International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (03), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Ultra Secure Programmable LockBox

Dr.Suneetha Uppala

Dept.of Electronics

Sri krishnadevaraya university

Anantapur(India)

ABSTRACT

The present paper we describe how an ultra-secure programmable lockbox which is unlocked using a keypad and a fingerprint sensor authorization based on RFID. The user must provide the proper inputs to each of the various systems using the directions displayed on a LCD screen. Once the box is unlocked, the user may update the password combinations and fingerprints that must be provided to unlock the box again. The present work is done for something that was useful and appealing to a wide variety of people. This box can be used to securely store jewelry and other valuable merchandise. This lockbox is a highly marketable product which provides real security in a unique way. This product may be particularly attractive to younger children who would like to have a toy box to which only they know the pass code.

***Key words*- Ultra secure; lock box; fingerprint sensor; lcd; rfid reader/tag & potentiometer unlock.**

I.INTRODUCTION

The main purpose of this paper is to implement a locker system with the keypad password, heat sensor and fingerprint is preset. This technology which can be used in banks, offices and other places where high security is required. In this only authorized person can open the locker. The initial security levels are RFID, PASSWORD and finger print sensor along with this we added the heat sensor can access the alarm when anyone try to open the locker by using electrical machine which produce heat.

The password is set to 1234 then the user sends in a fingerprint, or a set of fingerprints, when ordering the box. This set of lock stages provides for ultimate security. Upon retrieving the box, the user unlocks it for the first time using these settings and then can reset the four digit password, the unlocking values of each potentiometer. RFID reader can read the tag value if it matched then access to type the password.

II.WORK ORGANIZATION

The user can access the system accordance to the block diagram with the code, then moving on to the tunable potentiometers, heat sensor and finally onto the fingerprint scanner. The detailed schematic diagram of the project is dividing in to different blocks they are shown in below figure1.

A. Keypad

B. RFID reader/Tag

C. potentiometer

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (03), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

D. Finger print sensor

E. Multiplexer

F. Arduino uno

G. Atmega 328P

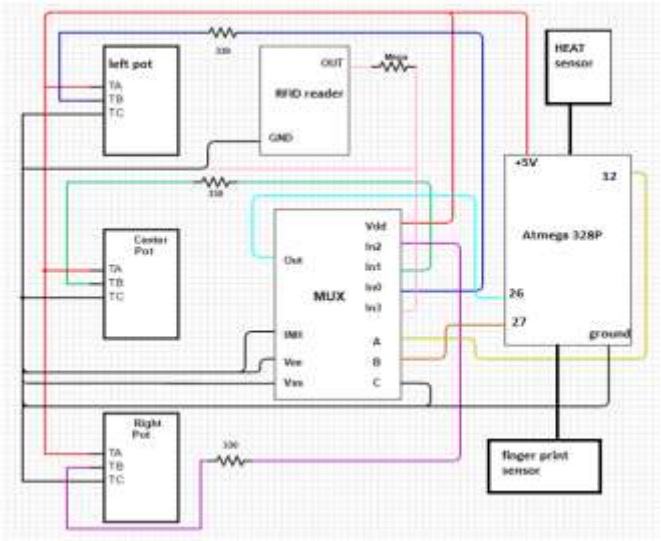


Figure 1: Schematic diagram for ultra security lock box

A. Keypad

The keypad used for entering an unlocking code it used seven pins on the atmega 328P, with rows 1-4 taking up pins 2, 3, 5, and 6 on the controller, and columns 1-3 taking up pins 13-15 on the microcontroller. The keypad uses 10 Kiloohm pull-down resistors on each column to provide a viable path to ground from the column pins, and uses 300 Ohm resistors on the rows to provide a viable path to ground from the row pins. Each switch connects a row wire to a column wire. By using these pins such as potentiometer values or the current passcode being entered. This thread implements a finite state machine (FSM) to debounce button presses on the keypad and stores in a buffer the values input by the user so that it can be checked against the passcode required to pass this stage.

Once the finite state machine has yielded a valid keypress, the number is stored in a buffer. Once there are four numbers in that buffer, the controller checks if the number sequence in the buffer matches the pass code. If it does, then the keypad stage is passed and the user moves onto the potentiometer. If the number sequences do not match, then the user must input another four-digit sequence and the data in the buffer is overwritten by this next fourth-digit sequence. The circuit is shown in figure 2.

