# Access Control Using Facial Recognition with Neural Networks for Restricted Zones

Rodrigo Reaño, Piero Carrión and Juan-Pablo Mansilla
*Universidad Peruana de Ciencias Aplicadas, School of Engineering, Lima, Peru*

Keywords: Facial Recognition, Access Control, Neural Networks, Artificial Intelligence, Facial Recognition System.

Abstract: A new technology that has proven to be effective and accurate in identifying people today is facial recognition. This technology, when used with IP cameras, provides a very effective and practical access control system. Moreover, this system is able to learn and improve its facial recognition capability over time through the use of neural networks, leading to higher accuracy and a lower false positive rate in the field. Thus, this paper shows a face recognition system, based on neural networks, for monitoring and controlling access of people in small and medium-sized enterprises (SMEs); with the use of IP cameras for the versatility of continuous tracking to people circulating in restricted areas. On the other hand, common security problems that are identified in these environments are addressed and solutions are offered through the implementation of the proposed system. Finally, the results obtained demonstrate that the system offers an efficient and secure solution for monitoring and controlling access of people in restricted areas of small and medium-sized enterprises (SMEs). Its accurate identification capability, combined with the elimination of barriers and convenience for users, significantly improves security and user experience.

## 1 INTRODUCTION

Today, facial recognition has diverse applications in fields such as security, surveillance, commerce and healthcare. It is used to identify and authenticate individuals by capturing and analyzing unique facial characteristics. However, there are also privacy and security concerns regarding access control in the aforementioned areas. Access control in restricted areas is a constant concern for enterprises. The need to protect information, goods and people from unauthorized or potentially dangerous access has led to the implementation of security measures, such as the use of access cards, security keys, surveillance cameras and security guards. However, there are problems that can affect the effectiveness of these controls, such as unauthorized access, human error, lack of technology, lack of training and lack of maintenance.

There is research that uses facial recognition for other applications such as (Lee et al., 2020) in healthcare, who propose a video surveillance system to monitor and predict the behavior of patients using machine learning, which is a branch of artificial intelligence. Likewise, there is a study by (Talahua et al., 2021) that describes a facial recognition system that can identify people with and without a mask in real time; in addition, there are system proposals, oriented to the diagnosis of diseases, as described by (Pan et al., 2021) that performs an automatic facial recognition system based on deep learning to help in the diagnosis of Turner syndrome in patients. On the one hand, (Nyein and Oo, 2019) propose a classroom attendance registration system using face recognition and SVM machine learning technique to improve the efficiency of the attendance registration process in university classrooms. On the other hand, (Xu et al., 2021) propose a check-in system, in hotels, that uses facial recognition in order to realize a fast, secure and private way of check-in.

There are facial recognition systems that are focused on the student sector (attendance system in classrooms), health (system that identifies when a person has a mask or not), among others; however, access control is a difficulty encountered by companies and there is no solution. Thus, this project will not only focus on the business environment, but to all sectors, since the proposed software could also be able to be implemented in banks (biometric control) and airports (people search).

In this study, a facial recognition system using neural networks is proposed for access control in restricted areas that offers high accuracy in the identifi-

Reaño, R., Carrión, P. and Mansilla, J.
Access Control Using Facial Recognition with Neural Networks for Restricted Zones.
DOI: 10.5220/0012185800003584
In *Proceedings of the 19th International Conference on Web Information Systems and Technologies (WEBIST 2023)*, pages 310-318
ISBN: 978-989-758-672-9; ISSN: 2184-3252

cation of people. In addition, this system uses IP cameras where the facial characteristics of a person are analyzed and compared with a database of faces previously stored with the use of neural networks, also alerts are sent to the assigned users about their respective area.

The article follows a structure of five main chapters. Chapter I, Introduction, provides the context of the study and presents the problem to be addressed. The objectives of the study are established and the relevance of the topic is highlighted. Chapter II, Related Articles, includes a review of the literature and highlights previous work related to the research topic. Chapter III, Methodology, describes the project proposal and the algorithm used for face recognition. Chapter IV, Proposed Solution, details the solution or methodological approach used in the study; it also shows the physical and logical architectures of the solution. Chapter V, Results, presents the validation of the project, along with the costs and the optimality of the application with respect to other solutions. Chapter VI, Conclusions, discusses its implications and contributions to the field of study. In addition, Chapter VII, Recommendations, offers suggestions for future research and possible areas of improvement. This organizational structure provides a logical and coherent presentation of the study, from the introduction to the results obtained, to provide a clear and complete understanding of the research conducted.

