An Rfid-Based Access Control System Using Electromagnetic Door Lock and an Intruder Alert System

Philip Olawatimileyin Makanjuola [a], Emmanuel Segun Shokenu [a*], Haonat Olajumoke Araromi [a], Peter Olalekan Idowu [b] and Joshua Dada Babatunde [a]

[a] *Department of Computer Engineering, Ladoke Akintola University of Technology (LAUTECH), Ogbomoso, Nigeria.*
[b] *Department of Electronic and Electrical Engineering (EEE), LAUTECH, Ogbomoso, Nigeria.*

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Original Research Article

ABSTRACT

Aims: The study was conducted to develop a basic security system that integrates Radio Frequency Identification (RFID), an electromagnetic lock, and a GSM Module to produce a lowcost and effective access control system. This work uses the possibility of improving access control door security by replacing a door key with a dependable electromagnetic door lock system for only authorized persons utilizing RFID and a mobile call intruder warning system.
Methodology: The system is controlled by an ATMEGA328 microcontroller, which instructs the RFID reader to check and verify the users' unique identity tags before unlocking the electromagnetic lock to grant access or alert the administrators through the GSM module if an invalid tag is used. The microcontroller which also controls a liquid crystal display was programmed using Arduino C language; the data of identification tags were stored in its database. The RFIDbased access control with electromagnetic lock and intruder alert consists of three main parts – the INPUT (RFID), CONTROL (ATMega 328), and OUTPUT (Electromagnetic lock, LCD, Buzzer, and GSM Module). The RFID reader was able to scan tags and open a prototype door when a valid tag is used. The motor closes the door after a preset 5 seconds delay.

_____

Corresponding author: Email: seshokenu@student.lautech.edu.ng;

Conclusion: When compared to well-known techniques in the literature, the developed RFID Access control system outperforms them in terms of accuracy and cost-effectiveness.
The door locking system works in real-time because when the user places the tag in contact with the reader, the door opens and the check-in information, together with the user's basic information, is recorded in the central server.

1. INTRODUCTION

Various control mechanisms have been developed throughout the years to prevent unauthorized people from accessing sensitive information. The primary reason for installing locks in our structures (homes, offices, churches, schools, and so on) is to ensure the safety of our lives and belongings. As a result, having a stress-free and accessible way to accomplish this goal is critical. Today, security and safety are becoming increasingly popular, and they are improving and being used for our convenience. Because technology has become such an integral part of people's lives in recent years, home security must not be overlooked. The security system was separated into two types: one that used a traditional door lock key, and the other that employed an electronic automated identification system [1].

The electromagnetic lock is utilized as the door lock, the RFID module is used to access the door, and the GSM module is employed as an intruder alarm system in this project. The system includes RFID tags and RFID readers in the project. The Rx and Tx pins of the microcontroller are connected to the RFID reader. A user can gain entry to the door by placing his or her valid RFID card on the reader. The electromagnetic lock is unlocked and closed after some delay if the system detects a genuine RFID card. If an invalid card is discovered, the GSM Module sends a call to the administrator or owner, who then takes the appropriate action. Wireless automated identification assumes a very specific shape using RFID The object, location, or person is identified by a unique identifying code encoded in an RFID tag that is attached to or embedded in the target in some way [2].

2. RELATED WORKS

Several researchers have put a lot of time and effort into RFID-based security access systems. In this paper, an RFID-based automatic gate opening system for automobiles and a campus access system were developed [3] also, [4]. The systems provide access to authorized people with valid tags and prohibit entry to people with invalid tags, but they cannot send SMS alerts to security staff. [5] suggested a method that analyzed RFID and wireless Home/Office Automation in comparison. Three technologies were used in this case: RFID, Wireless Sensor Network (WSN), and GSM. In this system, RFID monitors access, sensors monitor temperature, lighting, and gas leakage, and GSM sends an SMS to the home's owner when the home's security is compromised.

In the [6] An RFID-based kindergarten intelligence security system was presented as part of the project. It automates the security supervision of children and integrates with the present kindergarten security management system, which uses RFID tags inserted in the children's clothes. When a threat was detected, however, the system was unable to alert security personnel.

