Año: 2018 Volúmen: 1
Número: 4 ISSN: 2448-623X

Control de Acceso Usando RFiD y una Tarjeta Raspberry Pi Zero W

J. I. Vega-Luna[1], J. F. Cosme-Aceves[1], F. J. Sánchez-Rangel[1], G. Salgado-Guzmán[1].

***Resumen*—Se presenta el desarrollo de un sistema de control de acceso a un centro de datos usando tarjetas RFiD y una tarjeta Raspberry Pi Zero W. El sistema se compone de cinco nodos de lectura y un nodo de validación. El objetivo fue reportar, desde cada nodo de lectura al nodo de validación, la información de la tarjeta RFiD y la imagen del rostro del usuario para consultar en una base de datos MySQL si el usuario puede acceder al área correspondiente al nodo de lectura. Cada nodo de lectura consta de una tarjeta Raspberry Pi Zero W, un lector de tarjetas RFiD y una cámara de video. El nodo de validación se compone de los mismos elementos que los nodos de acceso más una pantalla táctil usada en la interfaz de usuario. La comunicación entre los nodos es WiFi, logrando un alcance de 70 metros con línea de vista.**

***Palabras claves*—Cámara de video, MySQL, pantalla táctil, Raspberry Pi Zero W, RFiD, WiFi.**

***Abstract*—The development of an access control system to a data center using RFID cards and a Raspberry Pi Zero W card is presented. The system consists of five reading nodes and a validation node. The objective was to report, from each reading node to the validation node, the RFID card information and the user's face image to consult in a MySQL database if the user can access the area corresponding to the reading node. Each reading node consists of a Raspberry Pi Zero W card, an RFID card reader and a video camera. The validation node is composed of the same elements as the access nodes plus a touchscreen used in the user interface. The communication between the nodes is WiFi, achieving a range of 70 meters with line of sigh.**

***Keywords*—MySQL, Raspberry Pi Zero W, RFiD, touchscreen, video camera, WiFi.**

I. Introducción

Los centros de datos son lugares que concentran recursos y equipos necesarios para el procesamiento y almacenamiento de información, así como equipos de telecomunicaciones de empresas y organizaciones. Los centros de datos son grandes naves construidas con varias paredes paralelas de concreto reforzado divididas, cada una, en varias secciones llamadas bunkers [1]. Cada bunker está divido en áreas de diferente tamaño asignada a un cliente en particular de acuerdo a la cantidad de equipo a instalar. Periódicamente los centros de datos son sometidos a auditorias para poder estar certificados. Un punto importante que consideran las auditorías son los procedimientos y técnicas usados en la seguridad y acceso a las instalaciones. En la actualidad existen diferentes soluciones para la identificación de personas para controlar el acceso a los bunkers de un centro de datos [2]. Algunas soluciones de tipo biométrico se basan en el reconocimiento de huella digital, de rostro, de termograma de rostro, de geometría de la mano, de iris, de patrón de retina, de voz y firma de una persona [3].

Este trabajo se realizó a solicitud de una empresa propietaria de centros de datos. El objetivo planteado fue contar con un sistema de identificación de usuarios para controlar el acceso utilizando tarjetas RFiD (Radio Frequency Identification) y actuadores de puertas de acceso de los bunkers. Se solicitó que el sistema fuera confiable, de bajo costo, fácil de instalar y usar, que no se instale cableado adicional para transmisión de datos o que se modifique el existente, de respuesta rápida y que cuente con una base de datos de usuarios autorizados instalada en una oficina de monitoreo del centro de datos. Se requirió el uso de tarjetas RFiD por ser económicas y fáciles de adquirir. La distancia máxima de un bunker a la oficina de monitoreo son 50 metros.

