International Journal of Electronics Communication and Computer Engineering
Volume 8, Issue 1, ISSN (Online): 2249–071X

Development of Smart Card Door Access Control System

Oluyemi E. Adetoyi
Electrical and Electronic Engineering Department, University of Ibadan, Nigeria.
Corresponding author email id: yemi.ade@ui.edu.ng

Date of publication (dd/mm/yyyy): 17/02/2017

Abstract **– Access control is a fundamental security measure to ensure that only authorized persons are allowed into restricted areas. Many access control techniques have evolved with time in order to raise the standard. In this paper, two-level authentications based on smart card and pin code access control is presented. This system was developed and implemented for a small size sliding door. The sliding operation was carried out by motor controlled pinion and rack. The system at all times provided access or limitation accordingly.**

Keywords **– Access Control, Authentication, Personal Identification, Pin Code, Smart Card.**

I. INTRODUCTION

Preventing access of unauthorized person into restricted area in an electronically way, has been a vital approach to ensure that the security of an area is not compromised. A number of access control technique has evolved over time, each having its own merits and demerits. In biometrics method of access control, a person physiological and behavioral characteristic is extracted to perform person recognition. Among those characteristics are: fingerprint, hand geometry, handwriting, handprint, iris, palm vein, voice and retinal. These characteristics have been a subject of much research to provide human identification and access control functions. In [*1*], finger vein human identification system which can be used for access control was presented. Simple pattern matching method was used to reduce computation time for embedded environments, but the success rate is 97.6% and is therefore not suitable for personal security field. A finger vein and texture recognition technique based on repeated linetracking; Gabor filter and Neural Network was proposed in[*2*], though it may be cost effective and more accurate than some algorithm, long computation time will limit its usage. Palm vein authentication device that uses blood vessel patterns as a personal identify factor was presented in [*3*]. Although it has high level of accuracy, false acceptance and false rejection is still a problem. An Iris controlled door system was presented in [*4*], however costly image capturing equipment and long processing time is inherent in the system. Facial recognition and artificial neural network were combined to simulate a secure keyless door solution in [*5*]. However, it was simulated in MATLAB, which runs too slow. In [*6*], the acquired voice signal of authorized persons were used for comparing with a user voice and access is granted by opening the door, if it matches. However, the success rate is between 60% and 70%. Another voice based access control was presented in [*7*], whereby an adaptive network based fuzzy interference system was used to identify authorized user. Though the false acceptance rate and the false rejection rate were considered good, improvement is still possible. The edge that biometric systems have over other access control is that they provide a non-transferrable means of identifying people [*3*]. However, Single modality biometric identification systems have false rejection and false acceptance rates, which cannot be reduced simultaneously, but force users to trade-off between these two rates. Hence, algorithm for multimodal approach which combines two or more sensors to acquire same biometric feature was the subject of research in [*8*]. This however suffers the drawback of long transaction time and poor ease of use for the user. Another form of access control is based on GSM, whereby the code for access is sent to microcontroller or through a computer to an embedded phone. The limitation is that the security was based on code alone. The use of RFID and facial recognition system was considered in [*9*]. It provide added feature of turning alarm ON and placing emergency call to security van, in case of suspicious user. Though security is enhanced, the response time is slow. An NFC enabled smart phone access control and management system was presented in [*10*]. Although it may provide a high level of security, complexity and cost of software and hardware infrastructures placed a limit on its use. In [*11*], a contactless smart card was used to provide door access control. It has the advantage of being usable in harsh environment and more user friendly than contact type. However, it is less secured and slower than contact type, which was used for access control in this paper.The new trend in access control is to incorporate IP technology. An RFID networked system was proposed in [*12*]. Even though there is enhanced functionality, the cost might limit its usage. A combination of smart card and PIN code is being proposed for access control in this paper, to address the limitations posed by previous system.

II. SMART CARD DOOR SYSTEM

The implementation of the design of security door using smart card is based on hardware and software. It provides two level authentication; the smart card and a pin code. The block diagram of the design is as shown in Figure 1. The flow chart that summarizes the operation of the system is shown in Figure 2.

