International Conference of Science, Engineering & Environmental Technology (ICONSEET), 2(19): 148-153, 2017
ISSN 0794-9650

www.repcomseet.com

Design and Implementation of a Radio Frequency Identification and Password Door Access Control System

Adebayo A. K., Bamikefa I. A., Sanusi M. A., Abolarin M. O., Olagoke B. L., & Agbolade J. O.

Electrical/Electronic Engineering Department, Federal Polytechnic Ede Osun State Nigeria

Abstract- Security system solutions for strategic facilities are critical to prevent the intrusion of unauthorized persons, however there are many types of automatic access control systems which are expensive and complicated to use. This paper focuses on the development of a simple security system that combines Radio Frequency Identification and password to provide a low cost and formidable access control for entrances. The system is built on ATMEGA8 Microcontroller that directs the RFID reader to scan and authenticate users' identification tag and further request for password through a keypad before activating a motor to grant access. The Microcontroller which also controls a liquid crystal display was programmed using Microbasic language; the data of identification tags and password were stored in its database. The RFID reader was able to scan tags within 25cm range in two seconds, and open a prototype door within 3 seconds of entering the correct password. The motor closes the door after a preset 5 seconds delay. The system was implemented for 12 users, the components used are cheap and available; the system is formidable and reliable.

Keywords: Microcontroller, Password, Radio Frequency Identification (RFID), Security, Tag

1. Introduction

Security systems are very important in the protection of lives, premises and valuable resources. There are many advanced methods of providing security that have been developed and are in use in the last few decades, one important area is the security system required for strategic applications such as military bases, research centers, laboratories and other critical facilities. Such advanced security systems are complex and expensive making them implementable in high end applications only. However, with recent progress in technology and the growing need for increased security in civilian and other applications, many low cost solutions for security system have emerged with a range of degrees of sophistication, complexity and cost (Gill, Yang, Yao, and Lu, 2009).

Different access control automation techniques are available to reduce the system complexity and lower costs, these systems do not incorporate complex and expensive components. A home gateway is implemented to facilitate the interoperability between heterogeneous networks and provide a consistent interface, regardless of the accessing device (Udaya, Murty and Kurmar, 2013).

There is a wide range of Automatic Identification (Auto-ID) systems for access control in use, these includes magnetic stripes, Optical Character Recognition (OCR), barcodes, biometrics, smart cards and Radio Frequency Identification (RFID). However, each of these technologies has their advantages and drawbacks. The OCR systems allow the use of manual and auto-identification simultaneously but the very high cost of the readers prevented its widespread use (Finkenzeller, 2003)

The use of barcodes is a cost-effective way for managing inventory, they have some disadvantages such as limited information-storing capacity; a strict line of sight requirement between the scanner and the barcode, which effectively prevents multiple barcodes to be processed simultaneously; limited data redundancy and error correction; and a lack of inbuilt data-security standards. The use of biometrics, such as fingerprinting, retina scans, iris scans, and voice recognition are strong identification solutions in automatic access control but these technologies are expensive and privacy invasive (Sweeney and Patrick, 2005).

Smart card and its derivatives such as memory card or microprocessor card solutions use standard credit-card sized plastic cards with an integral data storage system designed to make financial transactions secure and fast, but a with high cost of maintaining the reader (Goodrum, McLaren and Durfee, 2006). RFID tries to overcome the disadvantages of previous systems by improving the speed and accuracy of data collection and dissemination as well as reducing the overall cost. RFID systems rely on Radio Frequency to transmit a tag-specific unique serial number to a reader or interrogator (Amit and Berghel, 2011).

A RFID system is composed of three basic units, a transponder unit or tag with a unique identifier that facilitates auto-identification of any object to which the tag is attached, a reader unit or interrogator that manages the radio frequency communication with the tag and a middleware or reader interface layer, which is essentially a software that acts as an interface between the basic RFID hardware components, and the software application (Shoewu and Badejo, 2006).