[7] built and implemented a neural network with RFID and face recognition for access control. This method compares the face of the person carrying the RFID card to the face of the person holding the RFID card and restricts access if the two don't match. To determine the face of authorized cardholders, a Radial Basis Function Neural Network (RBFNN) was used. Also, in the event of an unauthorized holder, there is no way to notify safety personnel through SMS. In [8] A paper was presented on asset theft security systems using frequency identification technology. The goal was to use RFID technology (Ultra high-frequency range; 905–925MHz) to construct a security system against motorbike theft. If the tag provides false information, the system alerts the security personnel, who will investigate further. Because the theft occurs, it can signal a further circuit to turn off the motorcycle engine and turn on the closed-circuit television (CCTV) for recording. To avoid uproar, the system would be better served by sending SMS to the guards.

The 8051 microcontrollers, having been invented by Gary Boone of Texas Instruments in 1971 [9], have seen tons of monumental uses within the course of history. [5] sees the 8051 as the brain of the circuit, also calling it the CPU of the circuit.

The 8051 which has a Program Memory of 2Kbytes (EEPROM) is used to store the predetermined password during the time of installation, which is taken into consideration during the operation to match the input password with the predetermined password. It is also used to show the input numbers from the input device through an LCD screen. To complete the system, two relays are used, one of them to drive the motor in such direction with which the door can be opened, this operates when the correct password is entered, whereas the second relay is used to block the direction of D.C motor drive or to rotate the drive in opposite direction to keep the door in a closed state, and this is often done when the incorrect password is entered. [10] similarly designed a password-based door lock system using an 8051 microcontroller to store a user-defined password that may be found during startup/booting. The password is set using push buttons which represent numbers from 0 to 9. A 16×2 LCD is used for the interface and displays the entered password. When anyone tries to enter the password, it is compared with the initially set password. If it matches, the LCD displays "system unlocked" or else it displays "wrong password". A lock button is employed to reset the system so that the password can be locked again. You can use a relay or a solenoid valve as an actuator to any system you would like to control using a password. [11] also developed a system that demonstrates a password-based door lock system wherein once the right code or password is entered, the door is opened, and therefore the concerned person is allowed access to the secured area. Again, if another person arrives it'll ask to enter the password. If the password is wrong then the door would remain closed, thus denying access to the person. The most component within the circuit is the 8051 microcontroller. A 4×3 keypad was wont to enter the password. The password which is entered is compared with the predefined password. If the entered password is correct then the system opens the door by rotating the door motor and displays the status of the door on the LCD. If the password is wrong then the door remains closed and displays "pwd is wrong" on the LCD.

[12] designed a microcontroller-based security system employing a matrix keypad & GSM/CDMA network. The microcontroller-based digital door lock security system is an access system that permits only authorized persons to access restricted areas. The password is stored during a PROM so that it is often changed at any time. The system features a matrix keypad. When anyone enters the code within the matrix keypad, the microcontroller verifies the codes. If that code is correct the device will operate and therefore the door is going to be opened. [13] designed a digital door locking system that is implemented and governed by an RFID reader which authenticates and validates the user and then opens the door automatically. It also keeps the record of check-in and check-out of the user. The system enables a user to check in and checks out under fast, secure, and convenient conditions. A new user would first be registered with the system and therefore the corresponding information is burnt into an RFID tag. This RFID tag is going to be accessible through the system. When a registered user involves the entry point and put the tag into the reader, the system checks whether it's a registered user or an imposter. If the user is registered, the tab information is matched with the user information stored in the system. The door only opens after the user has been successfully authenticated and closes automatically after a specified interval.

[14] developed the (MCUAT89S52), a microcontroller-based Home Security system to detect the intruder using diffused in-line Infrared (IR) and Shock sensors as well as the lock system itself which is used to automatically lock the intruder if he/she tries to get into the room. A GSM module is also used to send text messages to the house owner about the intruder in the room. [15] proposed a micro-controller-based automated Home Security System which is password-protected, and therefore the door lock uses an LED-based resistive screen input panel that operates by detecting the difference in candlepower captured by the photodiode which is emitted by surrounding red LEDs and reflected by the finger. IR Laser sensors are wont to detect any obstacle. [16] presented an Android-based control system to maintain the security of the home's main entrance and also the car door lock. The system also can control the general appliances in a room. The mobile to security system or home automation system interface is established through Bluetooth. The hardware part is meant with the PIC microcontroller. [17]

