INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Door Access Control Using RFID and Voice Recognition System

Okafor C.S.[1], Nnebe S. U.[2], Alumona T.L.[3], Onuzuluike V. C.[4], Jideofor U. C.[5]

[1, 2, 3, 4, 5]Electronic and Computer Engineering, Nnamdi Azikiwe University

Abstract: Security is one of the major challenges faced by individuals, organizations, and the world at large. The evolution of technology assists in solving this menace of insecurity and with the continuous growth in technology; several techniques have been used in tackling this problem of insecurity, starting from traditional systems like the door locks with handles to automated doors. In recent times, most of these doors lock security systems are based on microcontrollers, GSM, GPS, sensors, biometrics like eye scanner, fingerprint, face recognition, password, etc., and each of these techniques has its advantages and disadvantages. The developed system involves the design of a prototype door access control system that will control the access of personnel to a location/office using voice recognition and Radio Frequency Identification (RFID) authentication techniques. The system at first detects the movement of a person and prompts the person for verification. If verified either by voice or by RFID, the door automatically opens and closes after 5 seconds. The aim of this developed system is to restrict the access of an office/location using Radio Frequency Identification and voice recognition authentication, thus offering security to the lives and properties of people.
Keywords: Biometrics, Radio Frequency Identification (RFID), LCD, Arduino, GPS, GSM.

I. INTRODUCTION

Security and its essence cannot be overemphasized, as it is an important constituent of man's everyday life. Security plays a very vital role in our lives as it ensures that lives and properties are kept safe and in the best conditions. Security systems are systems that are used to see to the safeguarding of lives and properties. These systems prevent unauthorized personnel from gaining access into a secured physical or intellectual property.

Locks, which could be either mechanical or electrical, were designed to get the needed security requirements, but they can be easily cracked by unauthorized persons thereby granting access to unwanted persons into a secured environment and this leads to either loss of property, loss of lives, financial losses or loss of data.

Access control systems are devices or mechanisms that are created to control, check, limit, or detect before granting access or entrance to an object, which most often is a human being. Access control system recognizes, authenticates, and authorizes entry of a person into a premise thereby giving complete protection and ensuring the security of the premise with the system [1]. The access control system makes it easier for authorized personnel to access a facility. It allows one to set and determine those who will have access to a particular or every area of the premises or business, without having to worry. Access control system eliminates the need for a security guard, as it prevents unauthorized persons from gaining access to the building.

Access control systems help to reduce security issues like data breaches and theft because only authorized persons who are trusted are given access. Just like the mechanical locks, Access control systems can be installed at every entrance or exit to a building, room, or environment, however, one does not need to carry different unique keys at all times in order to have access. Access control systems work with biometrics.

Biometrics is physical or behavioural human characteristics that can be used to digitally identify a person, for him/her to be granted access to systems, devices, or data.

Biometric identifiers include facial patterns, fingerprints, voice or typing cadence. Each of these identifiers is considered unique to the individual, and they may be used in combination to ensure greater accuracy of identification [2], [3]. Some others worked with technologies like barcode, magnetic stripe, radio frequency identification (RFID). For this work, we made use of the Radio Frequency Identification (RFID) and Voice Biometrics.

Radio Frequency Identification or RFID is the fastest growing scanning and identification technology in the world today. RFID is an automatic identification method that can remotely retrieve data using devices called RFID tags or transponders from the RFID readers.

RFID readers can scan and identify so many tagged items at once. RFID technology operation is similar to the bar code identification system operation but the major difference between the two is that RFID does not rely on the line-of-sight reading needed by bar code. It can be done from any angle [3]. RFID technology depends on the communication between RFID tags and RFID readers.

Voice recognition refers to the ability to acknowledge or apprehend voice. Voice or speaker recognition is the ability of a machine or program to receive and interpret dictation or to understand and carry out spoken commands [4], [5]. It refers to identifying who the speaker is and not what he is saying.

Voice recognition entails the process of speech translation in a system that has already been trained on specific person's voice so as to verify the identity of a speaker as part of a security process [6], [7], [8].

The access control system designed for this work will grant access to persons whose voices have been trained to be recognized by the system and have an authorized key card. The voice recognition picks the enrolled user's voice, especially the pitch and the word spoken by the user.

