

Control de acceso basado en RFID sobre plataforma IoT

RFID-based access control over IoT platform

Ing. Yunior Ibarra Guerra ^{1*}, Ing. Alexander R. Ramírez Zaldívar, Dr.C. Eugenio Boudet Flore

Recibido: 10/2020 | Aceptado: 03/2021

Palabras clave

IoT
Control de acceso
RFID
Arduino Yún

Resumen

Se propone una solución factible para realizar el control de acceso a espacios restringidos empleando la tecnología de Identificación por Radiofrecuencia (RFID). A través de una red inalámbrica WiFi, el sistema puede ser accedido de forma remota, lo que posibilita su integración en una plataforma de Internet de las Cosas (IoT), empleando *hardware* y *software* libre como medios de obtención del conjunto. Mediante el uso de una placa Arduino Yún conectada a un lector RFID y un teléfono inteligente con sistema operativo Android, se establece un sistema de comunicación inalámbrica basado en el protocolo TCP. Resulta evidente la aplicabilidad de esta solución en entornos modernos donde la interconexión de los sistemas prevalece.

Keywords

IoT
Access control
RFID
Arduino Yún

Abstract

This paper proposes a feasible solution to implement access control in restricted places using Radio Frequency Identification (RFID) technology. Through wireless WiFi network, the system can be remotely accessible enabling its integration into an Internet of the Things (IoT) platform, using free hardware and open source as a means to obtain the array. With an ArduinoYún board connected to both a RFID reader and a smartphone with Android operating system a wireless communication system is set up based on the TCP protocol. It is clear the applicability of this solution in modern environments where system interconnection prevails.

Introducción

El abaratamiento en el mercado de los circuitos integrados de alta escala de integración ha posibilitado la creciente informatización de productos y servicios ligados a la aplicación del

Internet de las Cosas (IoT). El control de acceso automatizado no ha estado exento de tan significativos avances y sus variantes cubren un amplio rango de tecnologías, que abarcan desde lectores de tarjetas magnéticas, teclados con cerradura electrónica

^{1*} Centro de Investigación y Desarrollo de Electrónica y Mecánica, «CID MECATRONICS», La Habana, Cuba. cid3@reduim.cu

ca hasta lectores de huellas digitales. Hoy en día, los sistemas de identificación RFID –*Radio Frequency Identification*– presentan una elevada acogida a nivel mundial, pues han generado beneficios en las ramas de la vida social que la han adoptado. Su utilización incluye una amplia gama de aplicaciones, que van desde mecanismos de seguridad, acceso de personal, pagos a pequeña escala, identificación y logística de productos, ahorro de energía eléctrica (Mahdin, Abawajy y Yaacob, 2016 hasta llaves para puertas eléctricas entre otras (Jia, Feng y Lei, 2012. Ofrecen además la posibilidad de multifunción, al poder operar al mismo tiempo como medio de identificación y monedero electrónico de actividades que no requieran de transacciones considerables de efectivo, ni un alto grado de seguridad, tales como alimentación y transporte (Assaf y Williams, 2011 sin enunciar que constituye una tecnología clave en el Internet de las Cosas (Igoe, 2012).

Con el surgimiento del IoT y el desarrollo de los dispositivos inalámbricos, resulta relativamente sencillo el despliegue de estas tecnologías, en entornos donde el cableado constituye una barrera potencial. A nivel internacional se ha adoptado de forma generalizada, para regular la entrada del personal en espacios físicos restringidos, tales como centros de trabajo, bibliotecas, edificios u otros locales y un sinnúmero de aplicaciones prácticas que cada vez más facilitan la vida social. En el mundo, los primeros pasos en la automatización del control de acceso basado en esta tecnología ya supera la década, demostrando un marcado predominio en el mercado, la industria y la sociedad, sin embargo, en nuestro país aún no se han tomado muchas iniciativas para el despliegue de una tecnología que cada vez se vuelve más madura dado fundamentalmente por la falta de experiencias en su empleo. Aún persisten las cerraduras mecánicas sobre las electrónicas en la mayoría de las instalaciones domésticas y estatales, el pago del transporte público no posee ningún nivel de automatización y la mayoría de las instalaciones con acceso restringido poseen un nivel incipiente de automatización, lo cual genera demoras, disminuye los niveles de seguridad y la subutilización de la fuerza de trabajo en tareas repetitivas y en las cuales ni el costo del *hardware* ni la complejidad del *software* constituyen una barrera potencial. En (Díaz, Biosca, y González, 2018) se propone una al-