presented a neighborhood of a sensible home technology using the Bluetooth of a mobile device. A system named door locks automation system using Bluetooth-based Android Smartphone was proposed and prototyped. The hardware design for the door-lock system is the combination of an android smartphone because the taskmaster, Bluetooth module as command agent, Arduino microcontroller as controller center/data processing center, and solenoid as door lock output. [18] presented and analyzed the planning and implementation of a microcontroller-based home security system using GSM technology. Two microcontrollers with other peripheral devices which include an LED, LCD, Buzzer, and a GSM Module are responsible for the reliable operation of the proposed security system.

[6] developed two remote monitoring systems using a telephone with attention to wider utilization. The first system is designed with ARM LPC 2148 microcontroller based on commands received from the user's cell phone and presents sensor conditions to the LPC 2148 microcontroller system which sends signals through its ports to switch on/off appliances like lights, fans, T.V., etc. The second system incorporates additional features like capturing and storage of an intruder's images unknown to the intruder. [6] worked on a project on an automatic password-based door lock system by utilizing electronic technology to create an integrated and fully customized home security system at a reasonable cost. The project is beneficial to keep thieves and other kinds of dangers cornered. [19] designed a passwordprotected home automation system with an automatic door lock using the Arduino Uno board which is controlled by the ATmega-328. First, the user combination is getting to be compared with a pre-decided password stored within the system memory. If the user's combination matches the password, the door, light, and fan are going to be unlocked. The system was also inbuilt so that it'd be locked by just pressing one key. During this system, an Arduino UNO microcontroller board is employed for interfacing the varied hardware peripherals. If the password is matched with a pre-decided password then the Arduino simply operates the relay to open the lights and fan. The Arduino simultaneously operates a DC motor through a motor driver for operating the door.

[20] invented an electronic combination door lock with deadbolt sensing means. The electronic

combination door lock uses a push keyboard together with a door given a deadbolt manually operable by an outer turning knob. The electronic circuitry for the keyboard compares an input code with a stored code and generates an enabling signal as long as the input code is the same because of the stored code. The outer turning knob is restrained from being manually moved to retract the deadbolt when the door is in its locked condition. This restraining of the outer knob is removed by the enabling signal which needs little or no energy so that the deadbolt can then be manually retracted. [21] invented an electronically activated door lock assembly that incorporates an electronic card reader whereby when the clutch assembly is within the activated position, rotational movement of the surface handle is transmitted by way of a spindle through the mortise and the clutch assembly to a clutch disk disposed between the mortise and clutch assemblies and therefore the inside housing. The clutch disk is disposed of inside the door. Rotational movement of the clutch disk is then imparted back towards the door through a driver disk and hub drive to the mortise latch hub which is disposed of within the mortise housing disposed inside the door structure. As a result, the clutch disk and clutch assembly are often disposed of within the housing and therefore the inside door surface and the electronic components of the cardboard reader and clutch assembly are often conveniently housed within the inside housing assembly. An additional spacer hub is disposed of between the surface housing and therefore the mortise latch hub which makes it difficult to tamper with the mortise latch hub from the surface of the door.

[22] The electromagnetic door lock device was invented by the electromagnet, the brake to push electromagnet within the door frame, the electromagnetic driver to connect to the source of influence, the electromagnetic armor with a magnetic interest, the connector to push armor at the end of the door, the frame for the adjustable movement towards the electromagnet, and the lock component of the device. The lock component is composed of one or more rows around the electromagnetic and/or armor pair, and the armor can be connected to the electromagnetic armor network with a magnetic interest at the end of the door, and it is possible to be connected to the electromagnetic armor when it is connected to the electromagnetic armor and/or armor pair. Unlocking is affected by de-energizing the electromagnet and allowing the

armature to retract by gravity or spring action so that the lock component also moves out of the described engagement. The device is simple, durable, and effective.

The current research focuses on the design and implementation of a security access system that includes a Microcontroller as a control unit, a GSM/GPRS modem that can send a call signal (to the owner) when signaled by the controller, a relay to close and open the system, and an LCD that shows the results of the controller processing.

