Enhancing Role - Based Access Control with Embedded Facial Recognition RBAC - EFR System

Joe Essien

Department of Computer and Information Technology, Veritas University, Abuja, Nigeria
Email: *essienj[at]veritas.edu.ng*

Abstract: ***Over time, a range of control mechanisms have been devised to deter unauthorised individuals from gaining entry to restricted facilities. The principal objective of implementing an automated access control system is to guarantee the protection of individuals and assets. The proliferation of electronic devices that offer security measures has gained significant traction in recent times. The automated door access control system is a highly sophisticated method of identification that utilises both biometric and non-biometric techniques. Non-biometric methods of identification rely on the use of passwords and access cards, while biometric methods utilise techniques such as fingerprint, iris, or facial recognition to establish a person's identity. Nevertheless, the majority of these techniques do not incorporate algorithms that are based on roles, which assess access requests in relation to a predetermined set of roles. The study introduces a novel design and simulation of a role-based access control system that has been augmented with a facial recognition system, utilising the ESP32-CAM. The RBAC-EFR system has been developed with the aim of facilitating domain-specific expert systems. It leverages roles and facial recognition technologies to enable deductions or choices pertaining to user access that it actively monitors. The Arduino Integrated Development Environment (IDE) serves as a design tool for interacting with and uploading programmes to the Arduino hardware. On the other hand, Proteus is utilised as a circuit simulation and virtual system modelling application. This technology is utilised for simulating the interaction between microcontroller scripts and digital electronics components.***

Keywords: Door Control System, Expert Systems, Microcontrollers, Role-Based Access Control, Embedded Facial Recognition System

1. Introduction

Access control is concerned with identifying the permitted activities of authorized users and mediating all requests for access to a restricted facility or resource. Access control provides protection against unwanted visitors, allows employees to work whenever they need to, prevents data intrusions, and improves network security monitoring. Access control mechanisms generally require the administration of security attributes for users and resources [1]. User security attributes can include categories such as user identifiers, the groups and roles to which a user belongs, and security labels signifying the level of trust accorded to the user. There are numerous kinds of resource attribute categories. Some examples include sensitivity identifiers, data types, and access control lists [2, 3]. Access control mechanisms compare the user's security attributes to the resource's security attributes; a set of roles may be used to determine (evaluate) access control checks [4]. Access control evaluations can also be determined using attribute-matching algorithms, biometrics, and real-time facial recognition. Biometrics is the ability of a computer to identify an individual based on a distinct physical trait [4]. Today, biometrics is one of the most rapidly expanding fields of advanced technology [3], [5]. Biometrics is expected to expand in the twenty-first century in order to verify identities and prevent unauthorized access to networks, databases, and facilities. Face recognition enables a computer to identify a person based on their facial characteristics [6]. Comparing the structure, shape, and proportions of facial features is necessary for face recognition. In addition, [7] compares the distance between the eyes, nose, mouth, and mandible, the upper outlines of the eye orbits, the sides of the mouth, the location of the nose and eyes, and the area around the check bones. When employing a facial recognition algorithm, multiple photographs of the individual are captured from various angles and with various facial expressions [1]. Facial recognition is extensively utilized because of its advantages. Facial recognition is non-intrusive, can be performed from a large distance, and can be performed without the individual's knowledge [2]. In comparison to other biometric techniques, facial recognition systems are preferable because they can be utilized for surveillance purposes, such as the search for wanted criminals, suspected terrorists, and missing children. This paper focuses predominantly on providing security by preventing unauthorized access to a facility using facial recognition technology embedded with Role Based Access Control (RBAC-EFR). RBAC-EFR permits the customization of the type of access granted to a user based on their organizational role. Users can be categorized into categories based on their responsibilities within an organization, as their access requirements are generally determined by this [6]. The construction of role-based systems employs machine learning techniques and can be classified into two subtypes: supervised learning and unsupervised learning [8]. Supervised machine learning requires labelled input and output training data, whereas unsupervised machine learning processes unlabeled or unprocessed data [9]. This research is motivated by the fact that role-based access control systems are simpler to understand, modify, and maintain than other common access control system variants such as Discretionary Access Control (DAC) and Mandatory Access Control [10]. Integrating Role-Based Access Control with a Facial Recognition System improves the system by identifying and measuring facial features in an image and associating the pattern against a database of faces in order to authenticate users with roles for access to a resource or facility.

2. Review of Literature

Prior to the introduction of modern electronic locking systems, locks were mechanically constructed with levers,

