Congr. Int. en Ing. Electrónica. Mem. ELECTRO, Vol. 40, pp. 20 - 25, Oct 2018, Chihuahua, Chih. México
http://electro.itchihuahua.edu.mx/memorias_electro/MemoriaElectro2018.zip
ISSN 1405-2172

CONTROL DE ACCESO A UN CENTRO DE DATOS USANDO TRES MECANISMOS DE SEGURIDAD

Vega Luna José Ignacio, Lagos Acosta Mario Alberto, Sánchez Rangel Francisco Javier, Cosme Aceves José Francisco, Salgado Guzmán Gerardo
Área de Sistemas Digitales, Dpto. de Electrónica, Universidad Autónoma Metropolitana-Azcapotzalco.
Av. San Pablo 180, Col. Reynosa, C.P. 02200, Cd. de México.
vlji@correo.azc.uam.mx

RESUMEN.

Se presenta un sistema de acceso para un centro de datos usando una tarjeta RFiD, un lector de huellas digitales y verificación de rostro. El objetivo fue diseñar un sistema compuesto por un módulo central y tres módulos distribuidos usando tres mecanismos de identificación. Los módulos se componen de una tarjeta Raspberry Pi 3, un lector de tarjetas RFiD, un lector de huellas digitales, una cámara de video y una pantalla táctil. La información de los usuarios se almacena en el módulo central en una base de datos MySQL, en la memoria flash del lector de huellas y en un directorio de fotografías. Cuando un usuario intenta acceder al centro de datos, la información de su identidad se transmite al módulo central para su validación. Se logró un alcance de 48 metros en la comunicación WiFi entre los módulos y el punto de acceso con línea de vista.

Palabras Clave: lector de huellas digitales, MySQL, pantalla táctil, Raspberry Pi 3, RFiD, WiFi.

ABSTRACT.

An access system for a data center is presented using an RFID card, a fingerprint reader and face verification. The objective was to design a system composed of a central module and three modules distributed using three identification mechanisms. The modules consist of a Raspberry Pi 3 card, an RFID card reader, a fingerprint reader, a video camera and a touch screen. The information of the users is stored in the central module in a MySQL database, in the flash memory of the fingerprint reader and in a directory of photographs. When a user tries to access the data center, their identity information is transmitted to the central module for validation. A range of 48 meters was achieved in the WiFi communication between the modules and the access point with line of sight.

Keywords: fingerprint reader, MySQL, Raspberry Pi 3, RFiD, touch screen, WiFi.

1. INTRODUCCIÓN

En un centro de datos se encuentran instalados equipos de cómputo, almacenamiento de información y telecomunicaciones usados en las operaciones cotidianas de empresas e instituciones. Es importante que los mecanismos de seguridad para el acceso a estas instalaciones sean confiables y rápidos para permitir al personal autorizado realizar labores de mantenimiento a los equipos. Los centros de datos cuentan con diferentes entradas donde se encuentran instalados dispositivos biométricos que validan la identidad de la persona que intenta acceder. Estos dispositivos son lectores de huellas digitales, de geometría de la mano, de iris, de patrón de retina, de reconocimiento facial, lectores de tarjetas magnéticas y teclados, entre otros. La mayor parte de los centros de datos usan uno o máximo dos dispositivos de este tipo [1]. El sistema aquí presentado se desarrolló para una organización que administra centros de datos. El objetivo fue implantar un sistema de acceso con tres mecanismos de identificación de usuarios: una tarjeta RFiD (Radio Frequency Identification), la huella digital y la verificación del rostro. El módulo central se instaló en la oficina de control y los módulos distribuidos en tres puertas de acceso al centro de datos. La comunicación entre los módulos se llevó a cabo usando un punto de acceso WiFi instalado en el centro de datos. La distancia de la puerta más lejana al punto de acceso son 30 metros. Los dos tipos de módulos están integrados por un lector de tarjetas RFiD, un lector de huellas digitales, una cámara de video, una pantalla táctil y una tarjeta Raspberry Pi 3. A través de la interfaz gráfica, implantada en la pantalla táctil, el administrador del sistema puede dar de alta, remover o realizar cambios de usuarios. La información del usuario se almacena en el módulo central en una base de datos, las imágenes de las huellas digitales en la memoria flash del lector de huellas y los rostros en un directorio de imágenes entrenadas. Cuando un usuario intenta acceder a través de una puerta, los módulos distribuidos transmiten al módulo central el identificador único universal (UUID) leído de la tarjeta RFiD, la imagen de la huella digital y la fotografía del rostro para su validación. El primer mecanismo de seguridad fue a través de una tarjeta RFiD. La tecnología NFC (Near Field Communication) surgió por la combinación de la tecnología RFiD y las tarjetas inteligentes. Permite la identificación y caracterización de personas u objetos sin contacto físico usando las ondas de radio transmitidas por una etiqueta, permitiendo el intercambio de información entre objetos ubicados cerca uno del otro. Esta tecnología continúa siendo de las más seguras, ya que el transmisor y receptor están estrechamente acoplados y próximos, con una cercanía máxima de 10 centímetros y no necesita que se ejecute una aplicación [2]. El segundo mecanismo de seguridad fue de tipo biométrico identificando la huella digital del usuario. Actualmente, bastantes sistemas de control de acceso biométrico usan lectores de huellas digitales, ya que proporcionan un mecanismo de identificación sencillo, confiable y de bajo costo. La mayoría de estos lectores integran un sensor óptico y un