3. METHODOLOGY

3.1 System Design

The RFID-based access control with electromagnetic lock and intruder alert consists of three main parts – the INPUT, CONTROL, and OUTPUT. Materials explored for the input are essentially authentication necessary for granting access into the secured apartment. The components of the control system handle the overall organization of all the hardware components. Microcontrollers which serve as the brain of the system could be said to be one of the most vital electronic components in a security system. The output likewise consists of components like the lock, the GSM Module, the buzzer, the LCD, and the LED. They are necessary for the execution of the results of input and control systems. The block diagram is shown in Fig. 2.

3.2 System Flow Chart

The flowchart in Fig. 1 depicts the system design for this project. It depicts a diagrammatical stepwise method that demonstrates the operation of a programmed Rfid-based access control system with an electromagnetic door lock and an intruder alarm. The cycle will begin by scanning the user's RFID tag to see if it has been registered in the microcontroller database. If the user tag details are located on the microcontroller database, the door will open.

If the RFID tag does not match the record on the system database, this research effort finds novelty in the use of GSM technology to notify the building owner to warn him or her of the intrusion.

3.3 The Input System - RFID

RFID tags are utilized in these types of security systems for digital door locks (passive). This ensures that only legitimate people with access to the data can gain access. Such systems work on a real-time basis to open the door, requiring the user to place the tag in contact with an RFID reader, after which the entrance is opened, and the registration data is recorded in the central server with the necessary data of the users. The RFID-based access control system identifies and allows only those who are permitted. During secured door entry, this method is designed to reduce trained or specialized human mistakes. The Arduino platform is used in the latest RFIDbased door lock security system. Whenever the card is positioned close to the RFID module, it examines the card data and displays "authorized entry" if the data matches that stored in the program memory; otherwise, it displays "unauthorized entrance."

3.4 The Control System

The control system consists of all the components responsible for the computational functions of the entire system. It is organized in such a way that it accepts the input from the input (authentication) system, processes it, and produces the output. The hardware and software components of the control system are separate. The microcontroller and the boards on which it is soldered make up the hardware, while the source code responsible for the microcontroller's operation makes up the software. One of the most vital components of the control system which could be inferred from above is the microcontroller. A microcontroller is a device that incorporates or is built upon a microprocessor. The microprocessor itself is made up of billions of miniaturized transistors which are fabricated onto a single chip.

3.4.1 ATmega-328

The ATMEL company's ATMEGA range of ICs includes the ATmega-328 microcontroller. It has an electrically erasable programmable read-only memory of 1KB (Kilobyte) (EEPROM). The EEPROM is capable of retaining data even when the microcontroller's power source is turned off, making it ideal for data storage. The ATmega328 also features 2KB of static random access memory (SRAM).
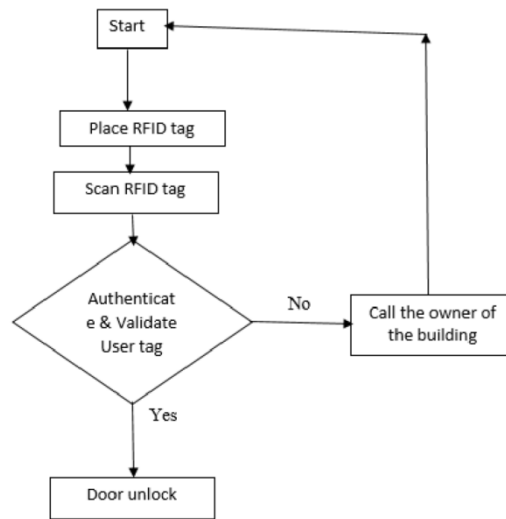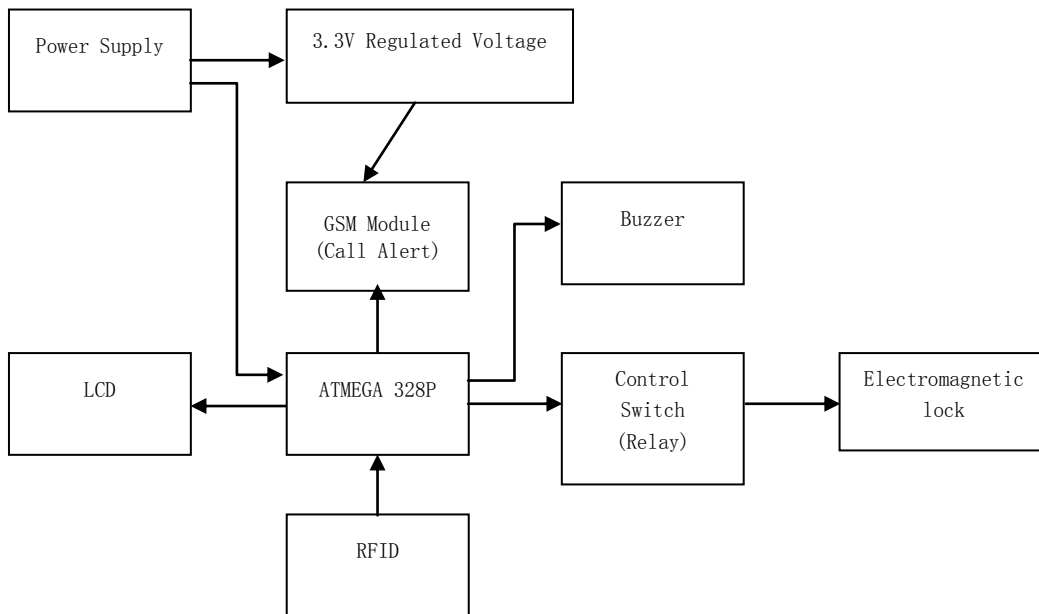
Fig. 1. System flowchart

