International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

General Article

Smart Security Solutions based on Internet of Things (IoT)

Chirag M. Shah[Å*], Vamil B. Sangoi[Å] and Raj M. Visharia[Å]

[Å]Electronics and telecommunication Engineering Department, D.J.Sanghvi College of Engineering, Vile Parle, Mumbai-4000056, India

Accepted 20 Sept 2014, Available online 01 Oct 2014, **Vol.4, No.5 (Oct 2014)**

Abstract

With increasing popularity of the IoT (Internet of Things) and devices getting smarter day by day, this paper presents an idea to reform the existing access control systems. This approach of enhancing the access control system ensures that the system is wireless thereby reducing wiring issues. The prototype described in this paper has the provision of accepting inputs from a smart card reader (RFID reader) or a biometric sensor. These inputs are processed inside the controller (TM4C123GXL-based on ARM Cortex-M4). If the inputs are found to be valid, access is granted to the user and the logs are wirelessly transmitted to the computer using a WiFi module (CC3100). Machine learning algorithms are implemented to monitor and analyse collected data.

Keywords: *IoT, Access Control , Security, Wireless, WiFi, Machine learning.*

1. Introduction

With increasing demand from the industry for better access control systems, this paper is an attempt to make the conventional access control systems smarter and thereby decreasing the risks of breaking in into the places where these access control systems will be installed. EK-TM4C123GXL is the development board which is used. Data from RFID reader and Biometric sensors are serially transmitted to the microcontroller. If valid fingerprint data or valid card no. is received, the microcontroller sends a signal to the WiFi module1. The WiFi module2 present at the door receives that signal and trips the relay according to the signal received. This is how the door opens. Also the WiFi module sends a signal to the PC via the same WiFi network. Hence the logs of people trying to access the door are maintained in the PC.

2. Block Diagram and Description

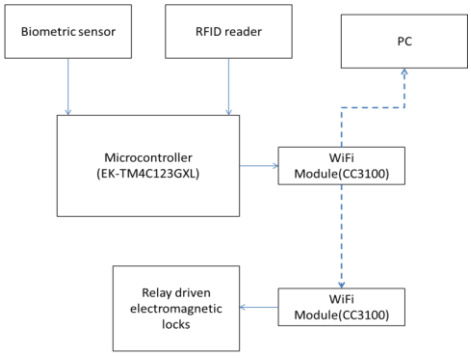

Fig 1: Block Diagram

2.1 RFID Reader

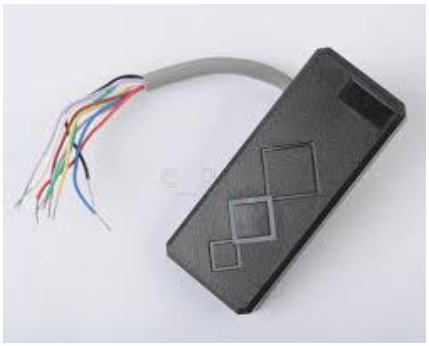

Fig 2: RFID reader

The smart card of the person is read by the RFID reader or wiegand reader near the door. The reader typically transmits a signal of 125 KHz. The card is a passive component with no power source. When it comes in proximity of the reader, the reader induces some voltage and hence the card transmits a unique 16 bit card number to the reader. The reader then transmits this card number to the microcontroller via the two data pins(D0,D1). Wiegand protocol is used for transmission. The 26 bit wiegand format is shown below.In the figure 3, the 1st bit is the even parity bit. This even parity is for the first 13 bits. This bit is followed by the 8 bit facility code(0-255). The facility code provides on more layer of security. This code is used in cases where the employees of 2 companies have the same card number. But they can be differentiated with the help of the facility code. The 8 bit facility code is followed by a 16 bit card number (0-65535). The last bit is the odd parity bit. The odd parity bit accounts for bits 14-26.

*Corresponding author: **Chirag M. Shah**

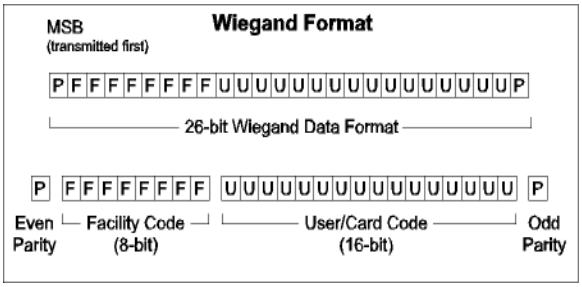

Fig 3. Wiegand protocol

The eight wiegand pins are as follows:

1. Vcc
2. Wiegand data D0
3. Wiegand data D1
4. Wiegand Red
5. Wiegand Green
6. Wiegand Buzzer
7. Wiegand tamper
8. Ground.

