Genoveva Vargas-Solar
EDITOR

CRITICAL FACTORS IN INDUSTRY 4.0

A Multidisciplinary Perspective

El Colegio de Chihuahua
Institución Pública de Investigación y Posgrado

Calle Partido Díaz 4723
Colonia Progresista, C.P.32310,
Ciudad Juárez, Chihuahua, México
Tel. 52 6566390397

Texto sometido a doble proceso ciego por académicos externos a esta institución.

Primera edición publicación electrónica 2021
ISBN: 978-607-8214-64-8

Coordinación editorial: E. Liliana Chaparro Vielma
Corrección: Carolina Caballero Covarrubias
Cubierta y diagramación: Karla María Rascón González

Editado en México/Edited in Mexico

Contents

CHAPTER 2

Facial Recognition & Fingerprint Based Authentication System for Industry 4.0 Cybersecurity

Francisco Enríquez[1,*], Jesus Silva[1], Salvador Noriega[1], Gabriel Bravo[1], Erwin Martínez[1]

[1]*Universidad Autónoma de Ciudad Juárez, Instituto de Ingeniería y Tecnología Av. del Charro no. 450 N, Col. Partido Romero, Ciudad Juárez, Chihuahua.*
**Corresponding Author: fenrique@uacj.mx*

Abstract. There is a growing demand for the use of digital information in present times. Thus, new challenges on cybersecurity like fending off attacks on vulnerabilities in current data storage systems. Industry 4.0 integrates technologies that handles private digital information, thus, the issues with cybersecurity are in the spotlight. The physical infrastructure—composed of: computers, routers, servers, switches, etc.—is one of the main aspects to consider. Its protection can be guaranteed through different means like the usage of biometric technologies to restrict access to a predetermined area, which is becoming crucial and stands out among other security techniques like the use of security guards, lockable doors, and those with electronic key access, etc. The application of digital image processing for facial and fingerprint recognition is presents throughout this work. Nonetheless, this chapter

ends with two low-cost proposals to control access to a given area that take advantage of facial and fingerprint recognition authentication technology.
Keywords: Cybersecurity, Fingerprint, Facial Recognition, Lattepanda, Biometry.

Introduction

The term cybersecurity is thoroughly revised in (Craigen et al., 2014), there, Craigen defines "cybersecurity" as "*[an] organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights*". This definition not only covers most of the ideas raised by various authors specialized in the cybersecurity field, but it also illustrates that a part of cybersecurity is access control to an installation that works with Information Technology (IT). Organizations such as the Information Technology Industry Council (ITI), the entity responsible for integrating cybersecurity principles for industry and government in the United States of America, comprises the world's leading technology companies. "*the Information Technology (IT) Industry refers generally to the technology industry, namely providers of computer and computer network hardware and software.*" (Council, 2011). Which basically consists of the hardware and software to be used in the IT. Although the software has security systems such as firewall, antivirus, etc., access to authorized personnel to the hardware is important to complement the IT security.

Three security components are mentioned in (Bishop, 2003):

1) **Requirements** (where the safety objectives are determined and they must answer the question "*What do you expect security can do for you*?")
2) **Policy** (determines the sense of security and must respond the question "*What steps do you take to reach the goal set out above?*")
3) **Mechanisms** (enforce policy and must answer the question"*What tools, procedures, and other ways do you use to ensure that the above steps are followed?*".

Moreover, to the components proposed by (Bishop, 2003), we can encompass the mechanism for protecting access to facilities by means of the following systems.

Biometry

Biometry can be defined as "*the statistical analysis of biological observations and phenomena*" (Merrian-Webster, n.d.). This concept covers the main topics studied in this chapter: facial and fingerprint recognition.

Fingerprint recognition

The fingerprint recognition process is a popular biometric method composed by enrollment and authentication. The former is when a human places a finger (generally the index finger), to a fingerprint sensor which is capable of capturing the image and, by means of a digital processor running Digital Image Processing (DIP), obtains a template. This template is subsequently stored into an internal memory to perform an authentication (Patel & Ramalingam, 2018). In accordance with (Maltoni, Maio, Jain, & Prabhakar, 2009), the fingerprint matching can be divided into three principal groups.