Fig. 2. Block diagram

The description of the pins on the ATmega-328 is given below:

3.4.1.1 VCC

Digital supply voltage.

3.4.1.2 GND

Ground. It has a voltage of 0v.

3.4.1.3 Port B

Port B has internal pull-up resistors and is an 8bit bi-directional I/O port (selected for each bit). The output buffers on Port B offer symmetrical drive characteristics and high sink and source capabilities. If the pull-up resistors are engaged, Port B pins that are externally pulled low will source current as inputs. Even if the clock is not running, the Port B pins are tri-stated when a reset condition is current. PB6 can be utilized as an input to the inverted Oscillator amplifier and as an input to the internal clock operating circuit, depending on the clock selection fuse settings.

3.4.1.4 Port C

Port C has internal pull-up resistors and is a 7-bit bi-directional I/O port (selected for each bit and

labeled from 0 to 7). Its output buffers have symmetrical drive characteristics and may sink and source a lot of data. If the pull-up resistors are engaged, Port C pins that are externally pulled low will source current as inputs. Even if the clock is not running, the Port C pins are tristated when a reset condition is active.

3.4.1.5 PC6/RESET

PC6 is used as an I/O pin if the RSTDISBL (Reset/Disable) Fuse is preset. PC6 has different electrical properties than the other Port C pins. PC6 is utilized as a Reset input If the RSTDISBL Fuse is not configured. Even if the clock is not running, a low level on this pin for longer than the minimum pulse length will cause a Reset.

Shorter pulses do not always result in a Reset.

3.4.1.6 Port D

Port D is an 8-bit bi-directional I/O port with pullup resistors built-in (selected for each bit). The output buffers for Port D have symmetrical drive characteristics and strong sink and source capabilities. If the pull-up resistors are engaged, Port D pins that are externally pulled low will source current as inputs. Even if the clock is not running, the Port D pins are tri-stated when a reset condition is active.

3.4.1.7 AVCC

AVCC is the analog to digital converter's supply voltage pin.

3.4.1.8 AREF

The A/D Converter's analog reference pin is AREF.

Fig. 3 shows the pinout diagram of ATMega 328.

3.5 Output

Output devices make up the majority of the output system. In most cases, they are the output of the input and control systems. The Electromagnetic lock, LCD, buzzer, and GSM Module are examples of output components that will be discussed further down.

3.5.1 Electromagnetic lock

A magnetic lock, commonly known as a maglock, is a locking device made up of an electromagnet and an armature plate. Electric locking devices are divided into two categories.

Locking devices can be "fail-safe" or "fail secure," depending on their design. When power is gone, a fail-secure locking device stays locked. When de-energized, fail-safe locking devices unlock. Direct-pull electromagnetic locks are designed to be fail-safe from the start. The lock's electromagnet is usually mounted to the door frame, with a matching armature plate attached to the door. When the door is closed, the two components come into touch. Current traveling through the electromagnet provides a magnetic flux that attracts the armature plate to the electromagnet when it is powered.