Since voice is peculiar to individuals and cannot be stolen, it is a very secure way to prevent unauthorized access into a place by trespassers. When the user is sick and is having difficulty speaking well, probably due to a cold or a dry throat, the key card containing the RFID chip can be used. The RFID chip makes access easy but the
security risk is high.

II. LITERATURE REVIEW

In [9], a biometric security system was designed to open the door automatically using the fingerprint, data storage in SD (Secure Digital), and using the C++ programming language for developing instructions for new fingerprint registration, deletion ID (identification). Data storage in the SD (Secure Digital) will assist in keeping a record of the hours of staff entry through the RTC sensor (real-time clock).

The components of the system were a biometric sensor, pushbuttons, 16x2 LCD screen, electric plate, an Arduino, relay, RTC (real-time clock), internal storage memory.

In [10], a smart card system was designed to open the door automatically. This system uses two authentication techniques, namely: a smart card and a pin assigned to that card to give access to the user. If the card inserted into the reader is validated by the microcontroller, the user sees a prompt on the LCD unit to input pin code, else "INVALID CARD" is displayed. If the pin code is not inputted 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 activated to open the door and the user will be prompted to remove the card. The door closes after a predetermined time interval. But if the pin code authentication fails, LCD will display "REMOVE YOUR CARD, INVALID PASSWORD".

The major components used were a PIC18F452 Microcontroller, ID Credential, and Reader, 16x2 LCD screen, Keypad Module, Power Supply Unit of three regulated unit 12V, 5V and 3.3V, two switching transistors, two 10A - 12VDC relays, 12V dc motor, rack, and pin system.

The authors in [11], [12] developed an IoT-based Smart Door System Model, which provides a double access authentication through fingerprint modules and is designed for hotels and guest houses. The proposed system architecture design specifies all the modules involved and the circuit diagram designed specifies various modules interconnectivity. The prototype implementation software is developed in the C programming language.

In [13], the authors presented a research work that entails the development of a door lock security system based on automatic speech recognition. The developed work was done to recognize and give access to certain users. In training the system, Mel-frequency Cepstrum Coefficients (MFCC) feature extraction technique was used to extract appropriate features from five different individuals' speech signals.

The authors in [14] presented a research work that entails part of smart home technology using Bluetooth in a mobile
device. It is also based on Android and Arduino platforms both of which are free open-source software. The developed system which is door locks automation system using Bluetooth-based Android Smartphones is proposed and prototyped. First, the hardware design and software development are described, then the design of a Bluetooth-based Smartphone application to lock/unlock the door is presented. The developed hardware design for this system includes the android smartphone, Bluetooth, Arduino microcontroller, and solenoid.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