procesador digital de señales para capturar la imagen de la huella digital de una persona. La imagen es caracterizada y convertida a una plantilla. La plantilla es una caracterización general de la huella digital y una vez creada se almacena en la memoria flash del lector asignándole un identificador (ID). A este proceso se le conoce como registro (enrollment). El ID de la plantilla se usa para su búsqueda, remoción o comparación con otra platilla. La memoria flash funciona similar a una base de datos de imágenes [3]. El tercer mecanismo de seguridad, también de tipo biométrico, verifica el rostro del usuario. Los recientes avances tecnológicos de la computación han permitido el desarrollo de algoritmos, técnicas y aplicaciones no intrusivas de reconocimiento facial automatizado más seguros y rápidos para identificar una persona usando una imagen digital [4]. Esto se realiza con uno de dos propósitos: 1) Verificación o autenticación del rostro, comparando una imagen del rostro de la persona con otra imagen almacenada en un conjunto de imágenes conocidas como imágenes de entrenamiento. La aplicación confirma o niega la identidad del rostro y 2) Identificación o reconocimiento de rostros, comparando la imagen de un rostro no conocido con las imágenes de rostros conocidos almacenados en una base de datos para determinar su identidad. El reconocimiento facial es un área que integra las siguientes tecnologías: procesamiento de imágenes, visión por computadora, reconocimiento de patrones, redes neuronales y aprendizaje de máquinas. El procedimiento usado por los sistemas de reconocimiento facial consiste de manera general de cinco fases: 1) Registro, se captura la imagen del rostro de la persona usando una cámara fotográfica o una cámara de video, 2) Procesamiento de la imagen, se alinea el rostro basándose en algunas propiedades geométricas y se obtiene una imagen independiente de la iluminación y gama de colores de la imagen original, 3) Extracción de información biométrica, se obtienen las características faciales como un patrón biométrico, 4) Comparación, el patrón biométrico se compara con el patrón de imágenes de rostros almacenadas en la base de datos. Se determina el porcentaje de similitud de la persona a identificar respecto a las imágenes de la base de datos y 5) Toma de decisiones, utilizando una matriz de similitudes, se identifica la persona que resultó con mayor porcentaje de similitud de la base de datos usando un rango establecido [5]. En los últimos años las técnicas de reconocimiento facial han mejorado bastante en exactitud, rapidez y confiabilidad aplicándose en diversas áreas de la vida humana, tales como: salud y tratamientos médicos [6-7], dispositivos móviles [8], sistemas de seguridad domésticos [9] y sistemas de video vigilancia [10]. Microsoft aplica reconocimiento facial para acceder a una computadora con Windows y Facebook y Google están desarrollando algoritmos de reconocimiento facial usados para etiquetar amigos y encontrar fotos de una persona. En 2015 Google presentó el sistema de reconocimiento facial denominado FaceNet el cual tiene una precisión de 99.63% al reconocer fotos en Google+ [11]. Este sistema usa aprendizaje de maquina generando un mapa en un espacio Euclidiano compacto a partir de la imagen de un rostro humano, donde las distancias corresponden directamente a la medida de similitud del rostro. Con este espacio, las tareas de verificación y reconocimiento de una imagen, se pueden realizar fácilmente usando técnicas estándar como la de vectores de FaceNet embeddings. El sistema FaceNet usa una red neuronal convolucional profunda entrenada con más de 260 millones de imágenes de rostros. Los autores de FaceNet indican que han desarrollado el estado del arte de los métodos de reconocimiento facial usando solo 128 bytes para cada rostro y más de 13,000 imágenes de rostros de la Internet para verificar si dos imágenes son la misma persona, mientras que el sistema de reconocimiento YouTube Faces logra 95.12%. Por su parte, Facebook usa la herramienta llamada DeepFace para reconocimiento facial, la cual fue desarrollada por la compañía face.com y liberada en 2013 [12]. Esta herramienta tiene una precisión de 97.25% comparando dos rostros humanos. Se pueden implantar sistemas de acceso confiables sin usar algoritmos tan sofisticados como los desarrollados y patentados por compañías como Google y Facebook que son el estado del arte y de uso exclusivo. Existen bastantes algoritmos implantados a través de código abierto que pueden ejecutarse en una computadora pequeña, de bajo costo y poderosa como la tarjeta Raspberry Pi 3 B+. Uno de estos algoritmos es el de histograma de gradientes orientados (HOG-Histogram of Oriented Gradients) [13]. Este algoritmo se desarrolló en 2005, es de los más avanzados y continuamente se incorporan mejoras para optimizarlo y lograr mayor precisión. Un HOG es un descriptor de características usado en visión por computadora y procesamiento de imágenes para la detección de objetos. Este algoritmo cuenta las ocurrencias de orientación de gradientes en partes definidas de una imagen. Los descriptores pueden utilizarse como datos de entrada o características para un algoritmo de aprendizaje de máquina. Existen bibliotecas de código abierto para implantar las fases de un sistema de reconocimiento facial con el algoritmo HOG y aprendizaje profundo de máquina, las cuales son fácil de instalar y utilizar optimizando la ejecución del programa [14]. Una de estas bibliotecas es *Face_Recognition*, la cual usa *dlib* y una red neuronal entrenada. Dlib es la herramienta estado del arte en reconocimiento de rostros construida con aprendizaje profundo. Los autores de *Face_Recognition* indican que su precisión es de 99.38% y proporciona varias funciones para realizar acciones tales como: encontrar rostros en una fotografía, determinar la ubicación de los puntos de referencia de un rostro, manipular las características faciales de un rostro, codificar biométricamente un rostro, comparar dos rostros codificados, reconocer rostros en video de tiempo real y reconocer rostros localizados en una fotografía usando un directorio de fotografías de personas obteniendo el nombre de cada una. Las funciones de *Face_Recognition* se pueden invocar en un programa en Python y requieren que se encuentre instalada la biblioteca de Python para *picamera (python3-picamera)*, *dlib* v19.6 y OpenCV.