Licensed Under Creative Commons Attribution CC BY

gears, and wheels [4]. Further innovations introduced the password-based locking system. A password-based locking system includes a keypad or touchpad attached to the door that allows the user to enter the password [6]. If the password entered matches the existing password stored in memory, the door is unlocked; otherwise, the door remains closed. Entering the wrong password more than three times may result in access being denied and, in some cases, the buzzer being activated, resulting in an alarm. There are also options to change the password as needed [1], [9]. This system consisted of two relays available for opening and closing the door[5]. A more advanced technology involved the use of the Radio Frequency Identification (RFID) Lock Systems. The RFID technology tracks tags and retrieves tag information by using electromagnetic fields for data transfer. When the RFID tag comes into contact with the RFID reader, the door opens if the information retrieved matches the data already stored in the memory. These systems are used in a variety of applications such as asset tracking, access control applications, people tracking, and many others [7], [2]. The benefits of RFID systems include data tracking, which means that an employee's movements can be recorded or tracked by a smartcard system while carrying an RFID card. Another advantage is secure data, which means that the data in an RFID card can only be read with special equipment [5]. They are application-specific in the sense that no single tag fits all. However, the RFID systems are easily disrupted because they use the electromagnetic spectrum, which is one of the system's major limitations. Active RFID tags can also quickly deplete the battery. Hackers can access the data on the RFID tag[3], [11]. A more contemporary approach involved the use of Biometric Locking System. A biometric system grants access to authorized users by verifying their unique physical or behavioral characteristics, such as fingerprints, face recognition, voice recognition, vein detectors, iris scanners, and so on [10]. Passwords are frequently passed, written down for convenience, or reused multiple times. Biometric logins are specific and makes it impossible for a person not configured in the system to use the technology[4]. The lock system works by scanning the biometrics and then converting them into a numerical template that is saved for the first time [8]. Then, the next time someone tries to open the door using their biometrics, it will be compared to the previously stored data. However, the system is not secure and it is easy for hackers to duplicate fingerprint copies and hack the iris scanner using current technologies. This is because for Biometrics, the "close enough" matching principle is used [1], [12]. To complement the (RFID) Lock Systems, the Wireless Locking Systemwas introduced[6].A wireless lock system consists of a door lock and a mobile computing device. The door lock is made up of a locking device, a Near Field Communication (NFC) device, and a microcontroller, while the mobile computing device is made up of an NFC device, a display, and a mobile application. In order to communicate with the mobile device, a server is used. In response to the server's communication, the mobile application generates a code that is transmitted via the NFC signal. After receiving this code, the microcontroller disengages the locking device, determining that the received code contains the correct data to unlock the door [4], [7]. An extension of the Wireless Locking System is the IOT-based Lock System. The Internet of Things (IOT) is a technology that connects devices smart phones and personal computers to internet, allowing these devices to communicate with each other people as well as other devices.

Organizations implementing access control systems consider three abstractions: policies, models, and methods [6]. Access control policies are high-level requirements that specify how access is managed and under what conditions certain individuals are permitted to access a resource [5]. For example, policies may pertain to the utilization of resources within or across.It may be based on organizational units or factors such as need-to-know, competence, authority, obligation, or conflict of interest [3]. At a high level, access control policies are enforced by a mechanism that translates a user's access request, typically in terms of a system-provided structure [2]. A common type of access control mechanism is an access control list. Models of access control reconcile the abstraction divide between policy and mechanism [9]. Rather than evaluating and analyzing access control systems solely at the mechanism level, security models typically characterize the security properties of an access control system [8]. Security models are formal representations of the system's security policy and are valuable for demonstrating a system's theoretical limitations [13]. Aside from the Role-Based Access Control (RBAC),many other Access control systems have been identified including Web-Based Access Control Systems (W-BACS), Mobile-Based Access Control Systems (M-BACS), IOT-Based Access Control Systems, Mandatory Access Control (MAC) and Discretionary Access Control (DAC).Web-based access control systems refer to security systems that are implemented through web-based applications. These systems are designed to regulate access to resources and information within an organization or network. Complement to W-BACS, Access control systems are also web-based but utilized to regulate access to resources and functionalities by means of interfaces that are web-based. These Access Control systems regulate user access by verifying user credentials, roles, or permissions that have been allocated within the web-based domain. In contrast, the purpose of mobile-based access control systems is to regulate access to resources and functionalities by means of mobile devices. They offer authentication and authorization mechanisms that are specifically customized for mobile applications. These systems regulate user access by utilizing mobile device identifiers, user credentials, or other authentication factors that are linked to mobile devices. In a similar implementation, the Mandatory Access Control (MAC) has been deployed as a security model that restricts access to resources based on the sensitivity of the information and the clearance level of the user. MAC has been classified as a security paradigm that primarily relies on the security classifications and labels that are assigned to subjects (users) and objects (resources) for making access control decisions. The determination of access decisions is contingent upon the pre-established security policies and rules that have been put in place by the system administrators. The level of control that users possess over access permissions is restricted due to the stringent regulation of the system, which usually necessitates higher levels of authorization. To implement accesses control characterized by the resource owner's discretion in making access control decisions, the Discretionary Access Control

Licensed Under Creative Commons Attribution CC BY

(DAC) security model has been proposed. Here, the determination of resource accessibility and the extent of access granted is at the discretion of the resource owner.Individuals possess greater authority over access permissions, as they are capable of bestowing or withdrawing access privileges to their respective resources. In comparison the security paradigm known as Role-Based Access Control (RBAC) operates by making access control determinations based on pre-established roles and their corresponding permissions.Individuals are designated particular roles according to their professional duties, and authorization privileges are conferred in accordance with those roles.Role-Based Access Control (RBAC) streamlines access management by categorizing users into roles and allocating permissions to roles instead of individual users.

In summary, web-based access control systems and mobile-based access control systems differ in the platforms they operate on, while mandatory access control, discretionary access control, and role-based access control differ in the underlying access control models they follow. Mandatory access control focuses on security classifications, discretionary access control gives resource owners control over access decisions, and role-based access control organizes access based on predefined roles and permissions. Each access control system serves a specific purpose and can be chosen based on the requirements and security needs of the system or organization.