ternativa abarcadora en el empleo de esta tecnología, aunque la propuesta de la aplicación de gestión está basada en el empleo en un entorno web, el cual ha demostrado poseer marcadas ventajas, sobre todo, debido a su elevada compatibilidad en la mayoría de los sistemas operativos. Independientemente de las ventajas anteriores, el empleo de las aplicaciones móviles nativas y de escritorio presenta también determinadas ventajas claves que han llevado a la mayoría de los usuarios finales a inclinarse por estas últimas. La experiencia de usuario de las aplicaciones nativas es muy superior a la de las aplicaciones web. Para el usuario, el flujo es más natural debido a que cada sistema operativo posee sus propias guías y estándares para las interfaces gráficas. En una aplicación nativa la utilización y el acceso de todos los recursos del *hardware* se produce sin que medie un navegador web lo que condiciona una mayor velocidad de la conexión.

En la presente investigación se propone una solución factible para el control de acceso a instituciones donde se requiera autorización previa. El sistema propuesto emplea tarjetas y lectores RFID, controlados por una placa de desarrollo (basado en *hardware* libre), enlazada vía WiFi con un centro de control y gestión programado con tecnologías de *software* libre. Teniendo en cuenta que la gestión del sistema no pretende llegar a desplegarse en un ambiente distribuido, para lo cual son más propicias las aplicaciones web, se decidió emplear la alternativa de desarrollar una aplicación nativa para la gestión del control de acceso.

Materiales y métodos

Para alcanzar los objetivos propuestos se realizó un estudio de mercado sobre las tecnologías más accesibles desde el punto de vista económico y de respaldo documental. Se empleó el método analítico sistémico para extraer los elementos fundamentales en la bibliografía consultada con el objetivo de establecer una propuesta adecuada según los requerimientos del sistema. Debido a las limitaciones tecnológicas en nuestro país con respecto a la fabricación de circuitos impresos, así como la importación de componentes electrónicos, se optó por la variante de emplear elementos de *hardware* y *software* libre en la mayor de las posibilidades.

Tecnología RFID

La identificación por radiofrecuencia (RFID), hace referencia a una tecnología para el intercambio inalámbrico de datos. De forma general, se compone de un dispositivo de lectura y grabación (denominado normalmente lector, codificador o interrogador) y una etiqueta (que posee internamente una antena y un chip encargado de realizar todo el proceso de comunicación) (metraTec RFID, 2010). El flujo de los datos se produce automáticamente, sin la intervención de un operador, cuando el procesador recibe a través de la antena la señal procedente del interrogador. La información enviada es almacenada en la memoria de la etiqueta, pudiendo ser, desde un simple código hasta un conjunto complejo de datos. Normalmente, el chip es energizado por la propia interfaz de radio, cuando se ubican lo suficientemente cerca, aunque coexisten variantes donde la tarjeta posee alimentación interna. Las etiquetas se adaptan a diferentes modelos, siendo las más comunes: tarjetas, llaveros, botones, medios adhesivos, e incluso incrustados en algunos productos. (Figura 1)