Tomando en cuenta lo anterior, la solución propuesta fue un sistema compuesto de cinco nodos de lectura y un nodo de validación. Se instaló un nodo de lectura en la puerta principal y en las puertas de los bunkers del centro de datos. Los nodos de lectura se encargan de leer la información almacenada en la tarjeta RFiD y transmitirla al nodo de validación, conjuntamente con la fotografía tomada del usuario, usando tecnología WiFi. No fue una opción usar un segmento Ethernet para transmitir la información de identificación del usuario a la oficina de monitoreo debido al requisito de no instalar cableado adicional o modificar el existente. El nodo de validación, instalado en la oficina de monitoreo del centro de datos, consulta en la base de datos si el usuario está autorizado a entrar al bunker asociado al nodo de lectura y registra en la misma la fecha y hora de solicitud de entrada. Si el usuario está autorizado a entrar, el nodo de validación transmite la orden al nodo de lectura para activar el actuador de la puerta del bunker correspondiente. Los nodos de lectura y el nodo de validación se implantaron usando una tarjeta Raspberry Pi Zero W.

[1]*Universidad Autónoma Metropolitana Azcapotzalco, Av. San Pablo No.180 Col. Reynosa Tamaulipas C.P. 02200. Delegación Azcapotzalco. Ciudad de México, CDMX México. Tel:(52 55) 5318-9000*

José Ignacio Luna Vega (vlji@correo.azc.uam.mx)

Año: 2018 Volúmen: 1
Número: 4 ISSN: 2448-623X

La razón principal de usar la Raspberry Pi en este trabajo fue porque usa el sistema operativo Raspbian, para el cual existe una gran cantidad de aplicaciones y bibliotecas desarrolladas por la comunidad de código abierto de fácil instalación, configuración y uso. En el sistema aquí presentado se utilizó también el dispositivo NFC/RFiD 532 para la lectura de tarjetas RFiD. La tecnología NFC (Near Field Communication) surgió por la combinación de la tecnología RFiD y las tarjetas inteligentes. La tecnología RFiD permite la identificación y caracterización de personas u objetos sin contacto físico usando las ondas de radio transmitidas por una etiqueta. 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.

Aunque fue un requisito en la implantación de este trabajo usar tarjetas RFiD, se exploraron tecnologías alternas para la identificación de usuarios. Tecnologías como los códigos QR (Quick Response) y el sistema iBeacon. Los códigos QR son una mejora a los códigos de barras, almacenan información en matrices de puntos o códigos de barras de forma bidimensional [4]. 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. Por otra parte, iBeacon es un protocolo usado en sistemas de posicionamiento en interiores (IPS-Indoor Positioning System) patentado por Apple Inc. [5]. Está basado en transmisores de bajo costo y bajo consumo de energía que indican su presencia a un dispositivo con sistema operativo iOS y a algunos dispositivos con sistema operativo Android.

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.

Con la explosión de servicios basados en la Internet, o Internet de las Cosas, la tecnología RFiD continúa usándose en distintos desarrollos y aplicaciones de identificación, incluyendo cadena de suministros, cuidado de la salud, localización de objetos, automatización de hogares, sistemas de seguridad y entrega de productos en restaurantes [6]. Se han realizado diversos trabajos de sistemas de acceso a instalaciones usando comunicación Ethernet a la base de datos, en este trabajo se usó tecnología inalámbrica WiFi cuya implantación es no intrusiva a las instalaciones del centro de datos [7].

Se han llevado a cabo también diversos trabajos que utilizan códigos QR [8] o una combinación de éstos con tarjetas RFiD [9] para controlar el acceso a instalaciones, para sistemas de localización y navegación [10] y para identificación de productos [11] e imágenes médicas [12]. Inclusive, se han realizado sistemas de acceso a centros de datos combinando códigos QR y marcas de agua [13]. El uso de códigos QR proporciona un nivel de seguridad más alto que las tarjetas RFiD [14], 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 [15].

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 [16] y otros leen la huella digital o iris del usuario [17] usando un lector instalado en la puerta de acceso o por medio del teléfono inteligente del usuario [18]. 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 el uso de componentes de reciente tecnología y bajo costo, como la tarjeta Raspberry Pi Zero W, 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.