1) *Correlation - based matching*, where two fingerprint images are overlaid with reason of estimating the correlation between them, using diverse orientations. The *eq. 1* shows that the similarity *S* between the template (*T*) and the image (*I*) achieved from the sensor is given by the maximum cross-correlation (*CC*) of *T* and the rotation of *I* by an angle θ, shifted by Δx and Δy in direction x and y.

$$S(T, I) = \max_{\Delta x, \Delta y, \theta} CC(T, I^{\Delta x, \Delta y, \theta}) \quad (1)$$

2) *Minutiae - based matching*, the most commonly used method, consists of identifying the alignment between a template and the minutiae obtained from the acquired image. For this technique, it is necessary to find the maximum number of minutiae pairings and to calculate a feature vector (of variable length)—whose elements represent the fingerprint minutiae. The minutiae are represented normally as a triplet $m = \{x, y, \theta\}$ where x, y denote the minutiae position coordinates and θ represent the minutiae angle:

$$T = \{m_1, m_2, ..., m_m\}, \quad m_i = \{x_i, y_i, \theta_i\}, \quad i = 1...m$$

$$I = \{m'_1, m'_2, ..., m'_n\}, \quad m'_j = \{x'_j, y'_j, \theta'_j\}, \quad j = 1...n$$

Where the number of minutiae is represented by *m* in *T* and *n* in *I*. Nevertheless, to ensure a concordance between the T and I minutiae, a distance (*sd*) with minimum tolerance r_o must be presented (*eq. 2*) and in the same way there must be a minimum angular tolerance θ_o (*eq. 3*).

$$sd(m'_j, m_i) = \sqrt{(x'_j - x_i)^2 + (y'_j - y_i)^2} \leq r_0, and \quad (2)$$

$$dd(m'_j, m_i) = min(\mid \theta_j - \theta_i \mid, 360° - \mid \theta'_j - \theta'_i \mid) \leq \theta_0 \quad (3)$$

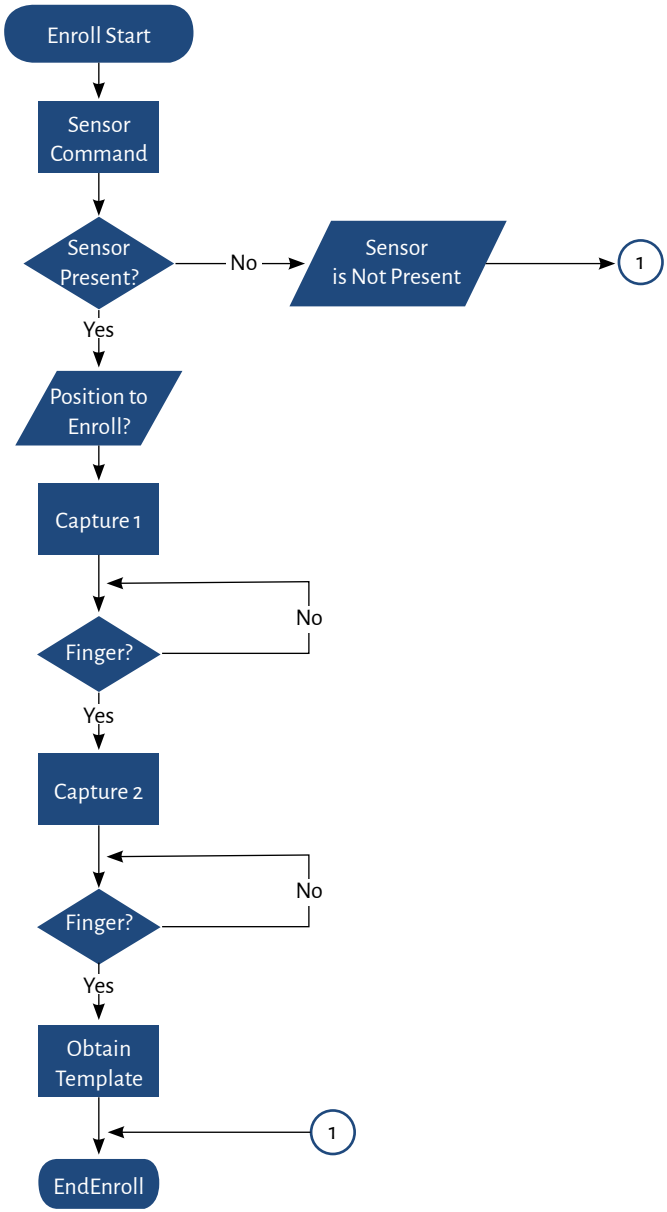
3) *Non Minutiae featured - based matching*. In this group, fingerprints are compared in accordance with features obtained from the ridge pattern. This technique is used with low-quality fingerprints images where the minutiae is almost impossible to detect, with fingerprints with small area and it also helps increase the system accuracy and robustness. *Non minute featured* has various match methods: geometrical attributes and spatial relationship of the ridge lines; number, type, and position of singularities; global and local texture information, etc. (Maltoni et al) indicates that "*the technique most popular to match fingerprint based on texture information remains the FingerCode approach by* (Jain, Prabhakar, Hong, & Pankanti, 2000)", represented by *eq. 4*.

