ACCESO A UN CENTRO DE DATOS UTILIZANDO UNA TARJETA RFiD Y HUELLA DIGITAL

ACCESS TO A DATA CENTER USING A RFiD CARD AND THE FINGERPRINT

José Ignacio Vega Luna
Universidad Autónoma Metropolitana
vlji@correo.azc.uam.mx

Mario Alberto Lagos Acosta
Universidad Autónoma Metropolitana
vlji@correo.azc.uam.mx

Francisco Javier Sánchez Rangel
Universidad Autónoma Metropolitana
vlji@correo.azc.uam.mx

José Francisco Cosme Aceves
Universidad Autónoma Metropolitana
vlji@correo.azc.uam.mx

Resumen

Se presenta un sistema cuyo propósito es permitir el acceso a usuarios registrados en una base de datos a cinco áreas de un centro de datos. El problema a resolver es identificar a los usuarios a través de una tarjeta RFiD y la huella digital para determinar si pueden entrar al área que intentan acceder. El diseño está compuesto por un módulo de control y cinco módulos de acceso. Los dos tipos de módulos se componen de una tarjeta Raspberry Pi 3, un lector de tarjetas RFiD y un lector de huellas digitales. La información de usuarios se almacena en una base de datos MySQL y las huellas digitales en la memoria del lector de huellas del módulo de control. Se logró un alcance de 50 metros con línea de vista en la comunicación WiFi entre los módulos y un punto de acceso y un porcentaje de confiablidad de 99.5%.

Palabras Claves: Lector de huellas digitales, MySQL, Raspberry Pi 3, RFID, Wi-Fi.

Abstract

A system is presented whose purpose is to allow access to registered users in a database to five areas of a data center. The problem to solve is to identify the users through an RFID card and the fingerprint to determine if they can enter the area they are trying to access. The design consists of a control module and five access modules. The two types of modules are composed of a Raspberry Pi 3 card, an RFID card reader and a fingerprint reader. The user information is stored in a MySQL database and the fingerprints in the memory of the fingerprint reader of the control module. A range of 50 meters was achieved with line of sight in the WiFi communication between the modules and an access point and a trust percentage of 99.5%.

Keywords: F*ingerprint reader, MySQL, Raspberry Pi 3, RFID, Wi-Fi.*

1. Introducción

Hoy en día, casi todas las organizaciones cuentan con un centro de datos o hacen uso de los servicios que ofrecen empresas propietarias de centros de datos. En un centro de datos se encuentran instalados equipos de cómputo, almacenamiento de información y telecomunicaciones utilizadas en las operaciones cotidianas de empresas e instituciones. Entre los mecanismos y procesos de acceso y seguridad en un centro de datos se encuentran los siguientes: sistemas de video vigilancia, torniquetes, puertas blindadas y herméticas, cerraduras electromagnéticas y detectores de movimiento, entre otros [Lima, 2017]. Los centros de datos se dividen en áreas denominadas bunkers. El acceso a un bunker solo está autorizado al personal de la empresa propietaria del equipo y al personal específico del centro de datos.

Presentación del problema a resolver

Este trabajo se realizó a solicitud de una empresa que ofrece servicios de alojamiento, instalación y administración de equipo en centros de datos. El objetivo planteado fue contar con un sistema de identificación de usuarios utilizando tarjetas RFiD (Radio Frequency Identification) y un lector de huellas digitales para controlar

el acceso a los bunkers. Se solicitó un sistema confiable, seguro y de respuesta rápida que no requiera la instalación de cableado adicional y use para la comunicación un punto de acceso WiFi del centro de datos.

Se requirió el uso de tarjetas RFiD por ser económicas y fáciles de usar y un lector de huella digital como mecanismo adicional de seguridad. La distancia máxima de un bunker a la oficina de monitoreo del centro de datos son 35 metros.

La solución propuesta fue un sistema integrado por un módulo de control y cinco módulos de acceso. El módulo de control se instaló en la oficina de monitoreo y un módulo de acceso en la puerta principal y en las puertas de los bunkers. Ambos tipos de módulos cuentan con un lector de tarjetas RFiD, un lector de huellas digitales y una tarjeta Raspberry Pi 3. Adicionalmente, el módulo de control cuenta con una pantalla táctil para implantar la interfaz de usuario.