II. Desarrollo

La metodología utilizada en el desarrollo de este sistema consistió dividirlo en dos componentes: los nodos de lectura y el nodo de validación. Posteriormente, se diseñó e implantó el sistema seleccionando los elementos adecuados y de menor costo de acuerdo a los requisitos indicados por el centro de datos. El diagrama de bloques funcional del sistema se muestra en la Figura 1.

A. Los nodos de lectura

Se construyeron cinco nodos de lectura, todos con la misma arquitectura como la mostrada en la Figura 2. La función principal de los nodos de lectura es explorar continuamente si se encuentra una tarjeta en el alcance del lector RFiD.

Cuando es leída una tarjeta, el nodo lectura captura, en un archivo formato JPEG, la fotografía del rostro del usuario. La información leída de la tarjeta y el archivo JPEG son transmitidos al nodo de validación. Posteriormente, el nodo de lectura espera la respuesta para

Año: 2018 Volúmen: 1
Número: 4 ISSN: 2448-623X

abrir la puerta en caso de que el usuario este autorizado a entrar.

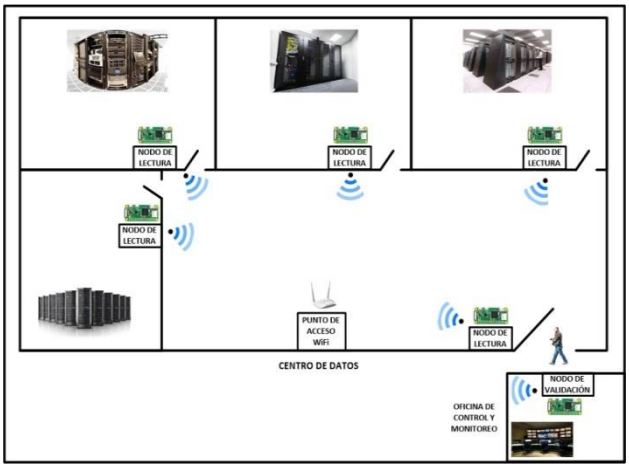

Fig. 1. Diagrama de bloques funcional del sistema

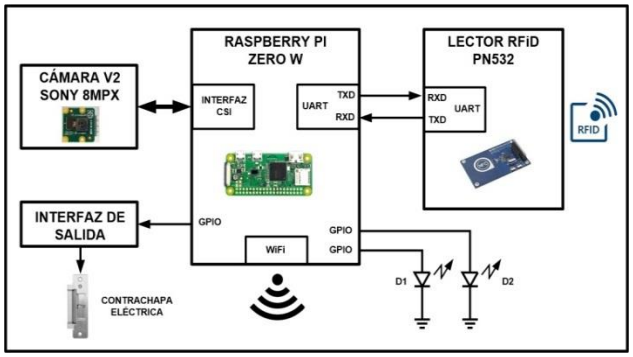

Figura 2. Diagrama de bloques de los nodos de lectura

Cada nodo de lectura está compuesto por: una tarjeta Raspberry Pi Zero W, un lector de tarjetas RFiD, una cámara de video y una interfaz de salida. En la tarjeta de memoria SD de la Raspberry Pi Zero W se instaló el sistema operativo Raspbian kernel 4.9. El lector de tarjetas RFiD usado es el dispositivo NFC/RFiD PN532. Se comunica con un controlador a través de un puerto I^2C, SPI o UART e integra una antena cuyo alcance son 10 centímetros. Existe una gran cantidad de herramientas de código abierto para realizar aplicaciones con el NFC/RFiD PN532. Una de estas herramientas es la biblioteca *libnfc*. Tanto en los nodos de lectura como en el nodo de validación, el lector RFiD se conectó al puerto UART de la Raspberry Pi y se descargó en ella la versión 1.7.0 de la biblioteca *libnfc*. A continuación, se instaló y construyó la biblioteca *libnfc* usando los siguientes comandos: *sudo make clean* y *sudo make install all*, los cuales crearon los drivers, archivos de documentación, binarios y ejecutables correspondientes. Los nodos de lectura integran el módulo de cámara para Raspberry V2 conectado a la interfaz dedicada CSI (Camera Serial Interface) de la Raspberry Pi Zero W. Este módulo de cámara permite capturar fotografías con una resolución máxima de 3238x2464 con diferentes formatos y video de alta definición. Existen bibliotecas de código abierto para usar la cámara y manipular