There currently is not a definite industry standard for frequency, but the most common applications around the world use frequencies of 125 KHz and 13.56 MHz. There are three classes of the RFID tags; Active tags, Passive tags and Semi-Passive (Battery –Assisted Passive) tags. The Active tag has its own battery that is used to broadcast signals over great distances; it is usually bigger in size and capable of carrying more information. The Passive tag has no inbuilt power source, the signal from the RFID reader creates an electromagnetic field that powers the tag, and it is cheaper than the active tag. The Semi-Passive tag or Battery Assisted Passive tag (BAP) is equipped with an onboard battery that drives the chip's circuitry but power for communication of the signal is derived from the reader's electromagnetic field as in the case of passive tags (Gyanendra and Pawan, 2010).

The password identification system requires the user to enter a password (a set of numeric or alphanumeric characters) on a keypad which then grants access to the user if it matches the required characters residing on a database (Kyuhee and Mokdong, 2006).

The RFID system has its vulnerabilities such as card skimming and tag killing, other security issues are card spoofing, tag cloning and malwares (Amit and Berghel, 2011). This gave rise to the need for a simple and affordable system that will utilize the advantages of the RFID and also overcome its drawbacks; leading to the use of password identification in addition to the RFID for access control, this is the aim of this study.

2. Methodology

The proposed security system makes use of a passive RFID tag and password combination supported by a microcontroller to provide access control to facilities or rooms within premises by opening and closing of a door. The system consists of a hardware module and an application program for the Microcontroller unit. The application program was developed using mikroC programming language. The hardware module comprises of the input units (RFID tag, RFID reader, and Password keypad), the display unit, the microcontroller unit and the power supply unit. The block diagram of the system is shown in Figure 1.

2.1 RFID tag

The Parallax key fob passive RFID tag is utilized in this study due to its low cost, lightweight, and availability. Twelve (12) units of RFID tags were used; each one of the tags has its own unique Electronic Product Code (EPC) which was programmed into the database of the microcontroller to enable their identification when scanned by the reader.

2.2 Parallax RFID reader module

This is a low-cost solution to read passive RFID transponder tags up to a distance of 30 cm depending on the tag being scanned. The RFID Reader Module is used in a wide variety of hobbyist and commercial applications, including access control, automatic identification, robotics navigation, inventory tracking, payment systems, and car immobilization. Specifications of the Reader are; single wire, 2400 baud serial TTL interface to a PC, single +5V DC supply and Bi-color LED for visual indication of its activity. It operates on a frequency of 125 kHz.

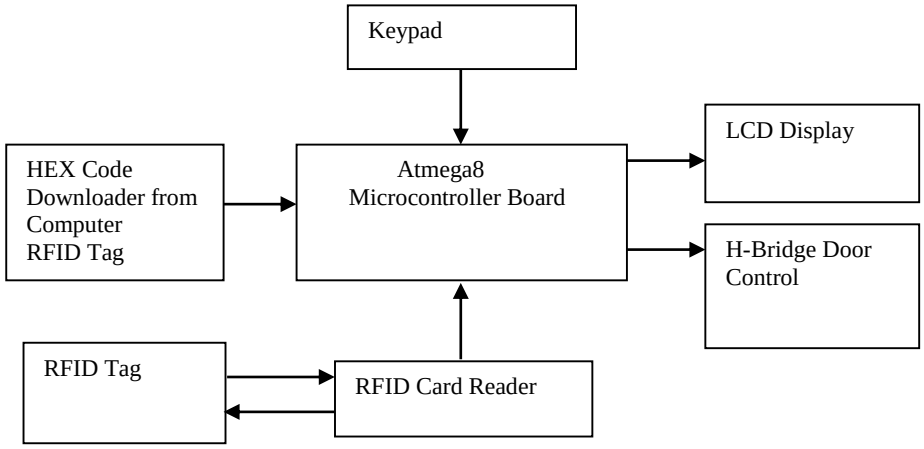

Figure 1: Block Diagram of RFID/Password Door Access Control System.

2.3 The Password keypad

The password keypad is a 16 button generic soft touch keyboard, it has 10 numeric buttons and 6 alphabet buttons enabling it to carry out alphanumeric functions. The keypad has 7 pins which are connected directly to the microcontroller. The password is a four-digit number which is stored in the database of the microcontroller, it is entered on the keypad and confirmed by pressing a designated alphabet key, it is also cleared by pressing another designated alphabet key.