A través de la interfaz de usuario el administrador del sistema puede dar de alta, remover o realizar cambios de usuarios. La información del usuario se almacena en una base de datos creada en el módulo de control y las imágenes de las huellas digitales se almacenan en la memoria flash del lector de huellas de este módulo. Los módulos de acceso tienen una copia de la base de datos y de las imágenes de las huellas digitales del módulo de control. Cuando el administrador del sistema realiza un cambio en la base de datos del módulo de control, éste transmite a los módulos de acceso el registro del usuario nuevo, removido o modificado y, si es necesario, la imagen de la huella digital correspondiente.

Con este mecanismo de funcionamiento se tiene un esquema similar a una base de datos distribuida. De tal forma que los módulos de acceso leen la tarjeta RFiD y huella digital de los usuarios que intentan acceder al bunker, validan esta información localmente y activan el actuador de la puerta correspondiente cuando el usuario está autorizado a acceder.

Descripción de la tecnología usada

La aplicación desarrollada en este trabajo utiliza, como primer mecanismo de seguridad, un lector de tarjetas RFiD conectado a una tarjeta Rspberry Pi para acceder la información de las tarjetas RFiD de los usuarios.

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. La comunicación con NFC es más segura que otras tecnologías ya que el transmisor y receptor están estrechamente acoplados y próximos, con una cercanía máxima de 10 centímetros, sin necesidad de ejecutar una aplicación.

El segundo mecanismo de seguridad implantado en este trabajo 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 y confiable.

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 en un buffer y convertida a una plantilla. La plantilla es una caracterización general de la huella digital. Una vez creada la plantilla, se almacena en la memoria flash del lector asignándole un identificador (ID).

El ID de la plantilla se usa para su búsqueda, remoción o comparación con otra platilla. Adicionalmente, desde un controlador externo se puede cargar o descargar una plantilla de la memoria flash del lector. La memoria flash funciona similar a una base de datos de imágenes.

Aunque fue un requisito en la implantación de este trabajo usar tarjetas RFiD y la huella digital como mecanismos de identidad, se exploraron tecnologías alternas de bajo costo y de respuesta rápida para la identificación de usuarios como los códigos QR (Quick Response) y el sistema iBeacon.

Trabajos relacionados

Los códigos QR almacenan información en matrices de puntos o códigos de barras de forma bidimensional [Dudheria, 2017]. Cuando un dispositivo móvil lee un código QR ejecuta una aplicación para realizar una acción específica. En la implantación de este trabajo pudo usarse una combinación de tecnología RFiD y

códigos QR pero resultaría un sistema poco más costoso y lento, ya que además de usar un método de impresión del código QR en las tarjetas RFiD, éstas no podrían re-utilizarse [Zhang, 2017].

Por otra parte, iBeacon es un protocolo usado en sistemas de posicionamiento en interiores patentado por Apple Inc. [Srinivasan, 2016]. Está basado en transmisores de bajo costo y bajo consumo de energía que indican su presencia a un dispositivo con sistema operativo iOS y algunos dispositivos con sistema operativo Android. Existen proveedores de transmisores, llamados beacons, compatibles con iBeacon. Los beacons usan transmisores de tecnología Bluetooth de bajo consumo de energía, o Bluetooth 4.0, los cuales transmiten su identificador único universal (UUID) a dispositivos electrónicos móviles, permitiendo que un teléfono móvil o tableta ejecute una acción o aplicación basada en la ubicación del beacon al recibir la identificación, o dar seguimiento a clientes o usuarios de beacons [Burzacca, 2014]. Pudo haber sido una opción usar iBeacon en el desarrollo de este trabajo, lo cual implicaría usar un beacon como identificador del usuario y un dispositivo con iOS en cada punto de acceso al centro de datos, lo que aumentaría la complejidad en el uso, instalación y costo del sistema. Se han realizado trabajos de sistemas de acceso a instalaciones basados en Arduino, tarjetas RFiD, lectores de huellas digitales y bases de datos MySQL, usando comunicación Ethernet a la base de datos, más rápida con respecto a WiFi. En este trabajo se requirió el uso de una tecnología inalámbrica no intrusiva a las instalaciones del centro de datos como WiFi [Palencia, 2015]. Se han llevado a cabo diversos trabajos que utilizan códigos QR o una combinación de éstos con tarjetas RFiD [Wang, 2017] para controlar el acceso a instalaciones, para sistemas de localización y navegación y para identificación de productos e imágenes médicas [Kavitha, 2017]. Inclusive, se han realizado sistemas de acceso a centros de datos combinando códigos QR y marcas de agua [Pramkeaw, 2016]. El uso de códigos QR proporciona un nivel de seguridad más alto que las tarjetas RFiD, pero el costo de implantación y operación de estos sistemas es elevado, ya que una vez usada una tarjeta con un código QR no puede utilizarse para otro usuario y el hardware de impresión y lectura de códigos QR es de más alto precio que un lector NFC [Lay, 2017].

