DESIGN OF TWO FACTOR AUTHENTICATION SECURITY SYSTEM WITH A DIAL-UP SYSTEM

Oghenerhoro, O.
Department of Physics, Delta State University, Abraka Nigeria
***(e-mail: ovie4u2000@yahoo.com*)**

ABSTRACT

This paper shows the design and construction of a two factor authentication security system, with a dial-up system. It is based on what the user knows (password) and what he has (smart card). The system consists of a microcontroller 89S52 which sends a signal to the multiplexers on insertion of the smart card in the card slot. consist The multiplexers of ICS which prompts for a display of the identity of the card user in the seven segment display. The seven segments display the status of the card. On validation of the card, the seven segments display a welcome note to the user and prompts for a pin code. The pin code is being keyed in from the key pad. If confirmed by the program written into the microcontroller access will be granted, otherwise no access, giving the user two more chances to insert the correct smartcard or pin code to it, before final denial of access which displays "Access Denied" on the Seven Segment Display and triggers an alarm and a dial-up system which will call a pre-programmed cell phone number. When access is granted, the card sends a 5volt signal to the microcontroller which triggers relay, resulting in the opening of the door.

INTRODUCTION

Creation of secured access path to office, home and administrative block has been an endearing creativity of man. As a result of this, it has been possible to create door/gates that are well secured using smart card. Individuals/administrators are increasingly aware of the dangers that result if they rely on keys or padlocks to provide security network to unauthorized rooms or offices. Attackers can forge keys or make master keys that will be used to break into such rooms or offices. To eliminate this insecure condition, there evolved the use of password in doors/gates mechanism.

Single secrets such as pass-word can be effective security controls. A long password of more than ten characters that consists of random letters, numbers and special character can be very difficult to crack. Unfortunately, users cannot always remember the sort of pass-word, partly due to fundamental human limitations. Miller (1956), Concluded that the memory limit of between five and nine random characters, with an average of seven is ideal.

However, most security guidance recommend at least eight character random password. Users rarely show great discretion when they write down password and so provided opportunities for attackers to have access into their security system. Where there are no restrictions on password complexity, users tend to choose easy passwords such as "1234" or other easily guessed words.

Two-factor authentication i.e. System that uses card and pin code for authentication overcome the issues of single secret authentication by the requirement of a second secret. Two-factor authentication uses a combination of the following items;

- Something that the user has, such as hardware token or a smartcard.
- Something the user knows, such as personal identification number (pin).

Smartcard and their associated pins are increasingly popular, reliable and cost effective form of two-factor authentication with the right control in place, the user must have the smartcard and know the pin code to gain access to rooms or offices or administrative places. The smartcard requirement significantly reduces the likelihood of unauthorized access to an organization's outfit.

Hence to reduce or eliminate the access of an unauthorized personal into rooms/ offices/administrative block, an automated door/access path is to be constructed. This in-

volves controlling the doors/gates by an artificial means (artificial intelligence). It involves the application of automated system that is incorporated into these doors/gates for efficient and optimum performance. Taking the advantage of the microcontroller as on of the fastest processing and intelligent instrument (Badawy and Julien, 2003). was incorporated into the system and interfaced with smartcard in order to achieve accuracy in processing.

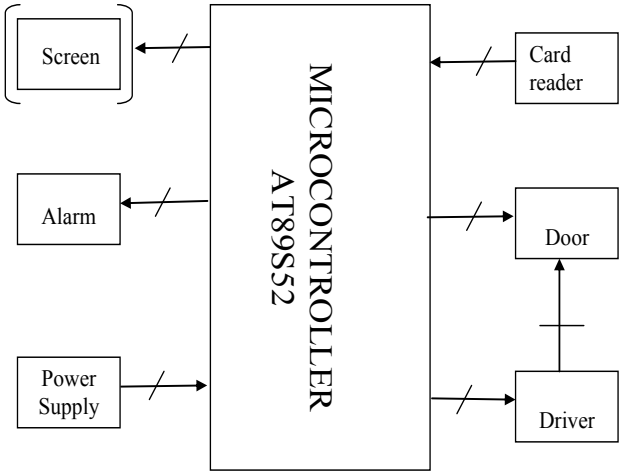
This device was constructed using microcontroller for better creativity and beauty in design. The microcontroller (programmable) has series of instruction fed into it, this help it to accomplish most intelligent task like the human brain (Adam, 1980). These include detection of card, identification of password, displaying "access granted", "access denied" and opening and closing of door/gate with the aid of the smart card.

