CONTROL AND ALERT MECHANISM OF RFID DOOR ACCESS CONTROL SYSTEM USING IOT

Haider Rasheed Abdulshaheed
Computer Engineering Techniques Department, Baghdad College of Economic Sciences University, Baghdad, (Iraq).
E-mail: haider252004@yahoo.com
ORCID: https://orcid.org/0000-0003-3963-875X

Haider Hadi Abbas
Computer Technology Engineering Department, Al-Mansour University College (MUC), (Iraq).
E-mail: haider.hadi@muc.edu.iq
ORCID: https://ORCID.org/0000-0002-0724-7829

Israa Al Barazanchi
Computer Engineering Techniques Department, Baghdad College of Economic Sciences University, Baghdad, (Iraq).
College of Computing and Informatics, Universiti Tenaga Nasional (UNITEN), (Malaysia).
E-mail: israa44444@gmail.com
ORCID: https://orcid.org/0000-0002-6798-6295

Wahidah Hashim
College of Computing and Informatics, Universiti Tenaga Nasional (UNITEN), (Malaysia).
E-mail: wahidah@uniten.edu.my
ORCID: https://orcid.org/0000-0002-7661-5146

Recepción: 23/09/2021 **Aceptación:** 25/11/2021 **Publicación:** 14/02/2022

Citación sugerida:
Abdulshaheed, H. R., Abbas, H. H., Al Barazanchi, I., y Hashim, W. (2022). Control and alert mechanism of RFID door access control system using IoT. *3C Tecnología. Glosas de innovación aplicadas a la pyme, Edición Especial,* (febrero 2022), 269-285. https://doi.org/10.17993/3ctecno.2022.specialissue9.269-285

ABSTRACT

The RFID Door Access Control System has been providing security and reliability to many secure medical and scientific facilities, official grounds, and locker rooms with confidential files with access key provided for a limited number of people. This system is an advanced hybridized one incorporating multiple access methods with enhanced security, making it easier for members to access the door and impossible for those without the access keys. The system uses three access methods to open the door. 1. A basic RFID Key tag and RFID EM reader, for permanent members. 2. A temporary password that can be input using a keypad, for temporary workers. 3. Remote Door access by administrator using IOT technology, for guests and visitors for a onetime visit. The system uses NIST to track time and data log all the details on the web server, data gets registered whenever the door is used. The date and time at which the door is accessed and the name of the person accessing the door gets registered every single time the door is used. If the system identifies a false access method or an intrusion, the base gets alerted through WI-FI and the door will be permanently locked unless the secure system is reset using a special administrator password. The door lock is activated by means of high torque servo motors with vibration sensors. In case if someone tries to damage the locking system, it will be identified by the system using the vibration sensor and the system alerts the base and gets locked.

KEYWORDS

Automation, Security, RFID, Face detection, Smart door lock

https://doi.org/10.17993/3ctecno.2022.specialissue9.269-285

1. INTRODUCTION

The RFID Door access Control System is more secure, reliable, adaptive, and flexible, the proposed method is flexible such that it can be used at homes, offices, schools, for medical and scientific organizations containing specimens or scientific equipment that needs protection, and for people who hold confidential files or any object that needs to be protected from public view or usage (Priyanka *et al.*, 2019). The system uses a primary microcontroller to control all the operations of the system such that the control loop is strongly designed to remove any possible errors that can occur. The preferred servo motor for the locking mechanism is MG995 Servo motor because this servo motor at its peak voltage can exert a torque of 11kg/cm making the lock immovable by human hands. The door material is decided based on the usage location, if it's an office environment the door can be made of tempered glass material, in case of a scientific military facility it can be made of titanium. Regardless of the door material, the control system can be easily installed making it superbly flexible (Sweta, 2021). The Face Detection technique is employed in extremely confidential cases. The IOT technology implements usage of WIFI modules/routers or Ethernet cables which can be remotely accessed by the administrator through the internet. The internet access for the system is made possible through a unique webpage or a personalized mobile application (Nehete *et al.*, 2016; Pavelic *et al.*, 2018).

