



ISSN: 0975-766X
CODEN: IJPTFI
Research Article

Available Online through
www.ijptonline.com

STUDY OF SMART SECURITY SOLUTIONS BASED ON INTERNET OF THINGS (IoT)

K.Saishiva¹, Mr.P. Dass²

B.E Student, Department of ECE, Saveetha School of Engineering, Chennai-602105, Tamil Nadu, India.

Assistant Professor, Department of ECE, Saveetha School of Engineering, Chennai-602105, Tamil Nadu, India.

Email: kumaravellatha@gmail.com

Received on: 10.08.2016

Accepted on: 06.09.2016

Abstract

With growing recognition of the IOT (net of factors) and devices getting smarter each day, this paper offers an concept to reform the prevailing get admission to manipulate systems. This technique of Improving the access manipulate gadget guarantees that the machine is wireless thereby decreasing wiring problems. The prototype defined in this paper has the availability of accepting inputs from a smart card reader (RFID reader) or a biometric sensor. Those inputs are processed in the controller (TM4C123GXL-primarily based on ARM Cortex-M4). If the inputs are located to be valid, get entry to is granted to the consumer and the logs are wirelessly transmitted to the laptop the use of a WiFi module (CC3100). Gadget gaining knowledge of algorithms are carried out to reveal and examine accrued information.

Keywords: IOT, get right of entry to manipulate, protection, wireless, WiFi , gadget studying.

1. Introduction

With growing demand from the industry for higher get right of entry to control systems, this paper is an try to make the traditional get admission to manipulate systems smarter and thereby decreasing the risks of breaking in into the places in which those get admission to control structures could be established. EK-TM4C123GXL is the improvement board which is used. Information from RFID reader and Biometric sensors are serially transmitted to the microcontroller. If valid fingerprint statistics or valid

Card no. is obtained, the microcontroller sends a sign to the WiFi module

1. The WiFi module

2. Present on the door gets that signal and trips the relay in keeping with the sign obtained. This is how the door opens.

additionally the WiFi module sends a signal to the computer thru the same WiFi

Now a days we are facing several security issues in home monitoring, and security issues. To reduce these problems IOT helps us a lot. For the home monitoring using IOT we can make home totally automated. Like watering plants and smart kitchen etc. So that we can have an overall idea on the things happening in our home the other problem is security to home. using finger print sensors for door lock and assembling them to the IoT devices makes us to get the total information on who are all visiting the home with the saved finger prints and we can able to view them using camera attached to it. So for this the home must be Wi-Fi enabled for the fast access to the data over a range .

2. Block Diagram and Description

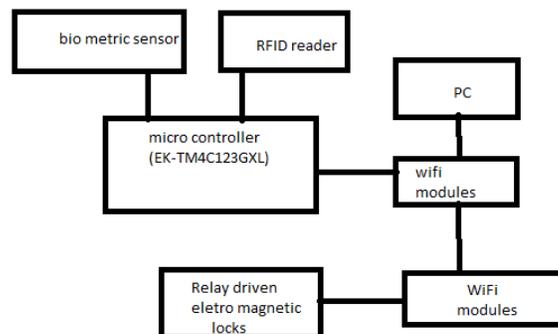


Fig 1: Block Diagram.



Fig 2: RFID reader.

The smart card of the character is read via the RFID reader or Wigand reader near the door. The reader usually transmits a sign of a hundred twenty five KHz. the cardboard is a passive thing with no electricity source. Whilst it is available in proximity of the reader, the reader induces a few Voltages and as a result the cardboard transmits a completely unique 16 bit card variety to the reader. The reader then transmits this card quantity to the microcontroller through the two statistics pins (D0,D1). Wigand protocol is used for transmission. The Wigand layout is shown below. Within the discern 3, the

first bit is the even parity bit. This even parity is for the first thirteen bits. This bit is accompanied by using the eight bit facility Code (0-255). The power code provides on greater layer of safety. This 26 bit code is utilized in cases in which the personnel of 2 businesses have the identical card wide variety. but they can be differentiated with the assist of the facility code. The eight bit facility code is followed through a 16 bit card number (0-65535). The remaining bit is the peculiar parity bit. The extraordinary parity bit debts for bits 14-26