fotos y video que pueden invocarse desde el intérprete de comandos de Raspbian o desde un programa en Python. La cámara puede controlarse usando el comando *raspinstall*, sin embargo en este trabajo se utilizó la biblioteca *python-picamera* de Python en caso de que a futuro en el sistema sea necesario modificar las características de captura de fotografías o video. La cámara de los nodos de lectura se habilitó a través de la herramienta *raspi-config* de Raspbian y posteriormente se instaló la biblioteca *python-picamera* utilizando el comando: *sudo apt-get install python3-picamera*. Una vez realizado lo anterior, se pudo usar la función *camera.capture('archivo.jpg')* para capturar una imagen en un archivo JPEG. El programa que se ejecuta en los nodos de captura se realizó en Phyton 3.6 y realiza las siguientes acciones: configura temporizadores, el puerto UART, la interfaz WiFi y terminales GPIO, a continuación entra en un ciclo continuo donde explora cada 0.5 segundos el lector RFiD ejecutando la función *nfc-pool_8c*. La comunicación entre los nodos de lectura y el de validación se llevó a cabo usando intercambio de mensajes con sockets bajo el esquema cliente-servidor, los nodos de lectura son los clientes y el de validación es el servidor. Cuando el lector detecta una tarjeta captura en un archivo JPEG la imagen del rostro del usuario. Acto seguido, el programa transmite al nodo de validación, a través de un socket, el UUID leído de la tarjeta RFiD y el archivo JPEG. Posteriormente, el programa espera en el socket la respuesta del nodo de validación. Si la respuesta indica que el usuario está autorizado a entrar, el nodo de lectura activa el actuador de la puerta de acceso, a través de la interfaz conectada a una terminal GPIO de la tarjeta Raspberry, y enciende un led verde (D1), conectado a otra terminal GPIO, durante 3 segundos. Si el usuario no está autorizado, enciende un led rojo (D2) intermitentemente durante 5 segundos. En la Figura 3 se indica el diagrama de flujo de este programa. Para poder usar sockets desde Python debe instalarse la biblioteca correspondiente ejecutando el comando siguiente: *sudo apt-get install socket*. La interfaz de salida que controla el actuador de la puerta de entrada se conectó a una terminal GPIO de la tarjeta Raspberry.

B. El nodo de validación

El nodo de validación está constituido por componentes iguales a los nodos de lectura y adicionalmente cuenta con una pantalla táctil a través de la cual el administrador del sistema accede la interfaz de usuario. En la Figura 4 se indica el diagrama de bloques de la arquitectura del nodo de validación.