2. METHODOLOGY

The System works on three types of access methods and two types of alert method. The whole process happens with microseconds to ensure security at its best. The first access method is members of the organization who have been authorized and are provided a key card, which is mostly an ID card with a chip inserted within the ID card. On placing the ID card on parallel with the RFID EM reader, the chip is identified by the RFID reader. The name of the person accessing is collected from the database and the access date and time is obtained from NIST, and the access is granted, and the data gets logged in the Webpage server. The second method focuses on a temporary password for temporary workers or contract freelancers. The workers can type this password unto the keypad; the system crosschecks the password and will grant access if the password is a match. The date and time are obtained from NIST and the data is logged onto the web server. The third

https://doi.org/10.17993/3ctecno.2022.specialissue9.269-285

method is for guests and visitors who visit the secure facility under supervision, the door is activated through WI-FI from the reception or by any authorized person.

- NIST

The NIST stands for National Institute of Standards and Technology is a web server that can be accessed by the microcontroller through the WI-FI module to obtain the official US standard time. With this time, selected hours and minutes are added or subtracted to data log date and time depending on the user's time zone. There are many such web servers that provide date and time, but the NIST server is the simplest to use.

2.1. RFID DOOR CONTROL

2.1.1. HARDWARE REQUIREMENTS

The hardware requirements consist of a microcontroller, sensor modules to input password and key card, servo motor to physically maneuver the door lock mechanism and WIFI module to remotely control the door and the alert mechanism (Nwogu *et al.*, 2020).

- Sensors

RFID EM Reader Module

The RFID EM reader module is a RFID EM-18 Reader module with serial TTL communication. The Module consists of an electromagnetic reader, when the key tag or the ID card containing the RF chip is placed parallel to the electromagnetic reader (Al-Sudani *et al.*, 2018); the reader reads the data in the chip and sends it to the module. The module after processing the data identifies the secure number embedded in the chip and provides it to the micro controller, where the microcontroller crosschecks the data from its database with the received data to know if it's an authorized member or an intruder (Khabarlak & Koriashkina, 2020).

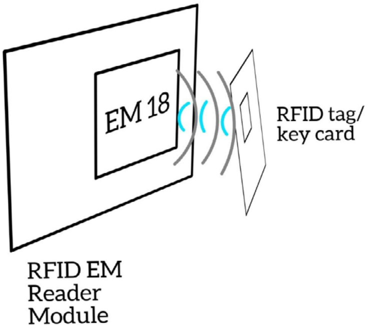

Figure 1. RFID EM Reader Module Working.
Source: own elaboration.

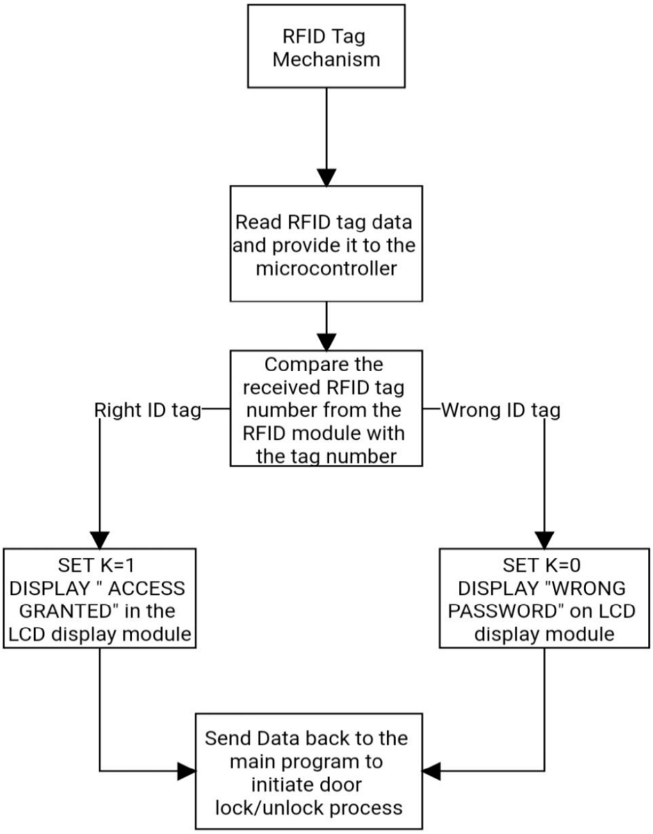
RFID Tag Mechanism
Read RFID tag data and provide it to the microcontroller
Compare the received RFID tag number from the RFID module with the tag number
Right ID tag
Wrong ID tag
SET K=1 DISPLAY " ACCESS GRANTED" in the LCD display module
SET K=0 DISPLAY "WRONG PASSWORD" on LCD display module
Send Data back to the main program to initiate door lock/unlock process