En este trabajo, se usó una tarjeta Raspberry Pi de costo un poco mayor a otras de su tipo, debido a que el sistema operativo Raspbian, similar a casi todas las distribuciones de Linux, incorpora Python. Desde Python se puede usar una gran cantidad de bibliotecas disponibles en la comunidad de software libre. La Raspberry Pi dispone de más recursos hardware que otras tarjetas. La aportación de este trabajo es que implanta tres mecanismos de identificación utilizando componentes de reciente tecnología y bajo costo, donde todo el software es de código abierto y la comunicación es a través de WiFi, tecnología inalámbrica no intrusiva que no modifica las instalaciones del centro de datos. Los sistemas de este tipo usados actualmente implantan solo dos mecanismos de seguridad donde uno o los dos son biométricos [15] y muy pocos usan reconocimiento facial 3D [16] cuyo costo de implantación es demasiado elevado.

2. DESARROLLO

La metodología seguida para el desarrollo del sistema consistió en dividirlo en dos tipos de módulos: el módulo central y los módulos distribuidos como se muestra en la arquitectura del sistema de la Figura 1. Posteriormente, el sistema fue diseñado e implantado seleccionando los componentes adecuados de menor costo para realizar la funciones de cada módulo.

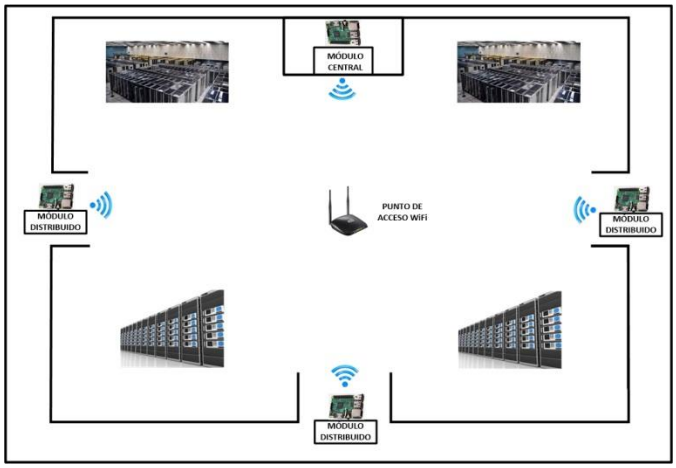

Fig. 1. Arquitectura del sistema desarrollado

2.1. El módulo central.

Los dos tipos de módulos del sistema tienen la arquitectura mostrada en la Figura 2. Están integrados por: una tarjeta Raspberry Pi 3 B+, un lector de tarjetas RFiD, un lector de huellas digitales, una cámara de video y una pantalla sensible al tacto. El módulo central cuenta con el lector RFiD y los dispositivos biométricos para dar de alta o realizar cambios en la información de usuarios. Las funciones del módulo central son las siguientes: mantener actualizadas la base de datos de usuarios, la memoria flash del lector de huellas digitales, el directorio de imágenes entrenadas e implantar la interfaz gráfica a través de la cual el administrador accede la información de usuarios.

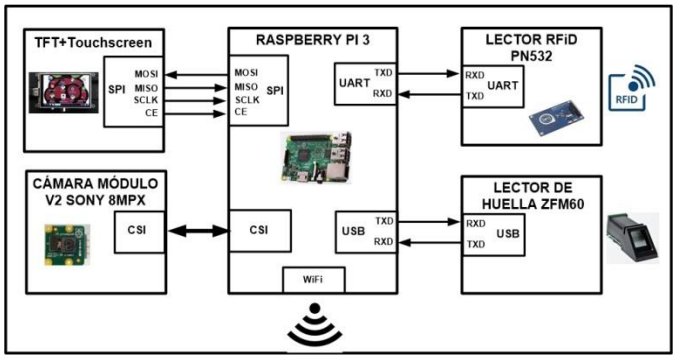

