Innovative electronically and mechanically assisted Garage door system: A review of the autonomous garage door system

Parupalli Ravi Kiran, Gautam Krishna, Chinatalpati Krishna Vinay

Lovely Professional University, Punjab, India

ABSTRACT: This project aims to increase home security construction of a low-cost system that monitors garage doors and transmits their status to a receiver conveniently located inside the user's home. This allows the user to monitor their garage doors from the comfort of inside their home without having to step outside and look at the garage. The receiver includes a screen for displaying system information and LEDs for easy viewing of garage door status from a distance. The system has sufficient range to place the receiver anywhere in the House while still providing accurate garage door status. This project aims to increase home security doing this simple, inexpensive system that is sufficient for the average household.

Keywords: Internet of things, Radio Frequency Identification, Stability, Garage door system, Arduino, Innovation.

INTRODUCTION:

Radiofrequency identification, or RFID, is an interesting technology that has grown in popularity in recent years. It creates the possibility of marking something with a very small passive chip which then allows the remote reading of information on that chip. RFID tags are commonly used for magnetic door security cards, lost animal identification, and, more recently, near field communication on smartphones. In this tutorial, I'll walk you through some basics of how RFID works, describe a few different types of RFID and show how an RFID garage door opener can be built. If the code matches, the opener increments its counter just above the corresponding code and opens the door. In addition to using remote controls, some users mount keypads in front of their garages that synchronize in the same way with door openers; these keypads broadcast a code when a user correctly enters a numeric password.

The easiest way for attackers to open a rolling code garage door opener is to sync it with a new remote. Replacement remotes are available at almost any hardware store and only take a few minutes to sync in the garage. An equally simple option is to attack the keyboard while spying on the user or to infer. Brutally force the code. A third option is a physical attack. Most door openers include an emergency release cord just inside the door. If an attacker can slide a metal hook over the door and lock onto that rope, a skilled tugboat can unlock the door. The last option for attacking traditional openers is to attack the rolling code mechanism itself. Many scientists have evolved over the last decade methods to derive a KeeLoq key giving access to a synchronized and functional remote control. A simpler but less effective approach is sniffing the code from the remote control pressing the "Open" button outside the range of the opener, then using that code before the owner do not go back to the door.

The House, all of these attacks, require close proximity to the garage or remote and are difficult enough that virtually any intruder would rather smash a window, force a door open, or pick a lock.

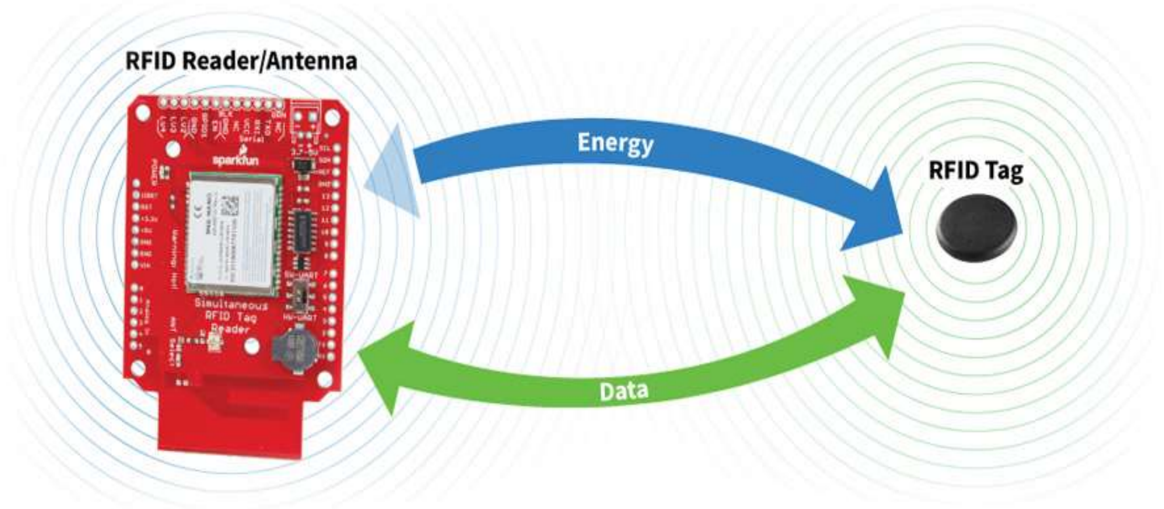


Fig1: RFID reader sensor

Checking as many codes as possible helps to ensure that the remote control and opener do not lose synchronization when a user presses the button outside the reception area of the opener.

Different working mechanism:

Openers and The Keypad: -

The automatic garage door opener allows the door to be opened and closed with no effort other than the push of a button, which means you can open the door from the comfort of your car.

One downside to these openers is that some brands can use the same frequency. Therefore, if your neighbour has the same system as you, he may be able to open your garage door with his remote control. Fortunately, you can adjust the frequency of the garage door opener inside the garage.