Por otro lado, se ha realizado una gran variedad de sistemas de acceso a centros de datos a través de dispositivos biométricos. Algunos de estos sistemas llevan a cabo reconocimiento facial y otros leen el iris del usuario o movimiento del ojo usando un lector instalado en la puerta de acceso [Addy, 2016] o por medio del teléfono inteligente del usuario [Derawi, 2012]. Estos sistemas son más seguros que los que usan tarjetas RFiD o códigos QR con un lector de huellas digitales, pero su costo de implantación es mucho más alto.

La aportación del sistema construido en este trabajo es que cuenta con dos mecanismos de identificación: la lectura del UUID de la tarjeta RFiD y la lectura biométrica de la huella digital del usuario. Adicionalmente, se utilizan componentes de reciente tecnología, donde todo el software es de código abierto y la comunicación es a través de WiFi, la cual no impacta en las instalaciones del centro de datos, llevando a cabo una aplicación práctica que cumple con los requisitos solicitados por el usuario.

2. Métodos

La funcionalidad del sistema consiste almacenar la información de los usuarios en una base de datos y las huellas digitales en la memoria del lector de huellas del módulo ubicado en la oficina de monitoreo del centro de datos y replicar esta información a los cinco módulos ubicados en la puerta de acceso de cada una de las áreas del centro de datos, como se indica en la figura 1. La comunicación entre los módulos del sistema es a través de un punto de acceso WiFi instalado en el centro de datos.Tomando en cuenta lo anterior, la metodología seguida para el desarrollo del sistema consistió en dividirlo en dos tipos de módulos, el módulo de control y los módulos de acceso. Posteriormente, cada tipo de módulo fue diseñado e implantado seleccionando los componentes adecuados para realizar su función. Un componente fundamental de los módulos es la tarjeta Raspberry Pi 3. Se optó por usar esta tarjeta cuyo costo es mayor a otras de su tipo, como por ejemplo la Arduino, por dos razones:

- El sistema operativo Raspbian, similar a casi todas las distribuciones de Linux, incorpora Python. Esto representa la ventaja tecnológica de poder

utilizar una gran cantidad de bibliotecas para Python, a través de la comunidad de software libre, que permiten la creación segura, rápida y eficiente de aplicaciones

- La Raspberry Pi cuenta con interfaz WiFi y una mayor cantidad de recursos hardware que otras, como por ejemplo más puertos serie e interfaz para memoria SD, siendo una computadora real que permite la posibilidad de crecer las aplicaciones como la aquí presentada.

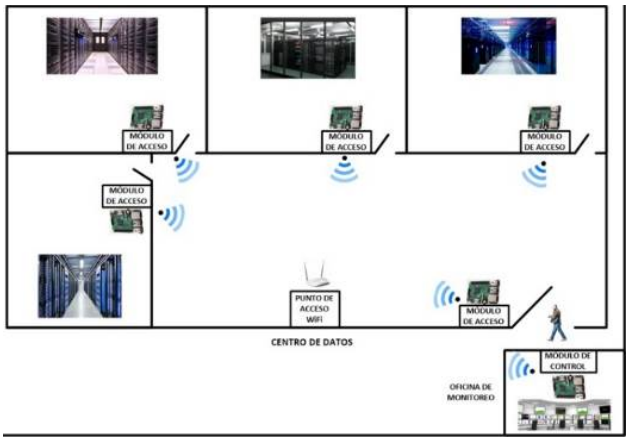

Figura 1 Funcionalidad del sistema desarrollado.

El módulo de control

El módulo de control está compuesto por: una tarjeta Raspberry Pi 3 B+, un lector de tarjetas RFiD, un lector de huellas digitales y una pantalla sensible al tacto, como se muestra en la arquitectura del módulo de la figura 2.