3. Method for Semantics and Architectural Design

The RBAC-EFR system adopts the facial recognition methodology. Facial recognition is a biometric technology that employs algorithms to authenticate an individual's identity by detecting and quantifying distinctive facial attributes within a given visual representation [1]. Facial recognition technology exhibits variability in its systems, yet generally operates on the fundamental principles of face detection, facial analysis, conversion of image to data, and subsequent matching. The ESP32-CAM is utilized in this implementation for the purpose of capturing facial patterns. The ESP 32 CAN is a diminutive camera module that provides Wi-Fi and GPIO accessibility [6]. Several authors have conducted research on the utilization of ESP-32 CAM for facial recognition, whereby the sensor data is transmitted to the server by Arduino through the ESP32 CAM module [3], [5], [7], [13]. This methodology possesses the ability to transmit images automatically upon detection of any motion. The system is capable of automatically executing tasks such as capturing photographs, activating lighting, fans, and PIR sensors through its web interface [4], [9]. The study by Qiu et al. [14] investigated the implementation of Time-Based One Time Password (TOTP) as a means of enhancing the security of online accounts through two-factor authentication. The Time-based One-Time Password (TOTP) algorithm employs the Hash-based Message Authentication Code (HMAC) technique. The investigation involves the dissemination of TOTP generation utilizing a secret key to users via a QR Code or bar code that is associated with the user's account and local time setting [4]. The verification code for the original user account ownership shall be derived from the passcode generated by TOTP. The proposed design for an improved role-based access control systemis based on the principles of TOTP. The design identifies the physical components of the system, specifically the facial recognition technology, and their interrelationships with the various roles within the system. The specification additionally delineates the manner in which said components are integrated within the system's architecture, as well as the tangible hardware and circuitry construction.

The RBAC-EFR model consists of four distinct categories of entities, namely users (U), roles (R), facial imaging, and permissions (P). Figure 1 illustrates a collection of limitations pertaining to Role, Groups, and Imaging. Within this paradigm, a user is considered to be an entity. The concept of a user can be broadened to encompass intelligent autonomous agents, which may include robots, software agents, stationary computers, and computer networks. For the sake of clarity and ease of analysis, our focus is directed towards the user as an autonomous entity. A role refers to a specific job function or job title that is assigned within an organization. The semantics of a role are associated with the authority and responsibilities that are granted to an individual who holds that role. According to reference [3], a permission refers to the granting of a specific mode of access to one or multiple objects within a system. In scholarly literature, the term "permission" is commonly used interchangeably with "authorization," "access right," and "privilege." Affirmative permissions enable the permission holder to perform certain actions within the system. Within the system, there exist data objects and resource objects which are both represented by data. The conceptual model utilized allows for a variety of permission interpretations, ranging from broad permissions, such as granting access to an entire facility, to more specific permissions, such as granting access to a particular facility or resource. The process of combining individual permissions into a generic permission for singular assignment is heavily reliant on implementation specifics [4]. Figure 1 depicts the level of granularity of the model under consideration. Multiple roles can be assigned to a single user, while a role can encompass multiple users. Multiple permissions can be assigned to a single role, and conversely, a single permission can be assigned to multiple roles. The fundamental concept of RBAC-EFR is embedded within this framework.

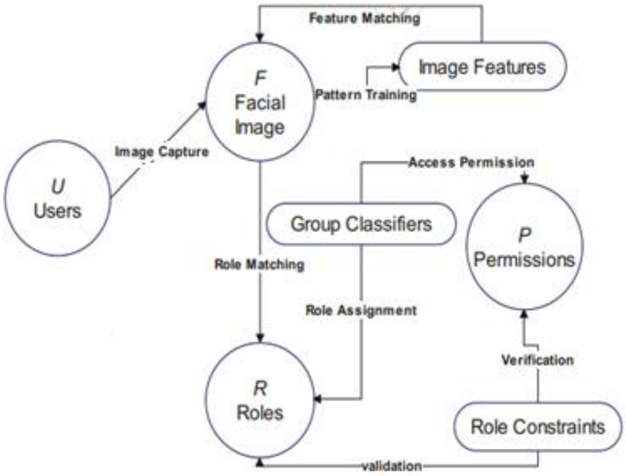


Figure 1: Conceptual model of the RBAC-EFR

Licensed Under Creative Commons Attribution CC BY

A functional access control system connects door controllers, keycards, and additional components to the same network. This study examines sliding doors, which typically consist of flat panels that can be arranged in a variety of ways. The panels move horizontally and in a straight line [3]. This work's automated sliding system consists of three parts: the detecting mechanism, the primary controller circuit, and the motor [9]. The circuit module serves as the system's principal controller. Utilizing sensors permits the identification of individuals approaching the movable doors. Motors are used to glide in either a forward or reverse direction to reach the desired location [5]. The circuit of the module consists of two distinct activators (sensors), one of which is located outside the chamber and the other inside [2], [10], [12]. The corresponding action is carried out when the door's limit switches detect that it has been completely opened or closed. Photodiodes, phototransistors, and light-based resistors (LDR) are used to operate the automatic sliding door control system [10]. These sensors sense light in order to function. There are two categories of sensors: presence protection sensors and activation sensors. Each variety serves a distinct function. A sensor activates when a person approaches and opens the door. The presence protection sensor detects the obstruction and prevents the door from opening or closing if a pedestrian is impeding its passage [3]. Mechanical limit switches connect an electric circuit to a mechanical motion or location. One of the most prevalent varieties of limit switch is the single-pole contact block, which consists of one normally open (NO) contact and one normally closed (NC) contact [13], [5]. Additionally, there are limit switches with a time-delayed contact shift. Limit switches are frequently used as input devices to signify the presence or absence of a particular condition within a monitored or regulated system or process [14]. A limit switch is a form of switch that detects when a system component reaches a predetermined location. Limit switches are a common component in a variety of industrial applications due to their capacity to determine the utmost range of motion for an object [6]. To monitor the motion of a mechanical component, limit switches are developed. Limit switches are frequently used in industrial control applications to automatically monitor and indicate if a system's travel restrictions have been exceeded [4], [7]. In this particular implementation, the limit switch is intended to be mounted underneath the lifter. There are a variety of potential automatic door designs. Others feature panels that collapse when people enter or exit, while others open and close conventionally by swinging in or out. The doors are equipped with a motion sensor that can identify humans as they approach, and the sensitivity of the sensor can be adjusted according to the circumstances [8].