In most cases, owners also have a keypad, which can be used to open the door. This keyboard

resides outside the home, so you need to make sure you choose a unique code: random numbers instead of your address, date of birth, etc.

Fig 2: Manually operated garage door opener.

PROPOSED WORKING MECHANISM:

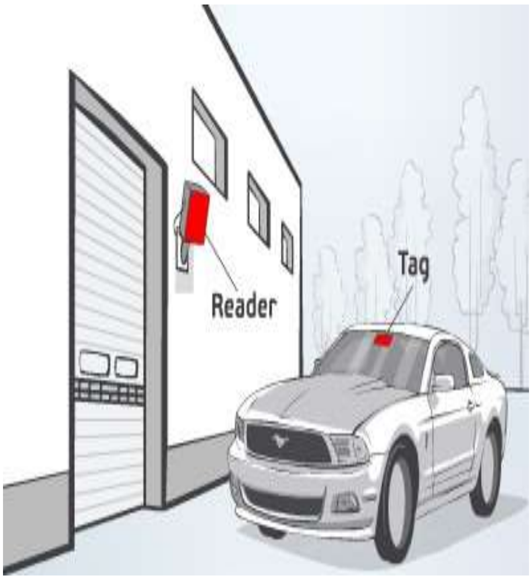
Openers and the Internet of Things: -

Internet exposure of garage door openers could make them such easy targets as to be a real one risk. What if an attacker could indefinitely send open commands to any opener, And if once an email account is hacked, the hacker has a clear path to find the user's home address and credentials to open this user's garage? What if an attacker managed to download an entire database?

User credentials for IoT openers? Either of these possibilities would make home intrusions so easy.

As inevitable. We are starting to see this development with cars that use Bluetooth dongles.

It became so easy and cheap to seize some that insurers began to demand additional security measures.



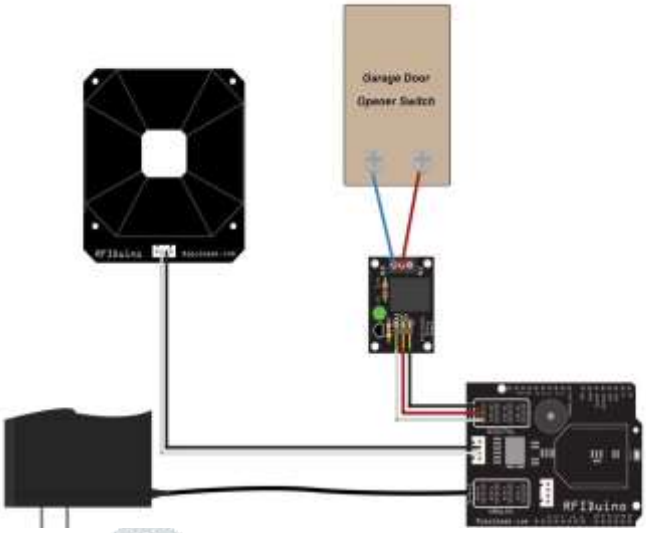


Fig1: An image of RFID reader and tag **Fig4:** 2 A setup of RFID reader and tag

WORKING MECHANISM:

The IoT industry has made it clear that having a central service serving as a clearinghouse for authentication, authorization, and commands is a necessity, and it's easy to see why: it frees them from configuring home routers, configuring dynamic DNS when client IP addresses change or have access to all relevant user data when it is unavoidable technical support calls arrive. The problem is, the cloud service opens another attack surface, and a big one: instead of having to hack a single IoT opening at a time, attackers can try to hack them through the cloud service. There is one point in failure for authentication, integrity and availability.