## 2 RELATED ARTICLES

There are articles that are related to facial recognition recognition as presented by (Hussain and Al Balushi, 2020) that has an effective solution for real-time facial emotion classification using a deep learning model, with a classification accuracy of 89.76 percent. Also found were (Carlos-Roca et al., 2018) and (Rahmat et al., 2019) that present a recognition oriented system using machine learning techniques to detect and verify the identity of passengers through a camera and a car security system that uses facial recognition techniques to verify the identity of the driver respectively. It is important to mention that the project will focus on restricted areas, therefore we rely on the proposed by (Sridhar Chakravarthy et al., 2020) that a security access control system that uses facial recognition techniques to verify the identity of people entering a restricted area.

On the one hand, there is another line of articles that perform studies of access control using facial recognition such as the study performed by (Lopez-Lopez et al., 2021) where he proposes an approach for facial recognition that uses a limited dataset and a deep learning model that is trained autonomously to improve the accuracy of a real-time facial verification system, as well as (Junquera-Sánchez et al., 2021) in access control architecture that provides a more complete and adaptive solution for access management in security systems and can help prevent more sophisticated security threats. There are also studies where access control systems are applied as performed by (Mendez et al., 2021), which uses facial recognition techniques to verify the identity of people entering a restricted area; (Lee et al., 2020) and (Lee, 2021), who propose an access control system using facial recognition that can be used in standalone access control systems and propose a system with facial detection and recognition algorithms for identity verification of people trying to access a restricted area; (Abou Loume et al., 2022), who present a facial recognition system that uses a deep learning algorithm and a cloud service to identify a person and grant access to a door. In the other hand, we find articles where access control using facial recognition converges with the use of neural networks. For example, what is described by (Almabdy and Elrefaei, 2019) and (Elmahmudi and Ugail, 2019) where they describe different approaches based on convolutional neural networks (CNN) for face recognition, including feature extraction and image classification techniques, and a new deep face recognition method that uses imperfect facial images to improve recognition accuracy (Araujo et al., 2018). Following this idea, (Salama AbdELminaam et al., 2020) and (Durán Suárez, 2017) proposed a face recognition system that uses computational intelligence algorithms and deep learning techniques to improve face recognition accuracy. In addition, there are proposals using face recognition, using neural networks, for the creation of real-time face recognition system capable of recognizing faces even when wearing masks, proposed by (Kocacinar et al., 2022) and a system using cameras embedded in medical devices to capture facial images and verify the user's identity before allowing access to the device for patient monitoring via IoT, proposed by (Hussain et al., 2022) and (Hussain and Al Balushi, 2020).

## 3 METHODOLOGY

The development of this project was based on the neural network methodology developed by AWS Rekognition. Neural networks are a fundamental component in the field of deep learning, which is a branch of machine learning. These networks are composed of layers of interconnected nodes that simulate the functioning of the human brain. Each node, or artificial neuron, processes information and performs mathematical operations on the input data. In addition, AWS Rekognition uses convolutional neural networks (CNNs) for computer vision tasks, such as object and face detection, as well as face recognition and feature extraction. CNNs are particularly well suited for image analysis because of their ability to learn patterns and visual features at different levels of abstraction.

It is important to mention that convolutional neural networks are a deep learning architecture specially designed for computer vision tasks. These networks are composed of multiple layers, including convolutional layers, clustering layers and fully connected layers. Convolutional layers are responsible for extracting important visual features, such as edges, textures and patterns, through the convolution of filters in the image. These features are then used to classify and recognize visual elements in the images. (IBM, 2022)

Therefore, the project aims to develop and implement a system that allows the control and monitoring of people in restricted areas within small and medium enterprises. The proposed technological solution is a face recognition system that will be used by the security area within small and medium companies, given its flexibility for indoor environments. This real-time face recognition system will be based on the identification of people inside a restricted area and will validate through facial recognition if these people are within a whitelist (i.e., previously registered in the database), otherwise alerts will be sent to those responsible for internal security (via Email and WhatsApp). The development will use components of Cloud Computing, AWS Rekognition as mentioned above, for the processing of images in real time where access control will be performed in these restricted areas.