$$V_{ij} = \frac{1}{n_i}\left(\sum_{C_i} \mid g(x, y : \theta_j, 1/10) \mid -\overline{g_i}\right) \tag{4}$$

Where C_i is the *ith* cell of the tessellation, n_i is the number of pixels in C_i, the Gabor filter is represented by *g()* and $\overline{g_i}$ is the mean value of *g* over the cell C_i.

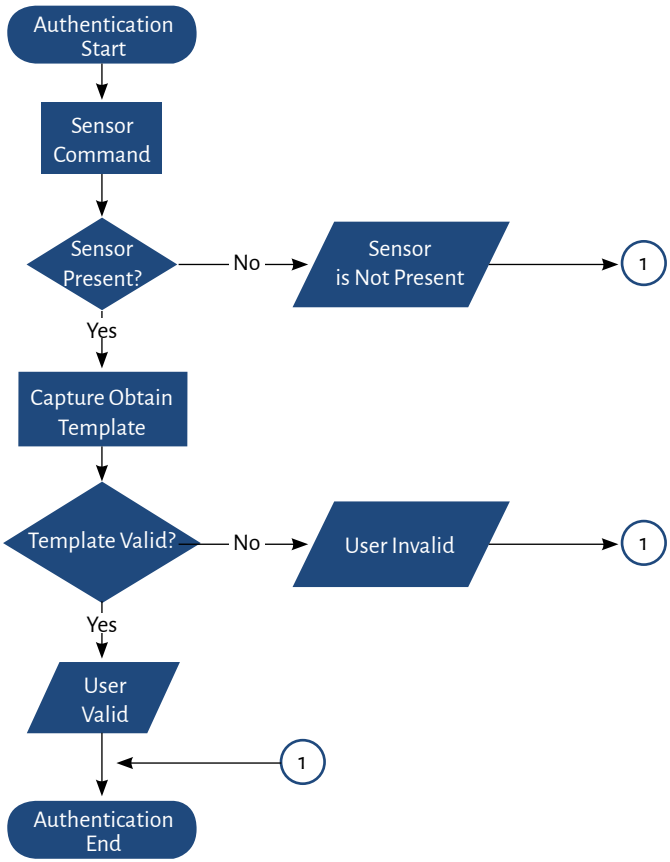
The flow charts for the enrolling and authentication in this work are showed in Figures 1 and 2 respectively. In Figure 1, you can see that it is necessary to acquire two images to obtain the user template to enroll. The sensor is a system that needs to receive messages via serial port and it is capable of making the process when it is indicated through a command.

Figure 1. *Data Flows for Enroll.*



Source: *Own elaboration.*

Figure 2. Data Flows for Authentication.



Source: Own elaboration.

Face recognition

Facial recognition is a technique used for identifying and verifying the identity of a person using DIP and interaction with the end user is not required. This procedure has been used in different situations, many authors have carried out the implementation of the Eigenface algorithm for face recognition in attendance system using Android and web technologies with geolocation extraction feature (Kurniawan, Wicaksana, & Prasetiyowati, 2017). The development of a facial recognition system with a mechanism for transmitting identification messages by e-mail was carried out by Okokpujie, Osaghae & Oputa in 2017. The attendance fraud is set to be reduced through the Fisherfaces algo-

rithm. In previous research, the facial recognition technology along with a physical access card, and a PIN were used to improve security in Automatic Teller Machines (ATM) (Eze, Gozie, & Aru, 2013).

