

CHOOSING MOST AFFORDABLE SMART DOOR LOCK

¹Padamanaava Karmakar,²Prof. Kaushal Gor

¹PG Student,MCA,Parul Institute of Engineering and Technology-MCA
Parul University , Vadodara,India

²Assistant Prof.,MCA, Faculty of IT & Computer Science,Parul Institute of Engineering and Technology-MCA
Parul University , Vadodara,India

¹karpadmanava16@gmail.com,²kaushal.gor@paruluniversity.ac.in

Abstract: Our generation is smart, people are getting smarter by using smart technologies. Smart devices make life simple, easy, and secure too. Now talking about security, the general public has significantly worried about conceptual security either in family units or in workplace conditions. So the setup of Smart Lock is much needed in present condition. Using the conventional key locks there are so many difficulties like what if your keys are lost, or thieves may break through old locks or maybe they can get your keys somehow and breakthrough your house or workplace. Many studies have developed or tried to develop Smart Door Lock in various techniques. But there is one thing to remember, not everyone can afford a high-cost security system wherein this vast population everyone needs an affordable security system or we can say smart door lock for them. So I am working on this to compare various Smart Door Locks already available and getting the conclusion which can be most affordable for all of us rather than only high profile rich people.

Keywords: Bluetooth, Internet-Of-Things, Smart Door Lock, Sensors, Servo.

1. INTRODUCTION

A door lock is an automated lock that uses a top connection and now a key exchange to perform locked and unlocks activities on a doorway when it receives such instructions from an internet - connected device. It also manages access and sends alerts for so many items it monitors, as well as a few more critical events related to the computer's health. A smart home would not be complete without keyless. The preponderance of access control systems are installed on biological locks (such as deadbolts) and practically enhance the standard lock. Smart securing mechanisms have just recently been developed. Smart locks, like regular locks, need two basic components that function: hardware locking and indeed the key. The key in these password protection is a phone or a bespoke door lock that's been configured expressly for such an application and instantly delivers the credentials needed to unlock the door remotely.

Passcode lock users must use a fictitious token to provide accessibility to a foreign entity. This key may be sent to the sender's smartphone using practices are adopted mechanisms like e-mail or SMS. The reception will be ready to unlock the home security system for said duration specified by the sender after getting this key. To grant or deny admission, access control systems may be operated remotely using an iPhone app. certain authentication technologies come with a built-in Wi-Fi network that allows for checking features like admission alarms and camera to demonstrate who is trying to get access. Several access points can be used with an interactive doorbell to let the user know that was at the gate and if they should be there. Many biometric systems now feature biometrics like touchscreens. Biometric system are becoming increasingly widespread as a result of their greater dependability than passcodes alone. This is due to the fact that they depend on physical traits so instead of file system.

The goal of our study paper is to detection out the most affordable door lock. So, I have taken mainly 4 different types of door locks for detailed comparison and then I can get the conclusion. Before concluding it would be in our mind that we are giving priority to the average people and trying to come out with their solution. I will compare their detailed techniques, methods, and implementations.

2. LITERATURE REVIEW

Arpita Mishra et al. in their study illustrated that they have created a GSM-based password-based smart door lock that allows the user to manage the operation remotely. The user may turn on or off the remote telephone simply by pushing the keypad. A matrix keypad, a GSM modems for secure digital display, and a latching mechanism extender are all included in the model, which is controlled by the microcontroller. The controller's keypad serves

as a password input method for opening and closing the door. The door lock unlocks as the time the user enters the proper password. The security alarm will sound if the combination is wrong. The GSM modem connects to the controller through a UART interface. When an unauthorized user enters an incorrect password, the controller sends a message to the owner over the modem. They used a Tmega 8 microcontroller, a 4*3 number keypad, a Automotive centering lock actuator, 16*2-character LCD display, as well as electricity to make the gadget. The essential notion of java programming is that the microcontroller should detect the press key values and, based on the make a dramatic difference of port D, returning the key pressed, and check when the input and saved passwords are the same or not. The motor is engaged and indeed the world is changing if they match [1].