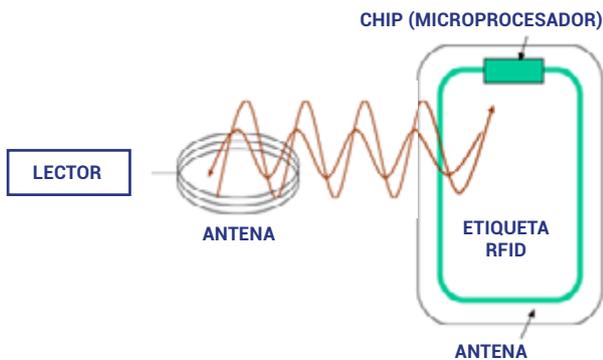


Figura 1. Composición de un sistema RFID

Estructura del sistema de control de acceso

El presente trabajo propone la implementación de un sistema con la arquitectura mostrada en la figura 2. Como se puede apreciar, está integrado por varias tarjetas RFID (cada una con un identificador único como clave de acceso y su correspondiente lector para realizar la adquisición de los datos). La placa de control se conecta directamente al interrogador, siendo la encargada de recibir los datos leídos y transmitirlos, a través de una red WiFi, al punto de acceso enlazado con el servidor de gestión y control, este último puede ser un equipo de escritorio o terminal móvil.



Figura 2. Estructura del sistema propuesto

La estructura será capaz de registrar la entrada y salida del personal, así como autorizar el acceso de acuerdo al sistema implementado, una variante puede ser controlar un actuador para abrir y cerrar una cerradura. El proyecto realizado se limita a la implementación de la etapa de registro y control del acceso, dejando como recomendación para futuros desarrollos el manejo del actuador para la regulación de acceso.

Hardware propuesto

Durante la selección de los elementos del diseño, fue tomada como premisa la condición de emplear *hardware* libre para garantizar la independencia tecnológica durante el proceso productivo, dado por el acceso a los diseños fuentes que permiten la generalización del sistema con costos mínimos de importación.

Lector RFID MFRC522

En la figura 3 se muestra el módulo seleccionado MFRC522, que permite operaciones de lectura/escritura para comunicación por radiofrecuencia a 13.56 MHz, empleando el protocolo SPI para el intercambio de información con el controlador.



Figura 3. Módulo lector RFID con el circuito integrado RC522

Tarjeta RFID MIFARE® Standard 1K

Considerando la relación costo-beneficio necesaria en la elección de los dispositivos, se seleccionó la tarjeta MIFARE® Standard 1K (metraTec RFID, 2011). En la figura 4 se muestra su estructura interna, compuesta por una antena espiral y el chip de control.



Figura 4. Estructura de una tarjeta MIFARE® 1K

La tarjeta RFID debe importarse en su totalidad, como consecuencia de sus elevadas exigencias tecnológicas en el proceso de fabricación.

Placa de desarrollo Arduino Yún

El Arduino Yún (figura 5) es una placa programable que soporta en uno de sus procesadores un sistema operativo en base Linux (OpenWrt-Yún).



Figura 5. Placa de desarrollo Arduino Yún

La principal novedad del dispositivo es la incorporación de un módulo capaz de generar una red WiFi permitiendo su programación y el acceso al sistema operativo de forma remota.

Descripción e interconexión del hardware seleccionado

Como se mencionó, el módulo RFID MFRC522 emplea el protocolo de comunicación SPI para conec-

tarse con el controlador. En la placa Arduino Yún los pines dedicados a este protocolo se encuentran presentes en el conector ICSP.

En la figura 6 se muestra la conexión entre la placa Arduino Yún y el Módulo RFID MFRC522.

