VISIÓN ELECTRÓNICA

Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido
Fecha de envío:
Fecha de recepción:
Fecha de aceptación:

SISTEMA DE ALERTA REMOTA Y CONTROL DE ACCESO MEDIANTE RFID

REMOTE ALERT SYSTEM AND ACCESS CONTROL BY RFID

Pulido Porras Fabian Antonio[1]. Carrillo Romero Cristhian David[2]. Fonseca Velasquez Aldemar[3].

Resumen*:* En el siguiente artículo se describe el desarrollo y la implementación de un sistema de alerta remota y control de acceso mediante RFID (Radio Frequency Identification), el cual está destinado para el grupo de investigación INTEGRA de la Universidad Distrital Francisco José de Caldas en la Facultad Tecnológica; con el fin de facilitar el ingreso a la sala a todos los estudiantes pertenecientes a dicho grupo, de esta manera quienes se encuentren desarrollando un trabajo de investigación u otro proyecto podrán usar la sala como lo requieran.

El sistema de control de acceso se compone de dos partes fundamentales, la primera es un dispositivo móvil con sistema operativo Android, en el cual se instala una aplicación que se encarga de llevar un registro de todas las personas que ingresan a la sala mediante una tarjeta con tecnología RFID, además de esto la aplicación es capaz de agregar y eliminar en tiempo real usuarios de la sala. Existen dos tipos de aplicación, la primera pertenece al administrador esta es capaz de agregar moderadores y de realizar todas las funciones, la segunda pertenece al moderador el cual puede ver los registros, agregar y eliminar usuarios del salón pero no agregar nuevos moderadores. En ambos casos se contara con una alerta en forma de notificación dentro del celular. La segunda parte es una base de datos no SQL

[1] Estudiante de Tecnología en electrónica. Universidad Distrital Francisco José de Caldas, Facultad Tecnológica. Correo electrónico e-mail: Fapulidop@correo.udistrital.edu.co

[2] Estudiante de Tecnología en electrónica. Universidad Distrital Francisco José de Caldas, Facultad Tecnológica. Correo electrónico e-mail: Cdcarrillor@correo.udistrital.edu.co

[3] Magister en Ingeniería Biomédica. Especialización En Teleinformática. Ingeniero en electrónica. Universidad Distrital Francisco José de Caldas, Facultad Tecnológica. Correo electrónico e-mail: Afonsecav@udistrital.edu.co

llamada Firebase, esta se encuentra en línea y es capaz de recibir y almacenar información en tiempo real siempre y cuando se cuente con una conexión estable a internet. Esta es parte importante del proyecto ya que en ella se encuentran los usuarios y los registros de toda la sala. Como tercer y última parte se encuentra un bloque de control el cual realiza una consulta a la base de datos para validar la información que se recibe mediante el lector RFID para así realizar el desbloqueo de la puerta y el posterior envió de información relacionada al acceso (hora, fecha y Nombre del usuario).

Palabras clave: Android, Base de datos, Control acceso, Firebase, Puerta, Tag RFID, Registro.

Abstract:

The following article describes the development and implementation of a remote alert and access control system using RFID, which is intended for the INTEGRA research group of the Francisco José de Caldas District University in the Technological Faculty; in order to facilitate the entrance to the room to all the students belonging to this group, in this way those who are developing a research work or another project can use the room as required.

The access control system consists of two fundamental parts, the first is a mobile device with Android operating system, which installs an application that keeps track of all people entering the room using a card with RFID technology, in addition to this the application is able to add and remove real-time users of the room. There are two types of application, the first belongs to the administrator and is able to add moderators and perform all functions, the second belongs to the moderator who can view the records, add and delete users from the room but not add new moderators. In both cases there will be an alert in the form of notification within the cell. The second part is a non-SQL database called Firebase, it is online and is able to receive and store information in real time as long as you have a stable internet connection. This is an important part of the project since it contains the users and the registers of the whole room. As a third and last part, there is a control block which performs a query to the database to validate the information received by the RFID reader in order to perform the

Fecha de envío:
Fecha de recepción:
Fecha de aceptación:

unlocking of the gate and the subsequent sending of information related to access (time, date and user name).