Fig. 2. Arquitectura del módulo central

La base de datos de usuarios y directorio de imágenes se encuentran creados en la memoria SD de 16 GB de la tarjeta Raspberry Pi, donde se instaló además el sistema operativo Raspbian kernel 4.9. El lector de tarjetas RFiD usado es el dispositivo NFC/RFiD PN532. Puede escribir tarjetas y etiquetas RFiD tipo 1 a 4 e integra una antena cuyo alcance son 10 centímetros. Se utilizó la biblioteca de funciones *libnfc* versión 1.7.0 para controlar y acceder al NFC/RFiD PN532. El lector RFiD se conectó a un puerto UART de la Raspberry Pi. Para leer la huella digital del usuario se usó el dispositivo ZFM60 de ZhianTec. Este lector se conectó a un puerto USB de la Raspberry Pi a través un convertidor TTL-USB comunicándose con la tarjeta usando un protocolo propietario de tipo orden-respuesta. El puerto UART del ZFM60 se configuró para trabajar a una velocidad de 57,600 bps. El lector ZFM60 presenta un tiempo de captura de imagen de la huella digital menor a 1 segundo, genera una plantilla de 512 bytes para cada huella y puede almacenar hasta 1,000 plantillas. La comunicación entre la Raspberry Pi y el lector ZFM60 se implantó utilizando la biblioteca de funciones *pyfingerprint*. Las funciones de la biblioteca *pyfingerprint* usadas en los dos módulos del sistema son las siguientes: *finger.get_image()*, para obtener la imagen de una huella digital, *finger.image_2_tz(1)*, para caracterizar la imagen, generar la plantilla y depositarla en un buffer, *f.storeTemplate(0)*, para almacenar la plantilla que se encuentra en un buffer a memoria flash, retornando el ID del registro, *f.deleteTemplate(positionNumber)*, para remover una plantilla dado su ID, *finger.finger_fast_search()*, para buscar una plantilla en memoria flash y compararla con otra contenida en un buffer y *f.uploadCharacteristics(0x01, eval(characterics)*, para cargar o almacenar en memoria flash una plantilla almacenada en un buffer. La pantalla táctil utilizada fue el dispositivo Pi+TFT de 3.5", el cual tiene una resolución de 480x320 y se conectó al puerto SPI de la tarjeta