# 4 SOLUTION

## 4.1 Facial Recognition Application Using AWS Rekognition

**Facial Registration and Comparison with AWS Recognition:** This section presents an easy-to-use face recognition application that uses the AWS Rekognition service for face registration and comparison. The application consists of two main steps: face registration and face matching for user validation. The general procedure and the graph of the steps that make up the solution (Figure 1) is as follows:

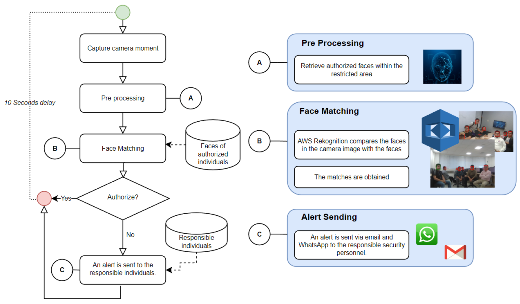

Capture camera moment
Pre-processing
A
10 Seconds delay
B
Face Matching
Faces of authorized individuals
Yes
Authorize?
No
Responsible individuals
C
An alert is sent to the responsible individuals.
Pre Processing
A
Retrieve authorized faces within the restricted area
Face Matching
B
AWS Rekognition compares the faces in the camera image with the faces
The matches are obtained
Alert Sending
C
An alert is sent via email and WhatsApp to the responsible security personnel.

Figure 1: Project architecture.

**Face Registration:** In the face registration process, images of the user's face are registered to the user. These images are sent to AWS Rekognition, which performs face detection and analysis. AWS Rekognition extracts facial features from the images and creates a unique face template for each registered user. The face template contains facial landmarks and feature descriptors that represent the user's face.

**Face Matching and Alert Generation:** During the user validation process, the application captures the camera image and sends it to AWS Rekognition for face matching. AWS Rekognition compares the captured face with the registered face templates stored in its database related to the area assigned to that camera. A similarity score is calculated between the two faces based on their facial features. If the similarity score exceeds a predefined threshold of 70%, the application considers that the user's face is a match. In this case, no alert is generated. However, if the similarity score is below the threshold, indicating a possible discrepancy, the application generates an alert via AWS Simple Notification Service (SNS). The alert is sent via mail and WhatsApp message to a designated administrator or security personnel, notifying them that there is an unauthorized person.

On the other hand, it is important to show the type of architectures that were used within the development of the project, in addition to show the interface of the web application of the facial recognition system. In this way, the following points are shown to reinforce the one described:

## 4.2 Physical Architecture

The physical architecture represents all the physical components of the system that meet the needs of the logical architecture and thus allow the correct operation and deployment of the project. The physical components, such as servers, resources, hardware, that play a role in the technological solution are shown, as well as the relationship between these components, as shown in Figure 2.

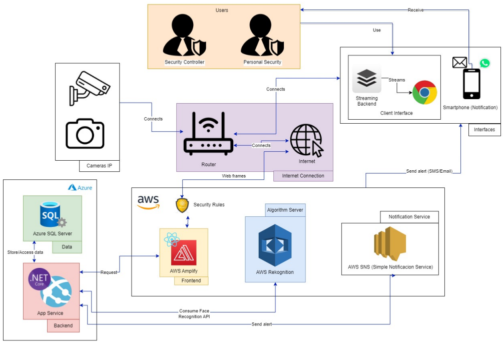


Figure 2: Project physical architecture.

### 4.2.1 Component Description

**Internal Devices**

- IP Cameras: These are video cameras that are designed to send audio and video signals over the Internet from a specific router.

**Users**

- Security Controller y Personal Security: SME users who will be able to use the system and/or receive alerts from unknown visitors.

**Internet Connection**

- Router: Router that enables local connections within the company and provides access to the Internet.
- Internet: A network of computers that are connected by the Internet, worldwide, in the form of a spider's web.