III. METHODOLOGY

The developed door access control system comprises mainly of a power unit and control unit as shown in the block diagram of figure 1.
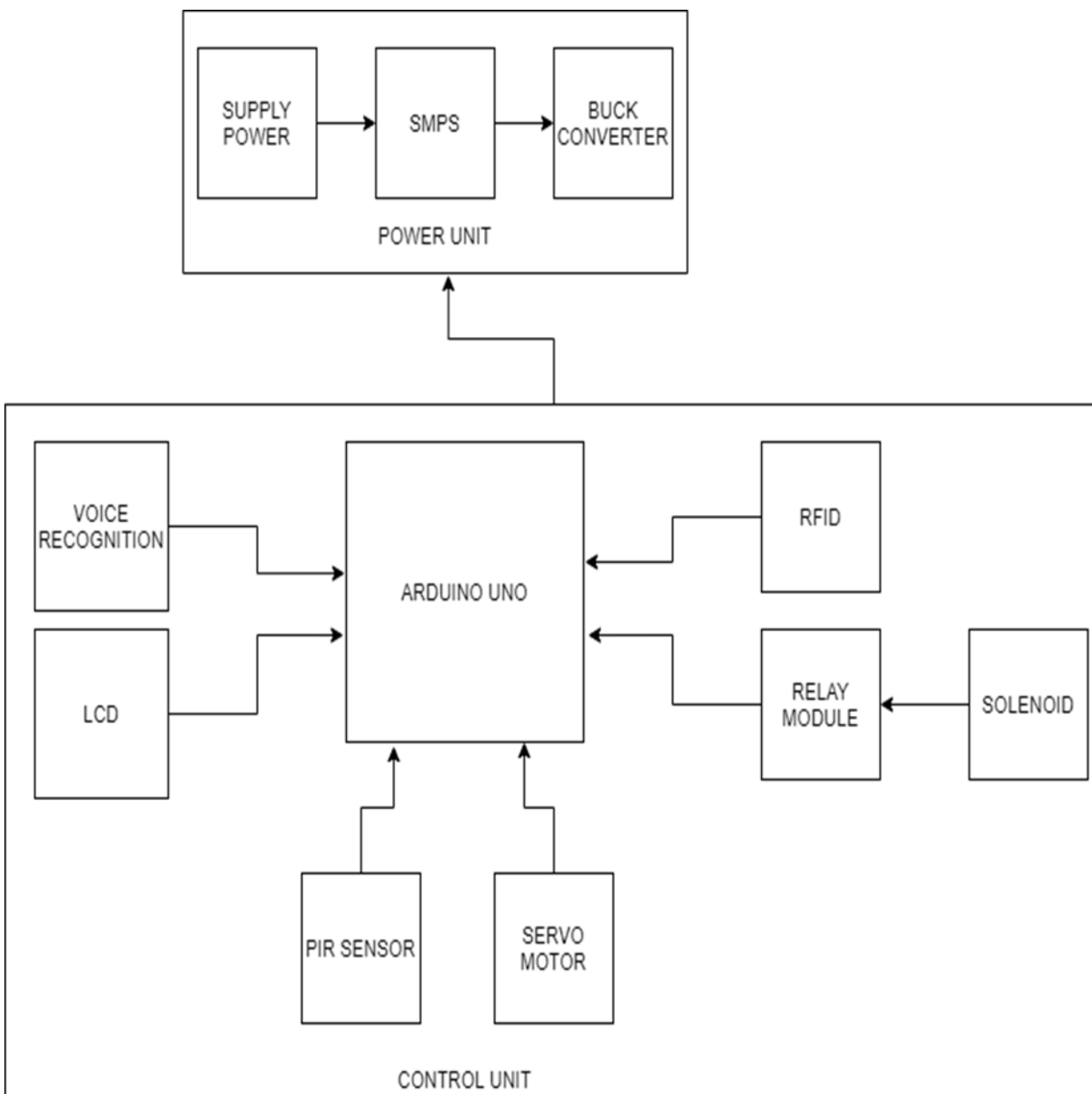

Fig. 1: Block diagram of the developed door access control using RFID and voice recognition system

A. Power Unit

For this work, the supply power is connected to a switched-mode power supply (SMPS) circuit which is designed for obtaining the regulated DC output voltage from an unregulated AC voltage. It contains a switching regulator to convert electrical power efficiently. The SMPS is of the value 12V which is too high for most components; therefore it is fed into a buck converter. A buck converter is a DC-DC power converter that steps down the voltage from its input to its output. The buck converter steps down the voltage to 5V which is enough to power the majority of the components. The system is making use of dual charging; therefore rechargeable batteries are connected in series to the SMPS to charge the device when there is no power from the main supply. The batteries are connected in series and have a reading of 12V. This will be connected to the buck converter to step down the voltage; with this, the battery can power the access control system.

B. Control Unit

The control unit is powered by the power unit and it consists of various control subsystems that are involved in the door access control.

1) *Microcontroller:* The controller used is the ATmega328p. The hardware features an open-source board designed around an 8-bit Atmel AVR microcontroller or a 32-bit Atmel ARM. The board is made up of sets of analog and digital input/output (I/O) pins that can be interconnected to other circuits. The board contains 14 digital I/O pins, 6 analog I/O pins, and is programmable with the Arduino IDE using a type-B USB cable. It has an operating voltage of 5volts as it can be powered by a USB cable or via an external battery. The greatest advantage of Arduino Uno is that its structure comes as a complete package comprising the 5V regulator, burner, oscillator, micro-controller, serial communication interface, LED, and headers for the connections. The controller is programmed in embedded C language. After the code for the access control system is written, the code is verified and uploaded into the Arduino board. Once the Arduino board is powered, the system executes the code that was uploaded. The components RFID, Voice Recognition, PIR sensor, LCD, and relay module are connected to the Arduino board and are controlled by it.