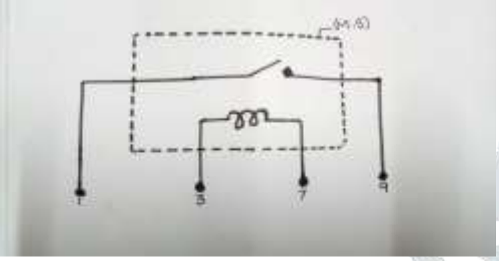
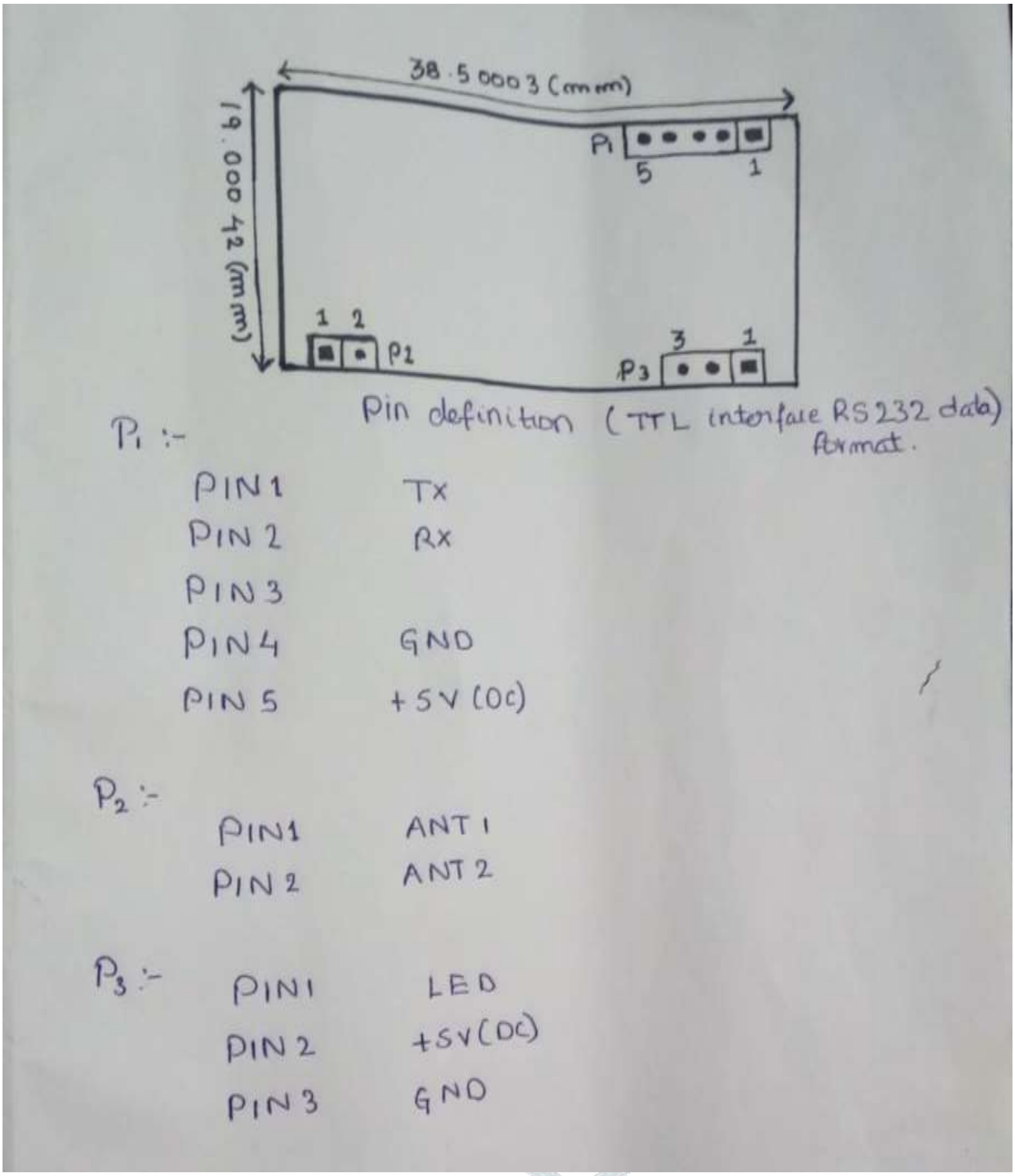


Fig5: The connection of pins

1. Run pin 4 of the Arduino to pin 3 of the messenger race. When pulled high, it will provide enough current to close the exchange rate.
2. Run relay pin 7 to ground.
3.Add the diode between pins 3 and 7 with the paint stripe towards pin 3 of the relay.

The Body:-



Pin definition (TTL interface RS232 data) format.

P1 :-

PIN 1	TX
PIN 2	RX
PIN 3	
PIN 4	GND
PIN 5	+5V (DC)

P2 :-

PIN 1	ANT 1
PIN 2	ANT 2

P3 :-

PIN 1	LED
PIN 2	+5V (DC)
PIN 3	GND

Fig6: The setup and wiring for the RFID system

Open Garage door:

Most garage door openers work very simply, opening when they have a closed contact. When you press the button on the wall, you close the contact. On my garage door opener, I have bollards

where the button wires are connected. You can see the terminals highlighted here:

1.Hook up Pins 1 and 9 from the relay on the breadboard to the terminals on the garage door opener.