4. RBAC-EFR Modelling, Simulation and Results

The initial stage entails conducting a design consideration, which entails analyzing the various components and choosing which ones to use. In this work, the Arduino Integrated Development Environment (IDE) is used as a design tool that communicates with and uploads programmes to the Arduino hardware, while Proteus is used for circuit simulation and virtual system modelling. In addition, it is utilized to simulate the interaction between microcontroller scripts and digital electronics components. After completing the required configurations, a blank schematics file known as a root sheet was created. Figure 1 depicts the selection of components from the available library.

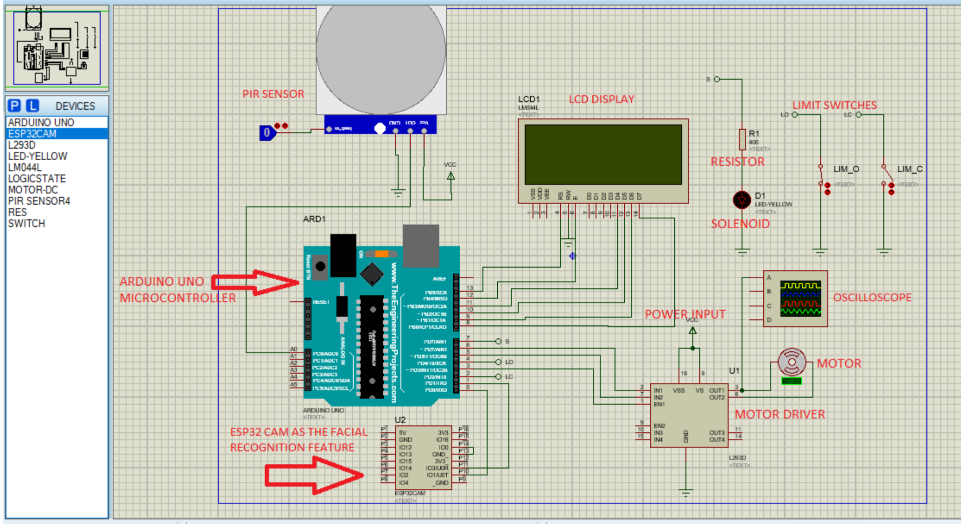
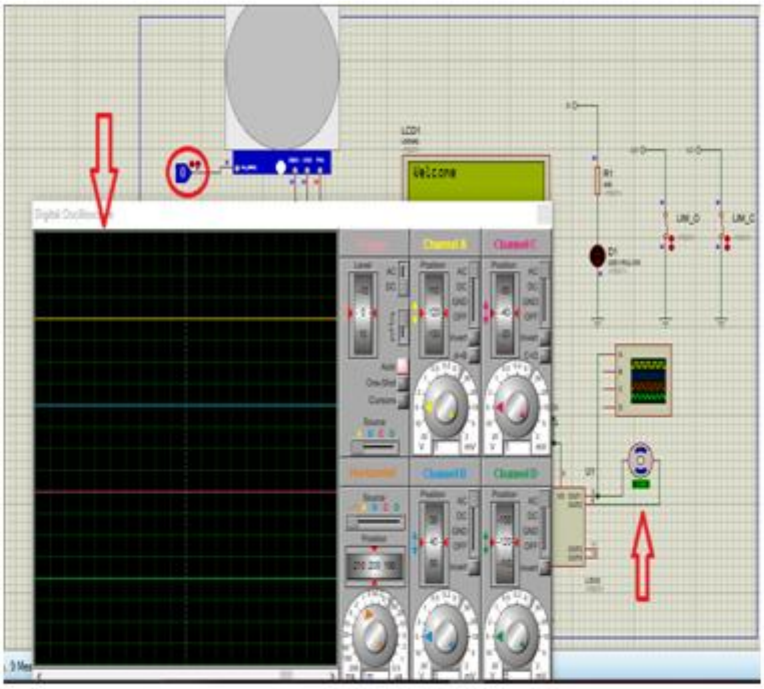


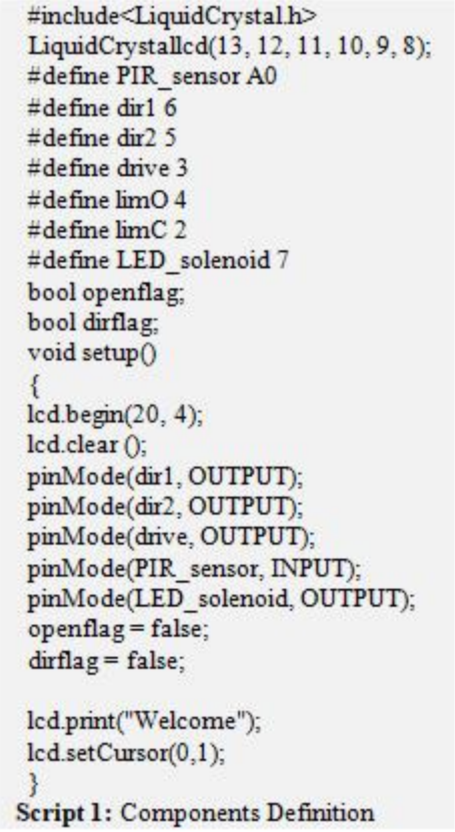
Figure 2: Schematic design of the door access control system using the ESP32 CAM