OpenCV

Open Source Computer Vision Library (OpenCV) is a software library for computer vision and machine learning created by Intel®. OpenCV can be used for quick software development since the code can be modified and adapted to the user's needs (OpenCV, n.d.). With this tool you can implement computer vision algorithms like object detection, tracking, movement analysis, segmentation, 3D reconstruction, etc. (Yin & Yang, 2017). OpenCV main algorithms of facial recognition are: Eigenface, FisherFace and LBPFace.

These algorithms use characteristics or features extractions to search the coincidence between a patron image and an acquired image. The OpenCV libraries are distributed to Windows operating systems like Dynamic Link Library files (Shen, Yang, Wei, Chou, & Hu, 2017).

Eigenfaces

Eigenface is a facial recognition method that projects the space of an image linearly. Its algorithm needs eigenvalue and eigenvector estimate of a matrix, considering that a face image can be represented as a two-dimensional array of numbers (Turk & Pentland, 1991). To find the eigenfaces it can be done as follows (Kurniawan, Wicaksana, & Prasetiyowati, 2017):

Given $X = \{x_1, x_2, \ldots, x_n\}$ a random set of vectors with observations $x_i \in \Re^d$, where *n* is the number of images trained.

1) Take facial image $I_1, I_2, \ldots, I_M$ (training images). The facial image must be in the middle of the frame and has the same size.
2) Change each image matrix I_i in a vector Γ_i.
3) Estimate the average face vector Ψ *eq. 5*.

$$\Psi = \frac{1}{M}\sum_{i=1}^{M}\Gamma_i \tag{5}$$

4) Search the difference (ø) between the t rained image x_i and the mean μ, *eq. 6*.

$$\phi = \Gamma_i - \mu \tag{6}$$

5) Estimate the Covariant Matrix *S*, *eq.7*.

$$C = \frac{1}{M}\sum_{i=n}^{M}\phi_n\phi_n^T = AA^T(N^2 \times N^2 matrix) \quad (7)$$

where $A = [\phi_1, \phi_2, \phi_3 ... \phi_M](N^2 \times M\ matrix)$.

6) Estimate the eigenvalue λ and the eigenvectors Av_i from *C* (*eq. 8*).

$$A^T Av_i = \mu_i v_i \Rightarrow AA^T Av_i = \mu_i Av_i \Rightarrow$$
$$CAv_i = \mu_i Av_i \; or \; C\mu_i u_i \; where \; u_i = Av_i \quad (8)$$

7) Later the eigenvector *v* is achieved, the next step is estimating the eigenface μ.

$$\widehat{\phi_l} - mean = \sum_{j=1}^{k} w_j u_j, (w_j = u_j^T \phi_i \quad (9)$$

After finishing the eigenface training, it is possible to perform the facial recognition process. This procedure is done by calculating the Euclidian distance between the face training images and the face images acquired. Here, it is required to find the shortest distance and compare it against a threshold to know if the face is recognizable. Stages of face recognition are performed as follows:

i. An Eigenface is calculated from new face image Γ_{new}.

$$\mu_{new} = v(\Gamma_{new} - \psi) \quad (10)$$
$$\Omega = [\mu_1, \mu_2, ..., \mu_M] \quad (11)$$

ii. Estimation of the Euclidian distance between the new facial image with the facial images database.

$$e_d = \| \phi - \widehat{\phi} \| \quad (12)$$

iii. Search for the minimum distance, resulting from the calculations above, and compare it against the threshold, if it is lower, then the face is recognized.