Explanation of pins

1. Vcc: This pin provides +5/+12 Volts to the reader.
2. Data D0: Data D0 at this pin.
3. Data D1: Data D1 at this pin.
4. Wiegand red: Switches on the red LED on the wiegand reader indicating access is denied.
5. Wiegand green: Switches on the green LED on the wiegand reader indicating access is granted.
6. Wiegand buzzer: The buzzer is switched on for finite time duration each time the access is denied or granted.
7. Wiegand tamper: If the wiegand reader is tampered, the reader gives a high signal as output on the tamper pin. This pin is then connected to the micro-controller which controls the further action to be taken.
8. Wiegand ground: It provides ground or 0 Volts to the wiegand reader.

The Wiegand interface uses three wires, one of which is a common ground and two of which are data transmission wires usually called DATA0 and DATA1, alternately labeled "D0" and "D1" or "Data Low" and "Data High". When no data is being sent, both DATA0 and DATA1 are pulled up to the "high" voltage level — usually +5 VDC. When a 0 is sent the DATA0 wire is pulled to a low voltage while the DATA1 wire stays at a high voltage. When a 1 is sent the DATA1 wire is pulled to a low voltage while DATA0 stays at a high voltage.

2.2 Biometric Sensor

The biometric scanner used is a fingerprint scanner. The A fingerprint scanner system has two basic jobs -- it needs to get an image of your finger, and it needs to determine whether the pattern of ridges and valleys in this image matches the pattern of ridges and valleys in pre-scanned images. Only specific characteristics, which are unique to every fingerprint, are filtered and saved as an encrypted biometric key or mathematical representation. No image of a fingerprint is ever saved, only a series of numbers (a binary code), which is used for verification. The algorithm cannot be reconverted to an image, so no one can duplicate your fingerprints. The fingerprint scanner gives the serial data to the microcontroller. The data transmission takes place serially via UART(Universal Asynchronours receiver transmitter).

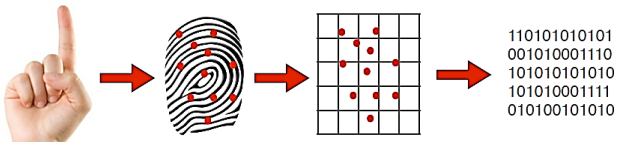

Fig 4 Basic working of the fingerprint scanner

Fig 5 Fingerprint Scanner - 5V TTL (GT-511C1R)

The fingerprint scanner shown in the figure above is from ADH-TECH and it communicates at TTL levels serially. The module itself does all of the heavy lifting behind reading and identifying the fingerprints with an on-board optical sensor and 32-bit CPU. The module can only store up to 20 different fingerprints but is capable of 360° fingerprint recognition and download and upload templates using serial interface. The module is small and easy to mount using two mounting tabs on the side of the sensor. The on-board JST-SH connector has four signals: Vcc, GND, Tx, Rx.

Features

- High-Speed, High-Accuracy Fingerprint Identification using the SmackFinger 3.0 Algorithm
- Download Fingerprint Images from the Device
- Read and Write Fingerprint Templates and Databases Simple UART protocol (Default 9600 baud)
- Capable of 1:1 Verification and 1:N Identification 360° Fingerprint Recognition

2.3 Microcontroller Unit

Tiva™ TM4C123G (TM4C123GH6PM) Microcontroller is used. The development board used is Tiva™ TM4C123G LaunchPad. The key features are as follows:

- ARM® Cortex™-M4F
- 64-pin 80MHz TM4C123GH6PM
- On-board USB ICDI(In-Circuit Debug Interface)
- Micro AB USB port
- Device/ICDI power switch