Keywords: Android, Access Control, Database, Firebase, Gate, RFID Tag, Registry.

1. INTRODUCCIÓN

Actualmente se buscan soluciones que lleven a tener un control permanente en determinado sitio, en respuesta se han desarrollado sistemas de control, los cuales generan restricciones a usuarios en estas áreas determinadas. Día tras día se ha visto la necesidad de elevar niveles en términos de seguridad y como se ve actualmente , el acceso es uno de los mas importantes, en respuesta a esto se entregan al mercado miles de soluciones las cuales cumplen distintos requerimientos de seguridad.

Hoy en día existen gran variedad de tecnologías que son capaces de validar la información para realizar el control de acceso, entre ellas se encuentran tarjetas de banda magnética, tarjetas de chip (Smart Card), tarjetas RFID y lectores biométricos, algunas de estas con validación más confiable que otras. En este artículo se mostrara el RFID como base principal de identificación y validación dentro de un control de acceso.

Se presenta una revisión del estado del arte para un sistema de alerta remota y control de acceso mediante RFID. Se definirán los conceptos básicos que permitirán reconocer los alcances y ventajas de dicho proyecto dentro de un espacio específico, se hace un análisis de los diferentes tipos de identificación de personas dentro de un sistema. Se mostrara el desarrolló una aplicación móvil en la plataforma de Android Studio con lenguaje de programación basado en Java, en la cual se diseñó una interfaz de fácil manejo donde se utilizaron los servicios de google para observar en tiempo real los accesos que se presentan,además de ver y modificar los usuarios habilitados a ingresar.

Fecha de envío:
Fecha de recepción:
Fecha de aceptación:

Finalmente se presentaran los detalles de la implementación del sistema de acceso y alerta remota dentro de la sala del grupo de investigación INTEGRA y se resaltaran las características, ventajas y desventajas que se pudieron encontrar durante dicho proceso.

2. ESTADO DEL ARTE

Desde hace varios años existe un sin número de tecnologías enfocadas al reconociendo por medios electrónicos, estas han brindado una gran cantidad de aplicaciones que han facilitado la identificación de muchas cosas de la vida cotidiana. Una de estas aplicaciones es el control de acceso a personal en un ambiente específico, como lo es una empresa, una sala de eventos o algún sitio con acceso restringido. [1]

RFID es un sistema que se usa para la identificación de objetos usando tecnología de campo eléctrico cercano , es decir envía un ID único a través de ondas de radio.

Hace algún tiempo se han estado implementando torniquetes, estos son dispositivos constituidos por tres o cuatro barras que giran sobre un eje vertical, comúnmente se ubican en la entrada de un lugar para hacer pasar a las personas de una en una. Estos torniquetes se han venido complementado con sensores biométricos y tarjetas RFID proporcionando seguridad mediante reconocimiento de huellas o mediante el uso de una tarjeta personal. [2]

El NFC (Near Field Communication) es una tecnología de identificación inalámbrica que en 2003 fue aprobada como estándar ISO/IEC, es una rama del RFID, funciona en la banda de los 13.56MHz y esto la hace muy atractiva para proyectos simples, puesto que no se necesita licencia para usarla.[3]

El NFC en la vida cotidiana está poco a poco expandiéndose para abarcar varios aspectos y actividades en los que nos puede ayudar. Nokia es una compañía que se ha interesado en dar un gran uso a esta tecnología mediante sus teléfonos inteligentes, tanto así que realizó una encuesta para conocer los usos que se le da a la tecnología NFC además de esto preguntaron cuáles podrían ser los usos que los usuarios comunes desearían darle a esta tecnología.[4][5]

Fecha de envío:
Fecha de recepción:
Fecha de aceptación:

Según los datos obtenidos por la compañía finlandesa, el 22% de los usuarios mencionó que usa el NFC y el RFID para conectar accesorios esto es debido a que facilita el emparejamiento entre dispositivos por medio de un solo toque.