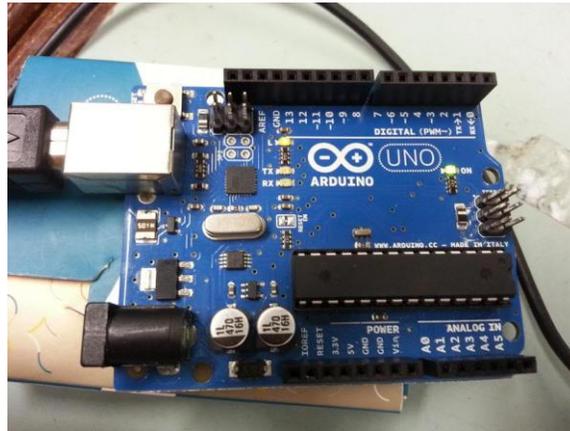


Fig 3. Wigand protocol.

The eight Wigand pins are as follows:

- Vcc
- Wigand data D0
- Wigand data D1
- Wigand pink
- Wigand inexperienced
- Wigand Buzzer
- Wigand tamper
- Floor.

2.1. Explanation of pins

- Vcc: This pin provides +5/+12 Volts to the reader.
- Facts D0: data D0 at this pin.
- Statistics D1: records D1 at this pin.

- Wigand crimson: Switches on the pink LED at the Wigand reader indicating get entry to is denied.
- Wigand green: Switches at the green LED on the Wigand reader indicating get right of entry to is granted.
- Wigand buzzer: The buzzer is switched on for finite time length every time the get admission to is denied or granted.
- Wigand tamper: If the Wigand reader is tampered, the reader offers a excessive sign as output at the tamper pin. This pin is then related to the micro-controller which controls the in addition action to be taken.
- Wigand ground: It offers ground or 0 Volts to the Wigand reader.
- The Wigand interface uses three wires, one in all that is a common floor and of which are facts transmission wires usually called DATA0 and DATA1, alternately categorized "D0" and "D1" or "information Low" and "records excessive". While no facts is being sent, both DATA0 and DATA1 are pulled as much as the "high" voltage degree — usually +5 VDC. Whilst a 0 is sent the DATA0 wire is pulled to a low voltage whilst the DATA1 twine remains at a excessive voltage. While a 1 is sent the DATA1 wire is pulled to a low voltage while DATA0 stays at a excessive voltage.

3. Biometric Sensor



Fig 4 working of the fingerprint scanner

The biometric scanner used is a fingerprint scanner. The A fingerprint scanner system has fundamental jobs -- it desires to get an photograph of your finger, and it needs to determine whether the pattern of ridges and valleys in this photograph fits the pattern of ridges and valleys in pre-scanned images. only precise characteristics, that are unique to each fingerprint, are filtered and saved as an encryptedBiometric key or mathematical representation. No picture of a fingerprint is ever stored, simplest a series of numbers (a binary code), that is used for verification. The algorithm can not be reconverted to an photo, so no person can reproduction your fingerprints. The fingerprint scanner gives the serial

records to the microcontroller. The statistics transmission takes area serially via UART(well-known Asynchronous receiver Transmitter). The fingerprint scanner proven in the parent above is from ADH-TECH and it communicates at TTL degrees serially. The module itself does all the heavy lifting at the back of analyzing and figuring out the fingerprints with an on-board optical sensor and 32-bit CPU. The module can only save up to 20 one of a kind fingerprints but is able to 360° fingerprint recognition and down load and upload templates using serial interface. The module is small and clean to mount the use of mounting tabs at the aspect of the sensor. The on-board JST-SH connector has four indicators: Vcc, GND, TX, Rx.