Año: 2018 Volúmen: 1
Número: 4 ISSN: 2448-623X

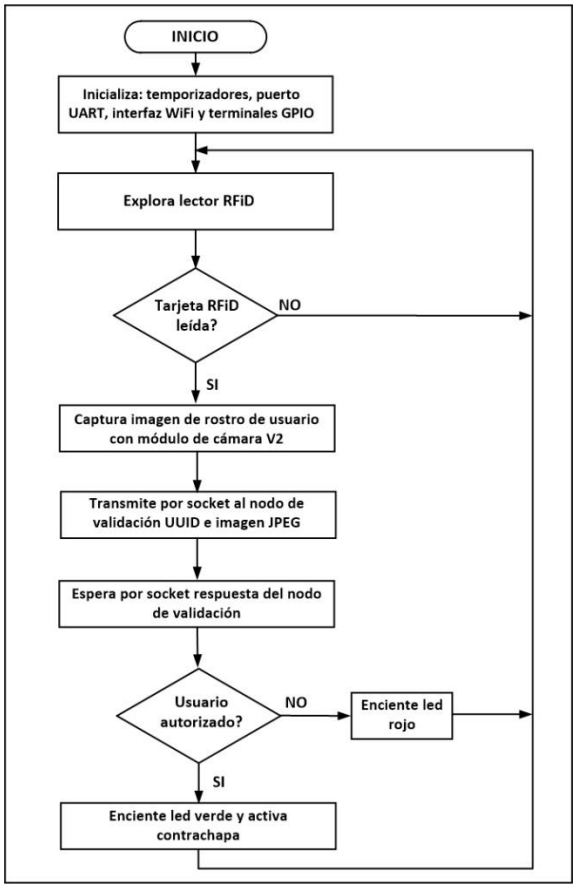

Figura 3. Diagrama de flujo del programa de los nodos de lectura

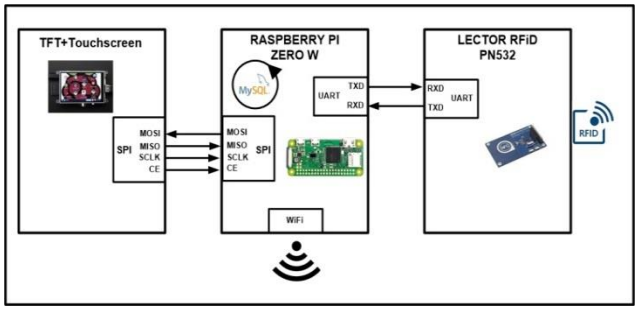

Figura 4. Diagrama de bloques del nodo de validación

La programación del nodo de validación se realizó en Phyton 3.6 y se divide en tres partes: el programa principal, la rutina de comunicación con los nodos de lectura y la rutina de la interfaz de usuario. El programa principal configura los temporizadores, el puerto UART y la interfaz WiFi e invoca las dos rutinas del sistema. La rutina de comunicación con los nodos de lectura se ejecuta en segundo plano y realiza las siguientes funciones: 1) Crea un socket a través del cual recibe desde los nodos de lectura el UUID y el archivo JPEG, 2) Accede la base de datos MySQL para determinar si el usuario tiene permiso de entrada al área correspondiente, 3) Actualiza el registro del usuario con fecha y hora de entrada de la solicitud de acceso, 4) Transmite el mensaje al nodo de lectura para activar el actuador de la puerta o negar la entrada y 5) Actualiza la bitácora de registro de intentos de acceso almacenando en ella el archivo JPEG. La base de datos se implantó usando el manejador MySQL y reside en la tarjeta SD de 16 GB de la Raspberry Pi. 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, la fotografía del rostro capturada cuando el usuario fue dado de alta, 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. A continuación, se realizó el programa en Python para acceder la misma. 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 (CRUD-Create, Read, Update, Delete) en la base de datos. El programa ejecuta de manera general las siguientes acciones: 1) Importa el API de Python para MySQL, 2) 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 un query para insertar, actualizar o remover y 6) Ejecuta el query: *db.commit()*. La rutina que implanta la interfaz gráfica de usuario, permite acceder y administrar la base de datos usando la pantalla táctil. La pantalla utilizada en el nodo de validación es 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 de usuario, el administrador puede realizar las siguientes operaciones: altas, bajas y cambios de usuarios, así como mostrar los usuarios registrados y la bitácora de registro de intentos de acceso. El lector de tarjetas RFiD y la cámara del módulo de validación se usan al dar de alta o realizar cambios en el registro de un usuario. La interfaz de usuario 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, ya que permite mostrar texto, imágenes y sonidos en una pantalla táctil y controlar la posición del cursor. Esta herramienta se instala por defecto con la versión de Raspbian para Raspberry Pi. La dirección IP de la interfaz WiFi de cada nodo de lectura es estática y es usada por el nodo de validación para determinar el número de puerta en la que está intentando el usuario acceder.