3.5.2 Liquid Crystal Display (LCD)

The LCD shows everything that happens in the system, starting with a welcome message when the system is turned on and ending with a "Place Your Tag/Card" message. After the system determines if the tag is valid or not, the system displays permitted or unauthorized access.

The 16x2 LCD Module display, which can show 32 ASCII characters on two lines, is the most commonly used LCD module on the market (16 characters in 1 line). The 16x2 LCD Module has 16 pins and can be used in 4-bit or 8-bit mode (using only four data lines) (using all 8 data lines). The LCD module is set to the 4-bit mode in this case. The pinout of a 16x2 LCD Module diagram is shown in Fig. 4.

Below are the names and functions of each pinout on the 16x2 Liquid Crystal Display (LCD) module.

3.5.2.1 Pin1 (Vss)

The LCD module's ground pin.

3.5.2.2 Pin2 (Vcc)

This pin receives a 5V supply to power the LCD module.

3.5.2.3 Pin3 (VEE)

Pin for adjusting the contrast. The slider pin is connected to the VEE pin after attaching the ends of a 10K potentiometer to +5V and ground. The contrast is determined by the voltage at the VEE pin. Normally, the voltage is fixed between 0.4 and 0.9V.
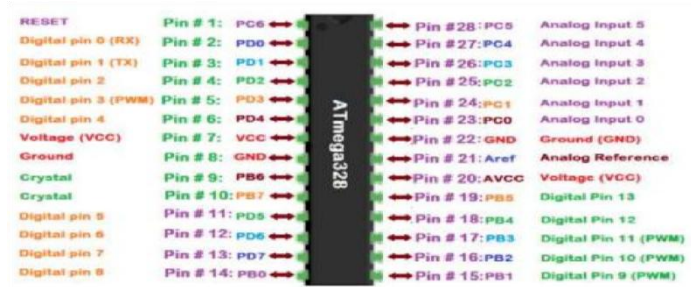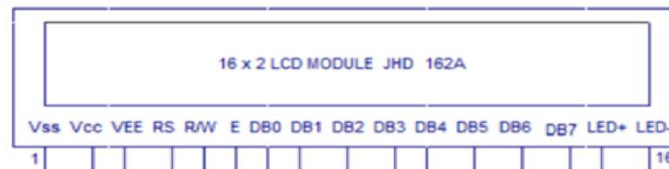
Fig. 3. Pinout diagram of ATMega-328

Fig. 4. Schematic of 16×2 Liquid Crystal Display (LCD) Module

3.5.2.4 Pin4 (RS)

Select a pin and register it. The command register and the data register are the two registers on the 16x2 LCD Module. The data register is selected by logic HIGH on the RS pin, whereas the command register is selected by logic LOW on the RS pin. If we set the RS pin to HIGH and feed data to the data lines (DB0 through DB7), the input will be regarded as data for an LCD display. If we set the RS pin to LOW and feed data to the data lines, this will be interpreted as a command (a command to be written to the LCD controller, such as cursor positioning, screen clearing, or scrolling).

3.5.2.5 Pin5(R/W)

Read/write modes are available. This pin allows you to switch between reading and writing modes. This pin's logic HIGH initiates read mode, whereas logic LOW activates write mode.

3.5.2.6 Pin6 (E)

This pin is used to turn on the LCD module. The module is turned on by a HIGH to LOW signal on this pin.

3.5.2.7 Pin7 (DB0) to Pin14 (DB7)

This is a set of data pins. These pins carry the commands and data to the LCD module.

3.5.2.8 Pin15 (LED+)

The anode of the backlight LED. When operating at 5V, the 560ohm resistor is generally connected in series with this pin. In other Arduino-based applications, the backlight LED on the Arduino board can be powered from the 3.3V supply.

3.5.2.9 Pin16 (LED-)

The LED backlight's cathode. TFT (Thin Film Transistor) LCD screens, 8x8 dot matrix displays, and 4-bit digital tube displays are examples of other types of displays.