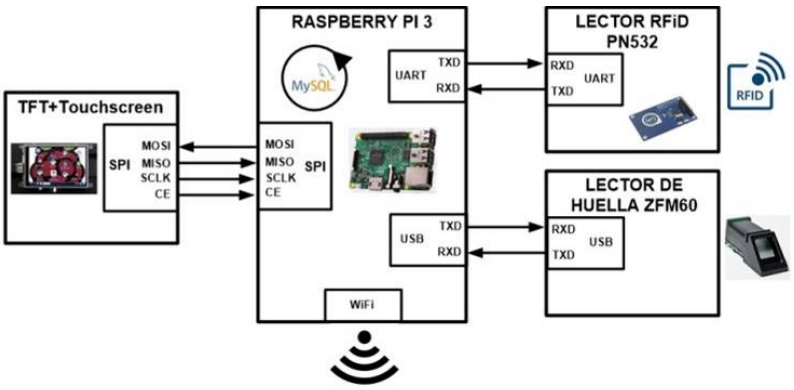

Figura 2 Arquitectura del módulo de control.

Las funciones del módulo de control son las siguientes: mantener actualizada la base de datos de usuarios y el contenido de la memoria flash del lector de huellas digitales de este módulo y de los módulos de acceso e implantar la interfaz gráfica de usuario mediante la cual el administrador del sistema accede la base de datos de usuarios e imágenes de huellas digitales.

En la tarjeta Raspberry Pi se utilizó una memoria SD de 16 GB para instalar el sistema operativo Raspbian kernel 4.9 y almacenar la base de datos de usuarios. 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.

Tanto en el módulo de control como en los módulos de acceso el lector RFiD se conectó al puerto UART y se utilizó la biblioteca *libnfc* 1.7.0 para accederlo desde la Raspberry Pi. El lector de huellas digitales usado fue el dispositivo ZFM60 de ZhianTec. Este lector se comunica con un controlador externo a través de un puerto UART usando un protocolo propietario de tipo orden-respuesta. El voltaje de las señales TXD y RXD del ZFM60 es 5V, por lo que no es adecuado conectarlas directamente a las terminales GPIO RXD y TXD del UART de la Raspberry Pi y además el UART se usó en este módulo del sistema para conectar el lector RFiD, razones por la cuales se conectó el ZFM60 a un puerto USB de la Raspberry Pi a través un convertidor TTL-USB.

El puerto UART del ZFM60 se configuró para trabajar a una velocidad de 57,600 bps. Para llevar a cabo la comunicación entre la Raspberry Pi y el lector ZFM60 se usó la biblioteca de funciones para Python de código abierto *pyfingerprint*.

La pantalla táctil utilizada en el módulo de control para implantar la interfaz de usuario fue el dispositivo Pi+TFT de 3.5”, el cual se conectó al puerto SPI de la tarjeta Raspberry Pi.

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.

El programa principal configura los temporizadores, el puerto UART, la interfaz WiFi, la pantalla táctil, inicializa el lector de huellas digitales, invoca la rutina de

comunicación con los módulos de acceso y entra a un ciclo donde implanta la interfaz de usuario, como se indica en el diagrama de flujo de la figura 3.

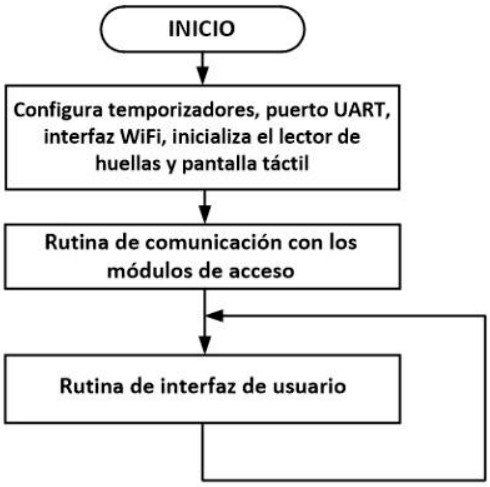

Figura 3 Diagrama de flujo del programa del módulo de control.

La comunicación entre los módulos de acceso y el módulo de control se llevó a cabo usando intercambio de mensajes con sockets bajo el esquema cliente-servidor, los módulos de acceso son los servidores y el módulo de control es el cliente. La rutina de comunicación con los módulos de acceso ejecuta un programa en segundo plano para crear un socket a través del cual el módulo de control transmite a los módulos de acceso los cambios en la base de datos de usuarios y en la memoria flash del lector de huellas para mantenerlas sincronizadas.