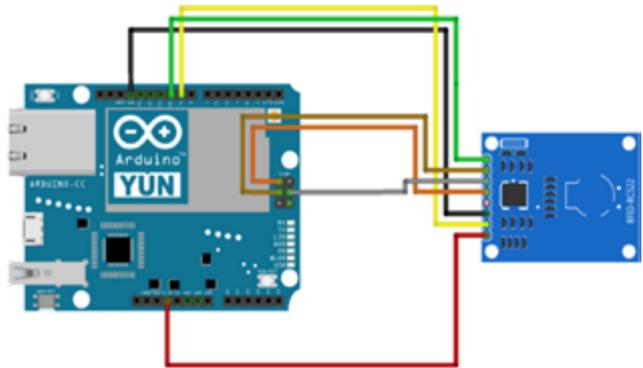


Figura 6. Conexión del módulo RFID MFRC522 a la placa Arduino Yún

Programa en Arduino Yún

La programación de la placa Arduino Yún se realizó desde el IDE Arduino 1.8.2. Para lograr la comunicación con el protocolo TCP, fue empleada la clase “BridgeClient” disponible en el IDE, a través de la cual se intercambia información de cualquier interfaz de red (WiFi o Ethernet). En la lectura de la tarjeta RFID se utilizó la clase de uso libre “MFC522” disponible en (GitHub, 2020). En la figura 7 es mostrado el diagrama del algoritmo implementado.

Aplicación de gestión y control

En el desarrollo de la aplicación de gestión y control se tuvo en cuenta la posibilidad de conexión inalámbrica vía WiFi o cableada a través de Ethernet, así como la multiplataforma con el objetivo de instalarla tanto desde una computadora de escritorio con sistema operativo Windows® o Linux como en dispositivos móviles con sistema operativo Android. Por tales motivos, fue seleccionado el framework Qt Creator 5.7 (Qt (a), 2020). Esta investigación se limita a describir únicamente el proceso de desarrollo de la aplicación en Windows® y Android, diferenciándose solamente por la inclusión de las herramientas de compilación correspondientes. En (Qt (b), 2020) se explican las configuraciones pertinentes en las opciones del *framework* para realizar la compilación para el sistema operativo Android. En la figura 8 se muestra la selección de los