The ESP32-CAM is incorporated with the Role-Based Access Control system for facial recognition. The ESP32-CAM is a camera module with a compact form factor and low power consumption [3], [7]. It features an integrated TF card port and an OV2640 camera. The ESP32-CAM is widely employed in the development of intelligent systems and Internet of Things applications, including wireless video monitoring, Wi-Fi image upload, and QR identification [8]. The ESP32 CAM Bluetooth Wi-Fi module with OV2640 2MP Camera Module [15]. For face recognition, it includes a highly competitive small-size camera module that operates independently as a minimum system with a footprint of only 47 x 42 mm; a deep sleep current of up to 6mA; and is extensively used in a variety of IoT applications. In this design, an ATmega328P-based Arduino UNO microcontroller board is used. It has 14 digital input/output

Licensed Under Creative Commons Attribution CC BY

terminals (six of which are PWM outputs), 6 analogue inputs, a 16 MHz ceramic resonator, a USB port, a power jack, and an ICSP header [5].





```
#include<LiquidCrystal.h>
LiquidCrystallcd(13, 12, 11, 10, 9, 8);
#define PIR_sensor A0
#define dir1 6
#define dir2 5
#define drive 3
#define limO 4
#define limC 2
#define LED_solenoid 7
bool openflag;
bool dirflag;
void setup()
{
lcd.begin(20, 4);
lcd.clear ();
pinMode(dir1, OUTPUT);
pinMode(dir2, OUTPUT);
pinMode(drive, OUTPUT);
pinMode(PIR_sensor, INPUT);
pinMode(LED_solenoid, OUTPUT);
openflag = false;
dirflag = false;

lcd.print("Welcome");
lcd.setCursor(0,1);
}
```

Script 1: Components Definition

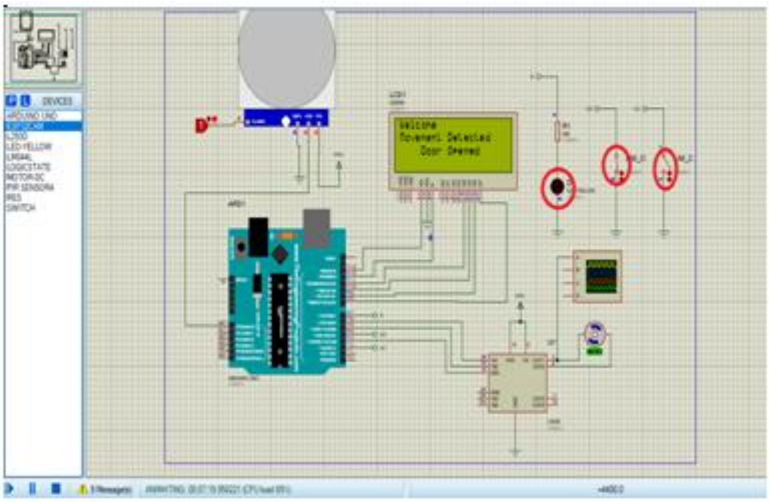
Figure 3: Simulation of no detected Movement shows No signal on the Oscilloscope

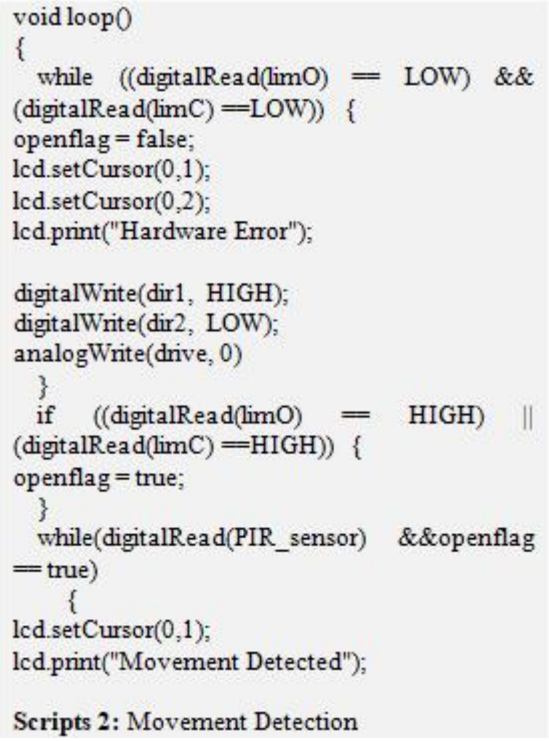
According to the Arduino code being used, for motion detection, the motor will not move if the PIR does not detect motion. No signal is present on the oscilloscope. As depicted in Figure 3. If motion is detected and both limit switches are closed, the LCD displays a hardware enabled message. In the unlikely event that both limit switches close simultaneously, the limit switches are defective and must be replaced. When motion is detected and one of the limit switches (LIM O) is Open and the other is Closed (LIM C), simulate door opening.