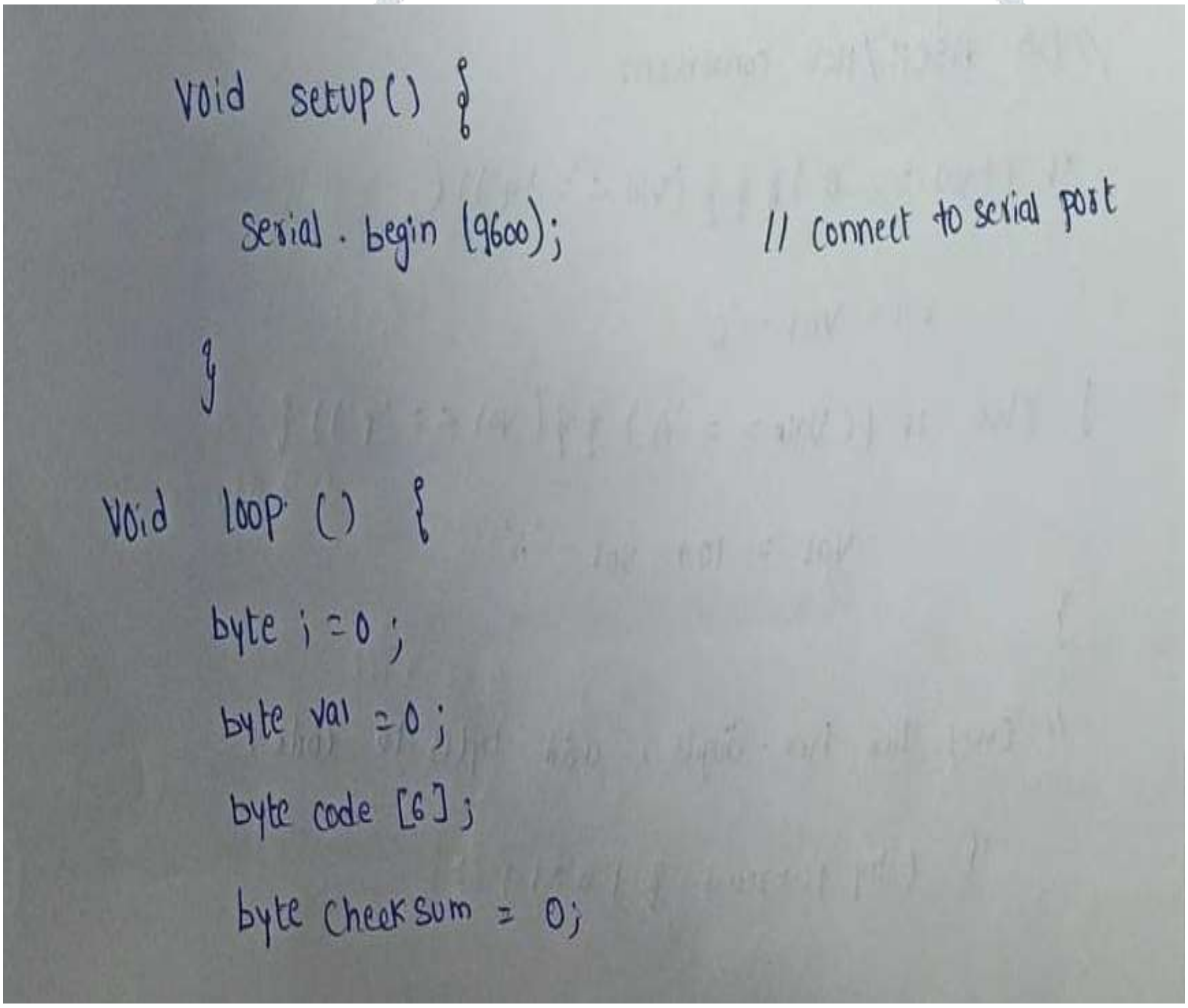
2.Wave your RFID tag near the antenna.

3.Watch the door open.

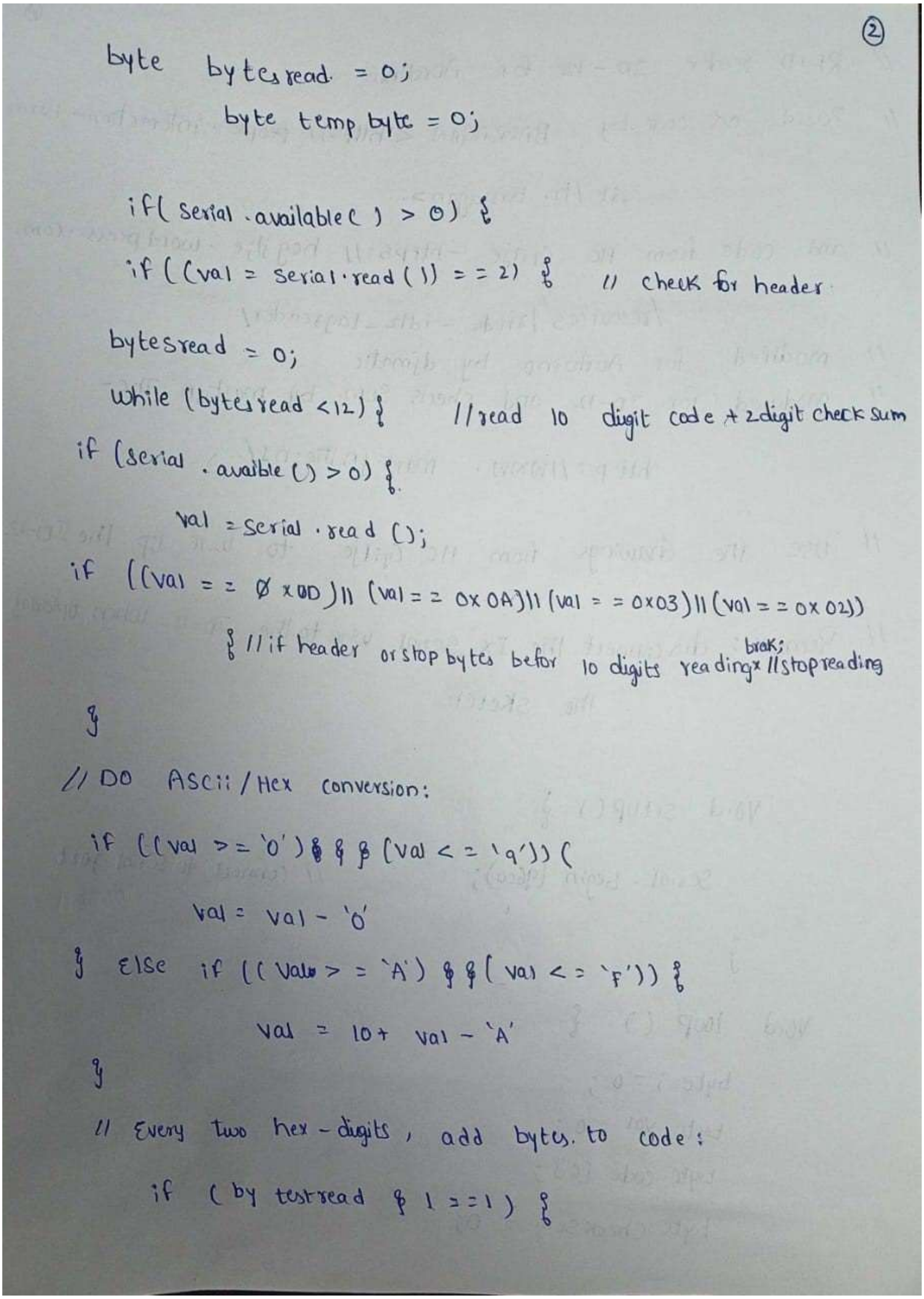
Fig7: The garage door opener.