**Interfaces**

- Smartphone: Smart cell phone where notifications of alerts will be sent to users via WhatsApp or email.
- Browser client: Browser that will access the client of the technological solution.

**Data**

- Azure SQL Server: Microsoft Azure service that provides a database with the SQL Server engine. This Microsoft Azure service was chosen because it is much smaller than other services, according to Microsoft Azure (2022).

**Frontend**

- AWS Amplify: Amazon Web Services (AWS) resource that will contain the ReactJS frontend (client) of the technological solution.

**Backend**

- AWS Lambda: Amazon Web Services (AWS) resource that will contain the backend in .NET Core (Web API) of the technological solution.

**Algorithm Server**

- AWS Rekognition: Amazon Web Services recognition service. This system has the ability to recognize faces in images and videos. Through this, it is possible to obtain details about the location where a face was recognized in an image or video, as well as information about the position of the subject's eyes and any detected emotions (e.g., a happy or sad expression).

**Notification Server**

- AWS SNS: Amazon Simple Notification Service is a messaging service that is managed application-to-application (A2A) and application-to-person (A2P), as reported by (Services, 2022a).

**Security Rules**

- The security rules that will protect the integrity, confidentiality and availability of user and system data.

## 4.3 Logical Architecture

This section presents the description of the logical architecture, which represents all the layers of the system that satisfy the needs of the logical architecture and, in this way, allow the correct operation and deployment of the technological solution of the project, as shown in Figure 3 below.

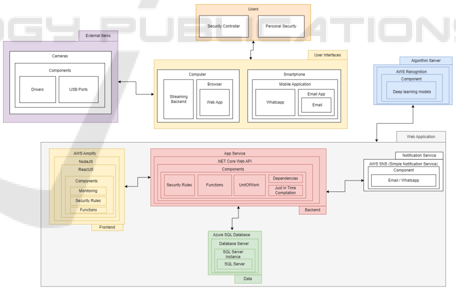


Figure 3: Project Logic Architecture.

### 4.3.1 Component description

**External Items**

- IP Cameras: These are video cameras designed to send video and audio signals over the Internet from a router.
  - Drivers: Drivers for compatibility with other external and internal devices.
  - USB Ports: USB ports for direct connection to other devices.

**Web Application**

- Azure SQL Server: Microsoft Azure service that provides a database with the SQL Server engine. This Microsoft Azure service was chosen over Amazon Web Services because of the price which is much lower, according to (Azure, 2022).
  - SQL Server Database: Database where all system information and facial recognition analysis will be stored.
  - SQL Server Instance: Database instance.
  - SQL Server: SQL language that will allow data queries.
- AWS Amplify: Amazon Web Services (AWS) resource that will contain the ReactJS frontend (client) of the technological solution.
  - Monitoring: Monitoring module within the technology solution that will allow reviewing the core business indicators.
  - Security Rules: Security rules that protect the confidentiality, integrity and availability of data.
  - Functions: Functions implemented within the development that allow to achieve the stated objective.
- AWS SNS: Amazon Simple Notification Service is a fully managed messaging service for application-to-application (A2A) and application-to-person (A2P) communication, according to (Services, 2022a).
  - Email / SMS Reminder: Internal service of the resource for sending notifications.

**Users**

- Personal Security y Security Controller: SME users who will be able to use the system and/or receive alerts from unknown visitors.

**Algorithm Server**

- AWS Rekognition: Amazon Web Services service for facial recognition. According to (Services, 2022b), Amazon Rekognition can detect faces in images and videos, as well as obtain information about where faces are detected in an image or video.
  - Face Recognition API: API that will allow facial recognition by comparing two photos.
  - Deep neural network models: Model used to perform face recognition.

**User Interfaces**

- Browser Client: Browser that will access the client of the technological solution.
  - Web App: Customer of the technological solution.
- Smartphone: Intelligent cell phone where alerts notifications will be sent to users by SMS or e-mail.
  - Message App: Cell phone messaging application.
  - Email App: Cell phone email application.

# 5 RESULTS

In this section, you can see the results of the project from the validation that was performed by testing the web application of the facial recognition system where neural networks were used for access control in restricted areas; in addition, the costs presented by this project are shown and finally how feasible its development is and how optimal this development becomes.