2) *Radio Frequency Identification (RFID):* Radio Frequency Identification (RFID) is one of the fastest-growing technologies in the world today. RFID is an automatic identification system that can recover remotely data using RFID tags or transponders. RFID is based on the coupling effects. Components of RFID are Reader and Tag. The function of the reader is to transmit a signal called carrier signal and to receive the response from the tag near to the reader. The reader will be mounted on the door frame to receive tag data from the person passing through it. The reader emits radio waves from one inch to feet based on the power output. The reader detects the tag as it comes in contact with the electromagnetic zone, with the activation signal sent and data passed to the control room through the server. The reader is powered by 3.3V and the power source for the RFID reader is from the Arduino. The pin connection of the RFID reader to the Arduino is shown in Table 1 below.

Table 1: Pin Wiring of the RFID Reader

PIN	Wiring to Arduino Uno
SDA	DIGITAL 10
SCK	DIGITAL 13
MOSI	DIGITAL 11
MISO	DIGITAL 12
IRQ	UNCONNECTED
GND	GND
RST	DIGITAL 9
3.3V	3.3V

3) *Voice Recognition:* Voice Recognition system is a method of analyzing someone's voice with the help of its features. It then compares it with the features saved in the database for pre-recorded signals. It displays an output that tells if any other audio of the same person is present in the database or not. If yes, it displays the name or the file number. The voices that were trained were tested and the result showed that the system will verify your voice according to the word said by the user and the pitch used. The voice recognition module has a power of 5V; therefore it made use of the central power source and common ground. The pins Tx and Rx in the voice recognition module were connected to digital 2 and digital 3 pins on the Arduino respectively.

4) *Display Unit:* A 16 x 2 Liquid Crystal Display (LCD) was used in this work. It displays in 2 lines each containing 16 characters. The LCD display has a total of 16 pins for interface with processor but a 12c device was interfaced to reduce the number of pins to 4. The SCL pin was connected to port A5 on the Arduino, while SDA was connected to port A4 on the Arduino. The LCD in this system will be used to display characters like "SWIPE", "ACCESS GRANTED", "SPEAK", "ACCESS NOT GRANTED" and "WELCOME USER" to the user. This Guides the user on steps to take in other to gain access.

5) *Motion Sensor:* The device used to detect the presence of a human being is the passive infrared sensor (PIR). The PIR sensor uses a pair of pyroelectric sensors to detect heat energy in the surrounding environment. The passive infrared sensor has two slots on it, whereby each of them is made of special material that is sensitive to infrared. When the sensor is idle, both slots detect the same amount of energy (IR), the ambient amount radiated from the room or walls or outdoors. When a warm body like a human being or animal passes by, it first intercepts one-half of the PIR sensor, which causes a positive differential change between the two halves. The reverse happens when the warm body leaves the sensing area, thus the sensor generates a negative differential change. These change pulses are what is detected. The PIR sensor is connected to port 7 on the Arduino board and once it detects the presence of a human being, it sends a signal to the Arduino to start the access control system.