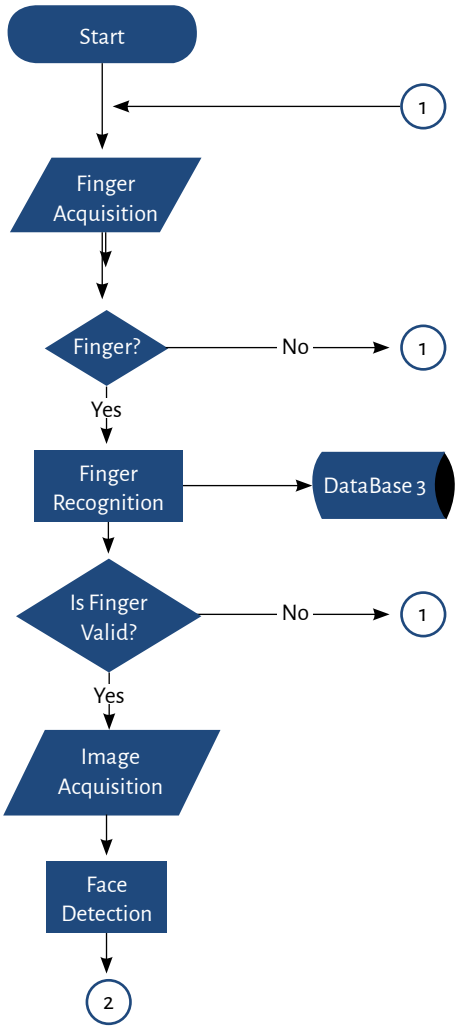
$$e_d < T_d \quad (13)$$

Case studies

The two requirements for the two study cases are to limit the use of facilities and equipment to people without authorization and to make a registry of the users who access the insured environment. The way to achieve these measure is by using a set of hardware and software, integrating the user validation procedures that can be performed by means of the dual biometrics presented in next section. The policy is to employ a dual biometrics system to find out if the person requesting entry is authorized. A record of any opening attempt will be made, informing if the entry was granted or denied.

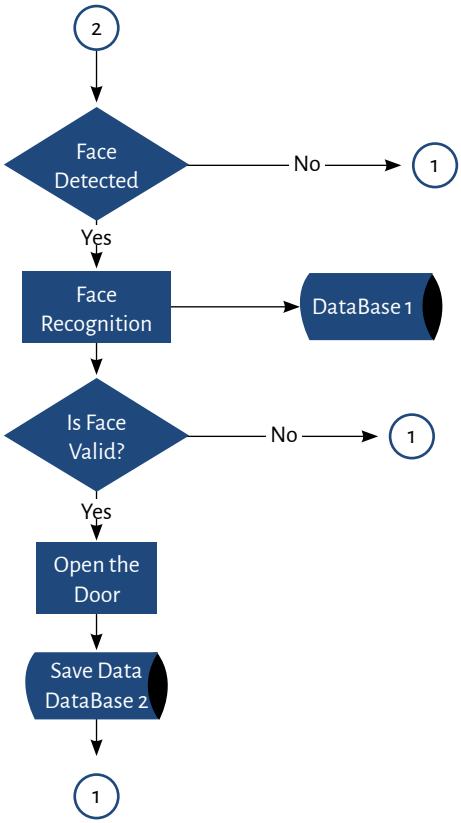
The Figures 3-a (first part) and 3-b (second part) show the data flow of the systems proposed, it indicates that the door opening is based on the sequential recognition of the fingerprint and the correct identification of the face. Even though the system could recognize the fingerprint of a user, it needs to recognize their face too. This configuration adds more security to grant the access to the computers room. It is not necessary to use an expensive camera to ensure that the picture is a real human. Additionally, the system takes a picture of the recognized face and sends it to the DataBase2, where the administrator could inspect it.