The RFID Reader Setup:

Using the RFID reader datasheet or instructions, connect the power, ground, serial, and antenna pins. Below is the pinout diagram of the drive I have. We use Arduino pins 2 and 3 for serial communication with the RFID card so that we can leave pins 0 and 1 as the console output.

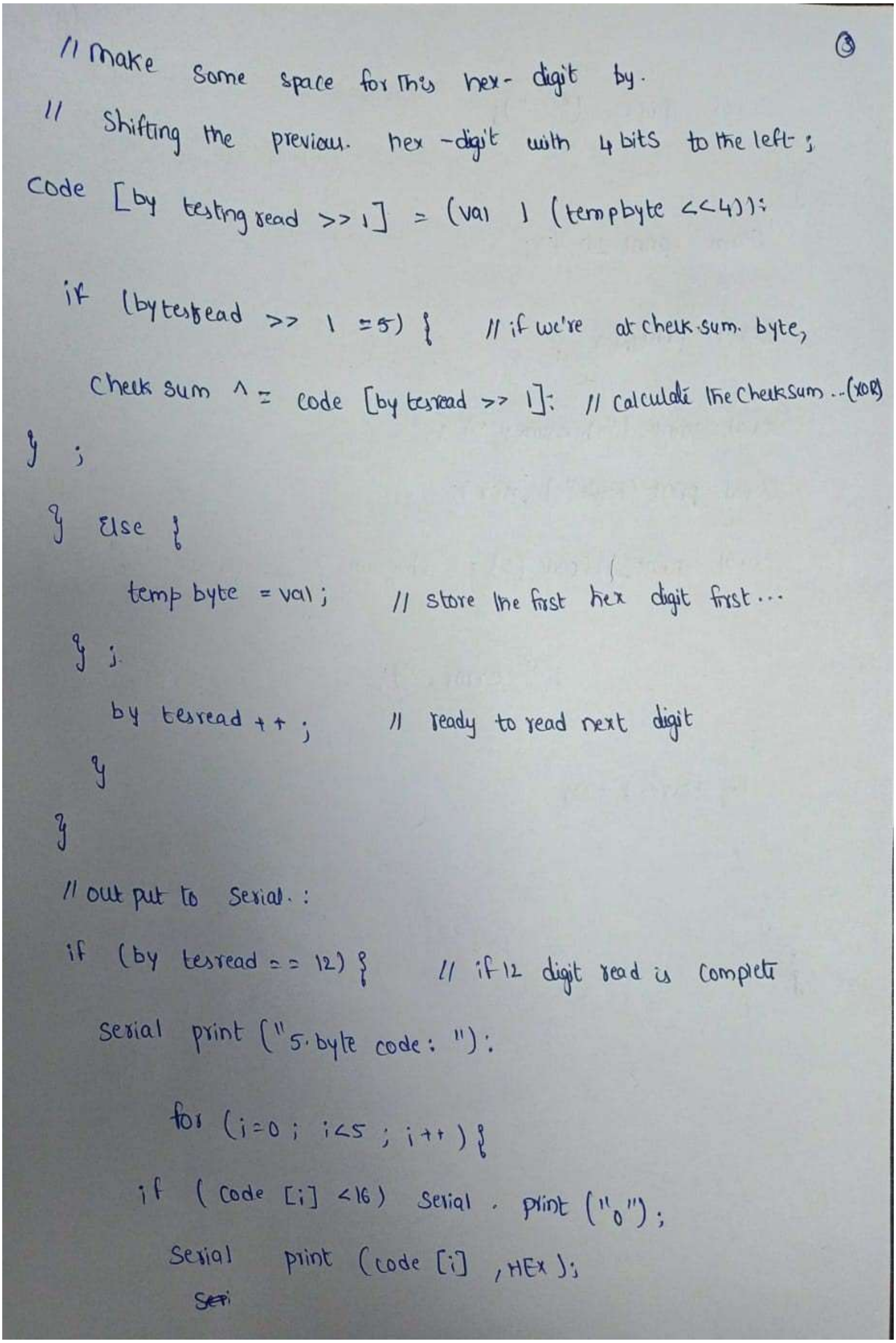


```
    void setup() {

        Serial . begin (9600);          // connect to serial port

    }

void loop () {

        byte i = 0 ;

        byte val = 0 ;

        byte code [6] ;

        byte CheckSum = 0;
```