6) *Door locking Unit:* The door locking unit makes use of a solenoid lock. The solenoid lock indicates a hook for electrical locking and unlocking. It is available in unlocking and locking type of power-on mode, which can be used selectively for situations. The power-on unlocking mode activates unlocking command only when the solenoid is powered on. A door of this type is locked and not opened in case of power failure or wire disconnection, ensuring excellent safety. This method is mainly used for places where crime prevention is of optimum importance. The power-on locking mode can lock a door when the solenoid is powered on. The door unlocks when the power is disconnected. The keeping type performs two operations, locking and unlocking by applying a positive or negative pulse voltage to the solenoid, and keeping the no-power state in each position. This type of feature is energy saving because it is unnecessary to always power the solenoid on. The solenoid must be powered to 12V before it unlocks. For the solenoid to unlock it must receive verification that the voice or card is valid and the user is granted access. The solenoid receives a signal from the relay. The Arduino sends signal to the solenoid through the relay to unlock or lock the door. A servo motor is connected to the door; it automatically opens the door after the solenoid is unlocked and closes the door after five (5) seconds.
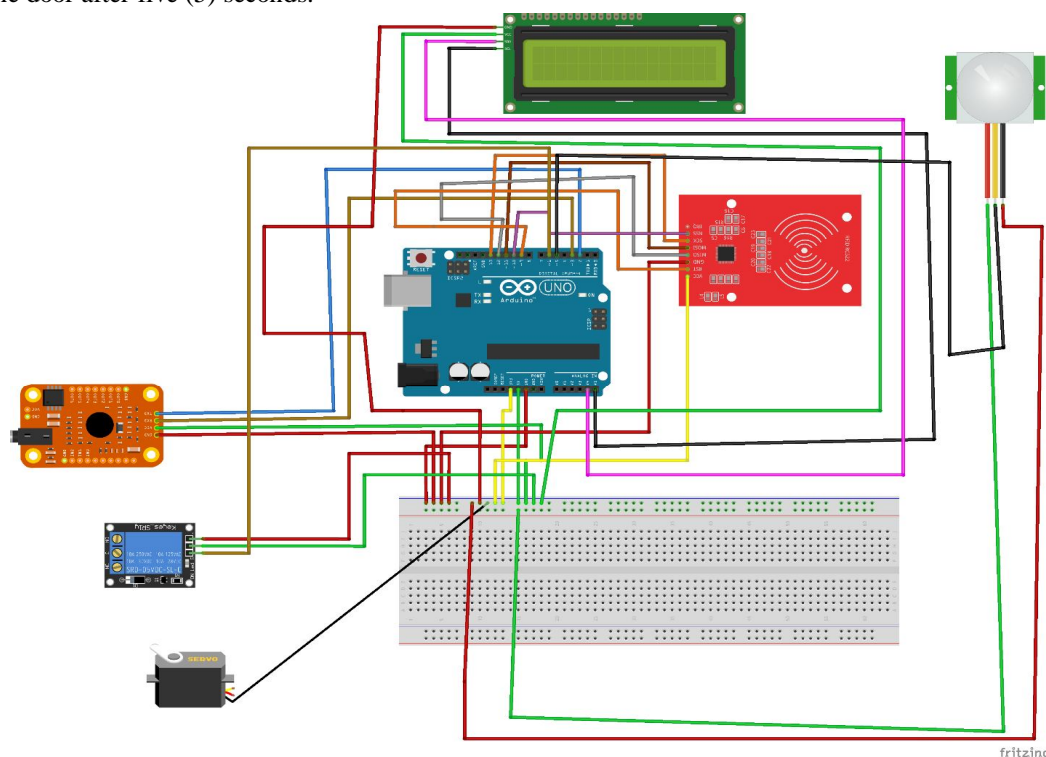