Figure 2. RFID Tag Mechanism Flowchart.
Source: own elaboration.

https://doi.org/10.17993/3ctecno.2022.specialissue9.269-285

Keypad Module

The Keypad Module is a button sensor device, so when a button is pressed the micro controller can recognize it. The keypad used here is a 3X4 Keypad Module, meaning that it has 3 columns and 4 rows. Once the password is entered; the micro controller will crosscheck the password with the administrator provided temporary password which is regularly obtained through the web server by the administrator. If the password is wrong, the LCD display module will display the message" Wrong Password", if the password is right the lock mechanism is opened. In case of multiple wrong entries, the door is locked until the door access control system is reset by the administrator's special password.

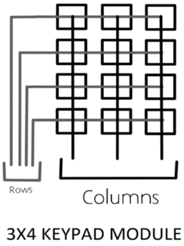

Figure 3. Keypad Module 3X4.
Source: own elaboration.

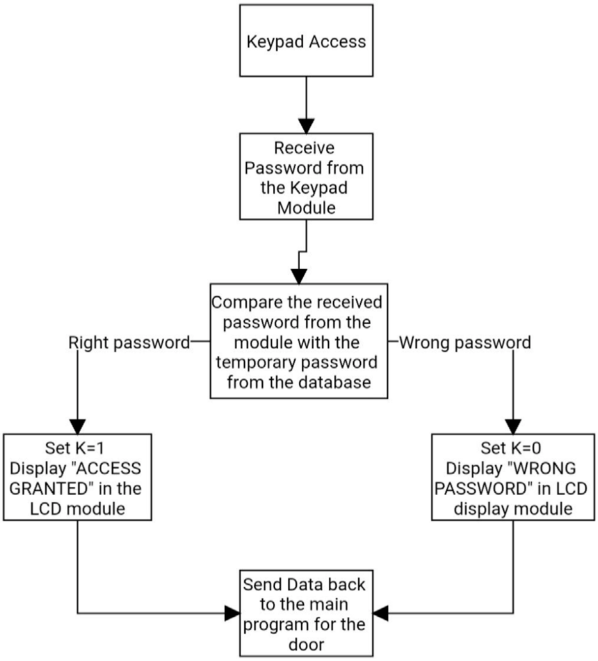
Keypad Access
Receive Password from the Keypad Module
Compare the received password from the module with the temporary password from the database
Right password
Wrong password
Set K=1 Display "ACCESS GRANTED" in the LCD module
Set K=0 Display "WRONG PASSWORD" in LCD display module
Send Data back to the main program for the door

Figure 4. Keypad Mechanism Flowchart.
Source: own elaboration.

https://doi.org/10.17993/3ctecno.2022.specialissue9.269-285

Vibration Sensors

The vibration sensor is a very sensitive device that is used to measure over a range of vibration and provide the analog values to the microcontroller; an analog value is set as a threshold above which if any vibration is sensed by the vibration sensor, the microcontroller perceives it as an intrusion and activates the alert mechanism (Sweta 2021). The vibration sensor is necessary device for homes, such that when a burglar tries to break the lock the alert mechanism is activated.

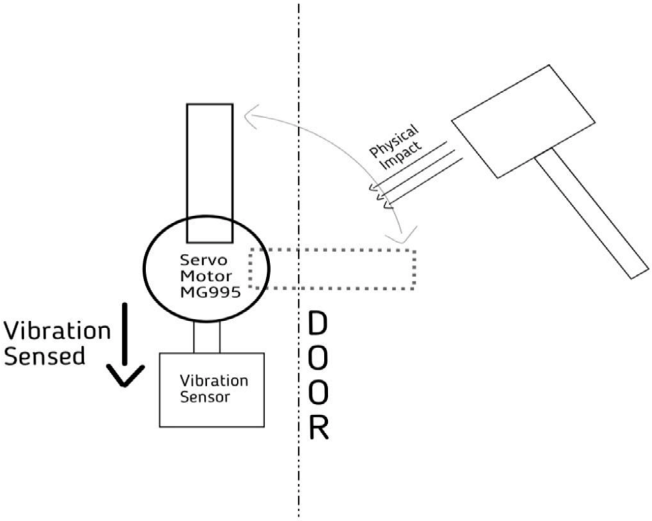

Figure 5. Working of Vibration Sensor.
Source: own elaboration.