Figure 3-a. *Data flow of the system based in Lattepanda (first part of two).*



Source: *Own elaboration.*

Figure 3-b. *Data flow of the system based in Lattepanda (second part of two).*

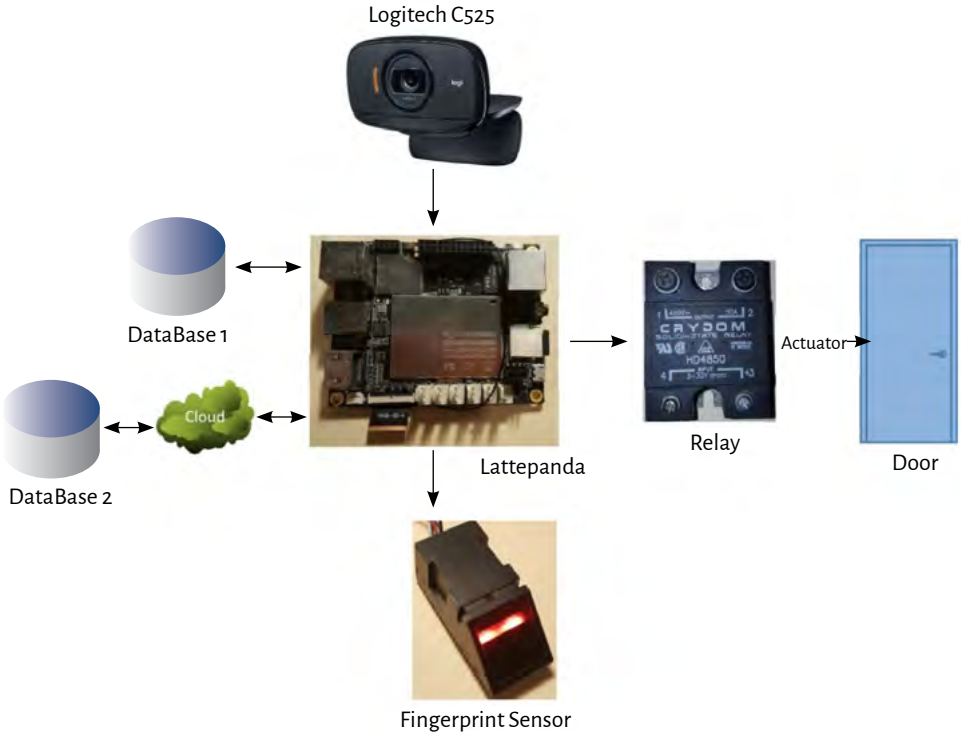


Source: *Own elaboration.*

Case 1 based in Lattepanda

In Figure 4 the case 1 is presented, the costs are obtained from www.amazon.com and the prices are in United States Dollar (USD).

Figure 4. *System architecture based in Lattepanda.*



Source: *Own elaboration.*

- Lattepanda 4GB/64GB. The first solution proposed is based in Lattepanda Board. It can connect to a USB camera, such as a Logitech C525, to acquire images, since it is run by Windows 10, it can execute programs made with C++. The program used in this board was coded in Visual Studio 2015, it uses OpenCV libraries to process the facial recognition with the help of the eigenfaces algorithm. It is equipped with an Intel Cherry Trail Z8350 Quad Core processor with three USB ports (two USB 2.0 and one USB 3.0) withintegrated Wi-Fi and Bluetooth 4.0. This device also includes an Arduino co-processor, which provides hardware acceleration for performing specific tasks, such as: control process, data acquisition, etc. and it costs $209.00 (Lattepanda, n.d.),

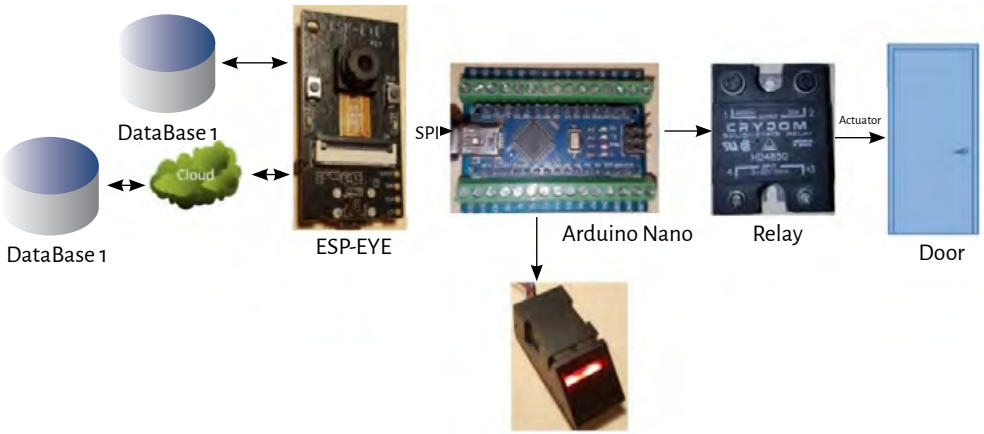
It is possible to connect an USB camera with Lattepanda to execute facial recognition in Windows 10. To do this one needs to connect the fingerprint sensor through the Arduino, control the relay to energize the actuator that allows door access and transfer data over a wireless and/or wired network, (Manoharan, 2019).