Año: 2018 Volúmen: 1
Número: 4 ISSN: 2448-623X

III. RESULTADOS

Se realizaron cinco tipos de pruebas. El primer grupo tuvo como objetivo medir el alcance del lector RFiD de los nodos de lectura. Para llevar a cabo este grupo de pruebas se colocaron varias tarjetas a diferentes distancias del lector, concluyendo que el alcance son 12 centímetros, un poco más de lo indicado por el fabricante del lector.

El segundo grupo de pruebas tuvo como objetivo determinar el tamaño del archivo JPEG generado por la cámara de video de los nodos de lectura. En estas pruebas se leyeron 50 tarjetas RFiD en cada nodo de lectura y la imagen capturada del usuario tuvo como resultado un archivo de 100 KB en promedio. Tomando en cuenta que el sistema operativo Raspbian y bibliotecas utilizan 3.4 GB de la memoria SD de 16 GB en el nodo de validación, restan más de 12 GB para la base de datos de usuarios.

El tercer grupo de pruebas tuvo como objetivo verificar el funcionamiento del sistema usando tarjetas RFiD registradas y no registradas en la base de datos. Después de estas pruebas se revisó la bitácora del sistema desde la interfaz de usuario del nodo de validación y se comprobó que todos los intentos fueron registrados.

El cuarto grupo de pruebas tuvo como objetivo medir el tiempo de respuesta del sistema. Para realizar estas pruebas se registró en un archivo en cada nodo de lectura la hora de lectura de una tarjeta RFiD y la hora al recibir respuesta del nodo de validación. El tiempo de respuesta fue 250 ms. en promedio. El último grupo de pruebas tuvo como objetivo medir el alcance de la transmisión WiFi de los nodos de lectura. Para efectuar estas pruebas se ubicó un nodo de lectura a diferentes distancias del punto de acceso WiFi Cisco WAP4410N. A continuación, se ejecutaron dos programas en el nodo: uno de ellos en segundo plano, cuya tarea fue transmitir continuamente un archivo al nodo de validación y el segundo programa ejecutó el comando *iwconfig* para registrar la velocidad de transmisión y nivel de la potencia de la señal WiFi recibida (RSSI-Received Signal Strength Indicator) desde el punto de acceso a cada punto donde ubicó el nodo de lectura. Los resultados indicaron que el alcance fueron 70 metros con línea de vista a una velocidad de 120 Mbps, menor a los 300 Mbps que pueden lograrse teóricamente usando el estándar 802.11n. A una distancia mayor a 70 metros la potencia decreció aceleradamente y se perdió el enlace cuando el nivel cayó a los -87 dBm como se muestra en la gráfica de la Figura 5.

IV. DISCUSIÓN, CONCLUSIÓN Y RECOMENDACIONES

El resultado de este trabajo fue un sistema de control de acceso basado en identificación por medio de tarjetas RFiD y una base de datos centralizada, el cual cumplió con las especificaciones solicitadas: compacto, de bajo costo, confiable y fácil de administrar.

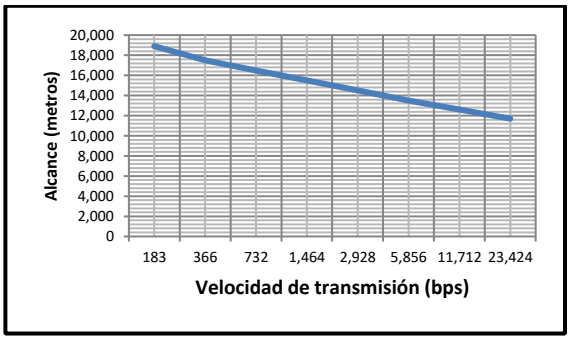

Figura 5. Alcance de la transmisión WiFi del sistema

Las ventajas o fortalezas del sistema son las siguientes: 1) Puede usarse fácilmente en cualquier tipo de instalación, no solo en un centro de datos, ya que usa comunicación inalámbrica WiFi, la cual es no intrusiva y está presente casi en cualquier laboratorio, industria u hogar a través de un punto de acceso, 2) El mecanismo de identificación, a través de tarjetas RFiD, es sencillo, rápido y seguro. El costo de una tarjeta RFiD es 0.5 USD y 3) Es fácilmente escalable, ya que si es necesario adicionar nodos de lectura solo deben realizarse ajustes sencillos en la programación del nodo de validación. Si el nodo de validación se localiza a más de 70 metros, el alcance de la transmisión inalámbrica puede incrementarse usando un router o un repetidor WiFi.