Detection of Motion

During the recognition procedure, the ESP32-CAM device detects the face using the face recognition algorithm PCA, which is part of the open CV library. PCA is an unsupervised machine learning algorithm that retains as much information as possible while reducing the dimensionality (number of features) of a dataset. PIR sensors for motion detection are used to determine if a person has entered or exited the sensor's range. These are compact, inexpensive, low-powered, user-friendly, and non-wearable [16]. As a result, they are commonly found in household and commercial appliances and devices. They are also referred to as PIR, "Passive Infrared," "Pyroelectric," and "IR motion" sensors [5],[13]. Initially, a Limit Switch is used to specify the utmost distance an object must be from the sensor before being detected. At this juncture, the switch that controls the proximity limit is activated. The Switch is an electromechanical device consisting of a mechanical actuator coupled to a series of electrical contacts [6, 9]. When an object makes physical contact with the actuator, the movement of the actuator plunger closes (for a normally open circuit) or opens (for a normally closed circuit) the electrical contacts within the switch [6]. The mechanical movement of the actuator plunger is utilized by limit switches to control or alter the state of an electrical switch. Without touching the object, similar devices, such as inductive or capacitive proximity sensors or photoelectric sensors, can accomplish the same result. In contrast to these other categories of proximity sensing devices, limit switches are therefore contact sensors [2]. The vast majority of limit switches have a mechanical operation [4], [3].

Licensed Under Creative Commons Attribution CC BY





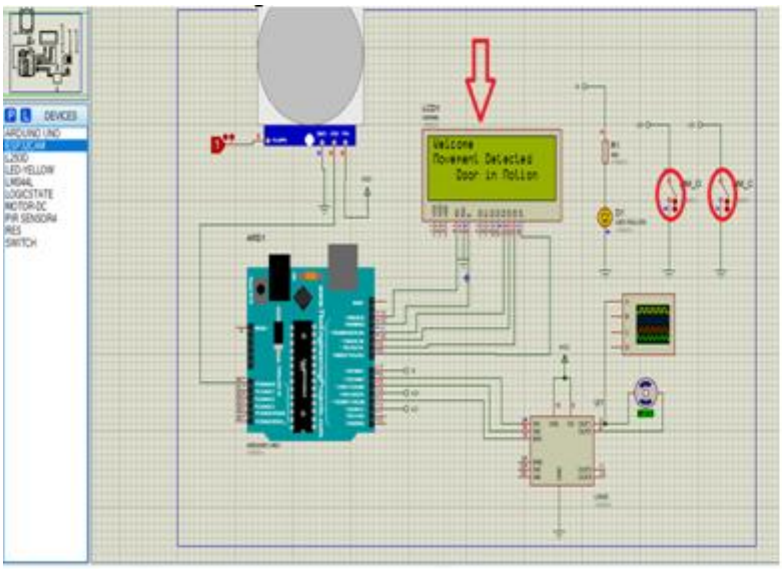
```
void loop()
{
  while  ((digitalRead(limO)  ==  LOW)  &&
(digitalRead(limC) ==LOW))  {
openflag = false;
lcd.setCursor(0,1);
lcd.setCursor(0,2);
lcd.print("Hardware Error");

digitalWrite(dir1, HIGH);
digitalWrite(dir2, LOW);
analogWrite(drive, 0)
  }
  if   ((digitalRead(limO)   ==   HIGH)   ||
(digitalRead(limC) ==HIGH))  {
openflag = true;
  }
  while(digitalRead(PIR_sensor)   &&openflag
== true)
      {
lcd.setCursor(0,1);
lcd.print("Movement Detected");
```

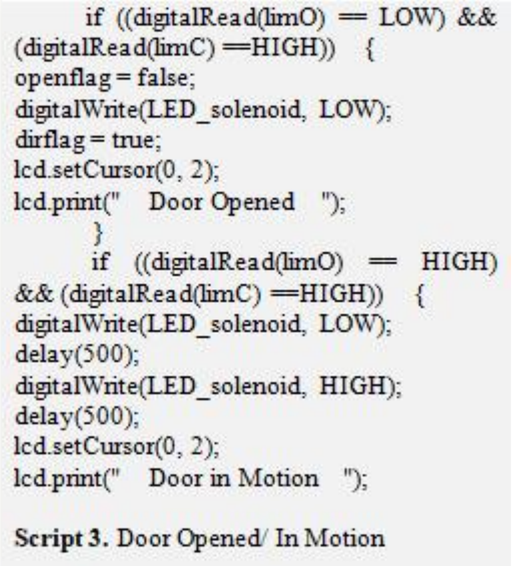
Scripts 2: Movement Detection

Figure 4: Movement Detected/Facial Recognition Activation

Door in Motion:

When the two Switches are Open and motion is detected, the door remains in motion. And the LCD displays “Door in Motion” as shown in Figure 5.





```
        if  ((digitalRead(limO)  == LOW)  &&
(digitalRead(limC) ==HIGH))   {
openflag = false;
digitalWrite(LED_solenoid, LOW);
dirflag = true;
lcd.setCursor(0, 2);
lcd.print("    Door Opened    ");
        }
        if   ((digitalRead(limO)   ==   HIGH)
&& (digitalRead(limC) ==HIGH))    {
digitalWrite(LED_solenoid, LOW);
delay(500);
digitalWrite(LED_solenoid, HIGH);
delay(500);
lcd.setCursor(0, 2);
lcd.print("    Door in Motion    ");
```