- 2 user pushbuttons(SW2 is connected to the WAKE pin)
- Reset button
- 3 user LEDs (1 tri-colour device)
- Current measurement test points
- 16MHz Main Oscillator crystal
- 32kHz Real Time Clock crystal
- 3.3V regulator
- Support for multiple IDEs:
  - Code Composer Studio
  - Keil
  - Mentor embedded
  - IAR systems
- Low power consumption.
- 256KB Flash memory
- 32 KB bit SRAM
- 2KB EEPROM (fast, saves board space)
- Serial Connectivity
  - USB 2.0 (OTG/Host/Device)
  - 8 - UART with IrDA, 9-bit and ISO7816 support
  - 6 - I2C
  - 4 - SPI, Microwire or TI synchronous serial interfaces
  - 2 - CAN
- 0-43 GPIO's
- Nested-Vectored Interrupt Controller (NVIC)

The data from the wiegand reader is read by using GPIO as digital input pins and writing a code in accordance with the wiegand protocol. The biometric fingerprint sensor transmits via UART using the Tx pin. The number received is compared to the predefined numbers in the flash ROM and then the microcontroller sends signal high to the WiFi module1 if the number is valid. This high value 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 is very quick and the number received is checked in the look up table quickly.

2.4 WiFi Module

CC3100 SimpleLink Wi-Fi Module is used.

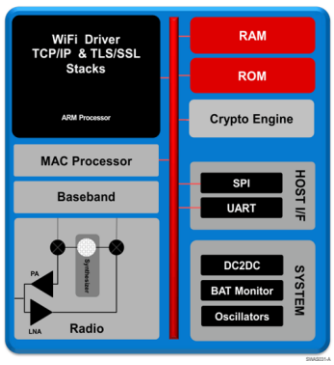

Fig 6 CC3100 Hardware Overview

CC3100 connects any low-cost, low-power microcontroller (MCU) to the IoT. The CC3100 wireless networking solution is part of the new SimpleLink Wi-Fi family that dramatically simplifies the implementation of Internet connectivity. The CC3100 device integrates all protocols for Wi-Fi and Internet, which greatly minimizes host MCU software requirements. With built-in security protocols, the CC3100 solution provides a robust and simple security experience. Additionally, the CC3100 device is a complete platform solution including various tools and software, sample applications, user and programming guides, reference designs and the TI E2E™ support community. The CC3100 device is available in an easy-to-layout QFN package. The key features are as follows:

- Consists of Wi-Fi Network Processor and Power-Management Subsystems.
- Wi-Fi Processor Subsystem
  - WiFi internet on a chip ™.
  - Dedicated ARM MCU
  - Wi-Fi driver and Multiple Internet Protocols in ROM
  - Powerful Crypto Engine
  - Station, AP, and Wi-Fi Direct® Modes
- Host Interface
  - Interfaces with 8-, 16-, and 32-Bit MCU or ASICs Over SPI or UART Interface
- Power Management Subsystems
- Advanced Low-Power Modes
- Clock Source
  - 40.0-MHz Crystal with Internal Oscillator
  - 32.768-kHz Crystal or External RTC Clock
- Package and Operating Temperature
  - Ambient Temperature Range: –40°C to 85°C

Fig. 7 CC3100 Wi-Fi Module mounted

2.5 Relay Driven Electromagnetic Locks

Magsafe 786-300 is used which will be controlled by a relay. The key design element was to lock door using magnetic force rather than by mechanical means. It now offers the ability to monitor upto 2 magnets from a single low cost (DIN Rail Mount) Control Unit or the system can be extended by connecting Extender Modules (DIN rail mount) to allow for upto 8 monitored magnets on one system. It incorporates a number of innovative designs including:

- Using safety light curtain technology which continuously monitors the on and off state of magnets.
- E-stop relay included reduces overall cost of installation.

A typical system comprises of electromagnetic gate locks, control unit/extender module(s), local access control unit and connection cables. The Control Unit contains all the control electronics for for the system including run-down timers, E-stop inputs, External Device Monitoring(EDM), connection for upto 2 monitored magnets, LED output display with output signals for driving a PLC input and dual channel safety output relay contacts.