LCD Display Module

The LCD Display Module is a 16X2 liquid crystal display panel that is used to provide feedback to the person who is trying to access the door. The LCD display module display the current time as obtained and calculated from NIST server, and a corresponding message as per actions performed as explained below.

1. "Wrong Password", is the password or RFID tag sensed doesn't match with the password provided by the administrator.

2. "Door Open", "Door Closed", is displayed whenever the door is opened or closed, after crosschecking the password.

https://doi.org/10.17993/3ctecno.2022.specialissue9.269-285

3. “Intrusion Detected” is displayed when wrong password is identified at multiple instances.

4. “DOOR LOCKED” is displayed when the administrator has locked the door from being accessed by anyone, including the members with the RFID tag.

Arduino Mega

The microcontroller forms the brain of the control system. Arduino Mega is the standard version with multiple features and specifications in the Arduino family. The Uno board consists of Atmega2560 R3, the most powerful microcontroller in the Arduino series. The microcontroller comes with 54 digital I/O pins and 14 of these pins can be used to provide digital PWM outputs. There are 16 analog pins, which can read analog data and can also be used to provide DC power as output. Arduino Uno is the preferred microcontroller because of its serial communication method. The microcontroller can communicate serially with multiple modules at the same time. Due to its simplicity, Arduino mega can be easily re-coded and experimented on the go, adding to its flexibility. The LCD display module and the keypad modules will require a lot of digital pins and control pins which the Arduino Mega will satisfy. Considering all the modules that are to be run in the same instance, the processing speed of the Atmega2560 mc will run the system without hitting a lag, snag or a breakdown and will provide a smooth operation of the control system (Nehete *et al.*, 2016).

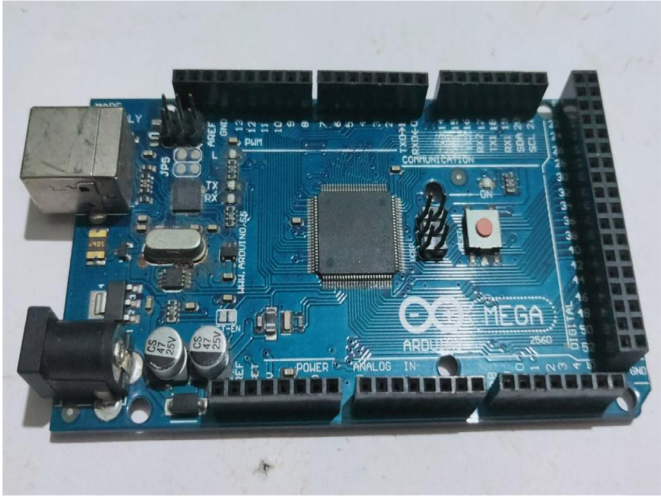

Figure 6. Arduino Mega 2560 R3.
Source: own elaboration.

WIFI module

The WIFI module is a very powerful and flexible device that can be used to connect the microcontroller with a specific web server, web page, web app or mobile app through means of internet. The IOT technology has made the remote control and alert mechanism of the door lock system far easier than before and makes it reliable and trustworthy for the consumers. In this security system (Barazanchi *et al.*, 2019; Bdulshaheed, Yaseen, & Al Barazanchi, 2019), the microcontroller is constantly in contact with the NIST server to obtain date and time, by using the NIST server we are removing the need of an RTC Clock Module. When the door is operated the status of the door lock and the name of the person accessing it, gets data logged on the web server. The administrator can open or close the door from a remote location using internet, and this information is also data logged on the web server for future reference. The preferred WiFi module type is ESP8266, but advanced and more secure WiFi module versions can also be used.

Servo Motor

The Servo motor is the most compatible for the door locking system because of its high torque output. The preferred servo motor here is an MG995 servo motor, because of its low operating voltage (4.8v to 6v) and high torque output (stall torque: 11kg/cm). The servo motor can exert a very high torque of 11 kilograms per cm, making it impossible for the human hands the handle or unlock the door. The only way to open the door is by using the servo motor, after all the security methods are satisfied.