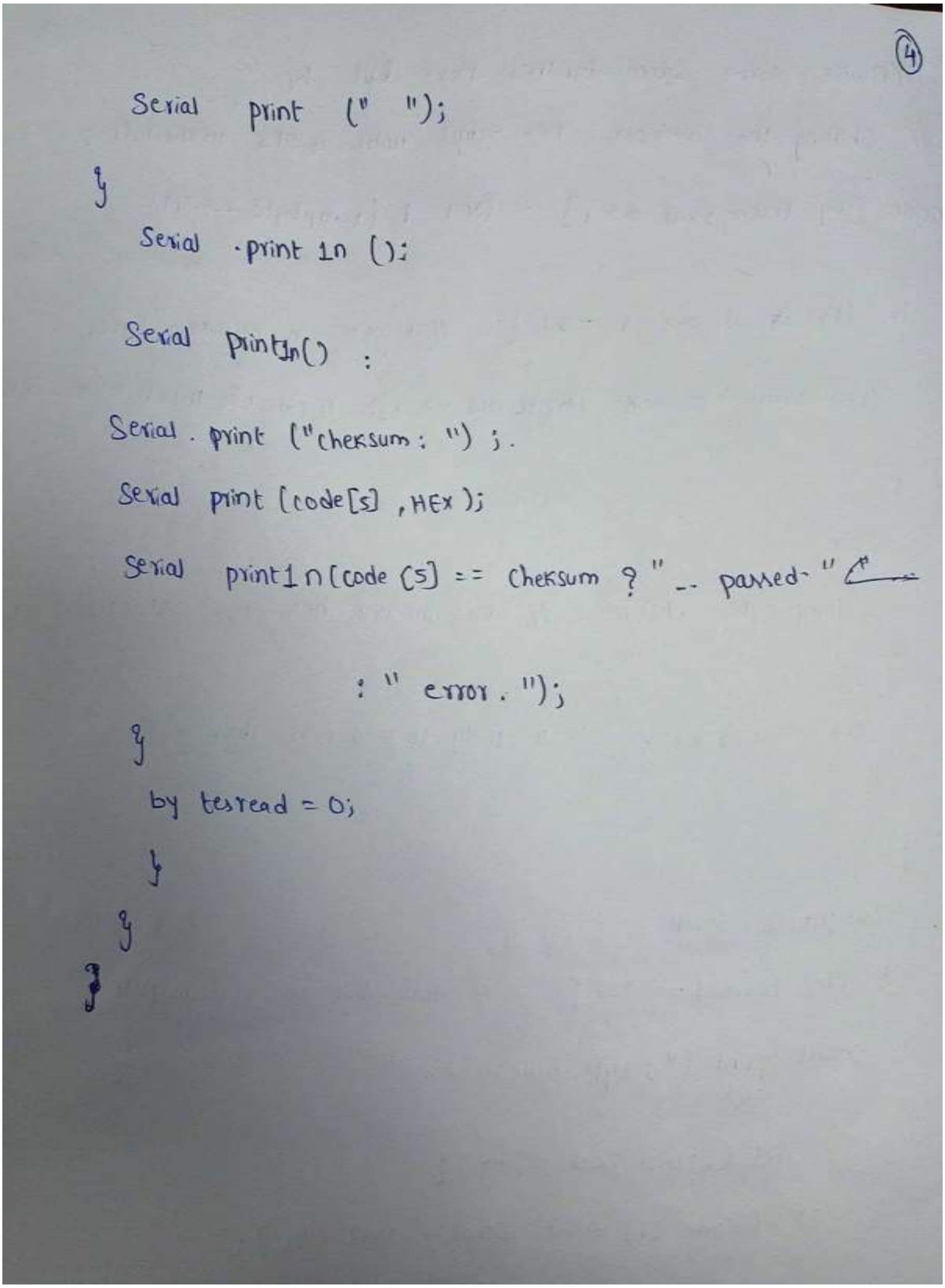
2

```
byte   bytesread = 0;
       byte tempbyte = 0;


   if( serial.available( ) > 0) {
   if((val = serial.read( )) = = 2) {    // check for header

 bytesread = 0;
 while (bytesread <12) {     //read 10 digit code + 2digit check sum
if (serial .avaible () > 0) {
        val = serial .read ();
if ((val = = Ø x0D)|| (val = = 0x 0A)|| (val = = 0x03)|| (val = = 0x 02))
             { //if header or stop bytes befor 10 digits reading brak; //stopreading

 }

// DO ASCii / Hex conversion:

 if ((val >= '0') && (val <= '9')) (
        val = val - '0'
} Else if (( val > = 'A') &&( val <= 'F')) {
           val = 10+ val - 'A'
 }
 // Every two hex-digits, add bytes. to code:
    if (bytesread & 1 ==1) {
```