Design Analysis

The implementation of the design of security door using smart card is based on hardware and software. The hardware comprises of modules that are segmented on the Vero board as well as physical wiring. The hardware ensures optimum performance of the whole circuiting. The hardware design of the device consists of six essential modules which include keypad select module, sliding gate module, display module, power supply, alarm unit module and dial-up module. The microcontroller is the heart of the entire circuiting. It gives instruction to the different modules. There is also the alarm signal which issues a signal in form of a sound when a wrong pin is entered in the system more than three times, and instructs the dial-up module to call the appropriate security agent/departments telephone number. Thereafter, the system remains idle until its being reseted by a security agent.

The figure 1.1 below shows the block diagram of the entire circuit

Fig.1.1 The block diagram of the the design



The keypad is an input device designed to issue instruction to the microcontroller. It consists of increment, decrement, adjust, enter and reset buttons. Each key upon being depressed transmit its instruction to the central processing unit of the microcontroller. (Buckey and Hoskyns, 1980) The keypad is found at the output port of the microcontroller. The interface is at port 2 bit 0,1,2,3 (P2.0, P2.1, P2.2, P2.3) and Pin 9 as the reset. Each of the button are tied with a putt-up resistor (1k), grounded through the 1k resistor, and the other side is connected to Vcc as shown in the figures below.