El 19% optó por el poder compartir fotos y videos, una de las características más comunes y la que se muestra en muchos comerciales. El 17% de usuarios no está utilizando el NFC, pero la encuesta no fue capaz de identificar a qué se debe, por lo que hay varias suposiciones al respecto como que su Smartphone o dispositivo no cuente con dicha tecnología o simplemente no le han encontrado un uso productivo. En la Figura 1 se pude observar el resultado de esta primer encuesta.[6]



Figura 1 Resultados de encuesta sobre NFC[6]

Un uso común de las tarjetas RFID para llevar control de las personas que ingresan a un lugar, se encuentra en un gran número de compañías donde se hace necesario el registro de la hora en la que los trabajadores comienzan o finalizan sus jornadas laborales. En el mayor de los casos se asigna una tarjeta a cada integrante de la compañía, la cual posee información específica, esta genera un registro puntual referente al ingreso. Un buen ejemplo de esto es el dispositivo de la empresa Asensio sistemas s.a. llamado “Control de personal GS4”, este sistema posee un módulo capaz de identificar un total de 30000 tarjetas distintas y añade un teclado opcional para identificar usuarios por medio una clave. [7][8]

Como vemos cuando de seguridad se trata una buena alternativa es el uso del RFID como identificación frente a un dispositivo. Esta tecnología ofrece ventajas respecto a las demás por ejemplo una tarjeta RFID es más cómoda de usar a comparación de una clave o un

patrón asignado , también es una tecnología de bajo costo, los desgastes de sensores son mínimos y su índice de clonación es muy baja debido a su corto alcance. [9][10]

3. PROTOTIPO

A continuación se observa el diagrama que muestra cómo se diseñó este prototipo.

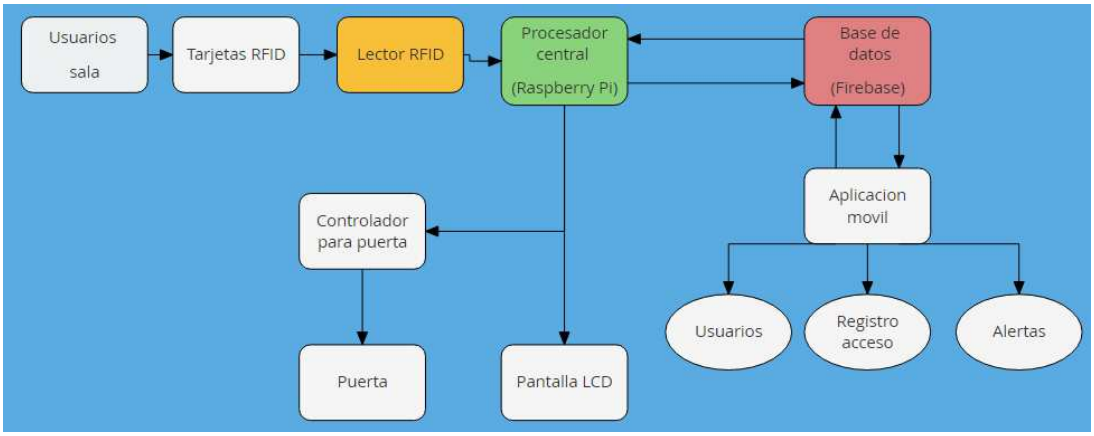


Figura 2: Diagrama del prototipo (Elaboración propia).

3.1. RFID

RFID o identificación por radiofrecuencia (del inglés Radio Frequency Identification) es un sistema de almacenamiento y recuperación de datos remotos que usa dispositivos denominados etiquetas, tarjetas o transpondedores RFID. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio. Las tecnologías RFID se agrupan dentro de las denominadas Auto ID (automatic identification, o identificación automática).[11]

Un sistema RFID consta de los siguientes tres componentes:

- *Etiqueta RFID o transpondedor:* compuesta por una antena, un transductor radio y un material encapsulado o chip.
- *Lector de RFID o transceptor:* compuesto por una antena, un transceptor y un decodificador.