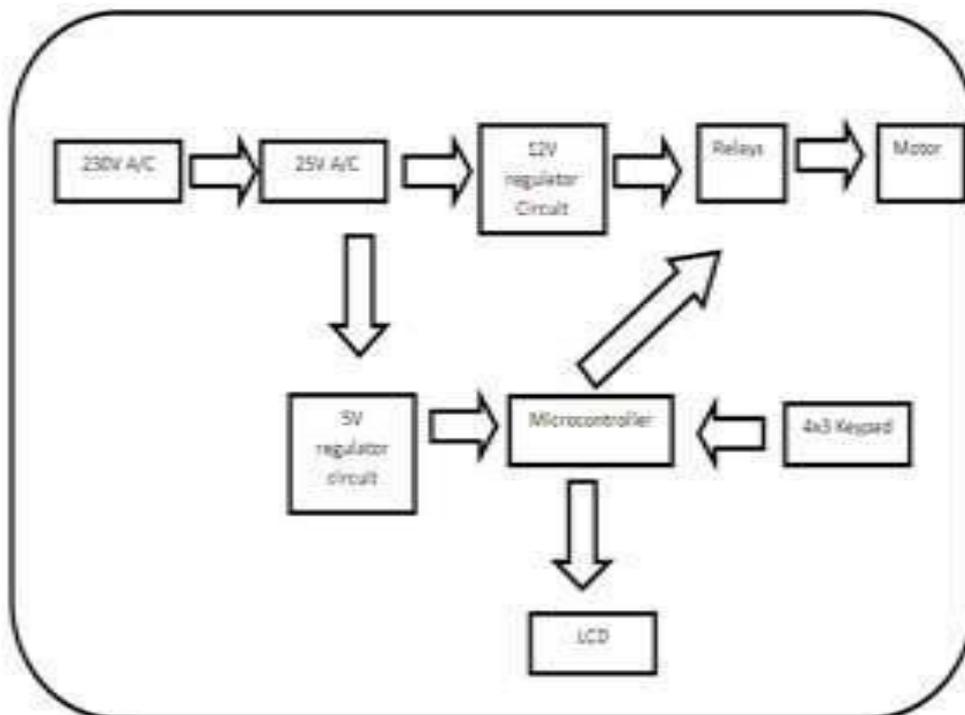


Figure 1: Illustrated the Block Diagram of The Suggested System.

Karthik A Patil et al. in their study embellished that They have created a budget-friendly smart door lock by using biometric authentication. They are using a mobile phone's fingerprint scanner. They are using Arduino Nano as a microcontroller, Bluetooth HC 05, Servo motor, wires 10 cm, battery 5-6 V, these components as hardware. They are using Kodular to bake Android app and Arduino IDE as software. Authord created a regular that saves the device ID. Sent via Bluetooth. It is stored in a "read" string. If the condition is used for verifying device id. If it is authenticated the application sends the device id to the Arduino Nano board. If authentication is matched the servo motor is unlocked. If authentication is not done that is fingerprint is not matched the lock has remained in lock position.

2.1.Arduino code checking device

Then they bake an android application. After the installation of the application and the code is uploaded into the smartphone. Then following components are connected then soldered together.

Pins Components

5V Bluetooth 5V

Rx Bluetooth TX

TX Bluetooth Rx

GND Servo Motor GND

GND Bluetooth GND

Pin 9 Servo Motor Signal Wire

Finally, a servo motor is installed in the broken lock, which is driven by a 5-9V battery. The Bluetooth on the telephone is then switched on, and it is coupled also with a Bluetooth module on the Arduino board. When you first launch the app, the Bluetooth symbol transforms into a lock icon. A message box appears when we tap the fingerprint sign, demanding that we unlock it with our fingerprints. Next, place your finger on the phone's fingerprint sensor. If it confirms the fingerprint stored on the cellphone, the lock is turned to the 'on' configuration, and the lock indicator transforms to an enabled icon. Figure 2 shows the Arduino setting servo system, Figure 3 discloses the system running code, and Figure 4 shows the connection of the code and Figure 5 discloses the application interface connection of the system, Figure 6 embellished the fingerprint scanner looks when it does not match with the system.