2.4 Liquid crystal display

The microcontroller board's LCD port provides the signals needed for a standard character based LCD modules. The display has 8 pins which are connected directly into the microcontroller. It displays 16 characters by 2 lines; the characters are black against a green background. The LCD includes a green LED backlight, which allows the characters to be viewed without ambient light. In normal room light, the characters are visible without the backlight. A resistor is included for current limiting to the backlight.

2.5 Motor rotation control knobs

The control knobs are sensors that act as feedback to the microcontroller by opening and closing of the circuit enabling it to determine when the motor should stop rotating. This occurs when the door has opened to its maximum length and achieved by the "open control knob" button. The principle also applies to the closing feedback that will also be sent to the microcontroller to indicate when the door is closed so that the motor will stop rotating and this is done by the "close control knob" button.

2.6 Microcontroller (ATMEGA8)

The ATMEGA8 is a low-power CMOS 8-bit microcontroller based on the AVR RISC (Advanced Virtual RISC – Reduced Instruction Set Computer) architecture. The device is manufactured using Atmel's high density non-volatile memory technology. The Atmel ATmega8 provides a highly-flexible and cost effective solution to many embedded control applications. Some of its features include; 8 kb of flash program memory, 512 bytes EEPROM, 1Kbyte internal SRAM, an inbuilt analog to digital converter and a 3ports system for communication needs. The microcontroller provides the base on which the system runs, it acquires the signals from the RFID reader and the password keypad, process it and send appropriate signals to the Liquid crystal display and door control motor mechanism.

2.7 *Power supply unit*

The power supply circuit consist of the circuit for conversion of 220 volts, 50Hz AC into 12V and 5V DC. This is achieved by the use of a step down 12V-0-12V centre tapped transformer with a full wave rectifier. The AC ripples are eliminated using the capacitor and the LM78 and LM79 voltage regulator series used to regulate the output voltages. The 5V DC is used to power the Microcontroller and the LCD. The 12V DC is used to power the DC motor that drives the door, it also powers the relay circuits. The circuit for the system was designed using Proteus software, the Printed circuit board layout was also done with the software, and the circuit diagram is shown in Figure 2.