- *Subsistema de procesamiento de datos o middleware RFID*: proporciona los medios de proceso y almacenamiento de datos.[12]

3.2. BASE DE DATOS No SQL

Parte importante de este prototipo son las bases de datos que se llevan a cabo para el sistema de control de acceso y para la alerta mediante la aplicación móvil.[13]

En informática, NoSQL es una amplia clase de sistemas de gestión de bases de datos que difieren del modelo clásico de SGBDR (Sistema de Gestión de Bases de Datos Relacionales) en aspectos importantes, siendo el más destacado que no usan SQL como lenguaje principal de consultas. Los datos almacenados no requieren estructuras fijas como tablas, normalmente no soportan operaciones JOIN, ni garantizan completamente ACID (atomicidad, consistencia, aislamiento y durabilidad), y habitualmente escalan bien horizontalmente.[14][15]

3.3. FIREBASE

Firebase es una plataforma de desarrollo de aplicaciones móviles y web desarrollada por Firebase, Inc. en 2011, luego adquirida por Google en 2014. Inicio como una plataforma de chat hasta que sus creadores descubrieron que estaba siendo empleada para almacenar otro tipo de datos. Luego de que Google la adquirió creció y amplió sus servicios para convertirse en una plataforma unificada para desarrolladores móviles. Firebase ahora se integra con otros servicios de Google para ofrecer productos más amplios y variados para desarrolladores. [16]

3.3.1. Servicios

Estos son algunos de los servicios más importantes de la plataforma Firebase:

- **Analytics**

  Firebase Analytics

- **Develop**

Firebase Cloud Messaging, Firebase Auth, Base de datos en tiempo real, Almacenamiento en Firebase,Firebase Hosting [17][18]

4. RESULTADOS

El primer componente de este proyecto es su aplicación para teléfonos móviles Android, esta se realizó en Android Studio que es una plataforma con leguaje de programación java, su estructura es de forma modular, lo cual hace que por medio de métodos tipo void la implementación de código sea más entendible y cómoda.

El primer paso que se tuvo en cuenta fue la configuración de la aplicación, esto por medio de la versión de APIs y SDK las cuales dotan de compatibilidad entre versiones de Android, en este caso se realiza el programa con la versión 26 del SDK y se da compatibilidad mínima con la versión 14, esto quiere decir que dicha aplicación se puede ejecutar a partir de Android 4.0 hasta Android 7.0. Luego de esto se importaron las dependencias necesarias, como Firebase, RecycleView, CardView, entre otras (Ver Figura 3), estas son las encargadas de traer todas las herramientas necesarias para la base de datos Firebase y todo lo relacionado a los cuadros donde se visualiza la información en pantalla.