Copyright © 2017 IJECCE, All right reserved

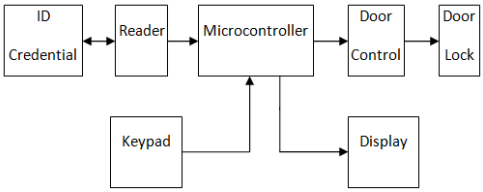

Fig. 1. Block diagram of smart card door system

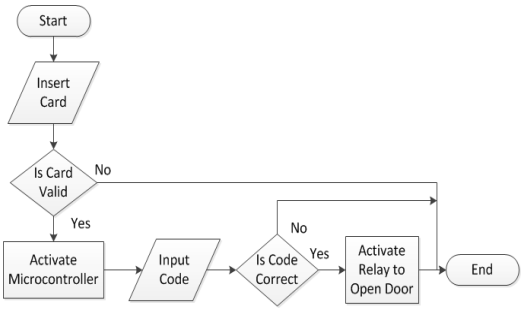

Fig. 2. Flow chart of smart card door system

A. *PIC18f452 Microcontroller*

One of the most important features of this microcontroller, whose pinout is shown in Fig. 3is the number of input/output pins used for connection with peripherals. There are thirty-five general purpose I/O pins available, which is more than enough for the application. In order for pins operation to match internal 8-bit organization, they are grouped into five ports denoted by A, B, C, D and E, similarly to registers. Every port has its "satellite", i.e. the corresponding TRIS register: TRISA, TRISB, TRISC etc. which determines performance, but not the contents of the port bits. By clearing some bit of the TRIS register (bit=0), the corresponding port pin is configured as output. Similarly, by setting some bit of the TRIS register (bit=1), the corresponding port pin is configured as input. In the PIC18 series of microcontrollers, serial communication can be handled either in hardware or in software. The hardware option is easy; PIC18 microcontrollers have built-in USART (universal synchronous asynchronous receiver transmitter) circuits providing special input-output pins for serial communication. For serial communication all the data transmission is handled by the USART, but the USART has to be configured before receiving and transmitting data. With the software option, all the serial bit timing is handled in software, and any input-output pin can be programmed and used for serial communication.

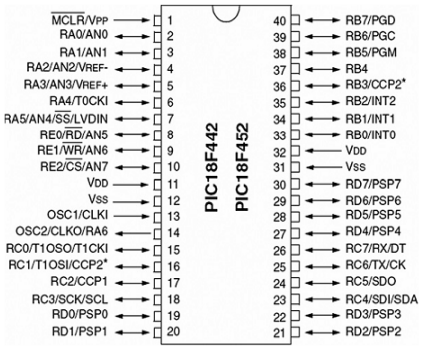

Fig. 3. Packaged view of PIC18F452 microcontroller

B. *ID Credential and Reader*

The smart card unit detects a card if it is configured for the system. It has a slot to insert the card, thereby providing direct coupling to the reader. This has the advantage of speed, larger data transport without the overhead of anti-collision and better security over contactless readers. The smart card and the reader use mutual active authentication protocol to identify each other. The card generates a random number and sends it to the reader, which encrypt the number with a shared encryption key before returning it to the card. The card then compares the returned result with its own encryption. The pair may then perform the operation in reverse. Once communication is established, each message between the pair is verified through a message authentication code. This is a number that is calculated based on the data itself, an encryption key, and a random number. If data has been altered (for any reason, including transmission errors) message must be retransmitted or the data can be verified through a digital signature. Once the extracted card information by the reader gets to the microcontroller, it compares with the pre-enrolled information. If the verification is successful, it initiates the display to prompt the user to "enter pin".