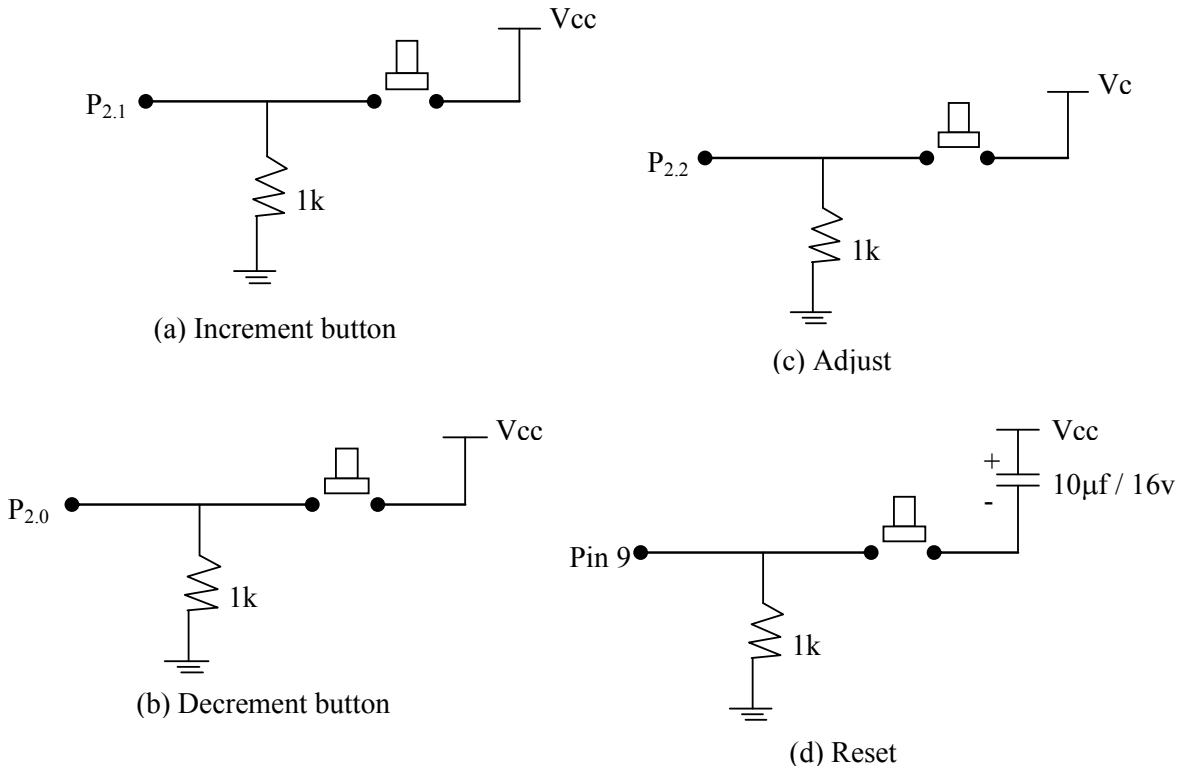


Fig. 1.2 The control switchs layouts

As seen, the keypad is connected as a normally low switch (Badawy & Jullien, 2003). The sliding unit consists of a dc motor and series of mechanism that drives the gate to open/close position. This occurs after the correct card and pin is detected. The process takes place after signal's receptions from the microcontroller through which the relay triggers the door from a pulsating 12v dc voltage as shown below.

N/C = Normally close

N/O = Normally open

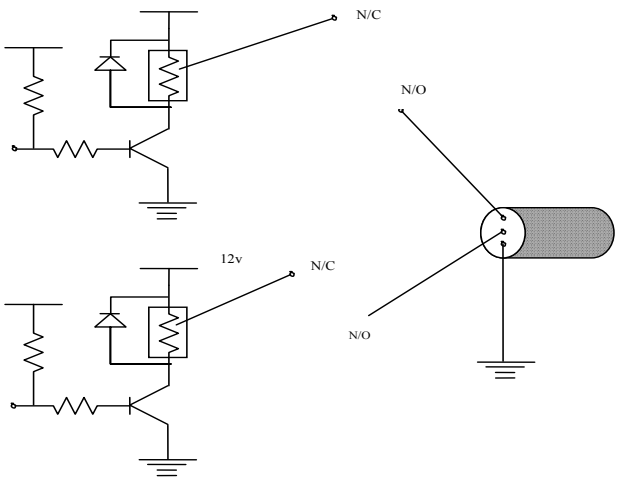


Fig 1.3 Relay connection to the door

A critical look at the figure shows two relay with contact point showing when it is normally open (N/O) and normally close (N/C). It depicts different connection of two transistors (NPN) at different port to the microcontroller which aid in the movement of the door in either direction. The first is a power transistor (NPN) found at port 3bit 6. This operates when there is movement instruction (that is an active high pulse) from the microcontroller after a card and its associated pin is detected. A pull up is tied to Vcc at the base of the power transistor for optimum switching. The process energizes the relay (normally closed) and allows a maximum current flow from the collector to the emitter of the transistor. Placing an active low pulse at this port terminates the current. The transistor is chosen to handle a high current of 10mA which is the IC max current and inductive effect of the dc motor.

The Alarm unit which comprise of a speaker, resistor, capacitors, 555 timer and a transistor connected to a +5v dc source, is used in the alarm section (Moore, 1965).

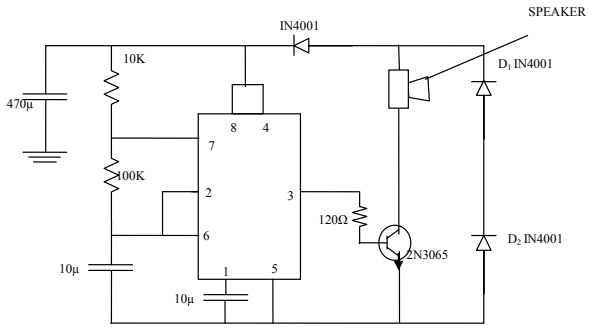


Fig 1.4 Alarm signal unit

As can be seen from the figure above, the frequency of the alarm signal can be obtained using

$$F = \frac{1.44}{(2R_B+R_A)} \quad \text{.....(1)}$$

R in ohms
C in farads
F in Hz
From the diagram above
$R_A = 10k = 10000W$
$R_B = 100k = 100000W$
$C_I = 10f = 10 \times 10^{-9}F$

$$\therefore F = \frac{1.44}{(2 \times 100000 + 1000) \times 10 \times 10^{-9}}$$