Figure 2: Circuit Diagram of the Developed Door Access Control System

IV. PRINCIPLE OF OPERATION OF THE DEVELOPED SYSTEM

At the initial stage, before the system detects any person, it displays "ACCESS CONTROL SYSTEM AUTHENTICATED BY RFID AND VOICE RECOGNITION" on the LCD. When the system detects the movement of a human being using the PIR sensor, it displays "WELCOME" using LCD and thereafter displays "SPEAK", which prompts the user to speak. The system has been implemented with passive RFID tags and a voice recognition module. The detection of the user's voice is done from the voice recognition module. The voice of the user must be recognized by the system and it will be cross-checked to know if the voice heard is in the system. If the voice heard matches any in the system, the LCD displays "ACCESS GRANTED" and thereafter displays "WELCOME, USER", as the magnetic door lock unlocks, and the user is granted access. If the user's voice is invalid, the LCD displays "SWIPES CARD" prompting the user to swipe his card. Detection of an RFID tag from a particular RFID card is being done by the reader module when the card is taken in a range of 200 millimeters. After RFID tag detection, the obtained information is passed to the central sub-system via a serial port. Matching of information initiates the event to unlock the magnetic door lock and the LCD displays "ACCESS GRANTED" and thereafter displays "WELCOME, USER". The servo motor on the door automatically pushes the door open and closes it after 5 seconds. In case of information mismatch, the LCD displays "ACCESS NOT GRANTED" and the door remains closed to prevent unauthorized access.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
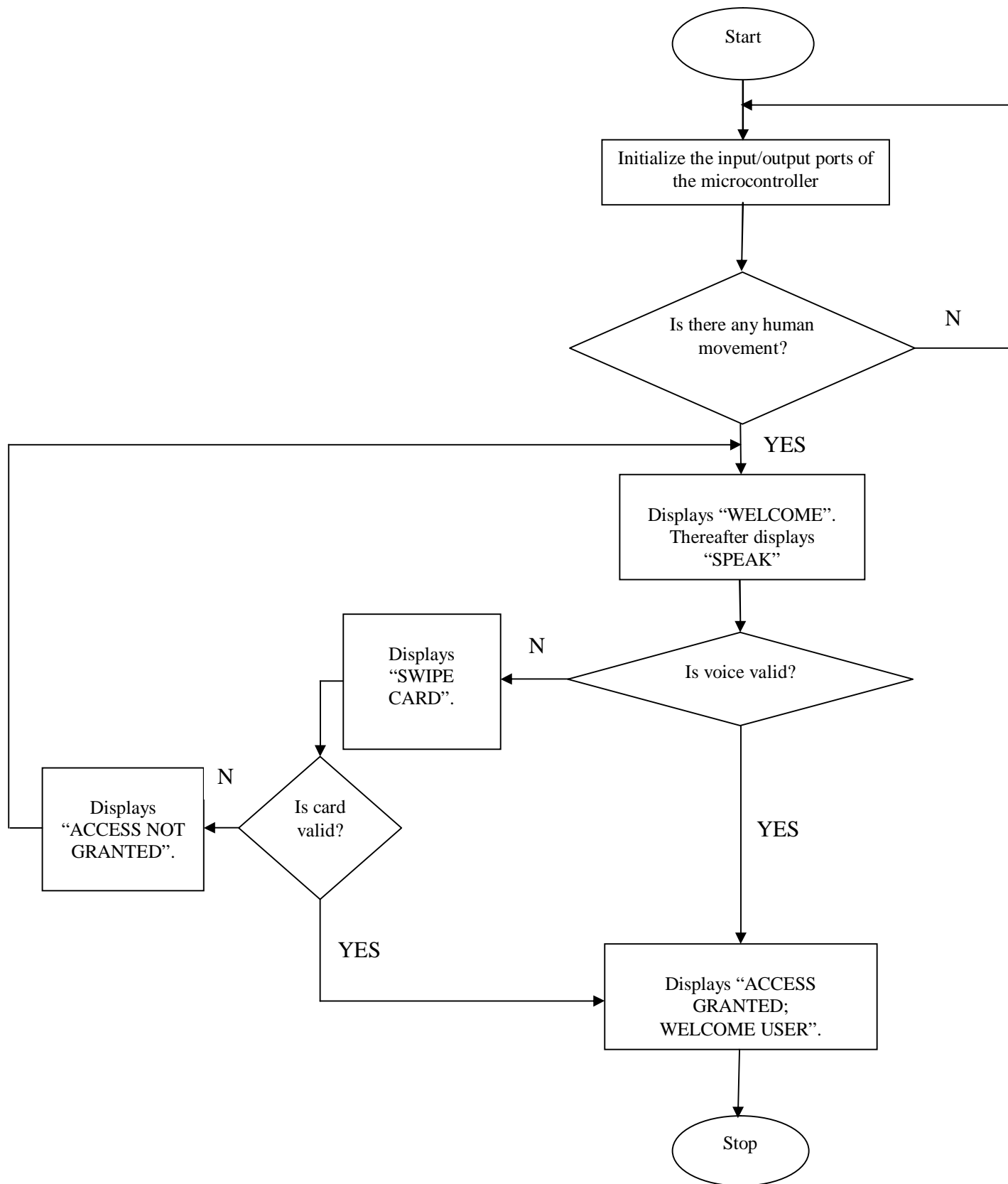*Volume 10 Issue III Mar 2022- Available at www.ijraset.com*

Figure 3: Flow Chart Showing the Operating Principle of the Developed Door Access Control System

V. CONCLUSION

The developed Door Access Control System only gives access to persons whose voice has been recorded in the system and have an authorized key card. Voice recognition is a way to recognize how your voice sounds and the word being said by you. Since your voice cannot be stolen, it is a secure way to prevent unauthorized access to an organization. If you have difficulty with your voice (probably sick), the key card containing an RFID chip can be used. The work was successful in a prototype format and the prototype door was able to unlock when the user spoke into the microphone and also when the user swiped the RFID card. With this prototype model, more improvements can be made to this work before it is deployed for use.