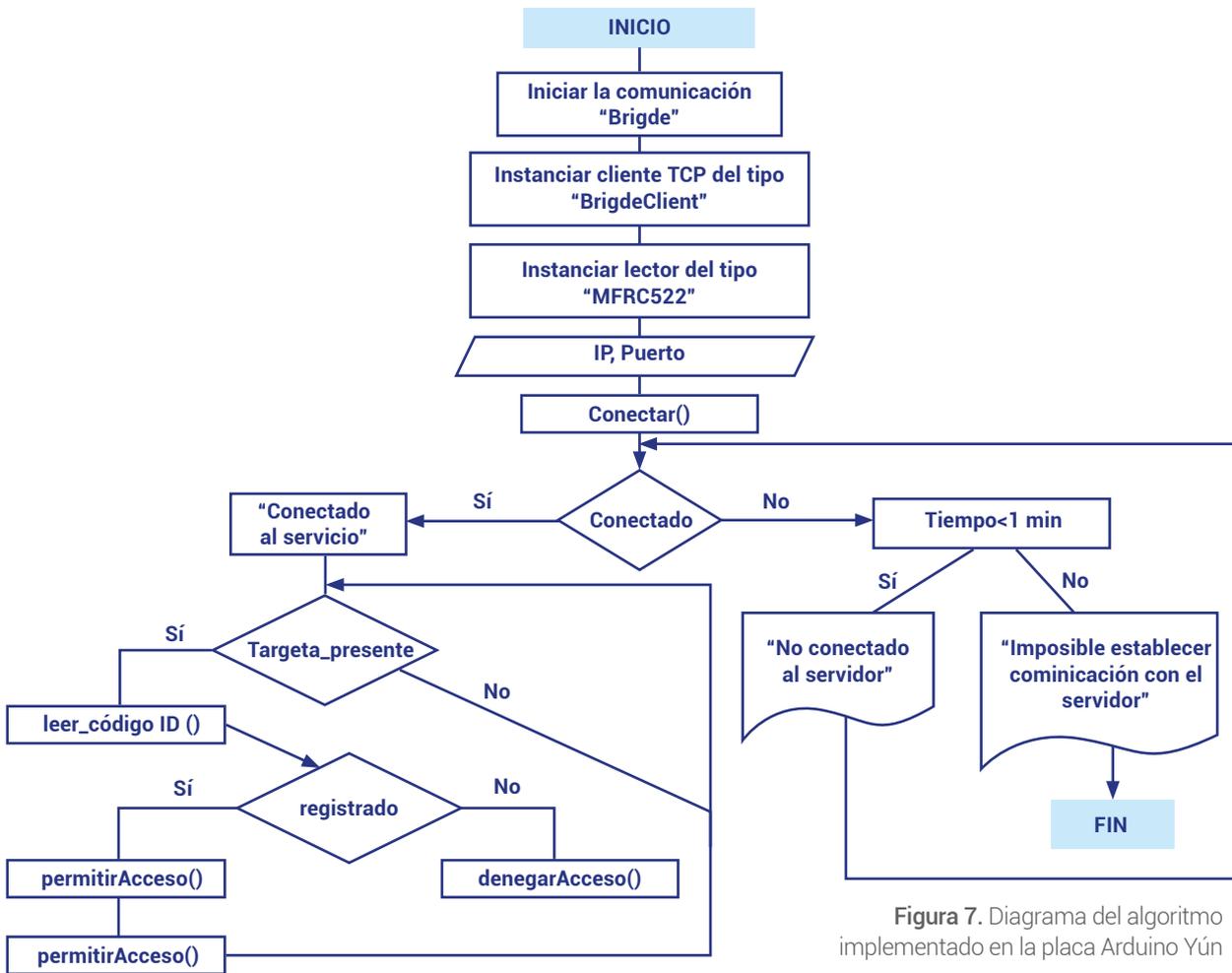


Figura 7. Diagrama del algoritmo implementado en la placa Arduino Yún

compiladores ya configurados para las diferentes plataformas.

Considerando la arquitectura de *hardware*, para realizar la programación de la aplicación se empleó el modelo cliente-servidor, donde la tarjeta Arduino Yún opera como cliente y el *software* de gestión y control es el servidor. El protocolo empleado en la capa de transporte de la arquitectura fue TCP, pues al ser orientado a conexión, proporciona un medio fiable para el flujo de bits entre aplicaciones (Goralski, 2017), teniendo en cuenta que no se transmitirán grandes volúmenes de datos la entrega de paquetes no implicará una demora significativa. Para el desarrollo del servidor fue utilizada la biblioteca “QTcpServer” (Qt (b), 2020) y “QTcpSocket”. El diagrama del algoritmo propuesto se muestra en la figura 9.

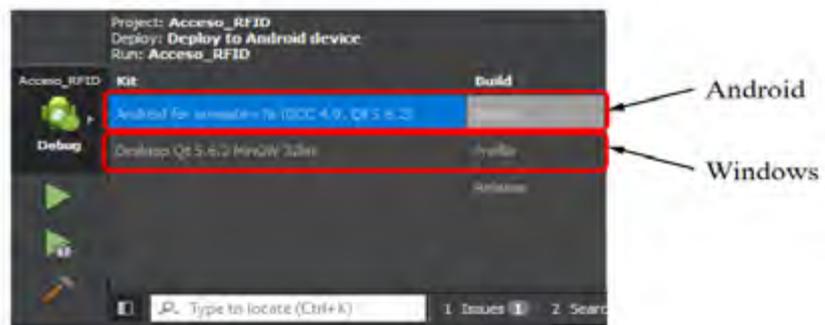


Figura 8. Selección del compilador para cada arquitectura

Resultados y discusión

Pruebas funcionales del sistema

Para llevar a cabo las pruebas funcionales del sistema, se realizó la interconexión de los componentes mediante una *protoboard* (Figura 10). El punto de control con el Arduino Yún fue situado a una distancia de 20m del servidor y alimentado por un cargador portátil.