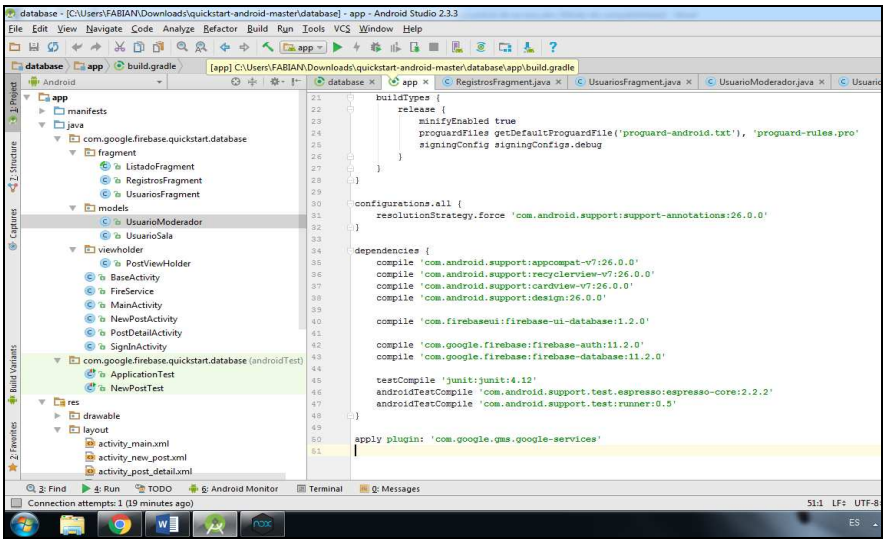


Figura 3 : Interfaz codigo Android Studio.

A partir de ahora se empezara a usar la siguiente notación para evitar confusiones; existen tres tipos de personas dentro de la aplicación, la primera es el administrador, este es quien

Fecha de envío:
Fecha de recepción:
Fecha de aceptación:

tiene la capacidad de hacer todo tipo de acciones dentro de la aplicación (posee el mayor rango de importancia, por lo tanto será el director de grupo), el siguiente es el moderador, este solo será habilitado para usar la aplicación por el administrador (los moderadores serán profesores pertenecientes al grupo, representante de semillero, etc.), y por último, con el menor rango posible, se encuentra el usuario, este será quien está registrado y habilitado para ingresar la sala de INTEGRA (Estudiantes y demás, estos no tendrán acceso a la aplicación). Teniendo claro lo anterior se explicara el uso y funcionamiento de las partes de la aplicación.

Para la correcta visualización de datos dentro de la aplicación se hizo necesario el uso de un RecyclerView el cual es un contenedor de elementos en forma de lista, este tiene la ventaja que "recicla" los ítems que ya no son visibles por parte de los usuarios de la aplicación (Administrador y moderadores), esto hace que se útil en aplicaciones como esta, en donde las listas y el volumen de datos es un poco extenso.

La primera interfaz con la que se encuentran los moderadores y el administrador es una pantalla de inicio de sección. Como se observa en la figura 4, existen dos versiones para la aplicación, una para el administrador y la otra para el moderador, estas se diferencian en que la del administrador tiene el botón Registrar habilitado, así cuando se introduzca un correo nuevo y se pinche este botón este quedara registrado para el uso de la aplicación, la del moderador tendrá este botón deshabilitado y cuando intente registrar un nuevo correo saldrá una alerta como la que se muestra en la figura 5.



Figura 4: Interfaz de inicio de seccion.



Figura 5: Alerta aplicación moderadores

Lo anterior denota que solo el administrador puede realizar registros de nuevos moderadores. Si quien está usando la aplicación no ingresa un email y contraseña valida no podrá hacer uso de ninguna función. Una vez dentro de la aplicación se observan dos

pestañas (ver Figura 6), por un lado la pestaña USUARIOS y por el otro la pestaña REGISTROS. La pestaña USUARIOS presenta una lista de todas las personas habilitadas a ingresar a la sala de INTEGRA, ahí se muestran detalles como el usuario que los agrego (En el ejemplo de la Figura 6 "*fabiann10*"), el nombre del usuario y su UID de tarjeta RFID.

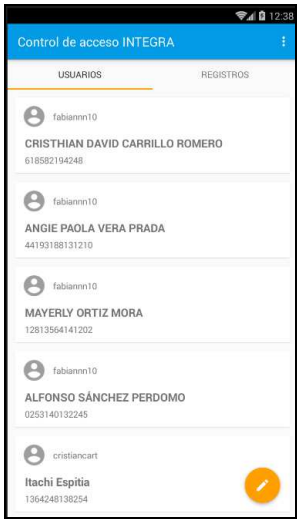


Figura 6 : Pestaña USUARIOS

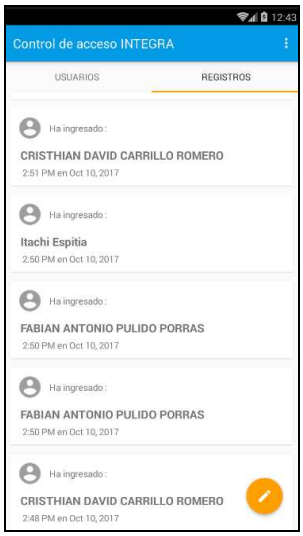


Figura 7: Pestaña REGISTROS

La pestaña REGISTROS muestra de una forma similar todos los usuarios que han ingresado a la sala de integra mediante su tarjeta RFID, la estructura de este listado entrega el nombre, la fecha y hora en que sucedió. (ver Figura 7).