4. Features

- excessive - speed, excessive-Accuracy Fingerprint identification the usage of the Smack set of rules
- down load Fingerprint photos from the device
- read and Write Fingerprint Templates and Databases easy UART protocol (Default 9600 baud)
- capable of 1:1 Verification and
- 1: N identity 360° Fingerprint popularity
- Microcontroller Unit
- Tiva TM4C123G (TM4C123GH6PM) Microcontroller is used. The development board used is Tiva TM4C123G launch Pad. the important thing functions are as follows:
- ARM® Cortex™-M4F
- 64-pin 80MHz TM4C123GH6PM
- On-board USB ICDI (In-Circuit Debug Interface)
- Micro AB USB port
- tool/ICDI power switch
- 2 person pushbuttons (SW2 is connected to the WAKE pin)
- Reset button
- 3 person LEDs (1 tri-coloration tool)
- current size test factors
- 16MHz important Oscillator crystal

- 32kHz actual Time Clock crystal
- three.3V regulator
- guide for multiple IDEs:
- Code Composer Studio
- Mentor embedded
- IAR systems
- Low strength consumption.
- 256KB Flash memory
- 32 KB bit SRAM
- 2KB EEPROM (fast, saves board space)
- Serial Connectivity
- USB 2.0 (OTG/Host/tool)
- 8 - UART with IrDA, 9-bit and ISO7816 guide
- 6 - I2C
- 4 - SPI, Micro cord or TI synchronous serial interfaces
- 2 - CAN
- 0-forty three GPIO's
- Nested-Vectored Interrupt Controller (NVIC)

The data from the Wigand reader is study through the use of GPIO as digital enter pins and writing a code according with the Wigand protocol. The biometric fingerprint sensor transmits through UART the use of the Tin pin. The variety acquired is compared to the predefined numbers in the flash ROM and then the microcontroller sends signal excessive to the WiFi module1 if the variety is valid. This excessive cost is transmitted to WiFi module 2 and the relay is tripped and the door is opened. The ARM® Cortex™-M4F architecture ensures that the program execution could be very quick and the number acquired is checked in the appearance up desk speedy.

5. WiFi Module

CC3100 simple hyperlink wifi Module is used.

CC3100 connects any low-value, low-energy microcontroller (MCU) to the IOT. The CC3100 wireless networking solution is part of the brand new easy link wireless family that dramatically simplifies the implementation of net connectivity. The CC3100 tool integrates all protocols for wifi and internet, which substantially minimizes host MCU software requirements. With built-in protection protocols, the CC3100 solution presents a strong and easy protection experience. Moreover, the CC3100 device is a complete platform solution together with diverse tools and software program, pattern programs, person and programming courses, reference designs and the TI E2E™ aid community. The CC3100 tool is to be had in an smooth-to-format QFN bundle. The important thing functions are as follows:

- Includes wifi network Processor and power-control Subsystems.
- wifi Processor Subsystem
- WiFi internet on a chip™.
- committed ARM MCU
- wireless driving force and multiple net Protocols in ROM
- effective Crypto Engine
- Station, AP, and wifi Direct® Modes
- Host Interface
- Interfaces with eight-, sixteen-, and 32-Bit MCU or ASICs Over SPI or UART Interface
- electricity management Subsystems
- advanced Low-electricity Modes
- Clock source
- 40.0-MHz Crystal with inner Oscillator
- 32.768-kHz Crystal or external RTC Clock
- bundle and operating Temperature
- Ambient Temperature variety: –forty °C to 85°C

Magazine safe 786-300 is used which will be controlled via a relay. The key design element become to fasten door using magnetic pressure in place of by means of mechanical approach. It now offers the ability to screen up to 2 magnets from

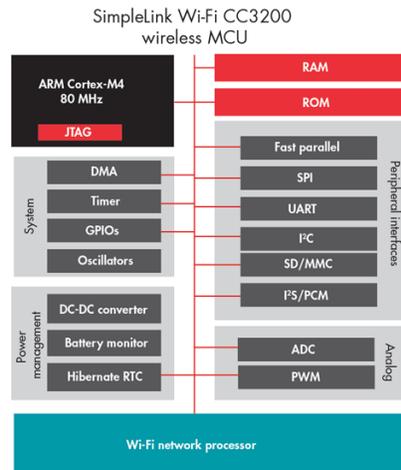
a unmarried low fee (DIN Rail Mount) control Unit or the gadget may be extended by means of connecting Extender

Modules (DIN rail mount) to permit for up to 8 monitored magnets on one device. It includes some of modern designs

CC3100 Wifi Modules Diagram



Fig. 5 CC3100 Wi-Fi Module mounted.