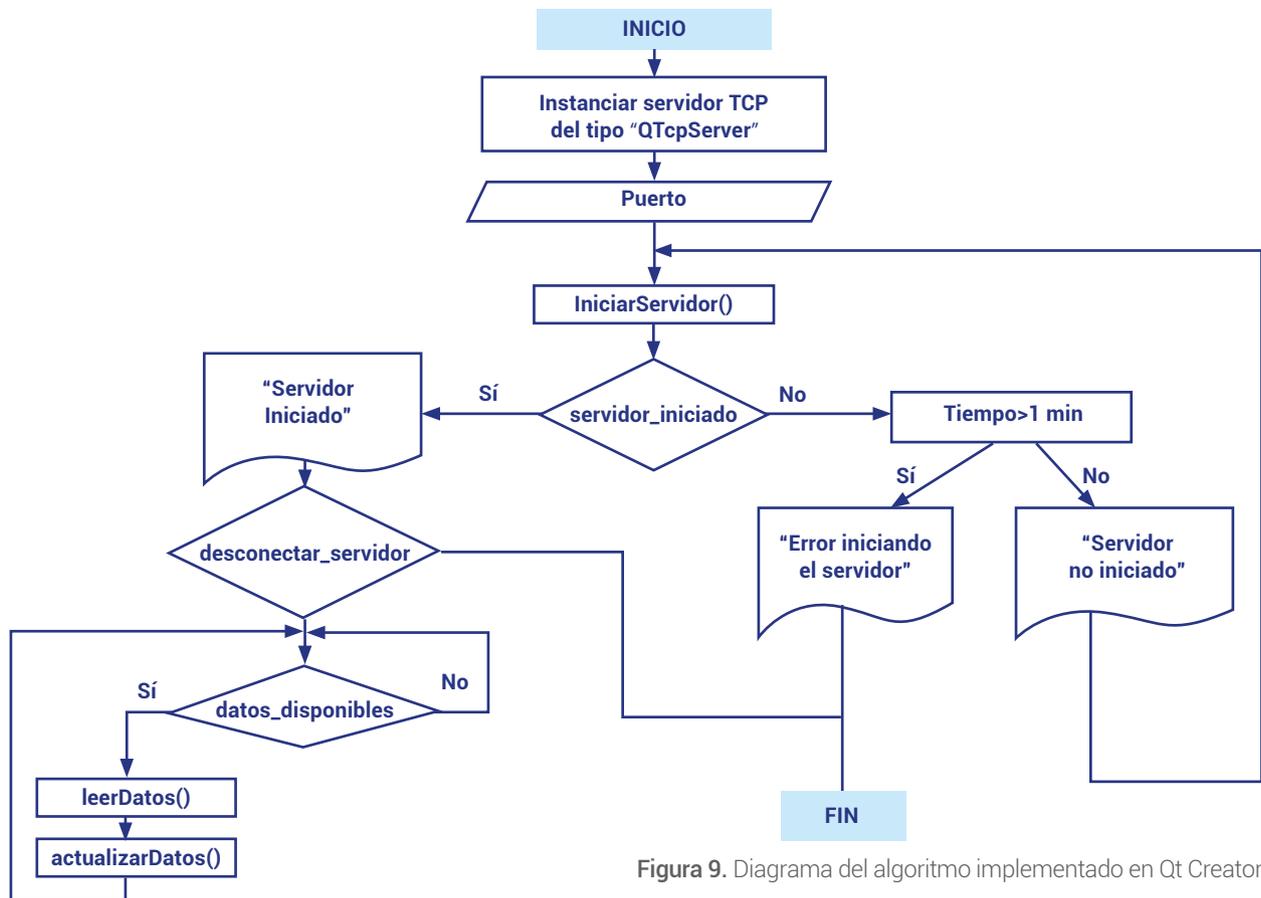


Figura 9. Diagrama del algoritmo implementado en Qt Creator

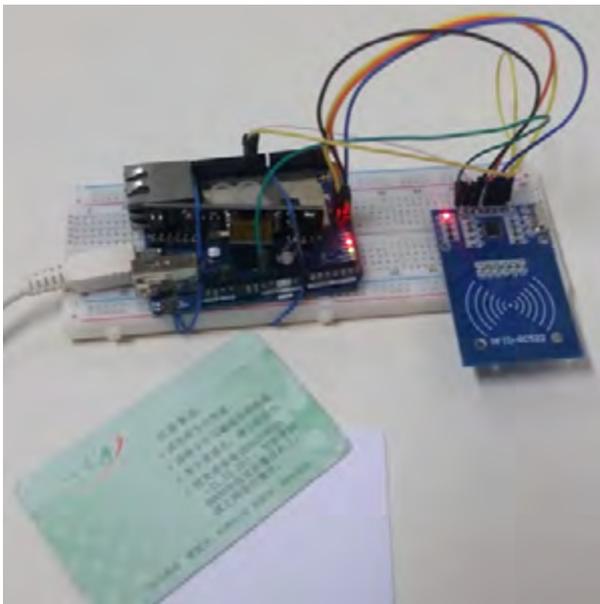


Figura 10. Hardware empleado durante las pruebas de funcionamiento

En un teléfono inteligente con Android 6.0, se alojó el servidor TCP creando un punto de acceso en la banda de 2.4 GHz (única soportada por el Arduino Yún) con el nombre de “AccesoRFID” y seguridad

WPA2 (Faruk, 2018). Los datos fueron introducidos en la página de configuración del Arduino, así como establecida la asignación estática de su dirección IP para diferenciar la existencia de más de una tarjeta conectada al servidor. En la conexión inalámbrica, la potencia recibida resulta un parámetro clave en la caracterización del enlace; por lo que se valoró la cobertura del sistema a diferentes distancias; empleando la antena integrada del Arduino Yún, determinando finalmente el valor máximo de alejamiento del emplazamiento. En la tabla 1 se muestra la dependencia de la potencia recibida contra la distancia al punto de acceso del servidor. Se puede apreciar que para distancias superiores a los 50m la potencia recibida se reduce significativamente haciendo inestable la conexión. Esta medición permite determinar la distancia máxima a la que se puede ubicar el punto de control con el empleo del punto de acceso embebido del Arduino Yún. Para mejorar los resultados obtenidos puede emplearse una antena direccional en el conector de radiofrecuencia presente en la placa o insertar un adaptador inalámbrico USB en su puerto para ser administrado por la distribución OpenWrt de Linux.

Distancia (m)	Potencia (dBm)
1	-33
5	-45
10	-50
20	-54
30	-58
40	-62
50	-69
60	-75

Tabla 1. Dependencia de la potencia recibida respecto a la distancia al punto de acceso Yún

En las pruebas fueron empleadas cinco tarjetas RFID; con diferentes identificadores, cuyos datos quedaron registrados en el servidor. En la figura 11 se muestra la aplicación durante el proceso de prueba.

Las pruebas corroboraron el correcto funcionamiento de la aplicación, así como el proceso de lectura y registro de los datos. El proceso de identificación se realizó de forma instantánea, a una distancia máxima de 7 cm entre la tarjeta y el lector, garantizando la rapidez requerida en el control de un punto clave en horario pico, durante la salida y entrada del personal.