F = 685.71Hz (Forrest, 2004)

The display unit is composed of resistor, transistor and cascaded LED (Seven–segment) display. The pull-up resistor are tied to the output port (port 1) of the microcontroller and interfaced to the cascaded LEDs through the transistors. The LED display can be compare to the VDU (visual display unit) in PCs. It does alpha-numeric display (both upper/lower case lifter). The NPN transistor that is connected to it has it's emitter being tied to Vcc through pull-up resistor (1k) as in the case of the relay, that is when a character is been displayed, a low voltage (usually 0 volts), turns it "ON". In this display unit, the transistor acts as a switch. The aim of the pull-up resistor is to increase voltage when there is a pulse signal "1" in order to ensure a bright display. The connection is from the output port 1 bit (0-6) and output port 3 bit (0-5).

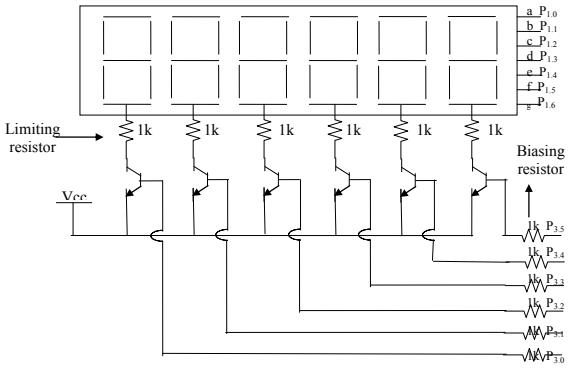


Fig. 1.5: Display Module

To Find the value of the limiting resistor connected to the common of the seven segment display, it should be noted that LED takes a current of about 10 - 40mA which is very high and the microcontroller has a dc supply of 5volts from the power source. So for a single display, LED will draw about 70-280mA and this takes about one third (⅓) of the 5v supply. In order to allow about 4mA in each LED, the value of the limiting resistor is obtained using ohm's law.

$$R = V/I \text{ Þ } R = 5/4 \times 10^2 = 125W$$

Hence, there should not be less than 125W resistor connected to the common of the seven -segment display in this design. 1k resistor was used as preferred choice in this design
Therefore the limiting current is

$$I = \frac{5}{1000} = 5mA$$

For the value of biasing resistor maximum base current of transistor is 5mA. The supply voltage is 5v dc.

$$R_b = \frac{V}{I_b} = \frac{5}{5} \times 103 = 1kW$$

So a resistor of value 1k is required to effectively biase the transistor.

The 89S52 was designed such that control of the microcontroller and all input/output between the microcontroller and external device is accomplished via special function Registers (SFR). The 89S52 microcontroller structure is showned below ;

PORT 1: This is an input/output port. Each bit of this SFR corresponds to one of the pins on the microcontroller. For example, bit 0 of

port 1 is P1.0, bit 7 is pin P1.7. Writing a value of 1 to a bit of this SFR will send a high level on the corresponding 1/0 pin whereas a value of 0 will bring it to a low level.

PORT 2: This is an input/output port. Each bit of this SFR responds to one of the pins on the microcontroller. For example bit 0 of port 2 is P2.0 bit 7 of port 1 is also P1.7. Writing a value of 1 to a bit of this SFR will send a high level on the corresponding 1/0 pin whereas a value of 0 will bring it to a low level.

PORT 3: This is an input/output port. Each bit of this SFR corresponds to one of the pins on the microcontroller. For example bit 0 of port 3 is P3.0, bit 7 is pin P3.7. Writing a value of 1 to a bit of this SFR will send a high level on the corresponding 1/0 pin whereas a value of 0 will bring it to a low level. (Axelson, 1994).