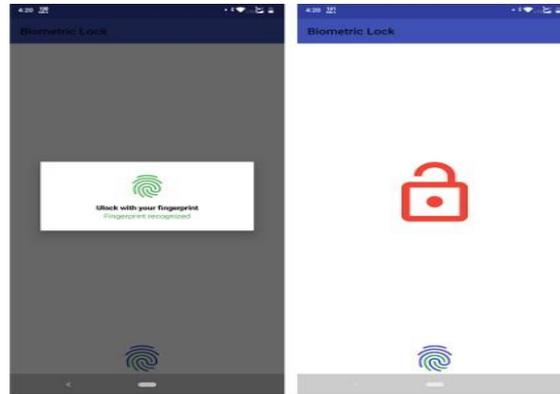


Figure 2: Illustrated the Arduino Setting Servo Used in the Study

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

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

Figure 3: Illustrated the Arduino Code Checking Device Used in the Study

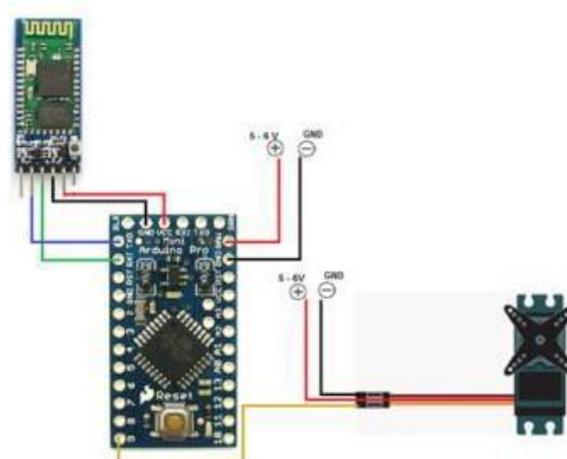


Figure 4: Illustrated the Connection of the System Used in the Study

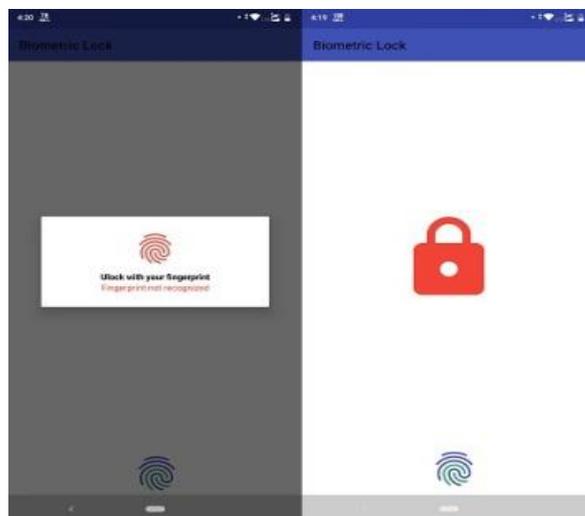
```

#include <Servo.h>
String reads;

Servo myservo;

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

```

Figure 5: Illustrated The App Interface Of The System.**Figure 6: Illustrated The App When Fingerprint Doesn't Match.**

Kristoffer et al. in their study embellished the installed a smart door lock with enhanced security. They employed a Particle Photon microcontroller, as well as a Bluetooth beacon from Estimate. A transistor has two circuits: one for control and one for the load. Only Latest runs through a coil when the controller is triggered, causing a force of attraction that pulls the magnetic and shuts the load circuit. A repeater is a system that enables a single signal to control various networks. When a moderate circuit has to control an increased or high-voltage circuit, relays are used. In terms of direct driving, microelectronics and many other minimal technologies may drive valves to control power flow. The Photon MCU was being used to demonstrate the basic functionality of the concept. A test program to drive an LED was written on the microprocessor itself. The electromotive force coming from the source is then managed via a resistor. A test plan was built upon a prototype to control an outside LED. The signal would be interpreted by the microcontroller to decide whether the LED should be turned on or off [2]. Figure 7 shows the system circuit with the door lock.