③

```
// Make Some space for This hex- digit by.
// Shifting the previou. hex -digit with 4 bits to the left ;
Code [by testing read >> 1] = (val | (tempbyte <<4));

 if (bytesread >> 1 =5) {   // if we're at check.sum. byte,
   Check sum ^= code [by tesread >> 1];  // calculate the Checksum ..(XOR)
} ;
 } Else {
     temp byte = val;   // store the first hex digit first...
  };
    by tesread ++;   // ready to read next digit
   }
 }
 // out put to Serial. :
 if (by tesread == 12) {   // if 12 digit read is complete
   serial print ("5.byte code: ");
      for (i=0; i<5; i++) {
    if (code [i] <16) Serial . Print ("0");
      Serial print (code [i] ,HEx);
      Seri
```



```
                                                            4
        Serial   print   ("   ");
  }
         Serial   .print 1n ();

        Serial  Print1n()   :

       Serial . print ("cheksum :  ") ; .
       Serial  print (code[5] ,HEx );
       Serial   print1n(code (5] == Cheksum ? " -- passed- " (

                          : " error . ");
    }
       by tesread = 0;
      }
    }
 }
```

Fig8: The code for RFIDuino

Results:

First, the RFID reader card reads the tag and transmits the code to the Arduino. The Arduino then reads the serial connection code and compares it to a list of authorized RFID codes. If the tag is on the allowed list, the Arduino will put a pin high to provide 5V to close a relay. When the relay closes, it connects the signalling contact terminals of the garage door. Then the garage door opens.

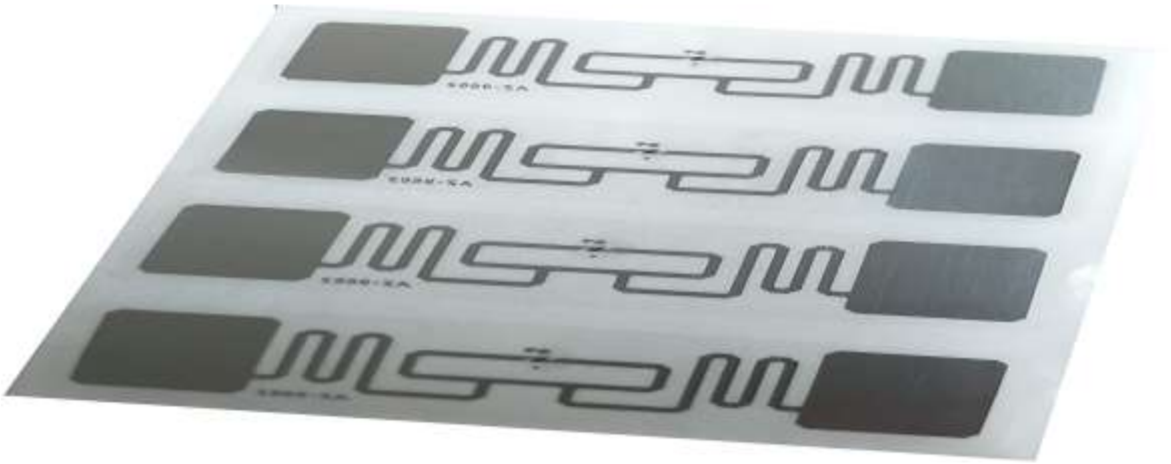


Fig9: RFID reader card.

Make it Permanent:

1. Mount the antenna where it can read the tag through the door or wall. RFID can pass.
2. Solid objects so that the antenna can be hidden behind the garage wall depending on the material.
3. To find one place to read the label. Transfer the circuit to a preboard and solder the permanent solution.
4. Place the project in a box and mount it in your garage.

CONCLUSION:

The formats and frequencies of RFID chips vary considerably. There is a whole alphabet of types. Many smartphones read NFC and MIFARE formats.

There are several types of RFID. Some labels may have a small amount of written data that can be read later. Others are so sophisticated that they require the reader to point to an encryption key before the tag can decode and return its content.

In this project, I will be using an RFID tag and an Arduino to open the garage door when the authorized tag is detected. Using a low-level RFID component is quite a complicated task, so we are using a connection board that does the low-level reading and transmits the tag code through serial pins.