Raspberry Pi. En la interfaz gráfica, el administrador puede realizar las siguientes operaciones: altas, bajas y cambios de usuarios, así como mostrar los usuarios registrados en la base de datos. La interfaz gráfica se realizó usando *pygame*. La herramienta *pygame* es un conjunto de bibliotecas que pueden usarse en un programa de Python para la implantación de videojuegos, programas multimedia e interfaces gráficas de usuario. La dirección IP de la interfaz WiFi de cada módulo de acceso es fija y es usada para identificar el número de puerta en la que está intentando el usuario acceder. La base de datos de usuarios se implantó usando el manejador MySQL. En la base de datos se creó una tabla que contiene los registros de usuarios. Cada registro almacena el UUID de la tarjeta RFiD asignada, el ID de la plantilla de la huella digital, el número de puertas a las que tiene acceso, nombre, compañía y correo electrónico del usuario. Para crear la base de datos y tabla de usuarios se llevaron a cabo las siguientes tareas: 1) Instalación del servidor y cliente de MySQL, así como el API de Python para acceder MySQL y 2) Creación de la base de datos. Una vez creada la base de datos, se realizó una rutina en Python, invocada desde la interfaz gráfica, para acceder la información de usuarios. Python usa un objeto o estructura de datos, llamada cursor, para acceder los datos de la tabla. Este objeto permite realizar operaciones de creación, lectura, actualización y remoción de registros en la base de datos. La rutina ejecuta de manera general las siguientes acciones: A) Importa el API de Python para MySQL, B) Realiza la conexión a la base de datos, 3) Define el objeto cursor, 4) Espera la opción seleccionada por el usuario en la interfaz gráfica, 5) Dependiendo la opción, define uno de los siguientes query's de sql: *cursor.execute*, *cursor.execute* o *cursor.execute* y 6) Ejecuta el query con *db.commit()*. Los módulos del sistema contienen una cámara de video para Raspberry V2 conectada a la interfaz CSI de la Raspberry Pi 3 B+. Esta cámara cuenta con un sensor de alta resolución Sony IMX219 de 8 Megapixeles. Permite capturar fotografías con una resolución máxima de 3238x2464 y video de alta definición. Existen bibliotecas de código abierto para usar la cámara y manipular fotos y video que pueden invocarse desde Raspbian o desde un programa en Python como la biblioteca *python-picamera* de Python, la cual contiene la función *camera.capture('archivo.jpg')* para capturar la imagen del rostro de un usuario en un archivo JPEG. En el directorio de imágenes entrenadas, el nombre de cada archivo corresponde al nombre del usuario registrado en la base de datos MySQL. Para verificar si la imagen del rostro del usuario, enviada por un nodo de validación, se encuentra en el directorio de imágenes se realizan las siguientes acciones: cargar en un *buffer* la imagen del rostro recibida utilizando la función *face_recognition.load_image_file*, codificar y aprender a reconocer la imagen almacenada en el *buffer* usando la función *face_recognition.face_encodings* y entrar a un ciclo donde se compara la imagen codificada del *buffer* con cada imagen codificada del directorio, el ciclo termina cuando se encuentra igualdad entre las dos imágenes analizadas o cuando se exploró el directorio completo sin encontrar igualdad. La comparación se realiza a través de la función *face_recognition.compare_faces*, la cual obtiene, en caso de ser exitosa, el nombre del usuario de la fotografía. Si el nombre obtenido es igual al nombre leído del registro del usuario en la base de datos, el usuario tiene acceso autorizado. La imagen recibida del módulo distribuido solo contiene un rostro, de lo contrario tendría que usarse la función *face_recognition.face_locations* para encontrar rostros en la imagen y codificarlos individualmente.

La programación de ambos tipos de módulos del sistema se realizó en Phyton 3.6. El programa principal del módulo central configura los temporizadores, el puerto UART, la interfaz WiFi, inicializa el lector de huellas digitales y la cámara de video, invoca la rutina de recepción de mensajes y entra a un ciclo donde implanta la interfaz gráfica. La comunicación entre los módulos distribuidos y el módulo central se llevó a cabo usando intercambio de mensajes con sockets bajo el esquema cliente-servidor, el módulo central es el servidor y los módulos distribuidos son los clientes. La rutina de recepción de mensajes ejecuta un programa en segundo plano para crear un socket a través del cual el módulo central recibe de los módulos distribuidos el UUID de la tarjeta RFiD del usuario, la plantilla de la huella digital y la fotografía del rostro. Se utilizó la función *finger.finger_fast_search()* de la biblioteca *pyfingerprint* para buscar la plantilla recibida en la memoria flash del lector. Después de validar la identidad del usuario, esta rutina transmite un mensaje al módulo distribuido para indicar si el acceso es permitido o negado. En la Figura 3 se indica el diagrama de flujo usado para implantar el programa principal.