To validate the operation of the web application, a case study was conducted in May 2023 in a restricted area of the district of San Miguel, in the city of Lima, Peru. The important points are shown below:

## 5.1 Case Study

The web application was validated in an area that is considered a ”restricted zone” in the district of San Miguel - Lima, Peru, where we focused on facial recognition of people whose age ranges from 22 to 45. In these restricted areas, there is a total of 0 to 1 person who are located and perform their activities; in addition, the access control will be performed in case a person who does not belong to that area is identified and also, that the camera does not recognize the face of the identified person. Regarding clothing, we test that people have 2 or more clothes to validate the correct functioning of our application.

## 5.2 Standards Adaptation

In the validation, it will be important to develop our tests in places whose lighting is optimal, although it is not determinant since our web application recognizes without depending on this factor. Some of these rules are presented below:

**R01.** If the person IS registered (previously) in the database, the IP camera placed in the restricted area will show a green bordered box signifying that the person is authorized to be in the area.

**R02.** If the person is NOT (previously) registered in the database, the IP camera placed in the restricted area will show a box with red borders meaning that this person is not authorized to be in the place; you will also receive by e-mail and WhatsApp the message ”1 unknown face(s) was identified in the ABC zone of the T floor”.

## 5.3 Experimentation

The validation was carried out with a sample of 17 people, where the sample was grouped into 3 different groups. The first group consisted of 6 people; the second, of 7 people; and finally the third group, of 4 people. Facial recognition in these zones was carried out in a period of 1 minute, during which time we waited until the alert message was received by the owner (authorized person) of the restricted zone. It is important to note that the participants in this validation were asked for their consent for the use and manipulation of data in the development of this project.

Regarding the metrics, the following questionnaire with 8 questions, which are shown below, was made to the group of people who use the facial recognition web application in order to obtain results that show us if our application meets the solution to the identified need. On the other hand, this questionnaire was carried out in a form made in *Google Forms*, which can be found in the following link https://forms.gle/CmwnK21xEUqC4Tzn6:

***Questions***

**Q1.** Is the facial recognition web application easy to use?

**Q2.** Do you think the facial recognition web application is scalable?

**Q3.** Do you consider the facial recognition web application to have a clear and easy to understand user interface?

**Q4.** Is the facial recognition web application intuitive?

**Q5**. Does the facial recognition web application meet industry security standards?

**Q6.** Is the facial recognition web application accurate in identifying people?

**Q7.** How often do you consider using the facial recognition web application to monitor and control access to restricted areas?

**Q8.** Would you recommend the facial recognition web application to other users to control and monitor access control in restricted areas?

*The answers to these randomized questions following the Likert scale (0: not at all, 1: very little, 2: a little, 3: moderately, 4: a lot). (Joshi et al., 2015)*

### 5.3.1 Indicators

**False Positive and False Negative Rate:** False positive rate refers to the number of people who were registered within the database; however, they are not recognized by the cameras and show the alert, besides enclosing the face with the red box (1). On the other hand, false negative rate refers to the users previously registered but the IP camera encloses the face with green color (2).

It should be noted that these values are obtained per image. As a minimum value, it was proposed that the rate should not be higher than 5%, thus, we would be getting closer to the efficiency presented by the web application.

$$FalsePositiveRate = \frac{a}{b} \tag{1}$$

Where:

a: *Number of unregistered but identified persons (red box).*

b: *Total number of people identified in an image.*

$$FalseNegativeRate = \frac{c}{d} \tag{2}$$

Where:

c: *Number of people registered but not identified (green box).*

d: *Total number of people identified in an image.*

**Average Alert Response Time:** The alert response time corresponds to the indicator that gives us the subtraction of the time in which the alert was sent to the user (either by mail or WhatsApp) and the time in which the alert was created (3). It is important to mention that the internet speed and other factors that could affect the delay of this alert are not considered. It should be noted that these values are obtained by image.