Features of Magsafe 786-300 are:

- Expandable system monitors from 1 to 8 magnetic locks
- Low maintenance, no moving parts
- Up to EN 62061 SIL 3, EN ISO 13849-1 PL e, EN 954-1, Category 4
- Stainless steel magnet option for use in food, drinks and other similar applications
- Continuous monitoring of the magnets
- Simple installation and alignment
- Safety monitoring (EDM)
- Self-contained control system
- Diagnostic and status indicators
- Selectable run down timers for gate release

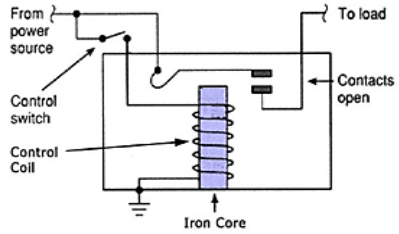

Fig. 8 Working of a relay

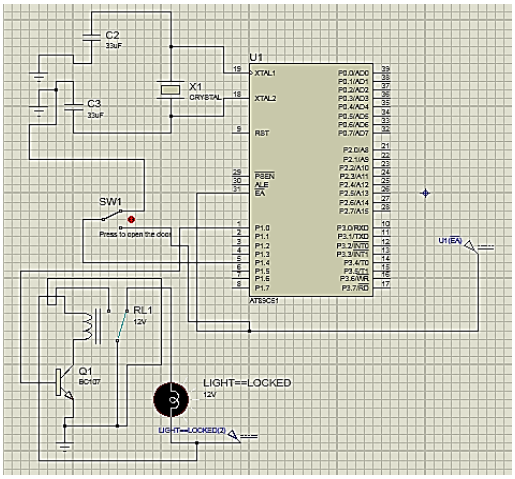

Fig. 9 Working of relay driven door lock prototype

Figure 9 represents the implementation of relay driven door lock using AT89C51 microcontroller.

The basic operation of relay driven electromagnetic door locks is as follows:

1. The microcontroller sends a trigger to a transistor.
2. The transistor is turned on and current flows through the coils of the relay.
3. When the current flows through the coils of the relay, the common terminal gets connected to normally open contact and hence the door is unlocked as it does not get the required power supply.
4. This delay of locking can be controlled by programming the mictrcontroller accordingly.

3. Limitations

In case of an emergency situation, we may require the fingerprints of the required persons in order to open the door. Until the fingerprints of that person are matched with the ones in the database, the door will not open. Also, failure in the WiFi connectivity due to any of the reasons, would make it difficult to open the door. Access of the RFID tag to a wrong person due to loss or robbery can lead to a theft or a miscreant activity.

In case of a large number of users, external Flash memory will have to be used as 256KB on chip flash would not suffice the needs.

4. Extensions to the Main Project

Given the advantages of any wireless network, a wireless access control system can be enhanced by adding a lot of additional features. Some of them are listed below:

1. Machine learning can be implemented and make the system smarter. It can be used to analyse timings and give access in the future. Apart from this, the data collected can be used to monitor the efficiency of workers.
2. A camera can be implemented connecting it wirelessly to the WiFi module, adding a second layer of security. A photograph can be clicked and sent on the server via WiFi every time the sensor comes across new data (entrant).
3. Wireless access control can be used in college classrooms to take attendance and also keep parents updated about pupils' attendance records. WiFi will help in transmitting attendance records on the server.

Conclusion and Future Scope

Recapitulating, the smart access control system is an efficient way in which existing problems faced by the industry can be overcome. Also, by proper selection of microcontrollers used, energy efficiency can be obtained.

In the recent years, products based on IoT(Internet of Things),like Google Glass, have been in the forefront of technological innovations and hence we can definitely hope that the best is yet to come. We can only imagine the manner in which the products based on the internet of things will revolutionize the world. The day is imminent when devices will be smarter and smart systems will be ubiquitous.

Acknowledgement

We would like to thank our respected principal Dr. Hari Vasudevan and Dr. Amit Deskhumk (Head of Dept.- Electronics and Telecommunication) of D. J. Sanghvi College of Engineering for giving us facilities and providing a congenial environment for working in the college. We would also like to thank our project guide Ms. Ranjushree Pal and Dr. Sunil Karamchandani for encouraging and helping us with the research related to the project.

References

https://www.sparkfun.com/products/13007
http://www.ti.com/tool/ek-tm4c123gxl#Technical Documents
http://www.bioelectronix.com/what_is_biometrics.html
http://www.ti.com/ww/en/simplelink_embedded_wi-fi/cc3100.html
http://www.circuitstoday.com/working-of-relays
http://www.wikiwand.com/en/Electromagnetic_lock