La innovación de este sistema en el mercado es que utiliza tecnología inalámbrica. Los dispositivos similares comercialmente disponibles usan tecnología alambrada. Otra innovación es que la administración del sistema se realiza desde un solo punto, en el nodo de validación, ya que usa una base de datos centralizada. Los sistemas comercialmente disponibles usan una base de datos distribuida y para dar de alta un usuario o realizar un cambio, el administrador debe acceder la base de datos de cada nodo del sistema. Adicionalmente, los componentes usados en el desarrollo de este sistema son de reciente tecnología, más confiables, rápidos y más económicos. El costo de este sistema es la cuarta parte de uno disponible en el mercado con funcionalidades similares.

El sistema ha sido probado y evaluado en el centro de datos y se ha solicitado realizar una segunda versión que incorpore en los nodos de lectura tres funcionalidades: A) Una pantalla LCD para mostrar el nombre de usuario leído de la tarjeta RFiD y el mensaje resultado de la validación, B) Un teclado numérico mediante el cual el usuario proporcione una clave y C) Que el nodo de validación realice reconocimiento facial del usuario. Estas características adicionales tienen como objetivo contar con tres validaciones: el UUID de la Tarjeta RFiD, la clave numérica y el reconocimiento facial.

Finalmente, el sistema construido no fue solo una investigación si no que actualmente se aplica en una situación real y práctica.

V. AGRADECIMIENTOS

Los autores agradecen a la Universidad Autónoma Metropolitana Azcapotzalco por las facilidades otorgadas para la realización de este proyecto.

VI. REFERENCIAS

[1] Lima, V. M., Lima, R. M. y Lins, F.A. (2017). "A multi-perspective methodology for evaluating the security maturity of data centers", *in Proceedings IEEE International Conference on Systems*, pp. 1196-1201.

[2] Miloslavskaya, N. (2017). "Security Intelligence Centers for Big Data Processing", *in Proceedings 5th International Conference on Future Internet of Things and Cloud Workshops*, pp. 7-13.

[3] Mittal, Y., Varshney, A. y Aggarwal, P. (2015). "Fingerprint biometric based Access Control and Classroom Attendance Management System", *in Proceedings Annual IEEE India Conference (INDICON)*, pp. 1-6.

[4] Dudheria, R. (2017). "Evaluating Features and Effectiveness of Secure QR Code Scanners", *in Proceedings International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pp. 40-49.

[5] Srinivasan, V. S., Kumar, S. T. y Yasarapu, D. K. (2016). "Raspberry Pi and iBeacons as environmental data monitors and the potential applications in a growing BigData ecosystem", *in Proceedings IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology*, pp. 961-965.

[6] Cui, J., She, D. y Ma, J. (2015). "A New Logistics Distribution Scheme Based on NFC", *in Proceedings International Conference on Network and Information Systems for Computers*, pp. 492-495.

[7] Palencia, G. P., Bernadez, H. L. y Enriquez, H. L. (2015). "Time-controlled access with power management using RFID acquisition and power control distribution", *in Proceedings International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control Environment*, pp. 1-7.

[8] Degadwala, S. D. y Gaur, S. (2017). "Two way privacy preserving system using combine approach: QR-code & VCS", *in Proceedings Innovations in Power and Advanced Computing Technologies (i-PACT)*, pp. 1-5.

[9] Wang, X. L., Wu, C. F. y Li, G. D. (2017). "A robot navigation method based on RFID and QR code in the warehouse", *in Proceedings Chinese Automation Congress (CAC)*, pp. 7837-7840.