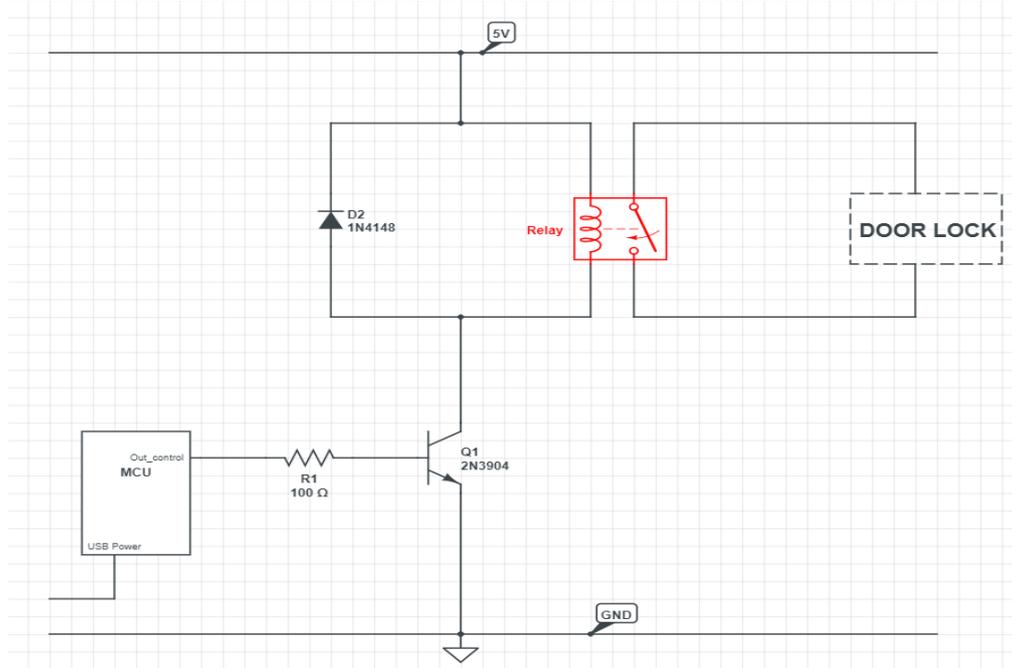


Figure 7: Illustrated the System Circuit Used in the Study

- The Android application requests authentication through HTTPS by delivering the username and password.
- With the password hashes, resource ID, and client ID supplied, the "Auth API" requests an authenticator from Azure AD.
- If the information given with the inquiry is correct, the Azure AD replies with a two-hour access token [3]–[8].
- The token is returned through HTTPS to the Android application. Authentication mechanism calls to that same Door API are now possible using the Android client.
- The Android app will begin listening for beacons that have been registered. When the program receives a beacon broadcast, it verifies that the transmitters are from a legitimate source.
- If the beacon certification is successful, the Android should request that the door be opened. The HTTPS call includes the authentication token and indeed the function name.
- If the received application is authenticated and approved, the proton would get a new Encrypted link from door. The Particle device's distinctive access control list and the device will be included in the Spark Cloud request.
- • Well with help of the listener, Glimmer of hope will convey the required function (in this case, "open window"). Right device ID.
- The Photoelectron machine will return a particular value indicating whether or not the function requested was properly performed.
- The door API will get an HTTPS response from Spark Cloud with information about the request's status.
- The Door API returns a response to Android, indicating whether or not the call was successful.

- It is, without a doubt, a highly secure and complicated process. LAN distrust, environmental difficulties, and app over privilege are some of the obstacles it faces. However, it is rather expensive to implement, hence it cannot be considered the cheapest SDL.

3. DISCUSSION

The system is intended for security purposes. It will work as follows: when the doorbell rings, the camera will be triggered, and the camcorder will capture video of the woman standing in front of the door, which will be shown to both the unique authentication UN agency is away from home, who will recognize the person and possibly share the key with them for a formulated amount. This will provide a great level of protection for houses while requiring no human participation [9]–[11].

The system is designed such that the user's motion is caught by the camera and the user is recognized so that only he is given a code to lock and unlock. Our Bluetooth-enabled smart lock system can function over a wireless network. There are five segments in total:

- The management module serves as the system's brain.
- The protective operation is controlled by the motor module.
- The communication and management modules are utilized to communicate amongst the devices.
- For authentication, the I/O module utilizes the Embedded System and the Smartphone.
- The device module includes the phone and Bluetooth.

To increase the system's security, the mobile device requires a word. A microprocessor is used in the door hardware to govern a linear drive that works as a protective mechanism. Because the Bluetooth protocol is already implemented into various golem products and is protected by the protocol itself, it was selected as a communication option. It also fits nicely within the project's planning requirements for a short-range, mobile affiliation mechanism. Our Bluetooth-enabled smart lock system can function over a wireless network. There are five pieces to a unit:

- The management module serves as the system's brain.
- The motor module is in charge of the protective system.
- The communication and administration modules, which are utilized to communicate amongst the devices.
- The I/O modules that authenticate with an RFID reader.
- The device module, such as a phone or Bluetooth

The owner of the residence is the primary user of the sensible lock. When the buzzer sounds, the camera is activated, and the user's movements are recorded. The owner is aware of who is present at the entryway, so he or she may identify the individual and perhaps share the handle for a particular essential amount. The technology gives excellent security throughout this procedure. They're using the Golem software package, version 4.0, with Tomcat as the web server and MySQL as the database. Hardware includes a Bluetooth phone, an ARM7 controller, and a motor [3]–[7]

4. CONCLUSION

For Password Based Security Lock System, we can conclude it's pretty much affordable as it is using Moto, microcontroller, LCD, and the keypad. They are easily implemented and budget-friendly too. It has a major

drawback if the password is forgotten it's quite difficult to unlock the door and goes through a lengthy process. Also LCD, Keypad remains outside door so anyone harms them or even environment can cause any harm so it must be protected.