The value determined as a limit is set at a time no longer than 10 seconds, so that, if this value is exceeded, it would not be optimal or beneficial for the user.

$$AlertResponseTime = TimeA - TimeB \tag{3}$$

Where:

TimeA: *Alert sending time in seconds.*

TimeB: *Alert creation time in seconds.*

**Average Face Recognition Response Time:** The facial recognition response time was found by subtracting the time in which the image processed by the camera was received by the cloud from the time in which the capture was created in the web application (4). It should be noted that these values are obtained per image. As with the previous indicator, it was established that the minimum allowable value (time) is no more than 8 seconds, so that our web application is useful and very functional.

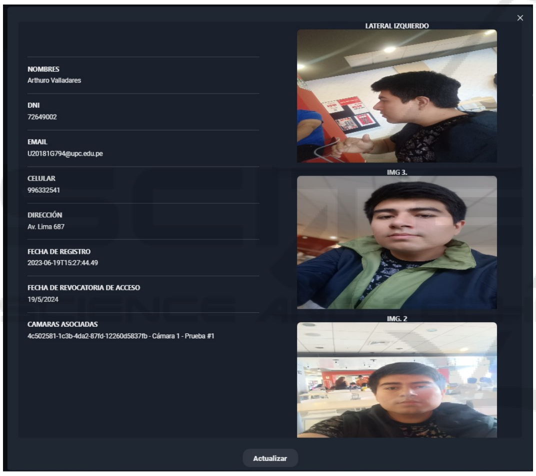
$$\text{Face Recognition Response Time} = \text{TiempoC} - \text{TiempoD} \tag{4}$$

Where:

TimeC: *Image reception time in seconds.*
TimeD: *Alert creation time in seconds.*

### 5.3.2 Results

Corresponding to the results obtained in the project, it is detailed that before performing facial recognition in the web application, the user was previously registered in the database (see Figure 4) so that he/she could be identified.


NOMBRES
Arthuro Valladares

DNI
72649002

EMAIL
U20181G794@upc.edu.pe

CELULAR
996332541

DIRECCIÓN
Av. Lima 687

FECHA DE REGISTRO
2023-06-19T15:27:44.49

FECHA DE REVOCATORIA DE ACCESO
19/5/2024

CAMARAS ASOCIADAS
4c502581-1c3b-4da2-87fd-12260d5837fb - Cámara 1 - Prueba #1

Figure 4: Prior registration of the user to the web application.

Previous to this registration, a first validation test was performed, as shown in Figure 5, to demonstrate that the user was neither identified nor previously registered in the face database and the web application issued an alert showing the face of the strangers inside the restricted area.

After that, a first validation was performed, in the same restricted area, with the same group of people (with the same characteristics as detailed in the section on experimentation) where it recognizes the registered user (green box) and does not recognize the other participants (red box) since they were not previously registered and the camera performs a correct facial recognition, as shown in Figure 6.

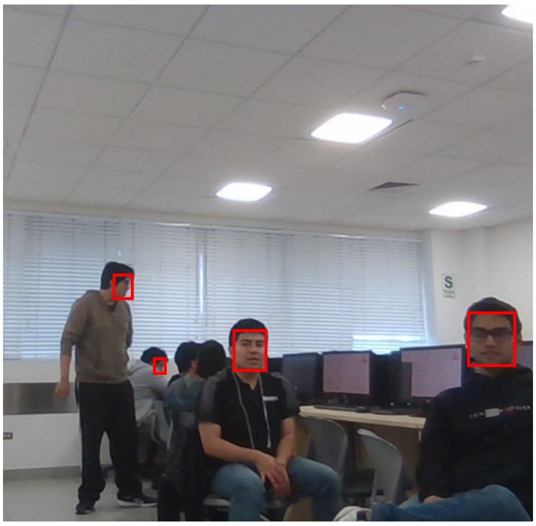


Figure 5: Test of alert sending by unregistered user.

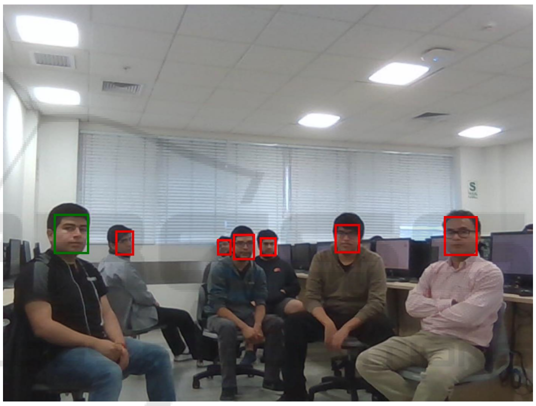


Figure 6: Image of first project validation.