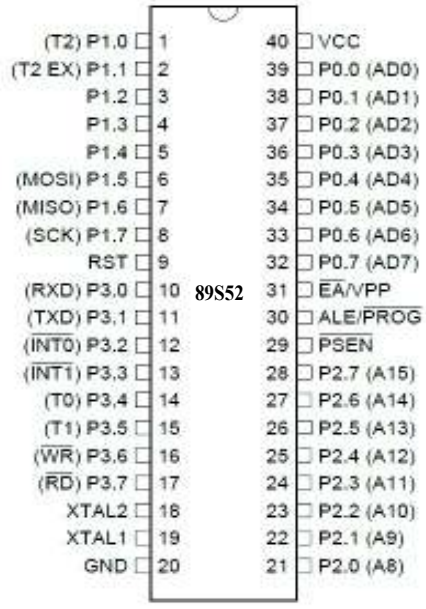


Fig. 1.6 *The 89S52 Microcontroller*

PORT 0: This is an input/output port. Each bit of this SFR corresponds to one of the pins on the microcontroller. For example bit 0 of port 0 is P0.0, bit 7 is pin P0.7. Writing a value of 1 to a bit of this SFR will send a high level on the corresponding 1/0 pin whereas a value of 0 will bring it to low level.

Smart Card Unit

The smart card unit is constructed using Vero board and PCI slot. It is constructed such that when the microcontroller receive a particular bit pattern from the card, it will give the appropriate response and display on screen "enter pin"

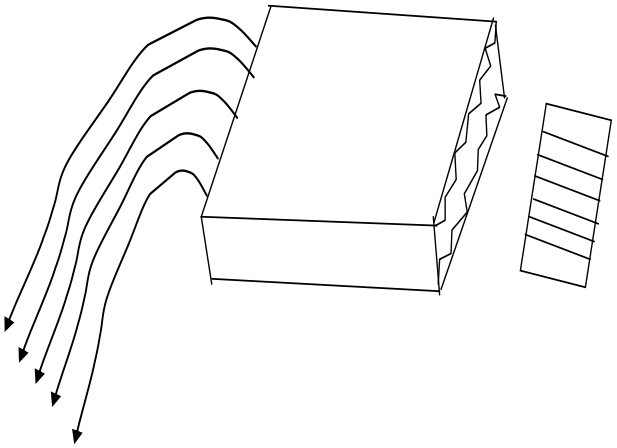


Fig.1.2: Smart card unit

The power supply section is constructed to serve as a source of electromotive force (EMF), which provides the electrical energy to drive the current in the circuit. The supply used was a direct current. The transformer used was a step down transformer (220VAc to 12VAC). The output of the supply is filtered using a 300uf. 50v capacitor to remove the AC ripples .