La rutina de interfaz de usuario permite al administrador realizar las siguientes operaciones: altas, bajas y cambios de usuarios, así como mostrar los usuarios registrados en la base de datos. Al registrar un usuario o realizar cambios a uno existente, la rutina transmite al módulo de acceso el índice del registro del usuario en la base de datos, su contenido y la plantilla de la huella digital. Al remover un usuario, la rutina solo transmite el índice del registro y el ID de la platilla de la huella digital. En la figura 4 se indica el menú de la interfaz de usuario mostrado en la pantalla táctil del módulo de control.

La base de datos de usuarios se implantó usando el manejador MySQL y contiene una tabla con 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 usó el API de Python para MySQL.

Figura 4 Menú de la interfaz de usuario del módulo de control

La rutina de interfaz de usuario ejecuta de manera general las siguientes acciones:

- Importa el API de Python para MySQL.
- Realiza la conexión a la base de datos.
- Espera la opción seleccionada por el usuario en la interfaz gráfica.
- Dependiendo la opción, define el query de sql para realizar la operación correspondiente sobre el registro del usuario.

Los módulos de acceso

Se construyeron cinco módulos de acceso, todos con la misma arquitectura como la mostrada en la figura 5.

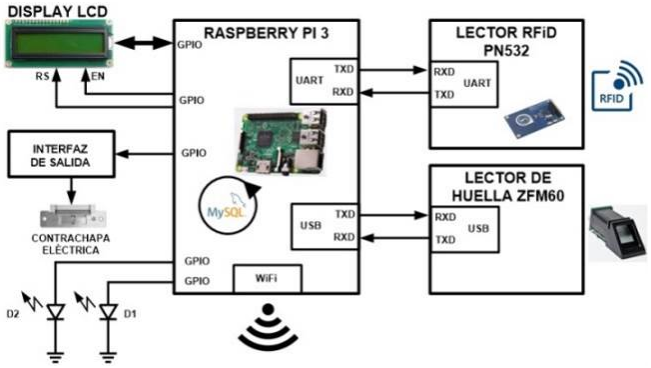

Figura 5 Arquitectura de los módulos de acceso.

Los módulos de acceso cuentan con componentes iguales al módulo de control, excepto que el lugar de una pantalla táctil, usan un display LCD 16x2, conectado a 6 terminales GPIO de la Raspberry Pi. En el display LCD se muestran al usuario los mensajes del sistema. La función principal de los módulos de acceso es explorar continuamente el lector RFiD para determinar si se encuentra una tarjeta en su alcance. En caso afirmativo, leen la información contenida en la tarjeta y capturan la imagen de la huella digital para determinar si el usuario está autorizado a entrar. La programación de los módulos de acceso se realizó en Phyton 3.6. El programa principal realiza las siguientes tareas: configura los temporizadores, el puerto UART, la interfaz WiFi, el display LCD, las terminales GPIO, inicializa el lector de huellas digitales, invoca la rutina de comunicación con el módulo de control y entra a la rutina de lectura de tarjetas RFiD. En la figura 6 se muestra el diagrama de flujo usado para desarrollar este programa.

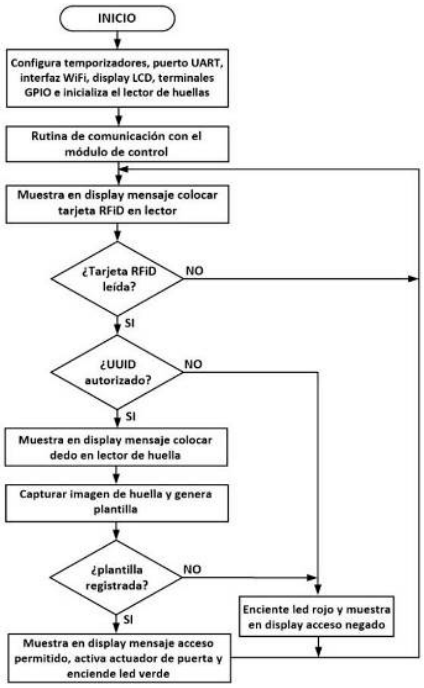

Figura 6 Diagrama de flujo del programa de los módulos de acceso.