CC3100 WORKING PROCESS

Fig 6 CC3100 Hardware Overview.

5.1. This Module includes:

- The usage of, protection mild curtain generation which continuously video display units the on and off kingdom of magnets.
- E-prevent relay blanketed reduces ordinary fee of set up.
- a regular device comprises of electromagnetic gate locks, manage unit/extender --module(s), nearby get right of entry to manipulate unit and connection cables. The control Unit carries all of the manage electronics for the device such as run-down timers, E-stop inputs, external tool monitoring(EDM), connection for 2 monitored

magnets, LED output display with output signals for using a pc input and dual channel safety output relay contacts

- Functions of mag safe 786- three hundred:
- Expandable system video display units from 1 to eight magnetic locks
- Low renovation, no transferring elements
- up to EN 62061 SIL 3, EN ISO 13849-1 PL e, EN 954-1, category 4
- Stainless steel magnet choice to be used in meals, beverages and different comparable applications
- continuous tracking of the magnets
- simple installation and alignment
- safety tracking (EDM)
- Self-contained manipulate system
- Diagnostic and standing indicators
- Selectable run down timers for gate launch

Represents the implementation of relay driven door lock the usage of AT89C51 microcontroller. The basic operation of relay pushed electromagnetic door locks is as follows:

- *The microcontroller sends a trigger to a transistor.*
- The transistor is became on and present day flows thru the coils of the relay.
- When the contemporary flows via the coils of the relay, the not unusual terminal gets connected to typically open touch and consequently the door is unlocked because it does not get the required electricity supply.
- This delay of locking can be managed via programming the microcontroller as a result. three. barriers

In case of an emergency scenario, we may additionally require the fingerprints of the specified men and women so as to open the door. until the fingerprints of that individual are matched with the ones inside the database, the door will now not open. additionally, failure within the WiFi connectivity because of any of the motives, could make it difficult to open the door. access of the RFID tag to a wrong character due to loss or theft can result in a robbery or a miscreant activity. In case of a massive range of customers, external Flash reminiscence will have to be used as 256KB on chip flash would now not suffice the needs.

5.2. Extensions to the principle mission

Given the advantages of any wireless network, a wireless access manipulate system can be more suitable by means of adding a variety of extra features. a number of them are listed beneath:

1. Gadget getting to know may be carried out and make the machine smarter. it may be used to examine timings and deliver get right of entry to in the destiny. aside from this, the information gathered may be used to screen the performance of employees.
2. A digital camera may be implemented connecting it wirelessly to the WiFi module, adding a 2nd layer of protection. A photo can be clicked and dispatched on the server via WiFi whenever the sensor comes throughout new information (entrant).
3. wifi get entry to manage can be used in university classrooms to take attendance and also preserve dad and mom updated about students' attendance records. WiFi will assist in transmitting attendance statistics at the server. end and destiny Scope

Recapitulating, the smart get entry to manipulate gadget is a good way in which existing issues faced by the enterprise may be overcome. Additionally, with the aid of proper selection of microcontrollers used, power performance may be obtained. Beside the recent years, products based on IOT(net of things),like Google Glass, were within the forefront of technological improvements and consequently we are able to definitely hope that the pleasant is but to come back. we are able to simplest consider the manner in which the goods primarily based on the net of things will revolutionize the arena. The day is approaching while gadgets can be smarter and clever systems might be ubiquitous.

Encouraging and supporting us with the studies related to the task.

6. Working of Relay

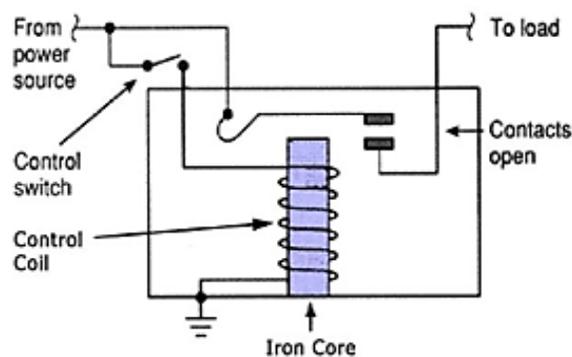


Fig. 7. Working of a relay