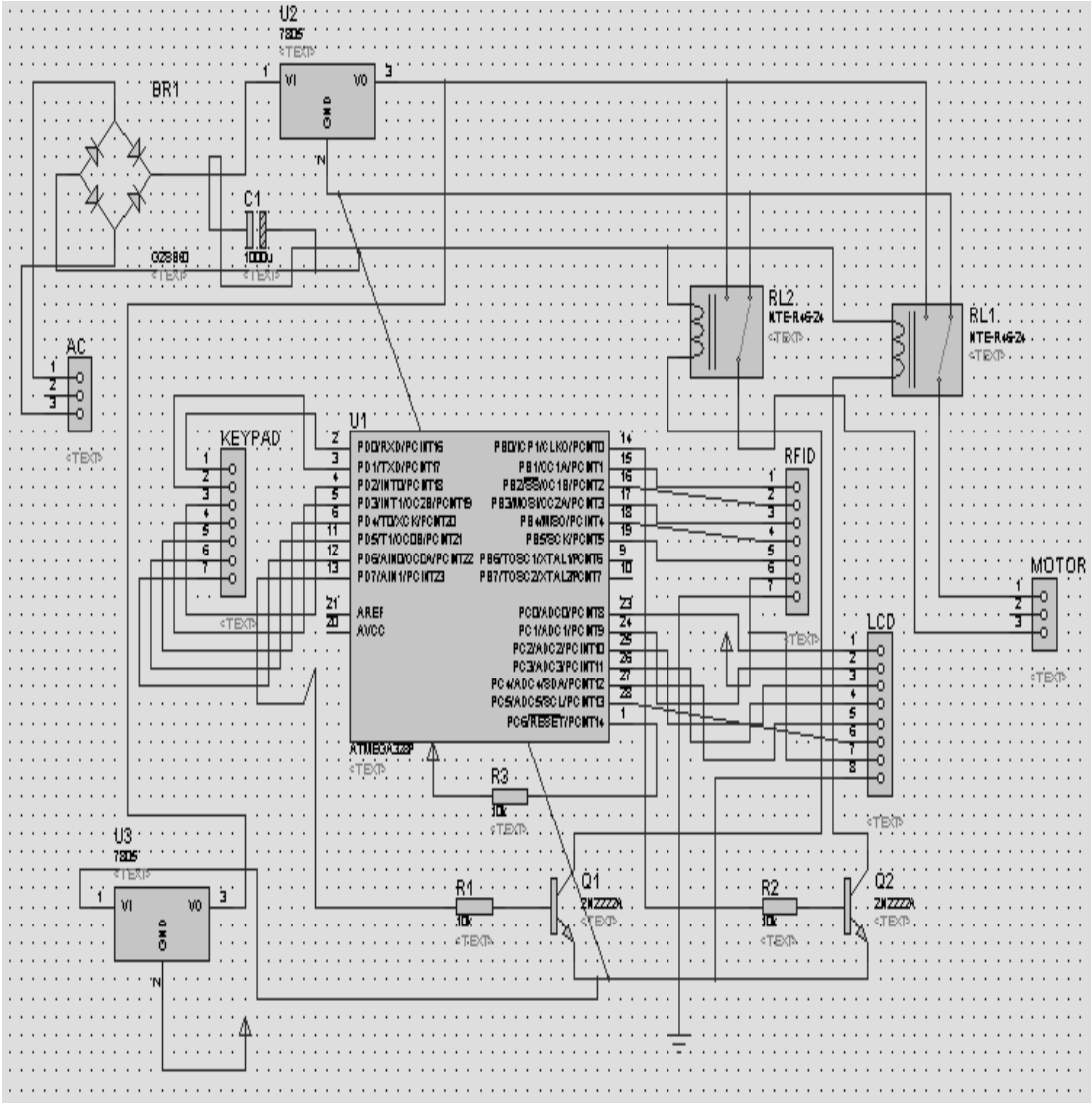

Figure 2: RFID/Password door access control system circuit diagram using *PROTEUS*

2.8 Software module

The software for the microcontroller was written in *mikroC* language, the equivalent hexadecimal file of the written code was loaded onto the microcontroller using an AVR programmer. The Flash program memory can be reprogrammed In-System through an SPI serial interface, by a conventional non-volatile

memory programmer, or by an On-chip boot program running on the AVR core. The boot program can use any interface to download the application program in the Application Flash Memory. Software in the Boot Flash Section will continue to run while the Application Flash Section is updated, providing a true Read-While-Write operation

3. Results and discussion

The PCB layout was transferred to a single sided Copper circuit board; it was then etched using appropriate techniques. The terminals of the circuit components were drilled on the board; the components were then mounted and soldered firmly. The connections of the RFID reader, the LCD, the keypad, the motor and power supply to the PCB were done, and then checked for consistency.

The circuit is housed in a prototype structure whose door is connected to and controlled by the motor. The RFID reader and the keypad are mounted on the surface of the rectangular box to enable input of the password and scanning of the tag. The components of the system are shown in Figure 3, when the power supply to the circuit was switched on, the system initialized in about 5 seconds and requested for the RFID tag to be scanned. The tag was brought to about 25cm in front of the reader, and then a request for input of the password was displayed on the LCD. The password was entered on the keypad and confirmed, a response 'Access Granted' was displayed on the LCD and the motor opened the door, and the door was closed after 5 seconds preset time.

The other cards whose EPC were not stored in the microcontroller were brought for scanning, the system refused to request for password. The password was also wrongly entered when requested after using proper RFID tags, access was denied which was also displayed on the LCD, and the complete access control system is shown in Figure 4.