En caso de que el usuario esté autorizado a entrar, muestra en el display LCD el mensaje indicando que debe colocar el dedo en el lector de huella digital, Si el UIID se encuentra en la base de datos, captura la imagen de la huella y genera en un

buffer la plantilla correspondiente, buscar la plantilla generada en la memoria flash del lector y en caso de ser exitosa la búsqueda, muestra en el display LCD el mensaje de acceso permitido, activa el actuador de la puerta de acceso y enciende un led verde (D1).

Los leds y la interfaz del actuador de la puerta se conectaron a terminales GPIO de la Raspberry Pi configuradas como salidas. Cuando en el módulo de control se registra un usuario nuevo o se realizan cambios a uno existente, la rutina de comunicación recibe, desde el módulo de control, el índice del registro en la base de datos, su contenido y la plantilla de la huella digital. Con esta información el módulo de acceso registra la plantilla nueva en la memoria flash del lector de huellas y ejecuta el query de sql para insertar o actualizar el registro en la base de datos, respectivamente. Cuando un usuario es dado de baja, la rutina de comunicación solo recibe el índice del registro y el ID de la platilla de la huella digital y ejecuta el query de sql para remover el registro del usuario.

3. Resultados

Para comprobar la funcionalidad del sistema se llevaron a cabo cinco grupos de pruebas. El primer grupo tuvo como objetivo medir el alcance del lector RFiD de los módulos de acceso. Para llevar a cabo estas pruebas se usaron 50 tarjetas colocadas a diferentes distancias del lector, determinando que el alcance son 12 centímetros, un poco más de lo indicado por el fabricante del lector. Usando estas tarjetas se registraron en la base de datos los usuarios correspondientes. A continuación, se ejecutó el segundo grupo de pruebas cuyo objetivo fue verificar el funcionamiento del lector de huellas digitales. En estas pruebas se capturaron y registraron las huellas digitales de los 50 usuarios del primer grupo de pruebas. Posteriormente, los mismos usuarios intentaron entrar en diferentes módulos de acceso colocando su dedo en posiciones que variaron ligeramente respecto a la posición cuando les fue capturada su huella en el módulo de control. El reconocimiento fue exitoso ya que la plantilla creada al capturar la imagen es una caracterización general de la huella, permitiendo variaciones en la posición del dedo. Esta caracterización crea la plantilla capturando dos imágenes de la huella

para tener mayor exactitud y libertad en la posición del dedo. A pesar de esto, se presentaron problemas con algunos usuarios y no se pudo capturar la imagen de la huella. Esto sucedió cuando el usuario tenía húmedo el dedo. De hecho, el manual del fabricante del lector de huellas indica que esto puede suceder y recomienda repetir el proceso una vez limpio el dedo. El tercer grupo de pruebas tuvo como objetivo medir el tiempo de respuesta del sistema. Para realizar estas pruebas se registró en un archivo en cada módulo de acceso la hora de lectura de las tarjetas de usuarios autorizados a acceder y la hora de apertura de la puerta. El tiempo de respuesta fue 100 ms. en promedio. El cuarto grupo de pruebas tuvo como objetivo medir el alcance de la transmisión WiFi de los módulos de acceso. Para efectuar estas pruebas se ubicó un módulo de este tipo a diferentes distancias del punto de acceso WiFi Cisco WAP4410N. A continuación, se ejecutaron dos programas en el módulo: uno de ellos en segundo plano, cuya tarea fue transmitir continuamente un archivo al módulo de control y el segundo ejecutó el comando *iwconfig* para registrar la velocidad de transmisión y nivel de potencia de la señal WiFi recibida (RSSI-Received Signal Strength Indicator) desde el punto de acceso a cada lugar donde ubicó el módulo de acceso. Los resultados indicaron que el alcance fueron 50 metros con línea de vista a una velocidad de 195 Mbps, menor a los 300 Mbps que pueden lograrse teóricamente usando el estándar 802.11n. A una distancia mayor a 50 metros la potencia decreció aceleradamente y se perdió el enlace cuando el nivel cayó a los -82 dBm como se muestra en la gráfica de la figura 7.