On the other hand, the results obtained from the usability surveys, with the questions shown in the previous table, show a great acceptance of the web application by the 15 users who participated in the validation.

The results were based on showing the following information (see Figure 7) because the question was considered a vital indicator within the project; since, whether or not they would recommend the web application alerts, in summary form, how viable, effective and secure the application is for the users who used the web application.

The graph above shows that for question 8, the total number of people who consider that they would recommend the application ”Very much” is 66.7% (equivalent to 10 people), while 20% (3 people) consider that they would recommend the web application ”Moderately”; finally, the remaining 13.3% consider that they would recommend the application ”Not very much”.

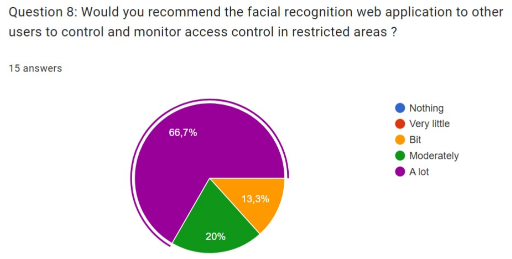


Figure 7: Question 8 pie chart.

## 6 CONCLUSIONS

The facial recognition system based on neural networks in IP cameras for access control of people in SMEs offers an effective and secure solution to strengthen security in facilities. Through the accurate and rapid identification of individuals, this system improves access control efficiency and reduces the risks associated with unauthorized entry. However, it is important to note that the successful implementation of this system requires a proper needs assessment and careful selection of IP cameras and face database.

In addition, supplementing the system with additional security measures and performing regular monitoring and maintenance to ensure its proper functioning over time is a way to enhance the final proposed solution, as the development of this project does. Therefore, 66.7% of the people who participated in the validation are willing to recommend the facial recognition system for access control.

## 7 RECOMMENDATIONS

Before implementing the system, it is important to evaluate the needs and problems that may be encountered in the sector to which the solution is to be provided. On the one hand, it is essential to select high quality cameras, with adequate resolution and image capture capacity to ensure accurate identification; it is also important to ensure optimal integration with the facial recognition software, as well as its use.

On the other hand, it is essential to perform regular monitoring and maintenance of this system to ensure its proper functioning, which involves verifying the calibration of the cameras, performing software updates, monitoring the database of faces and reviewing the access logs to detect any anomaly or attempted security breach in the sector in which this project was oriented. Finally, it is necessary that future research be based on this project since it can be oriented not only to the SME sector, but to any sector where the most successful solution is a new facial recognition system, also the sample size can be larger, in order to increase the metrics that benefit the development of the project.

## REFERENCES

Abou Loume, G., Abana, A. B., Tonye, E., and Kabiena, Y. (2022). Facial recognition in the opening of a door using deep learning and a cloud service. *International Journal of Intelligent Systems and Applications in Engineering*, 10(3):40–45.

Almabdy, S. and Elrefaei, L. (2019). Deep convolutional neural network-based approaches for face recognition. *Applied Sciences*, 9(20):4397.

Araujo, A., Pérez, J., and Rodriguez, W. (2018). Aplicación de una red neuronal convolucional para el reconocimiento de personas a través de la voz. In *Proc. Sexta Conferencia Nacional de Computación, Informática y Sistemas*, pages 77–81.

Azure, M. (2022). Azure SQL Database: servicio de base de datos en la nube administrado — Microsoft Azure — azure.microsoft.com. https://azure.microsoft.com/es-es/services/sql-database/campaign/#pricing.

Carlos-Roca, L. R., Torres, I. H., and Tena, C. F. (2018). Facial recognition application for border control. In *2018 International Joint Conference on Neural Networks (IJCNN)*, pages 1–7. IEEE.

Durán Suárez, J. (2017). Redes neuronales convolucionales en r: Reconocimiento de caracteres escritos a mano.