For the 2nd Smart door lock i.e. Smart door lock using IoT, it is using Arduino nano, BT HC 05, servo motor, and some budget-friendly batteries. This lock operates the whole system via your phone and the authentication it is using is your fingerprint which is already available nowadays in every mobile phone. As it is biometric based it provides you very strong security without any doubt and you don't even have to spend much cause it is using your mobile. Also, the whole system is not much complex and not much exposed to the outer side, so environmental harm is lesser here. So, we can keep it as our top choice till now.

On 3rd type of Door, the lock is IoT based smart door lock. It is also using a microcontroller, Bluetooth beacons, mobile along with cloud computing concepts. They are using Azure active directory to authenticate users, Google beacon API, and so on, They have tried high-class security door lock implement but the components are a bit costly. And it got some implementation flaws too, like LAN mistrust, application over privilege, environmental issues. There idea is very unique but the technologies they are using like Google Beacon API, Google messages API are quite new and needed more security updating. So the conclusion for this is we cannot completely rely on the security and its budget tight too. Smart lock: a Bluetooth-based locking system with camera verification uses arm 7 controllers, liner actuator, mobile with Bluetooth, dc motors and camera sensors .so, it is using more sensors like a camera which makes it a little bit costly and hard to maintain also .some sensors are exposed to environment so easily can be harmed .but if we talk about security, yes it provides sufficient security so it can be considered as a choice if one extends his budget. After analyzing all these points, I can get the conclusion that type2 is most affordable and secure at the same time.

REFERENCES:

- [1] S. . D. “ Arpita Mishra, Siddharth Sharma, Sachin Dubey, “PASSWORD BASED SECURITY LOCK SYSYTEM” International Journal of Advanced Technology in Engineering and Science www.ijates.com Volume No.02, Issue No. 05, May 2014”.
- [2] KRISTOFFER DJUPSJÖ MASAR ALMOSAWI, “EXAMENSARBETE INOM TEKNIK, GRUNDNIVÅ, 15 HP STOCKHOLM, SVERIGE 2018 IoT Security Applied on a Smart Door Lock Application”.
- [3] G. M. Janeksela, “US Workforce and Educational Challenges in the Global Economy,” *Int. J. Sociol. Study*, 2014.
- [4] F. Rizvi, “Global mobility and the challenges of educational research and policy,” *Teach. Coll. Rec.*, 2009, doi: 10.1111/j.1744-7984.2009.01172.x.
- [5] H. Malone andb. M. Koopmans, “Leading educational change. Global issues, challenges, and lessons on whole-system reform,” *Glo Educ. Rev.*, 2015.
- [6] P. Baladincz and J. Hancsók, “Fuel from waste animal fats,” *Chem. Eng. J.*, 2015, doi: 10.1016/j.cej.2015.04.003.
- [7] S. M. Hossain and M. M. Hasan, “Energy management through bio-gas based electricity generation system during load shedding in rural areas,” *Telkomnika (Telecommunication Comput. Electron. Control.*, 2018, doi: 10.12928/TELKOMNIKA.v16i2.5190.
- [8] S. Walitza *et al.*, “European research in early onset obsessive compulsive disorder (OCD) and the International College of Obsessive Compulsive Spectrum Disorders (ICOCS),” *Eur. Child Adolesc. Psychiatry*, 2011.
- [9] Sophos, “Internet Security Threat Report , SOPHOS,” *Security*, 2014.
- [10] R. Baiad, O. Alhussein, H. Otrok, and S. Muhaidat, “Novel cross layer detection schemes to detect blackhole attack against QoS-OLSR protocol in VANET,” *Veh. Commun.*, 2016, doi: 10.1016/j.vehcom.2016.09.001.

- [11] Y. Geng, H. Dong, B. Xue, and J. Fu, “An Overview of Chinese Green Building Standards,” *Sustain. Dev.*, 2012, doi: 10.1002/sd.1537.