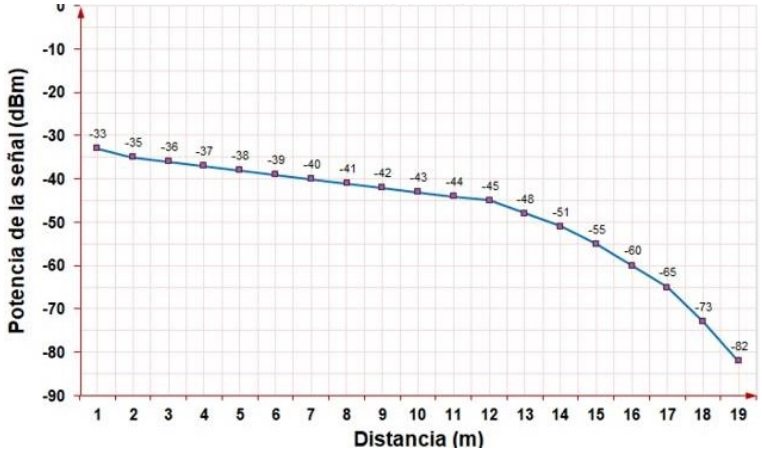

Figura 7 Alcance de la transmisión de los módulos de acceso

En el quinto grupo de pruebas se determinó el número de errores positivos del sistema. El lector de huellas digitales puede configurarse en uno de cinco niveles de seguridad, del 1 al 5, por defecto trabaja en nivel 3. El nivel de seguridad indica al lector la sensibilidad al comparar la plantilla de una huella con las imágenes almacenadas en la memoria flash, siendo el nivel 5 el de mayor sensibilidad.

El fabricante del lector indica que para el nivel 3 la tasa de rechazos falsos (FRR-False Rejection Rate) es menor a 1%. En este grupo de pruebas se configuró el lector de un módulo de acceso usando los cinco niveles de seguridad.

En cada nivel participaron 200 personas para contar con resultados más certeros. Se presentaron casos en cada nivel en los que el sistema indicó que el usuario no estaba autorizado a entrar aun cuando su huella estaba registrada. En el nivel 3 se presentaron 3 casos resultando un FRR de 1.5%, 0.5 % más que el indicado por el fabricante y un tiempo de respuesta de 100 ms. Los resultados obtenidos mostraron que usando un mayor nivel de sensibilidad el FRR disminuye y el tiempo de respuesta aumenta, como se indica en la tabla 1. No es grande la diferencia entre el tiempo de respuesta del nivel 1 con respecto al 5 y por esta razón, el lector de los módulos de acceso se configuró en nivel 5 para tener el menor FRR, mayor sensibilidad y 99.5 de confiabilidad.

En la figura 8 se muestra la gráfica que indica la relación entre el FRR y el tiempo de respuesta del sistema.

Tabla 1 Niveles de seguridad usados, FRR y tiempos respuesta obtenidos.

Nivel de seguridad	FRR (%)	Errores positivos (huellas no reconocidas)	Tiempo de respuesta (ms)
1	3	6	60
2	2	4	80
3	1.5	3	100
4	1	2	110
5	0.5	1	119

4. Discusión

Adicionalmente a las pruebas realizadas, para verificar que el nivel de potencia reportado por el comando *iwconfig* fuera correcto, en cada punto donde se ubicó el módulo de acceso se colocó una computadora portátil para medir el nivel de RSSI

utilizando el programa *inSSIDer*. Los valores de RSSI medidos con *inSSIDer* no tuvieron gran diferencia respecto a los indicados por el comando *iwconfig*. En caso de ser necesario incrementar el alcance de la transmisión inalámbrica pueden usarse extensores de rango o repetidores inalámbricos WiFi. Es importante considerar que el lector puede almacenar hasta 1,000 imágenes de huellas digitales, lo cual puede ser una limitación en instalaciones con grandes cantidades de usuarios. Finalmente, y tal vez lo más importante, el sistema implantado no fue solo una investigación o desarrollo tecnológico experimental, es una aplicación que resuelve una necesidad real.