- Webcam Logitech C525. The webcam C525 is a foldable USB HD 720p video camera. This camera works at 30 frames per second but the most important feature is that it has autofocus, which allows to carry out facial recognition processing It costs $59.99 (Logitech, n.d.), (Bulpin, n.d.).
- ELP-USB0230X2-KV90. ELP Face Recognition & Biological Detection Dual Lens USB camera RGB has a 2 megapixels WDR AR0230 sensor with wide dynamic range up to 105dB. This camera can be used instead of the Logitech C525 since it has an IR sensor. Post-processing can be added to ensure that the image obtained is from a person who is physically at the location where the image was taken and not from a photograph. It is equipped with dual lens of two different output, one RGB (Red, Green and Blue) mode and another is IR (Infrared) mode. The camera is used in applications like face recognition, (Ailipu Techology Co., n.d.).
- DataBase1. The DataBase1 is used to store the user face images that have authorization to enter at computer room, this information is stored in Lattepanda´s memory.
- DataBase2.In DataBase2 information is stored in the Cloud, name, date, hour of the person that enter to the protected space and a picture of the user who gained access to the room, this data is accessible to authorized users.
- Fingerprint Sensor. With the optical Fingerprint Sensor, the image of fingerprint is acquired, processed and the verification (if the user is authorized to enter the computer room) by a Digital Signal Processor (DSP). The system can enroll and store up to 162 fingerprints in the onboard FLASH memory called DataBase3 This sensor costs $24.88 (Geralde et al., 2017), (Patent No. US 6,750,955 B1, 2004).
- Relay. The Solid State Relay (SSR) HD4850 is used to control with low voltage (5V from Microcontroller (µC) embedded in Lattepanda) the actuator that is responsible for door access and the activation of a buzzer. It has Silicon Controlled rectifier (SCR) output, zero voltage or instantaneous turn-on output, AC or DC control and only 7mA of maximum input current. It costs $72.45 (ready to use directly with µC) (CRYDOM, 2016), (Patent No. US 2020/0014379 A1, 2020).

Case 2 based in ESP-EYE

The second case study is based in ES-EYE board and is showed in the Figure 5, although this proposal is cheaper than case 1, it is also slower in terms of time for the facial recognition. Nevertheless, the time required is enough to make a facial recognition in a second approximately. The component that changes for this system are described below.

Figure 5. *System architecture based in ESP-EYE.*



Source: *Own elaboration.*

- ESP-EYE is a development board that combines the ESP32 chip with an artificial intelligence (AI) development framework. This board can be used for image recognition an audio processing in different applications. It has the capability of using ESP-WHO development framework, which was planned for Artificial Intelligence of Things (AIoT) applications. "It also supports image transmission via Wi-Fi and debugging through a Micro-USB port". It costs around $31.24 (ESPRESSIF, n.d.). This board replaces the Logitech C525 and the Lattepanda.
- Arduino Nano with terminal expansion adapter. The Arduino Nano is a small development board based in the UC ATmega328, which has 22 Digital input/output (I/O) pins, 8 Analog I/O pins, 1 serial port, etc. This board is capable of interconnecting with the fingerprint through the serial port, the SSR via the digital pin and with the ESP-EYE by means of a Serial Peripheral Interface (SPI) communication protocol. The Terminal expansion adapter is used to

connect wires easily using the pin screw terminal blocks, (Badamasi, 2014). This board is required because the ESP-EYE does not have serial port, neither digital pins (only a SPI port), which are required for connecting to the fingerprint and the relay. It cost around $14.19.

Conclusions

This chapter discusses the importance of using biometric data in the cybersecurity implemented for Industry 4.0 through the security of a company's physical infrastructure. From the proposed works Case 1, it is noted that the Lattepanda microcomputer has the advantage of being able to update the facial recognition algorithm, make use of another camera such as the ELP-USB0230X2-KV90 which it can confirm that a real person is in the acquisition of the image and that the size is relatively small. For Case 2, which is based on ESP-EYE, it is a better option in terms of cost and size. Furthermore, the algorithm that employs artificial intelligence is good for what is required, however, the camera and algorithm cannot be updated as easy as in Case 1.