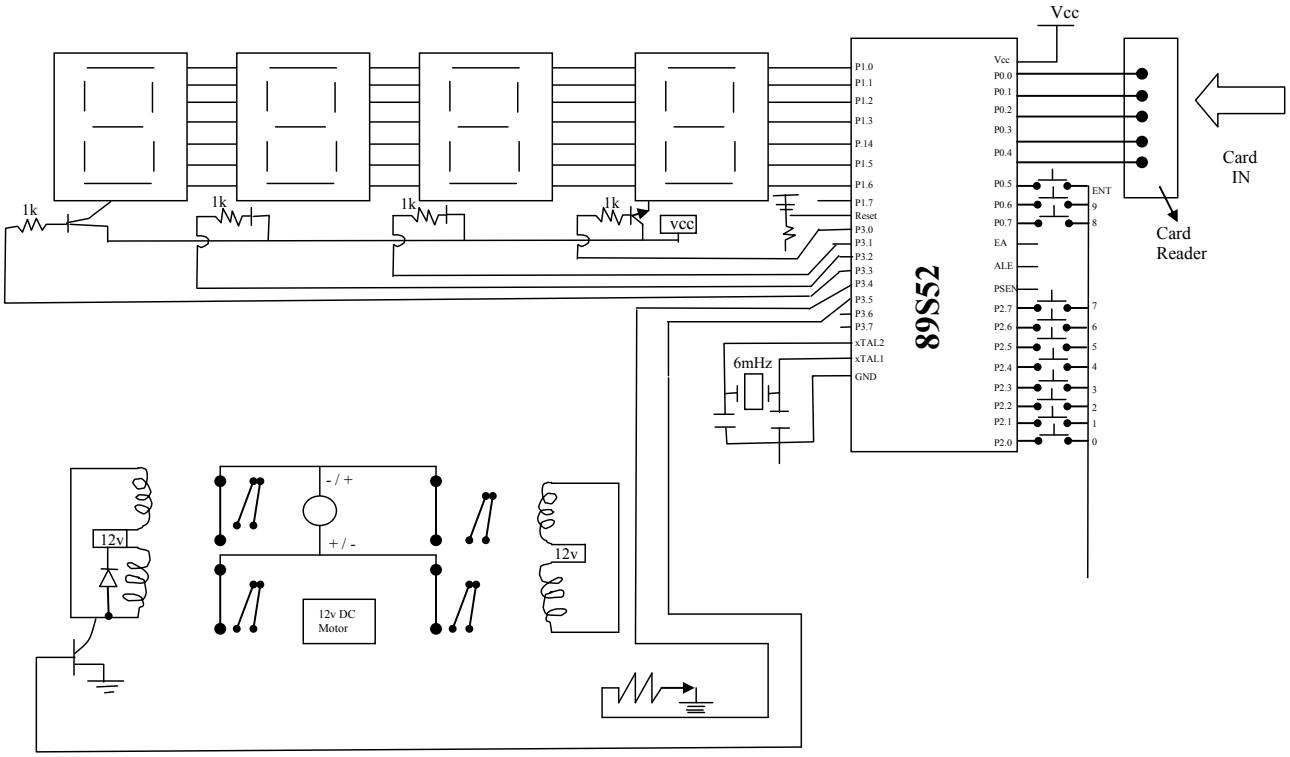


Fig 1.7 The Main Circuit Diagram

The circuit above is an assembly of the different sections of this work (Two factor authentication security system).

RESULTS AND DISCUSSION

This design is made up of software and hardware. The software program of this work is written with assembly language program (Britton, 2003.) while the hardware is comprised of the control unit, the input unit, the power supply unit and the display unit. Input unit have card slot where cards are inserted for access purpose and it is connected to the control unit through port zero (P0) of microcontroller. The sensor unit (keypad) is made of micro switches, which transmits information of the control unit through port two (P2) of the microcontroller especially when each of them is pressed. The display unit are made with seven-segment led display arranged serially to each other and are connected to the control unit through port one (P1). The control unit is made up of microcontroller. It is the heart of the device as it accepts from the sensor unit (keypad) and the input unit through port one (P1) to the display unit. These connections are performed using soldering techniques on a Vero board while the necessary connections are finished with Jumper wires.

CONCLUSION

This paper titled the design and construction of a two factor authentication security system with a dial-up system has been achieved. The smart card was able to transmit information to the control unit, the controller accepts the information transferred and process them by prompting for password (Enter Pin) when the code has been enter through the keypad the controller was able to interpret the information, and process it again without troubles. It displays ACCESS GRANTED OR ACCESS DENIED, depending on the information it has been fed with. This work has also satisfied the objective of becoming interactive since it can ask question to insert card. After the card insertion, another question goes requesting for the users password. It confirms the password and decides if the door will be open or remain closed. It is human friendly and can be used by any authorized person.

REFERENCES

Adam (1980). *An Introduction to Microcomputers*. Volume 1, **Basic Concepts** (2nd ed.), Osborne-McGraw Hill, Berkely.

Badawy, W. and Jullien, G. (2003). *System-on-Chip for Real-Time Applications*,

Springer, New York.

Buckey, P.M and Hoskyns, A.H. (1980) *Basic electronic circuit* E.F.M spon Ltd., London New York pp. 200-215

Miller, G. A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review* **63** (2): 81–97.

Moore, G. (1965). Cramming more components onto integrated circuits. *Electronics* **38** (8).N.N. Liner *IC (pocket Book) 555 Timer*

Forrest, M. M. III (2004). *Timer, Op Amp, and Optoelectronic Circuits and Projects*. Master Publishing Inc., Niles

Britton, R. (2003) *MIPS Assembly Language Programming*. Prentice Hall, New Jersey