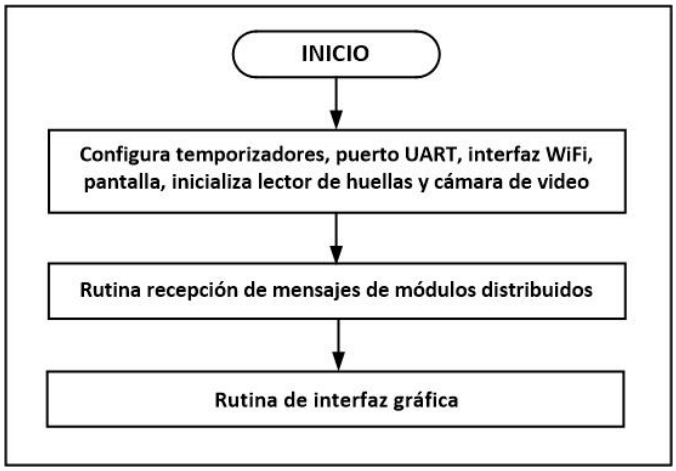

Fig. 3. Arquitectura del módulo central

2.2. Los módulos distribuidos.

Se construyeron tres módulos distribuidos. Estos módulos cuentan con componentes iguales al módulo central y son usados para obtener la identidad del usuario. En la pantalla táctil se muestran los mensajes del sistema dirigidos al usuario. La función principal de los módulos distribuidos es explorar continuamente el lector RFiD para determinar si se encuentra una tarjeta en su alcance. En caso afirmativo, se lee el UUID de la tarjeta, se captura la imagen de la huella digital y la fotografía del rostro del usuario. El programa principal realiza las siguientes tareas: configura los temporizadores, el puerto UART, la interfaz WiFi, inicializa el lector de huellas digitales y cámara de video y entra a la rutina de lectura de tarjetas RFiD. La rutina de lectura de tarjetas RFiD se encuentra en un ciclo continuo realizando las siguientes actividades: 1) Muestra en la pantalla táctil el mensaje que indica al usuario colocar la tarjeta RFiD en el lector, 2) Explora cada 0.5 segundos el lector RFiD ejecutando la función *nfc-pool_8c*, 3) Al leer el UUID de una tarjeta muestra en la pantalla táctil el mensaje indicando que se debe colocar el dedo en el lector de huella digital, 4) Invoca las funciones *finger.get_image()* y *finger.image_2_tz(1)* para capturar la imagen de la huella y generar en un buffer la plantilla correspondiente, 5) Muestra en la pantalla táctil el mensaje indicando al usuario colocarse frente a la cámara de video, 6) Captura la imagen del rostro del usuario en un archivo JPEG usando la función *camera.capture('archivo.jpg')*, 7) Transmite al módulo central, a través de un *socket*, la información de identidad del usuario y 8) Espera en el *socket* la respuesta del módulo central. Si la respuesta indica que el usuario está autorizado a entrar, el módulo distribuido activa el actuador de la puerta de acceso a través de la interfaz conectada a una terminal GPIO de la tarjeta Raspberry. Ya sea que el acceso sea autorizado o negado, se muestra en la pantalla táctil el mensaje correspondiente. En la Figura 4 se muestra el diagrama de flujo usado para realizar este programa.

3. RESULTADOS

Se registraron 60 usuarios en el módulo central. Y se realizaron tres grupos de pruebas. El objetivo del primer grupo fue comprobar la lectura correcta de huellas digitales en los módulos distribuidos. Para llevar a cabo estas pruebas se capturaron imágenes de la huella digital, en diferentes posiciones, de 20 usuarios en cada módulo distribuido y se transmitieron al módulo central para determinar si estaban registradas en la memoria flash del lector del módulo central. La mayoría de reconocimientos fueron exitosos pues la plantilla creada al capturar la imagen es una caracterización general de la huella y permite variaciones en la posición del dedo. Los reconocimientos no exitosos sucedieron cuando el usuario tenía sucio el dedo o húmedo. El fabricante del lector de huellas indica que esta respuesta es la esperada recomendando repetir el proceso con el dedo limpio. El segundo grupo de pruebas tuvo como objetivo medir el tiempo de respuesta del sistema. Para llevar cabo estas pruebas se registró en un archivo en cada módulo distribuido la hora de lectura de identidad, tarjeta RFiD, huella digital y rostro, de 20 usuarios autorizados y no autorizados a acceder y la hora de apertura de la puerta. El tiempo de respuesta fue 90 ms. en promedio. El tercer grupo de pruebas tuvo como objetivo medir el alcance de la transmisión WiFi de los módulos del sistema. Se tomó un módulo distribuido y se ubicó en diferentes puntos del centro de datos, a diferentes distancias del punto de acceso WiFi Cisco WAP4410N.