3.5.3 The buzzer

The buzzer is always activated in conjunction with an "Access Denied" message on the LCD when the tag does not match the programmed tags. Fig. 5. shows a buzzer.
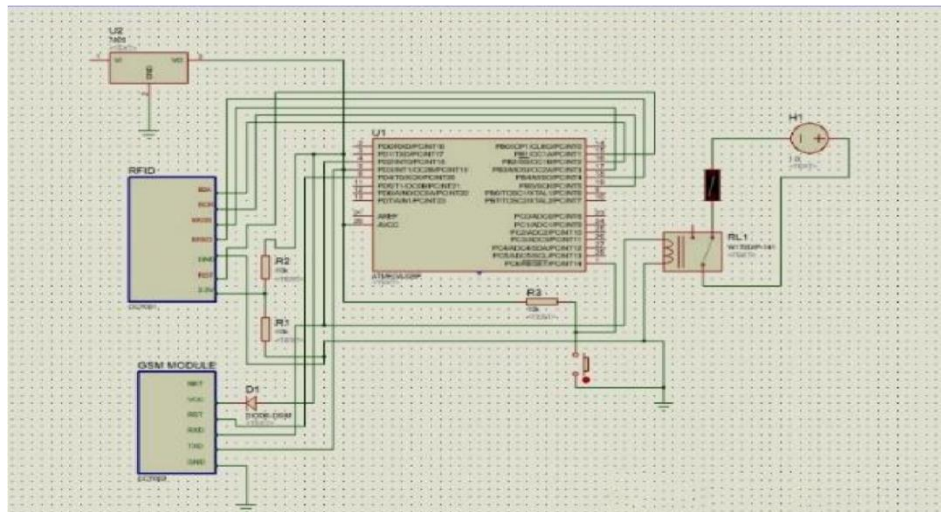

Fig. 5. Buzzer

Fig. 6. The Circuit diagram of An RFID-based access control system using an electromagnetic door lock and an intruder alert system

The audio signal is amplified by connecting the buzzer to an NPN transistor (BC547). The BC547 transistor's base is then linked to a 220k ohms resistor, which is also connected to the microcontroller through the analog input/port.

3.5.4 GSM module

GSM is primarily used for communication in various door lock security systems. The objective of work is nurtured through the use of circuits such as the GSM module, which is activated by a controller for sending SMS or CALLS to administrators in an emergency and for sending corresponding security services during a breakin. The system requires a variety of sensors to detect impediments. It receives data from the sensors before making a decision. A call signal is sent to the appropriate number using the GSM module.

3.6 Working Principle

All of the relevant information about the user is stored in the system. A new user is first added to the system, and the information is stored on a burn-in RFID tag. When a registered user approaches the entry point where the RFID reader is operated, the tag (transponder) is brought within the RFID reader's reading range, and the RFID reader uses its antenna (scanning antenna) to scan the data on the tag and compare it to the data on the microcontroller. When the data in the microcontroller matches the data in the door, the door opens to allow the user to enter after successful authentication and

closes automatically at a specified time interval or manually by the user - the electromagnetic lock assists in locking the door.

When a tag with valid or invalid information is brought close to the reader, the microcontroller displays messages on the LCD, and the buzzer activates. If the RFID tag does not match the record on the system database, this research effort finds it novelty in the use of GSM technology to notify the building owner to warn him or her of the intrusion. To open the electromagnetic lock, a relay with its driver closes and opens sub-circuits functioning at different voltages. A crystal (12MHz) is also required to provide the microcontroller with the required clocked pulses.

4. RESULTS AND DISCUSSION

Users must have a registered RFID tag that carries the personal information of that individual user. The created RFID-based access control system using electromagnetic door locks and an intruder alarm system proved to be effective because it was implemented using indigenous material. A relay controls the operation of a door and an electromagnetic lock. The Relay functions as a switch and an actuator, allowing the door to open and close in real-time. The RFID reader recognizes the tag in real-time and opens and closes the door automatically after a certain period. In this application, the database is searched first for user authentication information. The door will not be opened if the user does not have any previous records in the database, preventing unauthorized entries.

Fig. 7. Serial monitor to show test result on Arduino IDE

Fig. 8. Packaged prototype

The system was tested with both valid and invalid cards; when the card is valid, the LCD displays "ACCESS GRANTED," and the electromagnetic door lock is opened.