C. *Keypad Module*

The keypad was designed to issue instruction to the microcontroller. It is a 4 x 4 switch array, consisting of 0 – 9 digits; alphabets A, B, C, D and special characters # and *. The # button is used for changing password, the * button for canceling wrong entry, the remaining buttons are for 4-digit PIN code entry. Each key upon being depressed transmit its instruction to the central processing unit of the microcontroller. The keypad is connected to the microcontroller port via RDO to RD7.

D. *Display Unit*

Depending on how many lines are used for connecting an LCD to the microcontroller, an 8-bit or 4-bit LCD modes are possible. The appropriate mode is selected at the beginning of the operation in the process called 'initialization'. The 8-bit LCD mode uses outputs D0- D7 to transfer data. The main purpose of the 4-bit LCD mode is to save valuable I/O pins of the microcontroller. Only 4 higher bits (D4-D7) are used for communication in this mode, while others may be left unconnected. Each piece of data is sent to the LCD in two steps, four higher bits are sent first, then four lower bits. Initialization enables the LCD to link and interpret received bits correctly.

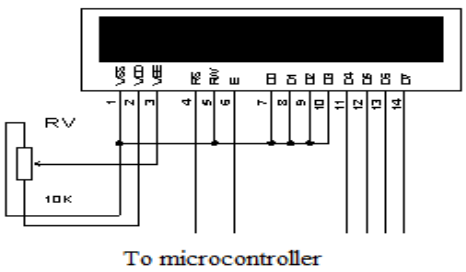

Fig. 4. LCD display connections to microcontroller

E. *Sliding Door Unit*

This unit shown in Fig. 5 consists of two switching

Copyright © 2017 IJECCE, All right reserved

transistors, two 10A - 12VDC relays, 12V dc motor and rack and pinion system that drive the gate into open or close position. The relays are connected in series to provide bidirectional DC switching. Therefore the DC motors can rotate in one direction to open the door and opposite direction to close it. Upon microcontroller verification of card information sent by the reader, a high pulse from the microcontroller port will bias one of the power transistorsON; its collector current triggers the relay responsible for opening the door. A high pulse from the microcontroller to the second power transistor will trigger the relay responsible for closing the door. Placing an active low pulse at these ports terminates the current and de-energize (normally open) the relay contacts. This allows current to be discharged from the inductor of the relay through the transistor emitter. In order to avoid the stored current from damaging the transistor, a diode is connected to act as a feedback. The constructed door unit in Fig. 6 reveals the motor and rack and pinion system for opening and closing the door.

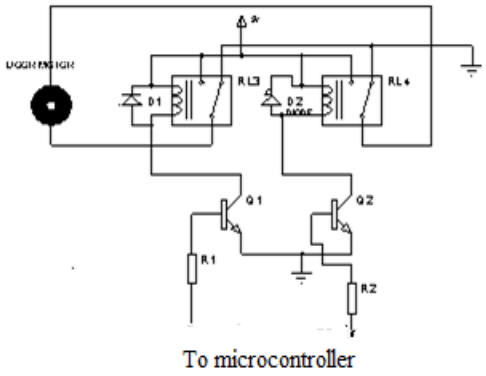

Fig. 5. Interface circuit for door control

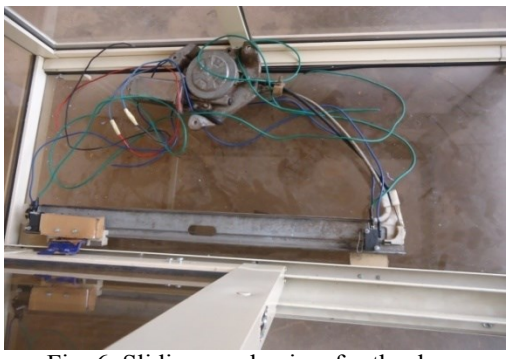

Fig. 6. Sliding mechanism for the door

F. *Power Supply Unit*

Three regulated supply of 12V, 5V and 3.3V are required in the circuit. The DC motor is powered by 12V supply, the card reader is powered by 3.3V and the rest of the circuit is powered by 5V. The schematics for the power supplies are as shown in Fig. 7. The process undergone in the design is the same; from transformation, rectification, filtration to voltage regulation. The sizing of the components is as follows:

Transformers secondary voltage are chosen such that

$$V_S \geq V_{NL} + V_R + 2V_D \qquad (1)$$

where V_S is transformer secondary voltage, V_{NL} is no load voltage (3.3V/5V/12V as case may be), V_R is regulator dropout voltage (2V was used), V_D is diode voltage drop (equal to 0.7V).