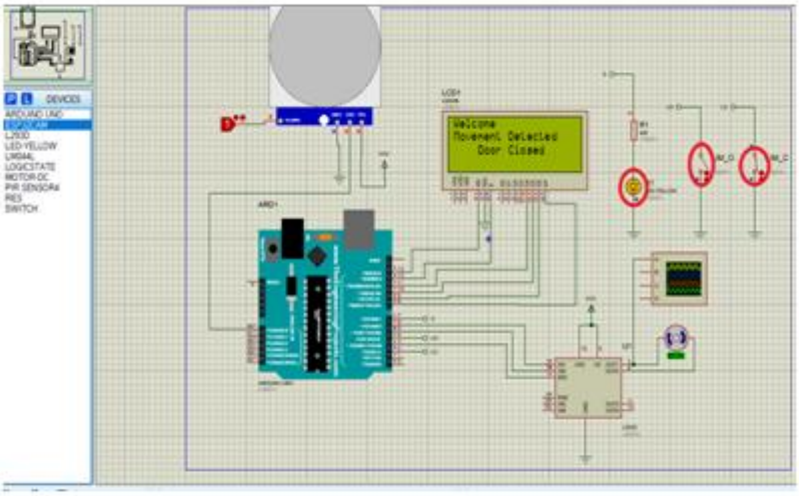
Script 3. Door Opened/ In Motion

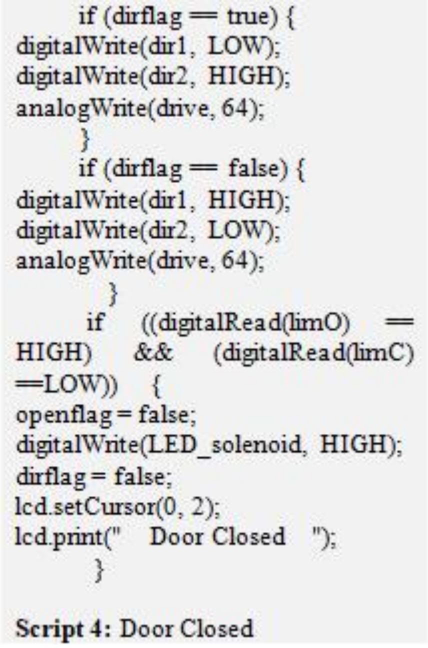
Figure 5: Door Opened/Door in Motion

Simulation of a door Access control System utilizing ESP32 CAM. This means that when it is implemented in a real environment, such as an office safe room, it ensures that access is permitted only to recognized (authorized) individuals based on their user role. This ensures the welfare of the office's personnel and property.

Door Closing: When the PIR sensor detects motion and the first limit switch is Open while the second one is closed, the door closes as shown in figure 6.

Licensed Under Creative Commons Attribution CC BY





```
        if (dirflag == true) {
digitalWrite(dir1, LOW);
digitalWrite(dir2, HIGH);
analogWrite(drive, 64);
        }
        if (dirflag == false) {
digitalWrite(dir1, HIGH);
digitalWrite(dir2, LOW);
analogWrite(drive, 64);
          }
        if    ((digitalRead(limO)    ==
HIGH)    &&    (digitalRead(limC)
==LOW))    {
openflag = false;
digitalWrite(LED_solenoid, HIGH);
dirflag = false;
lcd.setCursor(0, 2);
lcd.print("    Door Closed    ");
        }
```

Script 4: Door Closed

Figure 6: Door Closed

5. Discussion

Role-Based Access Control with Embedded Facial Recognition (RBAC-EFR) System is a widely used access control model that provides an efficient and scalable way to manage access to resources within an organization or system. It is based on the concept of assigning roles to users and granting permissions to those roles, rather than individually managing access for each user. In this work, the key features of a Role-Based Access Control were considered specified as Roles, Permissions, Users, Assignments and hierarchy: RBAC revolves around roles that represent job functions or responsibilities within an organization. Roles are defined based on common sets of tasks or permissions required to perform specific functions. Permissions were associated with roles to define the actions or operations that can be performed on specific resources. Each role is granted a set of permissions necessary to fulfill its responsibilities. Access Assignment for the RBAC enabled the assignment of access rights at a higher level of abstraction. Instead of managing access for each user, access is granted or revoked at the role level, simplifying administration and ensuring consistent access control policies and hierarchy structures for roles. This allows roles to inherit permissions from higher-level roles, reducing the effort required for access management. The benefit of enhanced RBAC-EFR include simplified access management. Enhanced RBAC-EFR simplifies access management by grouping users into roles and assigning permissions to roles. This reduces administrative overhead and the complexity of individually managing access for each user. RBAC-EFR is highly scalable as it allows for easy addition or removal of users and roles. It also offers flexibility by allowing dynamic role assignments based on changing job responsibilities or team structures. In terms of security, RBAC-EFR enhances security by ensuring that users have only the necessary permissions required for their roles. Unauthorized access is minimized, and the principle of least privilege is upheld. Considerations for Role-Based Access Control included proper role design and management which is crucial for effective RBAC implementation. Roles should be well-defined, and regular review and updates should be conducted to ensure they align with organizational needs [13]. In conclusion, Enhanced Role-Based Access Control with Embedded Facial Recognition (RBAC-EFR) System is a powerful access control model that provides significant benefits in managing access to resources within an organization. By properly designing roles, assigning permissions, and managing user assignments, RBAC-EFR helps enhance security, streamline access management.

6. Conclusion

Role-Based Access Control (RBAC) with an embedded facial recognition system is a powerful combination that enhances access control and security measures in various applications.Integrating Role-Based Access Control with an embedded facial recognition system can provide several contributions and benefitsincluding enhanced authentication, increased security, real-time access control, granular access control adaptability and scalability amongst others.The integration of RBAC with facial recognition technology provides an additional layer of security by verifying the identity of individuals based on their unique facial features. This significantly reduces the risk of unauthorized access, as it is challenging for an imposter to mimic someone else's facial characteristics accurately.The study introduces a novel design and simulation of a role-based access control system that has been augmented with a facial recognition system, utilizing the ESP32-CAM. The RBAC-EFR system has been developed with the aim of facilitating domain-specific expert systems. It leverages roles and facial recognition technologies to enable deductions or choices pertaining to user access that it actively monitors. The Arduino Integrated Development Environment (IDE) serves as a design tool for interacting with and uploading programmes to the Arduino hardware. On the other hand, Proteus is utilized as a circuit simulation and virtual system modelling application. This technology is utilized for simulating the interaction between microcontroller scripts and digital electronics components.