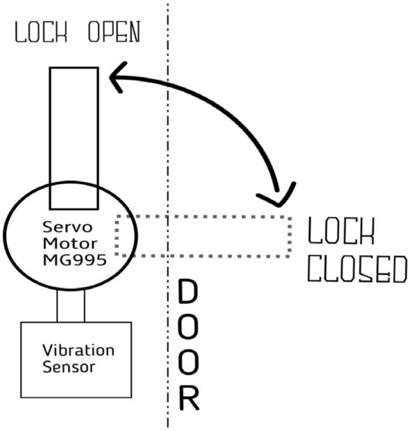

Figure 7. Working of Servo Motor.
Source: own elaboration.

Camera Module

The system uses two different cameras for the security operations. The first is a common CCTV camera, which are already installed external to this system. The second camera is a Arducam MT9D111 camera module, which is compatible with Arduino mega microcontroller. When a user has successfully unlocked the door with the right accessing methods, the Arducam MT9D111 live streams the video featuring the person accessing the door. The web server with the face identification neural network (Abdulshaheed *et al.*, 2018) technology captures the image of the user and checks it with database to identify the person. If the identity check has failed, the door stays locked, and an alert is sent to the administrator. The administrator is mostly the manager, or the operator at the reception. When the user has failed to access the door, the Arducam will live stream to identify the person. If the identification has failed, the image of the user gets captured and a control signal is sent to the server, through which the CCTV camera captures a high quality image of the user when the Access has failed (Al Barazanchi *et al.*, 2021; Al Barazanchi, & Jaaz, 2020).

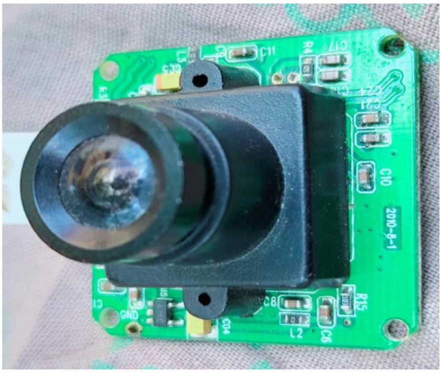

Figure 8. Arducam Camera Module.
Source: own elaboration.

https://doi.org/10.17993/3ctecno.2022.specialissue9.269-285

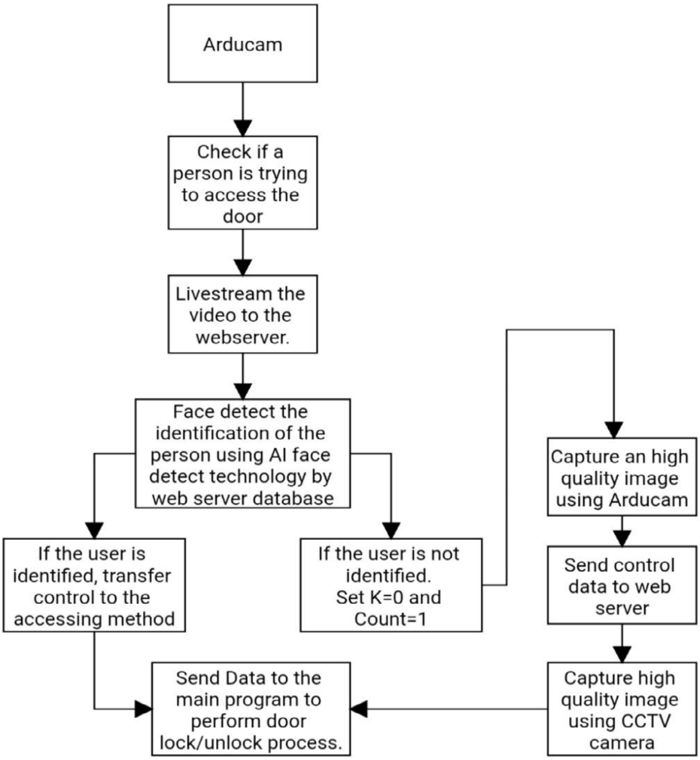
Arducam
Check if a person is trying to access the door
Livestream the video to the webserver.
Face detect the identification of the person using AI face detect technology by web server database
If the user is identified, transfer control to the accessing method
If the user is not identified. Set K=0 and Count=1
Capture an high quality image using Arducam
Send control data to web server
Capture high quality image using CCTV camera
Send Data to the main program to perform door lock/unlock process.