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (03), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

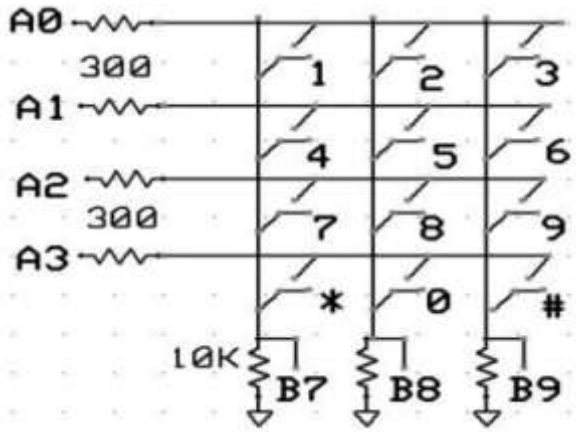


Figure 2: Keypad Diagram

B. RFID reader/Tag

RFID is an effective automatic identification technology for variety of objects and person. The most important functionality of RFID is to track the location of the tagged item. The RFID tags can be classified into three major categories which is based on power source, active tags, passive tags, and semi passive (semi-active) tags. An active tag contains both radio transmitter, receiver and a battery that is used to power the transceiver. Active tags are more powerful than the passive tags/semi-passive tags. RFID tags can also be classified into two categories: tags with read/write memory, and tags with read only memory. The tags with read/write memory are more expensive than the tags with read-only memory. RFID tags operate in three frequency ranges: low frequency (125-135KHz), high frequency (10–15MHz), and ultra-high frequency (850 –950MHz, 2.4–2.5GHz, 5.8GHz). The LF tags are less affected by the presence of fluids or metals when compared to the higher frequency tags. RFID reader is shown in the fig1.The most important functionality of RFID is the ability to track the location of the tagged item. Typical applications of HF tags are access control and smart cards. RFID smart cards, working at 13.56MHz, are the most commonly used tags.

C. Potentiometer

The potentiometer circuitry was accomplished through the addition of an analog multiplexer. This multiplexer was used in order to simplify the code necessary for the potentiometers by reducing the amount of ADC ports running from four to one. The three potentiometers acted as tunable knobs for the user to set and unlock the box, similar to a classic safe. Each potentiometer had one end terminal connected to +3.3V and the other end terminal conected to ground. The wiper of each potentiometer was connected through a 330 Ohm resistor to the first three inputs of the multiplexer. Meanwhile, the piezo electric sensor acted as another safety mechanism for the box. The multiplexer was powered through Vdd with its INH, Vee, and Vss terminals all tied to ground. Because only four inputs were required, select signal 'C' was also grounded. Select signals 'A' and 'B' were connected to digital pins of the microcontroller.

D. Fingerprint scanner

The fingerprint scanner was connected to the atmega 328P through an external connection through an Arduino microcontroller. The fingerprint scanner was connected via a 4-pin JST terminal with connections to VDD, ground, RX, and TX (pins 4, 5 on the Arduino). The Arduino was used due to the fact that there is public source code. The Arduino communicated with the atmega 328P by outputting a 5V signal from pin 12 to the atmega 328P microstick whenever a correct fingerprint was detected. In addition to sending a signal to the atmega 328P, a signal was sent to the solenoid valve to unlock the box, as the fingerprint scanner is the final security measure.

To detect a valid fingerprint, we used an Arduino Fingerprint Scanner library built by Josh Hawley. When the PIC32 is in the fingerprint scanner state, it polls the Arduino for a HIGH input. When the Arduino senses a valid fingerprint, it sends a HIGH signal to the atmega 328P and drives the solenoid valve to unlock the box. Otherwise, it continously sends a LOW signal to the atmega 328P. Once the atmega 328P has sensed a HIGH signal from the Arduino, the box is unlocked and the Atmega 328P moves onto the programmability state. It remains unlocked for three seconds, after which the solenoid valve closes again.