This is how most RFID patch plates work. This tutorial uses one of those breakout boards.

The relay to the breadboard. The two internal pins run the electromagnet that will close the relay. You can see how in the diagram below, the current through pins 3 to 7 will affect the relay.

Most garage door openers work very simply by opening when they have a closed contact. If you press a button on the wall, make contact. In my garage door opener, I have terminals where the button wires are connected.

If you press a button on the wall, you will lose contact. In my garage door opener, I have terminals where the button wires are connected.

For this project, however, we are going to use the EM4100 125K wagon type chip. This type of RFID uses cheap readers and tags.

REFERENCES:

[1] SK. Yong, "60 GHz channel characterizations and modelling" in 60 GHz technology for Gbps WLAN and WPAN, john Wiley & Sons, 2010, ch 2, pp 17-61. [January 31, 2016].

[2] K. Balasubramanian and A. Cellatoglu, "Analysis of Remote Control Techniques Employed in Home Automation and Security Systems," Consumer Electronics, IEEE Transactions on, vol. 55, no. 3, p. 1401-1407, Aug. 2009. [Online]. Available: IEEE Xplore, http://www.ieee.org. [Accessed January 21, 2016].

[3] Parallax Inc. (2000, January 27). “433.92 MHz Transceiver” [Online]. Available: http://media.digikey.com/pdf/Data%20Sheets/Parallax%20PDFs/27986-988pdf.pdf [January 30, 2016].

[4] Garage door remote system with the alert feature, by C. A. Redden. (2013, February 12). Patent US8373555 B1 [Online]. Available: http://www.google.com/patents/US8373555 [January 30, 2016]. This patent has similar aspects to the goals of my project.

[5] J. Margulies, “Garage Door Openers: An Internet of Things Case Study,” Security & Privacy, IEEE, vol. 13, no. 4, p. 80-83, Aug. 2015. [Online]. Available: IEEE Xplore, http://www.ieee.org. [Accessed January 31, 2016].

[6] Sharp. (2006, December 1). “Distance Measuring Sensor Unit” [Online]. Available: http://www.sharp-world.com/products/device/lineup/data/pdf/datasheet/gp2y0a21yk_e.pdf [January 30, 2016].

[7] V. Chunduru and N. Subramanian, “View-based approach to constructing reliable Home Appliance Control System,” in Proc. of the 2006 IEEE Region 5 Conference, 7-9 April 2006, San Antonio, TX [Online]. Available: IEEE Xplore, http://www.ieee.org. [January 30, 2016].

[8] D. Chizhik and R. A. Valenzuela, “Radio Wave Diffusion Indoors and Throughput Scaling with Cell Density,” Wireless Communications, IEEE Transactions on, vol. 11, no. 9, p. 3284- 3291, Sept. 2012. [Online]. Available: IEEE Xplore, http://www.ieee.org. [January 30, 2016].

[9] Texas Instruments. (2013, May). “Mixed Signal Microcontroller” [Online]. Available: http://www.ti.com/lit/ds/symlink/msp430g2553.pdf [January 30, 2016].

[10] R. S. Dilmaghani and H. Bobarshad, “Wireless Sensor Networks for Monitoring Physiological Signals of Multiple Patients,” Biomedical Circuits and Systems, IEEE Transactions on, vol. 5, no. 4, p. 347-356, July 2011. [Online]. Available: IEEE Xplore, http://www.ieee.org. [January 30, 2016].

[11] D. O'Brien, “Audible Alarm Basics,” Digikey. [Online]. Available: https://www.digikey.com/web export/supplier content/mallorysonalert_458/pdf/mallorysonalert_audiblealarmbasics.pdf?redirected=1. [February 20, 2016].

[12] N. Gromicko and K. Shepard, “Burglar-Resistant Homes,” InterNACHI. [Online]. Available: https://www.nachi.org/burglar-resistant.htm. [February 21, 2016].

[13] A. Weber, “Are You Inviting Burglars into Your Home?,” Erie Insurance, July 18, 2012. [Online]. Available: https://www.erieinsurance.com/blog/2012/are-you-inviting-burglars-intoyour-home. [February 21, 2016].

[14] N. Lesson, "Left Open, Garages Will Draw Thieves," Sun-Sentinel, 2006. [Online]. Available at: http://articles.sun-sentinel.com/2006-06-25/community/0606230283_1_garageopener-door-thieves. [February 21, 2016].

[15] J. Zander, “Performance of Optimum Transmitter Power Control in Cellular Radio Systems”, IEEE transaction on vehicular technology, Vol. 41, issue 1, pp 57-62, Nov 1991. [January 30, 2016].

[16] K. Vitkus et al., "Door ajar detection and recovery for a wireless door sensor" U.S. Patent 9 224 287, December 29, 2015. [January 30, 2016].

[17] Sharp, "Analog Output Type Distance Measuring Sensor," GP2Y0A41SK0F datasheet, March 2007. [January 30, 2016].