Figure 9. Working Flowchart of Arducam.
Source: own elaboration.

2.1.2. SOFTWARE REQUIREMENTS

The software system and the user display interface play a vital role in the door accessing methods. The focus of the software structure is divided into two parts, the first part focuses on the individual modules and their operations, and the second part focuses on the control system as a whole.

https://doi.org/10.17993/3ctecno.2022.specialissue9.269-285

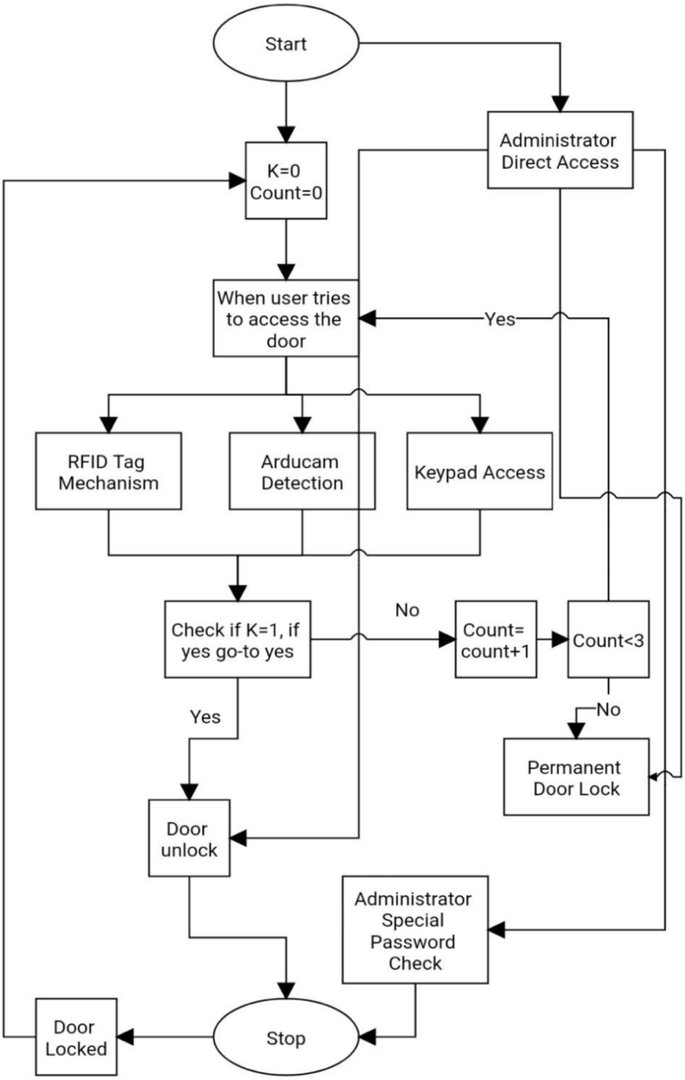

Figure 10. Flowchart of RFID Door Access Control System using IOT.
Source: own elaboration.

Web Server

The web server is essentially the fastest means by which the administrator can remotely control the door lock. The administrator is the person responsible and is authorized by the user organization, and can access the web server (Widadi *et al.*, 2021; Yaseen *et al.*, 2020). The web server also is protected by software security and passwords, by using the password the administrator can login to the web server and can use the option displayed to lock and

https://doi.org/10.17993/3ctecno.2022.specialissue9.269-285

unlock the door from a remote location and can view the registered data log to identify the list of people who have accessed the door.

Blynk App

This is a mobile application that allows separate repacking of its functionalities to remote access any IOT based system. Like the web server, the mobile application is also protected by the administrator himself and provides options to lock and unlock the door and also view the data log history of the members who have accessed the door from time to time. This app is either directly used, or an android app is built as per user's preference. Due to the flexibility of the system, the app too should be made flexible and must be able to support different devices and environments it is place in.