Elmahmudi, A. and Ugail, H. (2019). Deep face recognition using imperfect facial data. *Future Generation Computer Systems*, 99:213–225.

Hussain, S. A. and Al Balushi, A. S. A. (2020). A real time face emotion classification and recognition using deep learning model. In *Journal of physics: Conference series*, volume 1432, page 012087. IOP Publishing.

Hussain, T., Hussain, D., Hussain, I., AlSalman, H., Hussain, S., Ullah, S. S., and Al-Hadhrami, S. (2022). Internet of things with deep learning-based face recognition approach for authentication in control medical systems. *Computational and Mathematical Methods in Medicine*, 2022.

IBM (2022). ¿Qué son las redes neuronales convolucionales? — IBM — ibm.com. https://www.ibm.com/es-es/topics/convolutional-neural-networks.

Joshi, A., Kale, S., Chandel, S., and Pal, D. K. (2015). Likert scale: Explored and explained. *British journal of applied science & technology*, 7(4):396.

Junquera-Sánchez, J., Cilleruelo, C., De-Marcos, L., and Martinez-Herráiz, J.-J. (2021). Access control beyond authentication. *Security and Communication Networks*, 2021:1–11.

Kocacinar, B., Tas, B., Akbulut, F. P., Catal, C., and Mishra, D. (2022). A real-time cnn-based lightweight mobile masked face recognition system. *Ieee Access*, 10:63496–63507.

Lee, H., Park, S.-H., Yoo, J.-H., Jung, S.-H., and Huh, J.-H. (2020). Face recognition at a distance for a stand-alone access control system. *Sensors*, 20(3):785.

Lee, H.-W. (2021). Design of multi-functional access control system. *IEEE Access*, 9:85255–85264.

Lopez-Lopez, E., Regueiro, C. V., Pardo, X. M., Franco, A., and Lumini, A. (2021). Towards a self-sufficient face verification system. *Expert Systems with Applications*, 174:114734.

Mendez, D. F., Molina, M. V., Forero, M. G., and Lugo, C. (2021). Facial recognition system for security access control. In *Applications of Digital Image Processing XLIV*, volume 11842, pages 386–400. SPIE.

Nyein, T. and Oo, A. N. (2019). University classroom attendance system using facenet and support vector machine. In *2019 International conference on advanced information technologies (ICAIT)*, pages 171–176. IEEE.

Pan, Z., Shen, Z., Zhu, H., Bao, Y., Liang, S., Wang, S., Li, X., Niu, L., Dong, X., Shang, X., et al. (2021). Clinical application of an automatic facial recognition system based on deep learning for diagnosis of turner syndrome. *Endocrine*, 72:865–873.

Rahmat, R., Loi, M., Faza, S., Arisandi, D., and Budiarto, R. (2019). Facial recognition for car security system using fisherface method. In *Journal of Physics: Conference Series*, volume 1235, page 012119. IOP Publishing.

Salama AbdELminaam, D., Almansori, A. M., Taha, M., and Badr, E. (2020). A deep facial recognition system using computational intelligent algorithms. *Plos one*, 15(12):e0242269.

Services, A. W. (2022a). AWS — Servicio de notificaciones Push (SNS) — aws.amazon.com. https://aws.amazon.com/es/sns/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc.

Services, A. W. (2022b). Detecting and analyzing faces - Amazon Rekognition — docs.aws.amazon.com. https://docs.aws.amazon.com/rekognition/latest/dg/faces.html.

Sridhar Chakravarthy, G., Anupam, K., Harish Varma, P., Teja, G. H., and Rodda, S. (2020). Face recognition with voice assistance for the visually challenged. In *Intelligent Computing and Communication: Proceedings of 3rd ICICC 2019, Bangalore 3*, pages 701–709. Springer.

Talahua, J. S., Buele, J., Calvopiña, P., and Varela-Aldás, J. (2021). Facial recognition system for people with and without face mask in times of the covid-19 pandemic. *Sustainability*, 13(12):6900.

Xu, F. Z., Zhang, Y., Zhang, T., and Wang, J. (2021). Facial recognition check-in services at hotels. *Journal of Hospitality Marketing & Management*, 30(3):373–393.