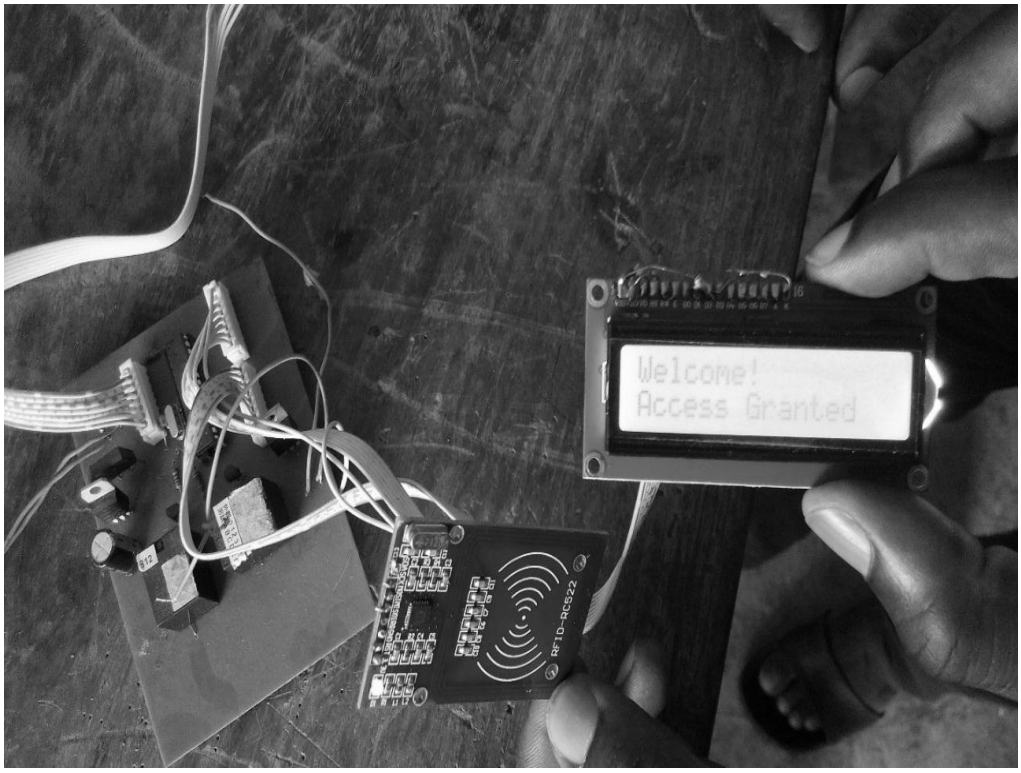

Figure 3: Components of the access control system on workbench.

Figure 4: Complete prototype RFID/Password based door access control system.

4. Conclusion

In this paper, a door access control system based on RFID and password combination was designed and implemented. The system scans the RFID tag presented by the user, if the identity is found on the database it requests user to enter the password on the keypad, otherwise it denies access to the user. When the password supplied matches that on the database access is granted and a motor opens the door. The components used are reliable, cheap and readily available.

The system can be further improved by including a finger print identification; also the provision of a database system for users' logging information will make the system more robust. The system can also include an alert and warning system for repetitive violation of password or wrong RFID tag usage.

References

[1] Amit Grover and Hal Berghel (2011). A Survey of RFID Deployment and Security Issues. *Journal of Information Processing Systems*, Vol.7, No.4, pp.561-581

[2] Finkenzeller, Klaus (2003). RFID Handbook, John Wiley & Sons, Chichester, West Sussex England, pp.5

[3] Gill K., Yang S.H., Yao F. and Lu X. (2009). A Zigbee Based Home Automation system, *IEEE Transactions on Consumer Electronics*. Vol. 55, No.22, pp.422-430

[4] Goodrum, P., McLaren, M. and Durfee, A. (2006). The application of active radio frequency identification technology for tool tracking on construction job sites. *Automation in Construction*, Vol.15, No. 3, pp 292-302

[5] Gyanendra K Verma and Pawan Tripathi (2010). A Digital Security System with Door Lock System Using RFID Technology. *International Journal of Computer Applications*. Vol.5, No.11, pp.6-8

[6] Kyuhee Ann, Kiyeal Lee, and Mokdong Chung (2006). Design and Implementation of an RFID-based Enterprise Application Framework based on Abstract BP and Kerberos. *International Journal of Information Processing Systems*, Vol.2, No.3, pp. 27-31

[7] Shoewu O. and Badejo O. (2006). Radio Frequency Identification Technology; Development, Applications and Security Issues. *The Pacific Journal of Science and Technology* Vol. 7, No.2, pp.144-153

[8] Sweeney II, Patrick J. (2005) RFID for Dummies. Wiley Publishing, Hoboken New Jersey, pp.37

[9] Udaya B.K., Murty D.S. and Kumar P. (2013). Implementation of Low Cost Ethernet Based Home Security Using Wireless Sensor Network. *Algorithms Research*, Vol. 2, No.1, pp. 1-7