Thus transformer is rated 230V/16V. The current rating is 1A, since it is well above load driven. For LM317, R_1 is chosen to be 240Ω, while R_2 is calculated thus

$$V = 1.25(1 + (R_2/R_1)) \qquad (2)$$

Next preferred value of 430Ω is chosen for R_2.

Capacitors rated voltage is at least twice the working voltage and capacitance is obtained thus

$$C = \frac{I}{V_{Rf}} \qquad (3)$$

where C is capacitance, I is load current (10mA for card interface,25mA for controller circuit, 30mA for relay), V_R is allowable ripple voltage (10% of no load voltage), f is twice the main frequency voltage and is equal to 100Hz.

For 3.3V:

$$C_{eq} = \frac{I}{V_{Rf}} = \frac{10\times10^{-3}}{0.33\times100} = 300\mu F$$

C_1 and C_2 can be chosen as 75µF respectively, C_3 equals 150µF

For 5V:

$$C_{eq} = \frac{I}{V_{Rf}} = \frac{25\times10^{-3}}{0.5\times100} = 125\mu F$$

C_4 equals 50µF

For 12V:

$$C_{eq} = \frac{I}{V_{Rf}} = \frac{30\times10^{-3}}{1.2\times100} = 250\mu F$$

C_5 and C_6 can be chosen as 75µF and 200µF respectively

G. *Control Program*

The program was written in C-language, the choice of C-language was to make the program small and enhance faster execution. Text editor was used to debug and correct errors in the program. The program was then translated to machine language. Thereafter, the link/locator pair was used to coordinate between the separate modules for smooth program execution. Fragment of the code is presented in the Appendix.

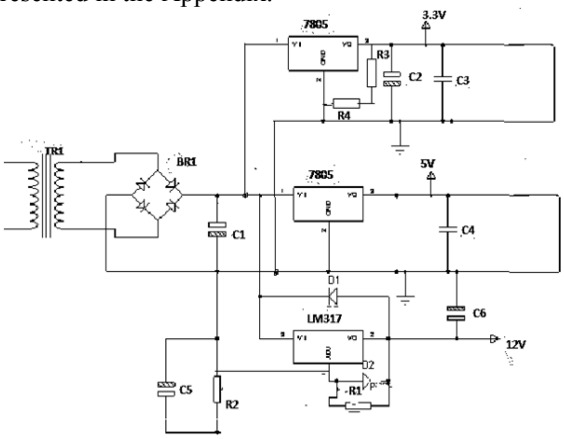

Fig. 7. Power Supply

Copyright © 2017 IJECCE, All right reserved

III. RESULT

If the card inserted into the reader was ascertained by the microcontroller to be valid, the user is prompted through the LCD display to input pin code, otherwise “INVALID CARD” is displayed. If the pin code was not input within a predetermined time interval, the LCD displayed "TIME OUT PLEASE, REMOVE YOUR CARD ". If the pin code authentication is successful, "ACCESS GRANTED” is displayed and the relay mechanism to open the door will be activated and the user will be prompted to remove card, the door closes after a predetermined time interval. If the pin code authentication failed, LCD will display “REMOVE YOUR CARD, INVALID PASSWORD”. More so, provision is made to change password, to ensure that password is not compromise. Summary of operation is presented in Table I.Twenty - five checks each of the system operation was carried out in turn on each case of Table 1, the result followed Table I accordingly. In all cases, the system operated correctly.