Como se observa en la Figura 6 y 7 en la parte inferior derecha se observa un botón flotante de color amarillo, este tiene la función de registrar usuarios nuevos para la sala INTEGRA, es decir, al pulsar este botón flotante la aplicación entra en una pantalla (Ver Figura 8) donde solicitan los datos para el nuevo registro.



Figura 8 : interfaz para registro de nuevo usuario

Con ánimos de crear una aplicación segura además de útil, se habilito la opción de eliminar usuarios de la sala. Para eliminar un usuario se debe presionar sobre este, entonces la aplicación desplegara una pantalla de confirmación como la de la Figura 9 donde pregunta si realmente se desea eliminar la entrada.



Figura 9: Pantalla de confirmacion para eliminar usuarios.

Una de las cosas más interesantes de esta aplicación son sus notificaciones push, esto hace que cuando una persona llegue a la sala de INTEGRA presente su tarjeta RFID ante el lector y se abra la puerta, se envié una notificación al celular de los moderadores y del administrador dando el nombre de la persona quien recién ingreso. Estas notificaciones se visualizan como se observa en la Figura 10 y aparecen sin importar que el celular se encuentre en modo espera o no se tenga abierta la aplicación, estas funcionan en segundo plano.

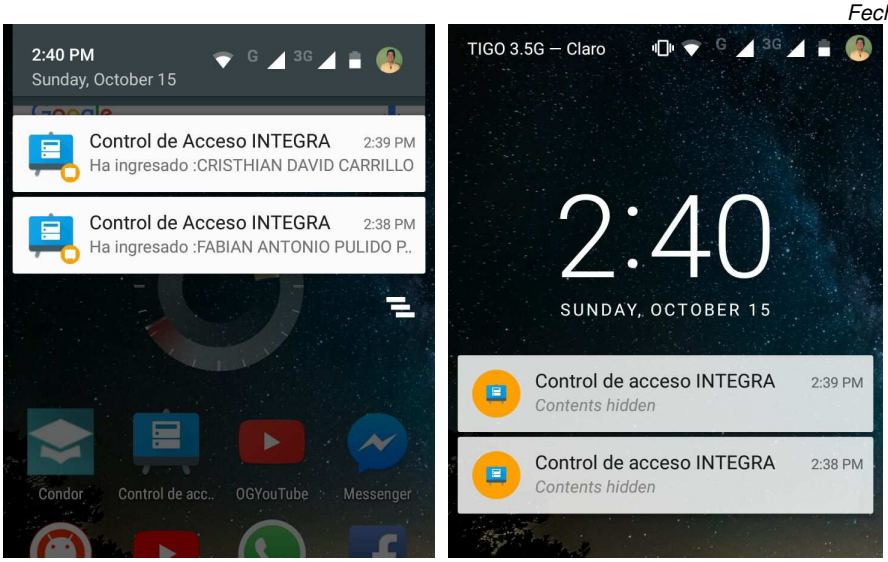


Figura 10: Notificaciones de ingreso a la sala INTEGRA

La base de datos implementada en este proyecto tiene como nombre Firebase. Firebase es una base de datos no JSON, esto quiere decir que no se organiza por medio de tablas ni métodos relacionales, si no que usa estructuras de directorios.

Se decidió usar Firebase por que tiene la posibilidad de interactuar con muchos lenguajes de programación en tiempo real siempre y cuando exista una conexión a internet por parte del dispositivo que requiera bajar o subir información a la base de datos. Para este proyecto se crearon dos variables y 3 ramas (Ver Figura 11).