[10] Cavanini, L., Cimini, G. y Ferracuti, F. (2017). "A QR-code localization system for mobile robots: Application to smart wheelchairs", *in Proceedings European Conference on Mobile Robots (ECMR)*, pp. 1-6.

[11] Harshith, K., Montana, E. y Manki, M. (2017). "Product authentication using hash chains and printed QR codes", *in Proceedings 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 319-324.

[12] Kavitha, K. J., y Shan, B. P. (2017). "Implementation of DWM for medical images using IWT and QR code as a watermark", *in Proceedings Conference on Emerging Devices and Smart Systems (ICEDSS)*, pp. 252-255.

[13] Pramkeaw, P., Ganokratanaa, T. y Phatchuay, S. (2016). "Integration of Watermarking and QR Code for Authentication of Data Center", *in Proceedings 12th International Conference on Signal-Image Technology & Internet-Based Systems*, pp. 669-672.

[14] Goel, N., Sharma, A. y Goswami, S. (2017). "A way to secure a QR code: SQR", *in Proceedings International Conference on Computing, Communication and Automation (ICCCA)*, pp. 494-497.

[15] Lay, K. T. y Zhou, M. H. (2017). "Perspective projection for decoding of QR codes posted on cylinders", *in Proceedings IEEE International Conference on Signal and Image Processing Applications (ICSIPA)*, pp. 39-42.

[16] Mishra, A., Kumar, K. y Rai, S. N. (2015). "Multi-stage face recognition for biometric access", *in Proceedings Annual IEEE India Conference (INDICON)*, pp. 1-6.

[17] Geralde, D. D., Manaloto, D. D. y Loresca, D. E. (2017). "Microcontroller-based room access control system with professor attendance monitoring using fingerprint biometrics technology with backup keypad access system", *in Proceedings IEEE 9th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM)*, pp. 1-7.

[18] Addy, D. y Bala, P. (2016). "Physical access control based on biometrics and GSM", *in Proceedings International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 1995-2001.

VII. BIOGRAFÍA

Vega-Luna José Ignacio. Estado de México, 1962. Ingeniería Electrónica, UAM-Azcapotzalco, Cd. de México, 1985. Maestría en Ciencias de la Computación, UAM-Azcapotzalco, Cd. de México, 1990.

Él labora actualmente en el área de Sistemas Digitales del Departamento de electrónica de la UAM-Azcapotzalco. Sus líneas de trabajo son: aplicaciones de microprocesadores y microcontroladores y sistemas operativos.

M. en C. Vega realiza investigación con redes inalámbricas de sensores y actuadores.

Cosme-Aceves José Francisco. Atlixco, Puebla, México, 1958. Ingeniería Electrónica, UAM-Azcapotzalco, Cd. de México, 1985.

Él labora actualmente en el Departamento de Electrónica de la UAM-Azcapotzalco. Su línea de trabajo es lenguajes de descripción de hardware.

Ing. Cosme realiza investigación con sistemas embebidos y seguridad en redes de computadoras.

Sánchez-Rangel Francisco Rangel. Cd. de México, 1968. Ingeniería Electrónica, UAM-Azcapotzalco, Cd. de México, 1987. Maestría en Ciencias de la Computación, UAM-Azcapotzalco, Cd. de México, 1999.

Él labora actualmente en el Departamento de Electrónica de la UAM-Azcapotzalco. Sus líneas de trabajo son: aplicaciones de microprocesadores y microcontroladores y lenguajes de descripción de hardware.

M. en C. Sánchez realiza investigación con redes de computadoras y sistemas embebidos.

Salgado-Guzmán Gerardo. Cd. de México, 1968. Ingeniería Electrónica, UAM-Azcapotzalco, Cd. de México, 1992.

Él labora actualmente en el Departamento de Electrónica de la UAM-Azcapotzalco. Sus líneas de trabajo son: aplicaciones de microprocesadores y microcontroladores y sistemas operativos.

Ing. Salgado realiza investigación con redes inalámbricas de sensores y actuadores.