Conclusiones

Se desarrolló un sistema de identificación por radiofrecuencia para garantizar el control de acceso basado en el Internet de las Cosas. A través del empleo del *hardware* y *software* libre se logra una elevada independencia tecnológica abaratando los costos de fabricación. La configuración adoptada permite sobre todo flexibilidad y escalabilidad siendo posible su despliegue en zonas donde resulta

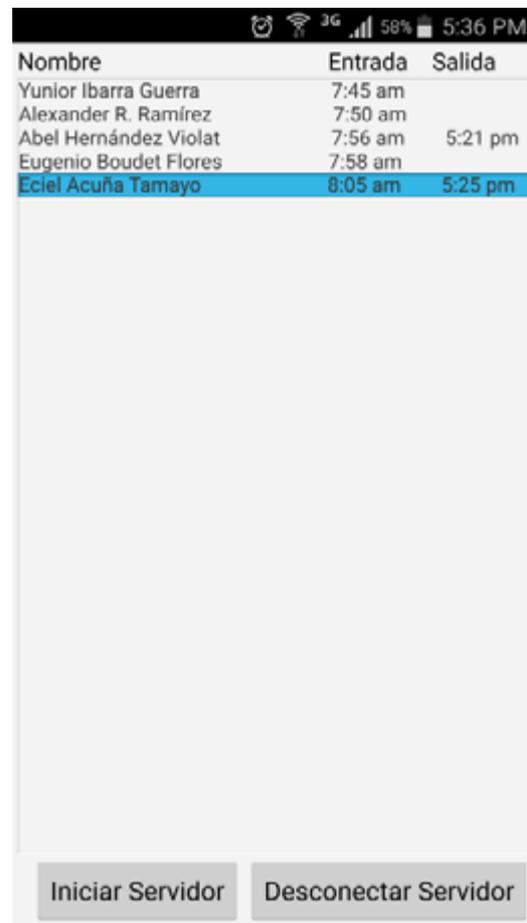


Figura 11. Aplicación de gestión y control programada en el SO Android

imposible una conexión cableada, así como la adición de nuevos nodos sin que repercuta significativamente en el diseño original. El empleo de tarjetas RFID posibilita la utilización del sistema como monedero electrónico simple y otras aplicaciones, coexistiendo con la implementación propuesta. Se recomienda para futuros trabajos incorporar en el módulo Arduino el control de los actuadores de acceso y de esa forma crear un punto de entrada no atendido.

Referencias bibliográficas

Assaf, M., y Williams, K. (2011). RFID for optimization of public transportation system. *Séptima Conferencia Internacional de Sensores Inteligentes, Redes de Sensores y Procesamiento de la Información*.

Díaz, C. P., Biosca, R. D., y González, J. G. (2018). Sistema IoT de control de acceso inteligente basado en Arduino y servicios web. *Revista Tono*, pp. 11-14.

- Faruk, S. (2018). *Building Smart Drones with ESP8266 and Arduino*. Estados Unidos: Pack.
- Goralski, W. (2017). *The Illustrated Network: How TCP/IP Works in a Modern Network*. Estados Unidos: Elsevier.
- GitHub (2020). Obtenido de: www.github.com/miguelbalboa/rfid
- Igoe, T. (2012). *Getting Started with RFID*. Estados Unidos: O'Reilly.
- Jia, X; Feng, Q. y Lei, Q. (2012). RFID technology and its applications in Internet of the Things(IoT). Trabajo presentado en la *Segunda Conferencia Internacional de Electrónica de Consumo, Comunicaciones y Redes(CECNet)*.
- Mahdin, H.; Abawajy, J. y Yaacob, S. (2016). Energy Efficient Approach in RFID Network. Trabajo presentado en el *Simposio Internacional de Ingeniería e Innovación (IRIS)*.
- metraTec RFID Solutions (2010). *MIFARE Protocol Guide*. Estados Unidos: metraTec RFID Solutions.
- metraTec RFID Solutions (2011). *MIFARE Classic 1K-Mainstream contactless smart card IC for fast and easy solution development, Rev 3.1. In*.
- Qt (a) (2020). *Qt Cross-platform software development for embedded & desktop*. Obtenido de: www.qt.io
- Qt (b) (2020). Qt Help. Obtenido de: <https://doc.qt.io/qt-5>