3. RESULTS

3.1. WORKING OF THE SYSTEM

The RFID Door Access Control System performs two operations, the first operation is the door accessing method, and the second operation is the data logging and alert mechanism. Regardless of these operations, the microcontroller gets data of date and time from the WIFI module. For this reason, the WIFI module is always connected to the NIST web server. But provided that the WIFI module can only be connected to a single web server, to handle this disadvantage the WIFI module is made to connect with the administrator web server only at certain intervals; intervals when the door is accessed, when data logging and when alerting the administrator (Abbas *et al.*, 2021). The administrator web server is not always connected to the system. So, the web server is designed to wait the connection, once the connection is set the control data is passed to the microcontroller, which will lock or unlock the door appropriately. Hence, the WIFI module is made to connect with the administrator web server to fetch control data for every 1 minute time limit in a 10 minute time interval. When a person tries to access the door using RFID tag or Keypad methodology, the microcontroller will receive the provided password from the modules and will crosscheck it with the password provided by the system or the organization's database. Upon success, the access to the door is granted. Upon failure, the LCD display module will display the message "WRONG PASSWORD", this entry will get registered in the data log

https://doi.org/10.17993/3ctecno.2022.specialissue9.269-285

on the web server and the user will have to provide the right password to gain access to the door. In case of multiple wrong entries, the system will finalize it as a fraudulent access and will permanently lock the door from anyone's access and also alerts the administrator. The permanent lock can only remove by resetting the system using a special administrator password by the admin. In case of a thief trying to break the door, the vibration sensor will sense this act and alerts the administrator and again permanently locks the door.

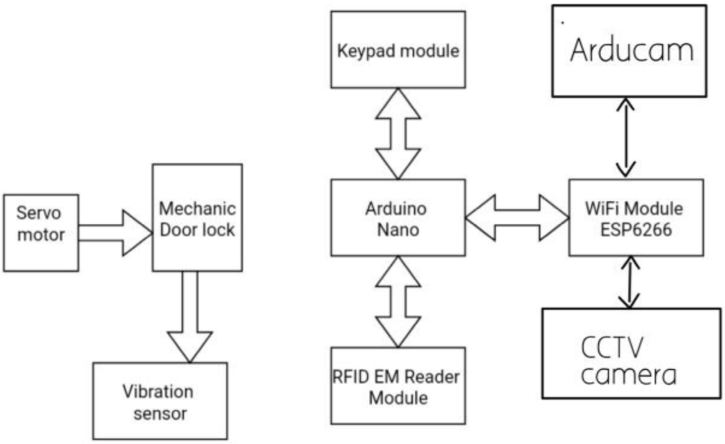

Figure 11. Block Diagram of Working System.
Source: own elaboration.

3.2. PERSONALIZED SYSTEM

Personalizing the security system is an easy task, because of the flexibility the system provides. Personalizing the system might include replacing the access methods by using Fingerprint sensor (Sweta, 2021), AI face detection, AI Eye detection or by advanced gesture control techniques using a camera interface. Depending on the devices to be included, other supportive devices should also be changed in terms of compatibility (Abdullah, Abed, & Al Barazanchi, 2019). The idea of personalizing the security system might help members of an organization who follow a specific culture, and the access methods will not be a trivial action in terms of their working ways.

4. CONCLUSIONS

The usage of Automation has been growing over the years and with the incorporation of IOT technology, existing security and automation systems have upgraded themselves to

https://doi.org/10.17993/3ctecno.2022.specialissue9.269-285

a new leash. People can now control their automation systems at office, in the comfort of home and vice versa. With the upgrades of science and engineering, the current system will be upgraded to a pure camera based sensor system, where the user doesn't need a password, key card or other ID. The AI system would be heightened that the users' face is automatically scanned and identified, without needing him to stand in front of the door; he or she can simply walk past the door without having to open with the upgraded systems. Such is the future of these systems and Automation.

ACKNOWLEDGMENT

This research is financially supported by UNITEN – UTM collaborative research grant 20200107CRGJ on the minor aid to get it presented and published.

REFERENCES

Abbas, H. H., Jaaz, Z. A., Al Barazanchi, I., & Abdulshaheed, H. R. (2021). Survey on Enhanced Security Control Measures in Cloud Computing Systems. *Journal of Physics: Conference Series 1878*(1), 012004. https://iopscience.iop.org/article/10.1088/1742-6596/1878/1/012004

Abdullah, A. S., Abed, M. A., & Al Barazanchi, I. (2019). Improving Face Recognition by Elman Neural Network Using Curvelet Transform and HSI Color Space. *Periodicals of Engineering and Natural Sciences, 7*(2), 430–37.