E. Multiplexer

We use ADC channels to continously read the outputs of the three potentiometers. Because each of the potentiometers is connected to a multiplexer, we must configure the select bits of the multiplexer accordingly before we read from each potentiometer. After reading the values from each potentiometer, we map them from (0,1024) to (100,999) using a simple linear mapping so that the user can only input 3-digit potentiometer values. We display this value on the screen so that the user can easily adjust the potentiometer knobs to the correct combination. Each potentiometer has its own unlocking value, and any number that is within 30 of that value is considered valid. For example, if the left potentiometer has an unlocking value of 230, then the user must input a value between 200 and 260 on the left potentiometer. We allow a range of plus or minus 30 to allow for a nicer user experience since the values read from the potentiometers oscillate slightly. The range could be modified to a smaller one to increase security.

F. Arduino uno

Arduino uno board designs use a variety of microprocessors and controllers. The boards are equipped with sets of digital and analog (I/O) pins that may be interfaced to various extension boards and other circuits. The boards feature serial communications interfaces, including (USB) on some models, which are also used for loading programs from personal computers. The microcontrollers are typically programmed using a dialect of features from the programming languages C and C++. In addition to using traditional compiler tool chains, the Arduino project provides an (IDE) based on the Processing language project.

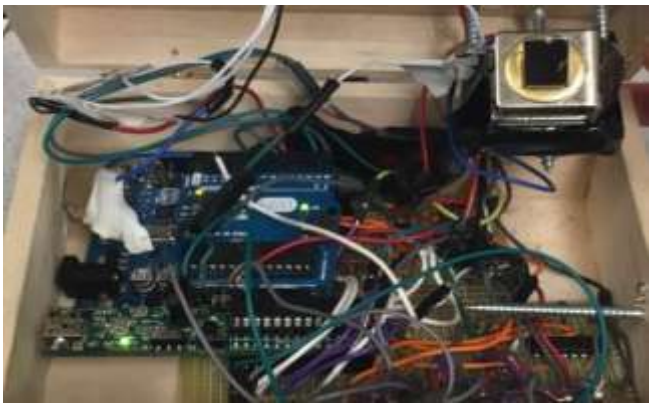
G. Atmega 328P

The Atmel 8-bit AVR RISC-based microcontroller combines 32 kB ISP flash memory with read-while-write capabilities, 1 kB EEPROM, 2 kB SRAM, 23 general purpose I/O lines, 32 general purpose working registers,

three flexible timer/counters with compare modes, internal and external interrupts, serial programmable USART, a byte-oriented 2-wire serial interface, SPI serial port, 6-channel 10-bit A/D converter, programmable watchdog timer with internal oscillator, and five software selectable power saving modes. The device operates between 1.8-5.5 volts. The device achieves throughput approaching 1 MIPS per MHz.

III.CONCLUSION

The designing and its cascading will increase the security of the box. Each goal was met, with the keypad, potentiometers, RFID reader/Tag and fingerprint scanner being integrated into the design. In addition, a four stage lock box with a final stage of a fingerprint scanner was felt to be very secure. we would focus on the re programmability aspect of the fingerprint scanner, as well as proper communication between the Arduino and atmega 328P, perhaps over an SPI or UART channel. It is little bit difficult to configure the fingerprint scanner to be re programmable by the user. The final result was reached what we supposed to do. The complete setup is shown in below photograph 1.



Photograph1: complete system of locker box

REFERENCES

[1]. Raghu Ram.Gangi, SubhramanyaSarma&Gollapudi,2013 Locker Opening And Closing System Using RFID, Fingerpri nt, Password 'International Journal of Emerging Trends&Technology in Computer Science (IJETTCS),Volume 2.

[2]. BalajiVenkatesh.A.M, KarthikKalkura&Shriraam A.C, 2013 'Student Locker Protection Using RFID Tag & Reader 'International Journal of Engineering and Advanced Technology (IJEAT) ,Volume -3,Issue-2.

[3]. Swetha.J, 2011, 'RFID Based Automated Bank Locker System' International Journal of Research in Engineering and Technology, Volume-1.

[4]. Bramhe, 2011'SMS Based Secure Mobile Banking', International Journal of Engineering and Technology, Volume-3.

[5]. Joshua Bapu.J &sirkaziMohdArif, 2013 'Locker security system using RFID and GSM technology' International Journal on Advances in Engineering and Technology, Volume 3.

[6]. Ramesh.S, Soundaria Hariharan & Shruthi Arora,2012' Monitoring and Controlling of Bank Security System', International Journal of Advanced Research in Computer Science and Software Engineering, Volume-2.