References

Ailipu Techology Co., L. (n.d.). ELP-USB0230X2-KV90. Retrieved February 10, 2020, from http://www.webcamerausb.com/elp-face-recognition-biological-detection-dual-lens-usb-camera-rgb-ir-dual-output-ar0230-sensor-wdr-105db-webcam-with-led-ir-p-256.html

Badamasi, Y. A. (2014). The working principle of an Arduino. *Proceedings of the 11th International Conference on Electronics, Computer and Computation, ICECCO 2014*, 1–4.

Bishop, M. (2003). What is Computer. *Security & Privacy, IEEE*, 3–14.

Bulpin, J. (n.d.). *Control Viewing Access to Documents in Collaborative Scenerios Using Facial Recognition From Webcams*.

Che, F. (2004). *Patent No. US 6,750,955 B1*.

Council, I. T. I. (2011). The IT Industry's Cybersecurity Principles for Industry and Government. Retrieved from http://www.itic.org/dotAsset/be5a3449-8323-422c-aba2-6b1e8cd91f7e.pdf

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21.

CRYDOM, C. (2016). *Relay HD4850*.

ESPRESSIF, C. (n.d.). ESP-EYE. Retrieved October 2, 2020, from https://www.espressif.com/en/products/hardware/esp-eye/overview

Eze, O., Gozie, I., & Aru. (2013). Facial Verification Technology for Use In Atm Transactions. American Journal of Engineering Research (AJER), 02(05), 188–193.

Geralde, D. D., Manaloto, M. M., Loresca, D. E. D., Reynoso, J. D., Gabion, E. T., & Geslani, G. R. M. (2017). Microcontroller-based room access control system with professor attendance monitoring using fingerprint biometrics technology with backup keypad access system. *HNICEM 2017 - 9th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management*, *2018-Janua*, 1–7.

Jain, A. K., Prabhakar, S., Hong, L., & Pankanti, S. (2000). *Filterbank-Based Fingerprint Matching*. *9*(5), 846–859.

Kurniawan, V., Wicaksana, A., & Prasetiyowati, M. I. (2017). The implementation of eigenface algorithm for face recognition in attendance system. *Proceedings of 2017 4th International Conference on New Media Studies, CONMEDIA 2017*, *2018-Janua*, 118–124.

Lattepanda, C. (n.d.). 4G/64GB. Retrieved February 8, 2020, from https://www.lattepanda.com/products/3.html

Logitech, C. (n.d.). C525 HD Webcam. Retrieved February 8, 2020, from https://www.logitech.com/en-roeu/product/hd-webcam-c525

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of Fingerprint Recognition*.

Manoharan, S. (2019). a Smart Image Processing Algorithm for Text Recognition, Information Extraction and Vocalization for the Visually Challenged. *Journal of Innovative Image Processing*, *1*(01), 31–38.

Merrian-Webster. (n.d.). Biometry | Definition of Biometry. Retrieved February 24, 2020, from https://www.merriam-webster.com/dictionary/biometry

Okokpujie, K., Noma-Osaghae, E., John, S., & Oputa, R. (2017). Development of a facial recognition system with email identification message relay mechanism. *Proceedings of the IEEE International Conference on Computing, Networking and Informatics, ICCNI 2017*, *2017-Janua*, 1–6.

OpenCV, T. (n.d.). OpenCV. Retrieved February 26, 2020, from https://opencv.org/about/

Patel, R., & Ramalingam, S. (2018). Advances in fingerprint technology. *Biometric-Based Physical and Cybersecurity Systems*, 13–36.

Shen, Y., Yang, M., Wei, B., Chou, C. T., & Hu, W. (2017). Learn to Recognise: Exploring Priors of Sparse Face Recognition on Smartphones. *IEEE Transactions on Mobile Computing*, *16*(6), 1705–1717.

Telefus, M. (2020). *Patent No. US 2020/0014379 A1*.

Turk, M., & Pentland, A. (1991). Eigefaces for Recognition. *Journal of Cognitive Neuroscience*, *3*(1).

Yin, J., & Yang, X. F. (2017). 3D facial reconstruction of based on OpenCV and DirectX. *ICALIP 2016 - 2016 International Conference on Audio, Language and Image Processing - Proceedings*, 341–344.