

We thank Dr. Satish G.C, department of Computer Science and Information Technology, Reva University who has been supporting us throughout the entire project as our guide and a mentor. He has always lent us a helping hand to accomplish our project by helping us come up with innovative ideas.

REFERENCES

1. Arpita Mishra, Siddharth Sharma, Sachin Dubey, S.K. Dubey, “Password Based Security Lock System”, International Journal of Advanced Technology in Engineering and Science, 2011.

2. Bhalekar Pandurang, Jamgaonkar Dhanesh, Prof. Mrs. Shailaja Pede, Ghangale Akshay, Garge Rahul, “Smart Lock: A Locking System Using Bluetooth Technology & Camera Verification”, International Journal of Technical Research, 2013.

3. Lia Kamelia, Alfin Noor hassan S.R, Mada Sanjaya and W.S., Edi Mulyana “Door-Automation System Using Bluetooth-Based Android For Mobile Phone”, ARPN Journal of Engineering and Applied Sciences(ISSN 1819-6608), Vol. 9, No. 10, October 2014.

4. Neelam Majgaonkar, RuhinaHodekar, Priyanka Bandagale, “Automatic Door Locking System”, International Journal of Engineering Development and Research, Volume 4, Issue 1,2013 ISSN: 2321-9939.

5. R.A. Ramlee, D. H. Z. Tang, M.M.Ismail, “Smart Home System for Disabled People Via Wireless Bluetooth”, in Proc. of IEEE International Conference on System Engineering and Technology, pp. 1-4, 2012.