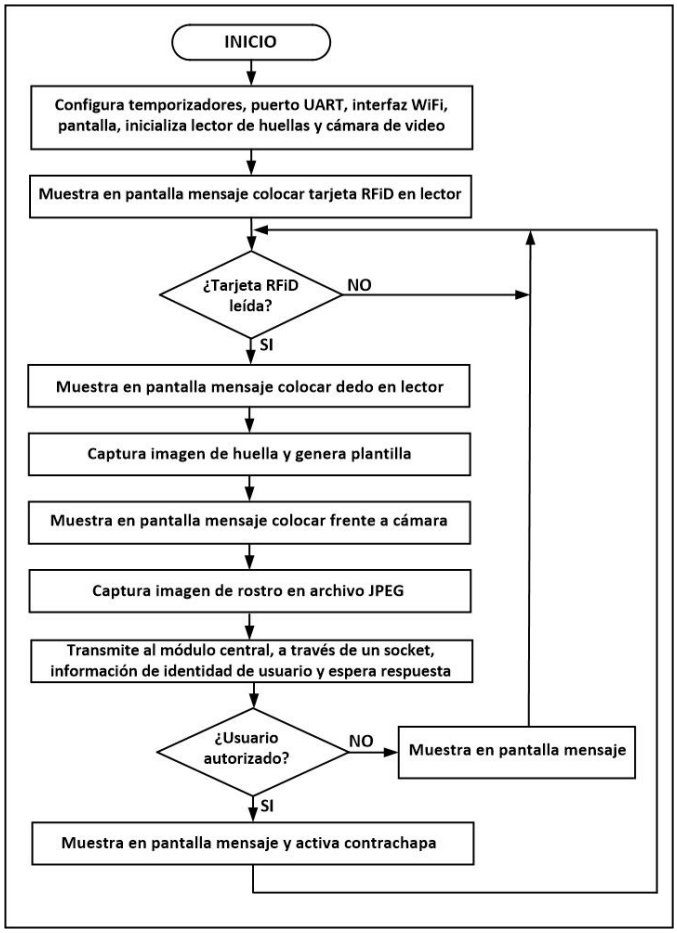

Fig. 4. Diagrama de flujo del programa de los módulos distribuidos

Se realizaron dos programas que se ejecutaron en el módulo. El primer programa se ejecutó en segundo plano y se encargó de transmitir continuamente un archivo al módulo central. El segundo programa ejecutó el comando *iwconfig* cuya salida muestra la velocidad de transmisión y nivel de potencia de la señal WiFi recibida (RSSI-Received Signal Strength Indicator) desde el punto de acceso. Los resultados indicaron que el alcance fueron 37 metros con línea de vista. A una distancia mayor a ésta la potencia cayó aceleradamente hasta perder el

enlace en los -82 dBm como se muestra en la gráfica de la Figura 5.

4. CONCLUSIONES

Se construyó un sistema de acceso a un centro de datos usando tres mecanismos de identificación, el cual cumplió con las especificaciones solicitadas: bajo costo, confiable, seguro y de respuesta rápida usando tecnología de comunicación no intrusiva a las instalaciones. Después de probado y evaluado el sistema se solicitó implantar una siguiente versión que incorpore dos funcionalidades: 1) La bitácora en el módulo central que registre los intentos de acceso exitosos y no exitosos incluyendo la información de identificación leída en los módulos distribuidos, fecha, hora y número de puerta, para ser consultada en la interfaz gráfica y 2) Acceso desde la internet al módulo central para que el administrador pueda realizar las mismas tareas desde una computadora remotamente, lo cual implica conectar a la computadora los lectores RFiD y de huella digital así como una cámara fotográfica o de video.