When the card is invalid, however, the LCD displays "DECLINED," the door lock remains locked, and the GSM Module calls the administrator. The serial monitor in Fig. 7. displays the signal received by the RFID reader as well as the results.

5. CONCLUSION

In this project, we used passive RFID to construct a digital security system that included a door lock mechanism. For controlling and carrying out operations, a centralized system is being used. The door locking system works in real-time because when the user places the tag in contact with the reader, the door opens and the check-in information, together with the user's basic information, is recorded in the central server. We use RFID technology to enable secure entry to a place, as well as a GSM Module for intrusion detection.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Edozie E, Vilaka K. Design and implementation of a smart sensor and RFID door. International Journal of Engineering and Information Systems (IJEAIS); 2020.
2. Patil M, Reddy. Design and implementation of home/office automation. International Journal of Computer. Applications (0975 – 8887); 2013.
3. Harri N. The study of business opportunities and value add of NFC application in security access control solution. Master thesis, Department of Business administration, Kemi-Tornio. 2011;17-19.

4. Fang Z, Dagu H, Zheng D, Viping H. Design and Implementation of an automatic Clearance Control System based on RFID. IEEE 7th world congress intelligent control and automation (WCICA). 2008;6621 -6626.

5. Arpita M, Siddharth S, Sachin D, Dubey SK. Password-based security lock system. International Journal of Advanced Technology in Engineering and Science. 2014;2(05):100-103.

6. Vijay P. Jadhao. ARM-based smart home automation. International Journal of Science and Engineering. 2013;1(2):53-56.

7. Meng XL, et al. RFID-based security authentication system based on a novel face recognition. Structure in proc. WASE International Conference on Information Engineering. 2010;97-100.

8. Jinaporn N, Wisadsud S, Nakonrat P, Suriya A. Security system against asset theft by using RFID technology. IEEE 5th international conference Electrical/ Electronic, Computer Telecommunication, and information (ECTICON). 2008;2:761 764.

9. John. Microcontroller – Invention History and Story Behind the Scenes. Circuit Today; 2013.
Available:http://www.circuitstoday.com

10. Raj M. 8051-based password lock system. Think Electronics; 2017.
Available:https://thinkelectronics.org

11. Chinaraja B. Password-based door lock system using 8051 microcontrollers. Slideshare; 2015.
Available:https://www.slideshare.net

12. Mohammad A. Microcontroller based reprogrammable digital door lock security system by using keypad & GSM/CDMA technology. IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE). 2013;4(6):3842.

13. Gyanendra K. Verma, Pawan Tripathi. A digital security system with door lock system using RFID technology. International Journal of Computer Applications. 2010;5(11):6-8.

14. Ajay M, Shelja D, Swati S. Design and development of sensor-based home automation and security system using GSM module and locking system. International Journal of Advanced Engineering Research and Science (IJAERS). 2014;1(4):37-39.

15. Nikhil A, G. Subramanya N. Microcontroller based home security system with remote monitoring. International Conference on Electronic Design and Signal Processing (ICEDSP). 2012;38-41.

16. Sadeque RK, Farzana SD. Android based security and home automation system. International Journal of Ambient Systems and Applications (IJASA). 2015;3(1):15-24.

17. Lia K, Alfin Noorhassan SR, Mada S, Edi M. Door-automation system using bluetooth-based android for mobile phone. ARPN Journal of Engineering and Applied Sciences. 2014;9(10): 1759-1762.

18. Raqibull H, Mohammad M. Khan, Asaduzzaman A, Israt J. Rumpa. Microcontroller based home security system with GSM technology. Open Journal of Safety Science and Technology. 2015;5: 55-62.

19. Ankit J, Anita S, Ritu R. Password protected home automation system with automatic door lock. MIT International Journal of Electrical and Instrumentation Engineering. 2016;6(1):28-31.

20. Ricky M. Electronic combination door lock with deadbolt sensing means. Google Patents; 1977.
Available:https://patents.google.com/paten t

21. Doucet C. Electronically activated door lock assembly. Google Patents; 1999.
Available:https://patents.google.com/paten t

22. Arthur VG, Richard GG, David AG. Electromagnetic door lock device. Google Patents; 1985.
Available:https://patents.google.com/paten t