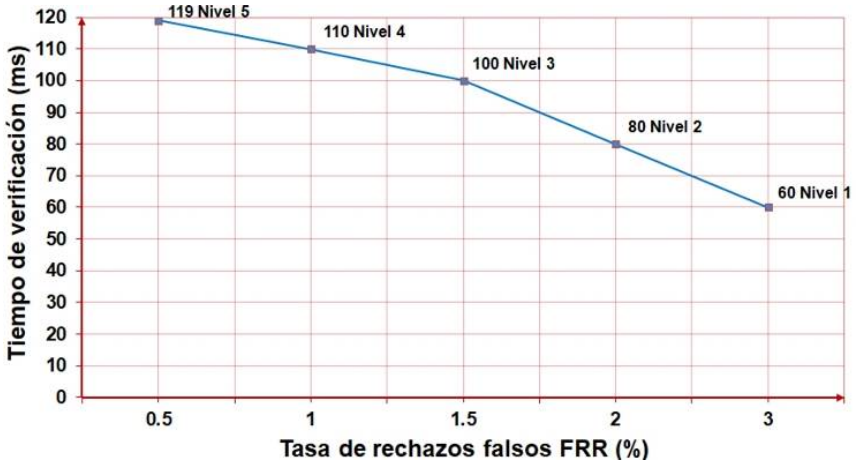

Figura 8 Tasa de rechazos falsos obtenida en las pruebas y tiempo de respuesta.

5. Conclusiones

Se desarrolló un sistema de acceso usando como mecanismos de identificación una tarjeta RFiD y la huella digital, el cual cumplió con las especificaciones solicitadas: confiable, fácil de administrar y de respuesta rápida. Una vez que se probó y evaluó el sistema en el centro de datos, se ha solicitado realizar una segunda versión del mismo que incorpore dos funcionalidades: 1) Una bitácora en el módulo de control que registre los intentos de acceso exitosos y no exitosos en los módulos de acceso, incluyendo la información leída de la tarjeta RFiD, fecha, hora y número de puerta, pudiendo ser consultada desde la interfaz de usuario de este módulo y 2) Reconocimiento facial del usuario en los módulos de acceso para contar con un nivel de seguridad más alto al logrado en este trabajo.

6. Bibliografía y Referencias

[1] Addy, D. & Bala, P. Physical access control based on biometrics and GSM. International Conference on Advances in Computing, Communications and Informatics (ICACCI) Proceedings. Jaipur, India. Sept., 2016.

[2] Burzacca, P., Mircoli, M. & Mitolo, S. iBeacon technology that will make possible Internet of Things. International Conference on Software Intelligence Technologies and Applications & International Conference on Frontiers of Internet of Things Proceedings. Hsinchu, Taiwan. Dec., 2014.

[3] Derawi, M. O., McCallum, S. & Witte, H. Biometric access control using Near Field Communication and smart phones. 5th IAPR International Conference on Biometrics (ICB). New Delhi, India. March, 2012.

[4] Dudheria, R. Evaluating Features and Effectiveness of Secure QR Code Scanners. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) Proceedings. Nanjing, China. 12-14 Oct., 2017.

[5] Kavitha, K. J. & Shan, B. P. Implementation of DWM for medical images using IWT and QR code as a watermark. Conference on Emerging Devices and Smart Systems (ICEDSS) Proceedings. Tiruchengode, India. March, 2017.

[6] Lay, K. T. & M. H. Zhou. Perspective projection for decoding of QR codes posted on cylinders. IEEE International Conference on Signal and Image Processing Applications (ICSIPA) Proceedings. Kuching, Malaysia. Sept., 2017.

[7] Lima, V. M., Lima, R. M. & Lins, F. A. A multi-perspective methodology for evaluating the security maturity of data centers. IEEE International Conference on Systems, Man, and Cybernetics (SMC) Proceedings. Banff, AB, Canada. Oct., 2017.

[8] Palencia, G. P., Bernadez, H. L. & Enriquez, L. P. Time-controlled access with power management using RFID acquisition and power control distribution. International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment Proceedings. Cebu City, Philippines. Dec., 2015.

[9] Pramkeaw, P, Ganokratanaa, T. & Phatchuay, S. Integration of Watermarking and QR Code for Authentication of Data Center. 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS) Proceedings. Napoles, Italy. Nov., 2016.

[10] Srinivasan, V. S., Kumar, S. T. & Yasarapu, D. K. Raspberry Pi and iBeacons as environmental data monitors and the potential applications in a growing BigData ecosystem. IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) Proceedings. Bangalore, India. May, 2016.

[11] Wang, X. L., Wu, C. F., & Li, G. D. A robot navigation method based on RFID and QR code in the warehouse. Chinese Automation Congress (CAC) Proceedings. Jinan, China. Oct., 2017.

[12] Zhang, X., Luo, H. & Peng, J. Fast QR code detection. International Conference on the Frontiers and Advances in Data Science (FADS) Proceedings. Xi'an, China. Oct., 2017.