Table I. System Operation

Card	Pin	Action
Valid	Correct	Door Opens
Valid	Incorrect	Door Remain Closed
Invalid	Incorrect	Door Remain Closed
Invalid	Correct	Door Remain Closed

IV. CONCLUSION

A prototype design for a low complexity, low cost access control technique has been presented, which offers high level authentication, based on pin code and smart card. It is unaffected by false acceptance ratio or false rejection ratio, which are inherent in biometric authentication systems. The system can be enhanced by incorporating an alarm systemor a dial call system to alert security personnel when an invalid card is used or when wrong pin code is entered a specific number of times.

ACKNOWLEDGMENT

The author wishes to appreciate Mr Udeze Ugo and Mr Olaoluwa Owoeye for carrying out, the laboratory aspect of the work. University of Ibadan is also appreciated for providing enabling environment to carry out the work.

REFERENCES

[1] K.W. Ko, J. Lee, M. Ahmadi, and S. Lee, "Development of Human Identification System Based on Simple Finger Vein Pattern Matching Method for Embedded Environments," International Journal of Security and Its Applications, vol. 9, no. 5, pp. 297-306, 2015.

[2] R. Kaur and R. Rani, "An Identity Authentification Using Finger Vein and Texture Images Using NN," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 7, pp. 983-988, July 2014.

[3] I. Sarkar, Alisherov F., T. Kim, and D Bhattachayya, "Palm Vein Authentication System: A Review," International Journal of Control and Automation, vol. 3, no. 1, pp. 27-34, March 2010.

[4] A. S. Falohun, E.O. Omidiora, O.A. Fakolujo, O.A. Afolabi, and A.O. Oke, "Development of a biometrically- controlled door system (using iris), with power backup," American Journal of Scientific and Industrial Research, vol. 3, no. 4, pp. 203-207, 2012.

[5] O. Omidiora, M. Olaniyi, and A.A. Ipadeola, "Development of Security System Using Facial Recognition," Pacific Journal of Science and Technology, vol. 9, no. 2, pp. 377-386, 2008.

[6] S. Achankunju and C. Mondikathi, "Voice Based Security System Using Matlab& Embedded System," International Journal of Scientific Research, vol. 4, no. 5, pp. 770-773, May 2015.

[7] W.A. Wahyudi and M. Syazilawati, "Intelligent Voice-Based Door Access Control System Using Adaptive-Network-based Fuzzy Inference Systems (ANFIS) for Building Security," Journal of Computer Science , vol. 3, no. 5, pp. 274-280, 2007

[8] L. Osadciw, P. Varshney, and K. Veeramachaneni, "Improving Personal Identification Accuracy Using Multi sensor Fusion for Building Access Control Application," in Proceedings the Fifth International Conference for Information Fusion, 2002, pp. 1176- 1183

[9] U. Farooq, M. Hasan, M. Amar, and A. Hanif, "RFID Based Security and Access Control System," IACSIT International Journal of Engineering and Technology, vol. 6, no. 4, pp. 309-314, August 2014

[10] N. Saparkhojayev, A. Nurtayev, and G. Baimenshina, "Access Control and Management System Based on NFC-Technology by the Use of Smart Phones as Keys," Middle-East Journal of Scientific Research, vol. 21, no. 7, pp. 1130-1135, 2014.

[11] V.K. Sehgal, Nitin, and D.S. Chauhan, "Embedded Controller Based Smart Card Access," in Proceedings of the World Congress on Engineering and Computer Science, San Francisco, 2008.

[12] J.L. Raheja, S. Nayak, and A. Gupta, "RFID Based Networked Gate Entry Control System (GECS)," International Journal of Computer Networks & Communications (IJCNC), vol. 1, no. 3, pp. 34-44, October 2009.

AUTHOR’S PROFILE

Oluyemi Adetoyi had B.Sc. and M.Sc. degree in Electrical and Electronic Engineering. She is currently pursuing her PhD in Communication Engineering. She has lectured at University level for eleven years. Her research interest is in wireless communication and data security.

Copyright © 2017 IJECCE, All right reserved