Licensed Under Creative Commons Attribution CC BY

While the integration of RBAC with facial recognition offers numerous benefits, it is important to address potential challenges and considerations. These include ensuring the accuracy and reliability of the facial recognition technology, addressing privacy concerns related to biometric data storage and usage, implementing robust security measures to protect against unauthorized access or tampering, and providing adequate user training and awareness regarding the system's functionalities and limitations.In summary, the incorporation of Role-Based Access Control (RBAC) in conjunction with an embedded facial recognition system establishes a sturdy basis for effective access management, enhanced security measures, simplified authentication procedures, and elevated user satisfaction across diverse domains and applications. In conclusion, the study successfully introduces a novel design and simulation of a role-based access control system that incorporates facial recognition technology, utilizing the ESP32-CAM. This system enhances security measures and facilitates domain-specific expert systems. The use of Arduino Integrated Development Environment IDE and Proteus for design and simulation has proven effective. Future research can further explorethe potential applications and improvements of this system in various domains.

Conflicts of Interest Statement

The authors of this article hereby certify that they have NO affiliations with or involvement in any organisation or entity with any financial interest (such as honoraria; educational grants; participation in speakers' bureaus; membership, employment, consultancies, stock ownership, or other equity interest; and expert testimony or patent-licensing arrangements), or non-financial interest (such as personal or professional relationships, affiliations, knowledge or beliefs) in the subject matter or materials discussed in this manuscript.

References

[1] Lourenco, F. and Almeida, C., 2009. RFID based monitoring and access control system. In Proc. INFORUM.

[2] Meng, X.L., Song, Z.W. and Li, X.Y., 2010, August. RFID-Based security authentication system based on a novel face-recognition structure. In 2010 WASE International Conference on Information Engineering (Vol. 1, pp. 97-100). IEEE.

[3] Farooq, U., ul Hasan, M., Amar, M., Hanif, A. and Asad, M.U., 2014. RFID based security and access control system. International Journal of Engineering and Technology, 6(4), p.309.

[4] Omije, B.O., Saturday, U.U. and Student, M.E., Design of an Access Control Facial Recognition System Using Raspberry Pi.

[5] Hung, C.H., Bai, Y.W. and Ren, J.H., 2015, June. Design and implementation of a door lock control based on a near field communication of a smartphone. In 2015 IEEE International Conference on Consumer Electronics-Taiwan (pp. 45-46). IEEE.

[6] Prathapagiri, D. and Kosalendra, E., 2021. Wi-Fi Door Lock System Using ESP32 CAM Based on IoT. The International journal of analytical and experimental modal analysis. XIII. 20002003.

[7] Majgaonkar, N., Hodekar, R. and Bandagale, P., 2016. Automatic door locking system. International Journal of Engineering Development and Research, 4(1).

[8] Nehete, P.R., Chaudhari, J.P., Pachpande, S.R. and Rane, K.P., 2016. Literature survey on door lock security systems. International Journal of Computer Applications, 153(2), pp.13-18.

[9] Al-Shebani, Q., Premaratne, P. and Vial, P., 2013, December. Embedded door access control systems based on face recognition: A survey. In 2013, 7th International Conference on Signal Processing and Communication Systems (ICSPCS) (pp. 1-7). IEEE.

[10] Jagdale, R., Koli, S., Kadam, S. and Gurav, S., 2016. Review on intelligent locker system based on cryptography wireless & embedded technology. International Journal of Technical Research and Applications, pp.75-77.

[11] Holat, R. and Kulac, S., 2014, April. ID identification by using face detection and recognition systems. In 2014 22nd Signal Processing and Communications Applications Conference (SIU) (pp. 866-869). IEEE.

[12] Rahouma, K. and Zarif, A., 2019. Face recognition based on correlation and back propagation neural networks. Egyptian Computer Science Journal, 43(3).

[13] Jaikla, T., Vorakulpipat, C., Rattanalerdnusorn, E. and Hai, H.D., 2019, September. A secure network architecture for heterogeneous iot devices using role-based access control. In 2019 International conference on software, telecommunications and computer networks (SoftCOM) (pp. 1-5). IEEE.

[14] Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S. and Fang, B., 2020. A survey on access control in the age of internet of things. IEEE Internet of Things Journal, 7(6), pp.4682-4696.

[15] Thilakarathne, N.N. and Wickramaaarachchi, D., 2020. Improved hierarchical role-based access control model for cloud computing. arXiv preprint arXiv:2011.07764.

[16] Asim, Y. and Malik, A.K., 2020. A survey on access control techniques for social networks. In Information Diffusion Management and Knowledge Sharing: Breakthroughs in Research and Practice (pp. 319-342). IGI Global.

[17] Ghazal, R., Malik, A.K., Qadeer, N., Raza, B., Shahid, A.R. and Alquhayz, H., 2020. Intelligent role-based access control model and framework using semantic business roles in multi-domain environments. IEEE Access, 8, pp.12253-12267.

Licensed Under Creative Commons Attribution CC BY