Abdulshaheed, H. R., Shah, W. B. M., Binti, S. A., & Sadiq, A. A. (2018). Proposed a Smart Solutions Based-on Cloud Computing and Wireless Sensing. *International Journal of Pure and Applied Mathematics, 119*(18), 427–49. https://acadpubl.eu/hub/2018-119-18/1/33.pdf

Al Barazanchi, I., Abdulshaheed, H. R., Shawkat, S. A., & Binti, S. R. (2019). Identification Key Scheme to Enhance Network Performance in Wireless Body Area Network. *Periodicals of Engineering and Natural Sciences, 7*(2), 895–906.

Al Barazanchi, I., Jaaz, Z. A., Abbas, H. H., & Abdulshaheed, H. R. (2020). Practical Application of IOT and Its Implications on the Existing Software. *In 2020 7th*

International Conference on Electrical Engineering, Computer Sciences and Informatics (EECSI), Yogyakarta, Indonesia. (October), 10–14.

Al Barazanchi, I., Niu, Y., Nazeri, S., & Hashim, W. (2021). A Survey on Short-Range WBAN Communication; Technical Overview of Several Standard Wireless Technologies. *Periodicals of Engineering and Natural Sciences, 9*(4), 877–85. https://www.researchgate.net/publication/357568972_A_survey_on_short-range_WBAN_communication_technical_overview_of_several_standard_wireless_technologies

Al-Sudani, A. R., Zhou, W., Liu, B., Almansoori, A., & Yang, M. (2018). Detecting Unauthorized RFID Tag Carrier for Secure Access Control to a Smart Building. *International Journal of Applied Engineering Research, 13*(1), 749–60. https://www.ripublication.com/ijaer18/ijaerv13n1_103.pdf

Bdulshaheed, H. R., Yaseen, Z. T., & Al Barazanchi, I. (2019). New Approach for Big Data Analysis Using Clustering Algorithms in Information. *Jour of Adv Research in Dynamical & Control Systems, 2*(4), 1194–97.

Khabarlak, K. S., & Koriashkina, L. S. (2020). Mobile Access Control System Based on Rfid Tags and Facial Information. *Bulletin of National Technical University "KhPI". Series: System Analysis, Control and Information Technologies, 2*(4), 69–74.

Nehete, P. R., Chaudhari, J. P., Pachpande, S. R., & Rane, K. P. (2016). Literature Survey on Door Lock Security Systems. *International Journal of Computer Applications 153*(November), 975–8887.

Nwogu, C., Eze, M., & Okunbor, C. (2020). Design and Implementation of Access Door Control with Mo-Bile Alert. *International Journal of Engineering & Technology 9*(2), 480. https://www.sciencepubco.com/index.php/ijet/article/view/30382

Pavelic, M., Loncaric, Z., Vukovic, M., & Kusek, M. (2018). Internet of Things Cyber Security: Smart Door Lock System. *Proceedings of International Conference on Smart Systems and Technologies 2018, SST 2018*, 227–232.

Priyanka, G., Rachana, J., Vijayalakshmi, N., Abhisheka, G. S., & Vinutha, D. C. (2019). IoT Door Lock Security System Using Google Assistance. *International Journal*

https://doi.org/10.17993/3ctecno.2022.specialissue9.269-285

of Innovative Technology and Exploring Engineering, 9(2S), 698–700. https://www.ijitee.org/wp-content/uploads/papers/v9i2S/B10181292S19.pdf

Sweta, A. K. (2021). Android Based Smart Door Lock Mechanism for Managing Security of Disabled People. *Psychology and Education Journal, 58*(2), 6341–6345.

Widadi, S., Munir, S. A. B., Shahu, N., Ahmad, I., & Al Barazanchi, I. (2021). Automatic Wireless Nurse Caller. *Journal of Robotics and Control (JRC), 2*(5), 380–84. https://journal.umy.ac.id/index.php/jrc/article/view/9995

Yaseen, Z. T., Murheg, H. D., Abdulshaheed, H. R., & Salman, A. M. (2020). Implementation of Mobile Robotics in Autonomous Mobility Tracking Robot. *International Journal of Advanced Science and Technology, 29*(4), 448–57.

https://doi.org/10.17993/3ctecno.2022.specialissue9.269-285