VI. RECOMMENDATION

This access control system can be operated in multiple places as it helps with reducing the security issues in the world today. In federal, State, and Local Governments, security is of utmost regard. Government buildings are subject to homeland security regulations, which mean restricting access. This access control system can verify employees whose voices are stored in the system or have an RFID card that limits access to departments, confidential information, and more whose voices are not stored in the system and don't have an RFID card while maintaining public access to other places. These access control systems can protect IT rooms, or even equipment racks from unauthorized persons. The current system design can be used in organizations that require a high level of security for human beings and properties. This system can be applied in banks as the security door for their vault or as the door for staff only (bank customers are not allowed here). It can be used as the security door for organizations that manage big data in their IT room and prevent access to unauthorized persons. It can be used in our home as the security system for our personal vault. In the process of designing a more robust access control system, we recommend that:

1) A 4x4 keypad matrix that can enable the user input his/her secret pin be included after the user has swiped the RFID card.
2) Inclusion of a database management system to monitor the movement of employees/users in and out of the secured door.

VII.ACKNOWLEDGMENT

We wish to acknowledge all the people that contributed to the successful completion and production of this research work.

REFERENCES

[1] Access control systems https://elprocus.com/understanding-about-types-of-access-control-systems
[2] Olayiwola A. A., Olayiwola D. S., Mosud Y. O., Ikedilo O. E., Famuyiwa K. S. A., Agboke A. J., Ugwu N. V., "Optimization Of An Identity Access Control System using Biometric Techniques", International Journal of Progressive Sciences and Technologies (IJPSAT), Vol. 27 No. 2, pp.647-653, (2021).
[3] Seng Chun H. and Haidi Ibrahim, "Biometric-Based Attendance Tracking System for Education Sectors: A Literature Survey on Hardware Requirements", Hindawi Journal of Sensors, Vol. 2 https://doi.org/10.1155/2019/7410478, (2019).
[4] UK Essays. History and Evolution of RFID Technology Information Technology Essay. (2018). Retrieved from https://www.ukessays.com/essays/information-technology/history-and-evolution-of-rfid-technology-information-technology-essay.php?vref=1
[5] What is voice recognition? https://searchcustomerexperience.techtarget.com/definition/voice-recognition-speaker-recognition
[6] Wahyudi, Winda A. and Syazilawati Mohamed, "Intelligent Voice-Based Door Access Control System Using Adaptive-Network-based Fuzzy Inference Systems (ANFIS) for Building Security", Journal of Computer Science, Vol. 3, Issue No. 5,   pp. 274-280, ISSN 1549-3636, (2007).
[7] Falohun A. S., Adedeji O. T., Adegbola O. A., Alade O. M., Makinde B. O., Isamot R. M., Ajadi M. S. "Voice Recognition System for Door Access Control using Mobile Phone", International Journal of Science and Engineering Applications, Vol. 10, Issue 09, pp. 132 - 139, ISSN:- 2319 – 7560, (2021).
[8] Adekola O. D., Akinsanya A., Olufowobi A., Babajide O., Olawale S. M., Ayorinde O, "Voice Recognition Door Access Control System" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Vol. 21, Issue 5, pp. 1-12, (2019).
[9] Lawrence O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", IEEE, Vol. 91, Issue No. 12, pp. 2021-2040, (2003).
[10] O. Adetoyi, "Development of Smart Card Door Access Control System" International Journal of Electronics Communication and Computer Engineering, Vol. 8, Issue 1, ISSN (Online): 2249–071X, (2017).
[11] C. O. Akanbi1, I. K. Ogundoyin, J. O. Akintola, and K. Ameenah, "A Prototype Model of an IoT-based Door System using Double-access Fingerprint Technique", Nigerian Journal of Technological Development, Vol. 17, No.2, (2020).
[12] J. Carmona, E. Mendoza, M. Sanchez, E. Aguila, L. A. Barrientos, G. Ceron, F. Galvez, and G. Martinez "Door Opening with Fingerprint" International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181, Vol. 8, Issue 11, (2019).
[13] Nnamdi O., Adebimpe E., Omodunbi B., Nwobodo L., Nduanya U. and OyedijI F "Development of a Door Lock Security System Based on Automatic Speech Recognition" FULafia Journal of Science & Technology, Vol. 4 No.2, (2018).
[14] L. Kamelia, A. S. R. Noorhassan, M. Sanjaya, and W. S. E. Mulyana, "Door-automation system using bluetooth-based android for mobile phone", Asian Research Publishing Network (ARPN) Journal of Engineering and Applied Sciences, Vol. 9 (10), (2014).

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)