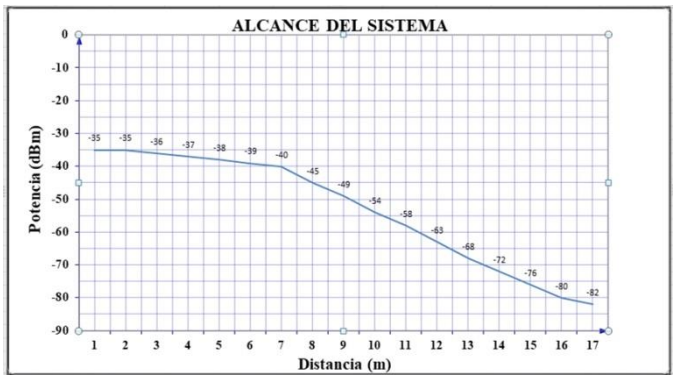

Fig. 5. Alcance de la transmisión del sistema

Si es necesario incrementar el alcance de la transmisión inalámbrica pueden usarse extensores de rango o repetidores inalámbricos WiFi. El sistema desarrollado fue resultado de trabajos anteriores realizados por los autores que no fueron únicamente una investigación o desarrollo tecnológico experimental, son aplicaciones que resuelves una necesidad real.

5. REFERENCIAS

[1] K. Nemati, A. Zabalegui, M. Bana, "Quantifying data center performance", 34th Thermal Measurement, Modeling & Management Symposium (SEMI-THERM), San Jose, CA, USA, 19-23 March, 2018, Pages: 141-147.

[2] Y. W. Bai, C. N. Fu, J. H. Yang, "Using NFC tags and smartphones to design a reliable mechanism to pick a child up from school", IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 12-14 Jan., 2018, Pages: 1-4.

[3] S. Thakre, A. K. Gupta, "Secure reliable multimodel biometric fingerprint and face recognition", International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 5-7 Jan., 2017, Pages: 1-4.

[4] M. A. Hmani, D. Petrovska-Delacrétaz, "State-of-the-art face recognition performance using publicly available software and datasets", 4th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), Sousse, Tunisia, 21-24 March, 2018, Pages: 1-6.

[5] R. Kaur, D. Sharma, A. Verma, "An advance 2D face recognition by feature extraction (ICA) and optimize multilayer architecture", 4th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 21-23 Sept., 2017.

[6] S. Wibawanto, K. C. Kirana, "Recognition of student emotion based on matrix-1 median fisher's face and backpropagation algorithm", International Conference on Electrical Engineering and Informatics (ICELTICs), Banda Aceh, Indonesia, 18-20 Oct., 2017, Pages: 103-108.

[7] C. Ying, S. Yaojie, "Face Recognition of the Rhinopithecus Roxellana Qinlingensis Based on Improved HOG and Sparse Representation", International Conference on Computer Network, Electronic and Automation (ICCNEA), Xi'an, China, 23-25 Sept., 2017, Pages: 499-503.

[8] C. Lunerti, R. M. Guest, R. Blanco-Gonzalo, "Environmental effects on face recognition in smartphones", International Carnahan Conference on Security Technology (ICCST), Madrid, Spain, 23-26 Oct., 2017, Pages: 1-6.

[9] D. A. Wati, D. Abadianto, "Design of face detection and recognition system for smart home security application", 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, 1-2 Nov., 2017, Pages: 342-347.

[10] N. A. Jamil, U. U. Sheikh, M. M. Mokji, "Improved face recognition on video surveillance images using pose correction", TENCON 2017-IEEE Region 10 Conference, Penang, Malaysia, 5-8 Nov., 2017, Pages: 1391-1395.

[11] F. Schroff, D. Kalenichenko, J. Philbin, "FaceNet: A unified embedding for face recognition and clustering", IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, 7-12 June, 2015, Pages: 815-823.

[12] S. Srisuk, S. Ongkittikul, "Robust face recognition based on weighted DeepFace", International Electrical Engineering Congress (iEECON), Pattaya, Thailand, 8-10 March, 2017, Pages: 1-4.

[13] B. Sugiarto, E. Prakasa, R. Wardoyo, "Wood identification based on histogram of oriented gradient (HOG) feature and support vector machine (SVM) classifier", 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, 1-2 Nov., 2017, Pages: 337-341.

[14] C. I. Orozco, F. Iglesias, M. E. Buemi, "Real-time gender recognition from face images using deep convolutional neural network", 7th Latin American Conference on Networked and Electronic Media (LACNEM 2017), Valparaiso, Chile, 6-7 Nov., 2017, Pages: 7-11.

[15] E. V. Zatonskikh, G. I. Borzunov, "Development of elements of two-level biometrie protection based on face and speech recognition in the video stream", IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, Russia, 29 Jan.-1 Feb., 2018, Pages: 1579-1583.

[16] J. A. Kusnadi, D. Julio, "Security system with 3 dimensional face recognition using PCA method and neural networks algorithm", 4th International Conference on New Media Studies (CONMEDIA), Yogyakarta, Indonesia, 8-10 Nov., 2017, Pages: 152-155.