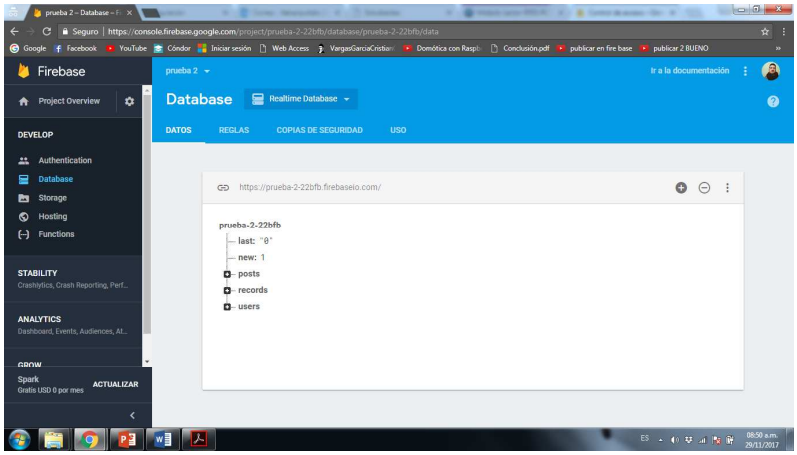


Figura 11 : Base de datos Firebase

La primera de las ramas tiene el key “last” y en la Figura 11 se observa que tiene un value “0”, esta variable es usada por el sistema para almacenar el nombre de la última persona que ingreso a la sala y poder publicar la notificación en la aplicación móvil de manera correcta, una vez la aplicación a generado la notificación este valor pasa a ser “0”. Esto con el fin de que si la notificación no ha llegado por falta de una conexión a internet en el móvil esta espere hasta que sea posible luego de publicada si se elimine. La siguiente key creada fue “new” esta alerta al sistema de un nuevo usuario registrado o así mismo de un usuario eliminado, esto con el fin de actualizar el sistema en tiempo real y no descargar siempre una copia de los usuarios si no que solo cuando sea necesario.

La base de datos actualmente cuenta con 3 ramas, una con key “posts”, otra con key “records” y la última llamada “users”. El key “posts se encarga de almacenar los usuarios con nombre, número de tarjeta y nombre del moderador que lo agrego” (Ver Figura 12).



Figura 12: Estructura de los usuarios en la base de datos Firebase

La rama con key “records” es la encargada de almacenar cada registro de ingreso a la sala, esta guarda el nombre del usuario que ingreso, la fecha y hora en que lo hizo y el número de tarjeta con el que ingreso. En la figura 13 se observa la estructura de este apartado.

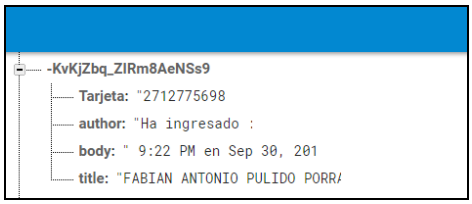


Figura 13: Estructura de registro de accesos a INTEGRA en Firebase

Por último, la rama users almacena los correos de los administradores y moderadores además de sus nombres de usuarios para así asociarlos a un key el cual será usado posteriormente para identificar quien ha registrado un usuario de INTEGRA nuevo. La base

de datos Firebase tiene una capacidad de 1 Gigabyte en su modo gratuito pero también ofrece planes pagos, el promedio de uso de espacio es de 20 Kilobytes cada dos días. Como vemos es una cifra despreciable en términos de almacenamiento.

Para el apartado de hardware del proyecto se uso una Raspberry pi 3B, al momento de esta encenderse se ejecuta automáticamente un código compilado en Python 3.4, el cual se encarga de usar una LCD de 16x2 para por medio de esta mostrar el estado del sistema. También se usa un lector de RFID con referencia RFID-RC522 (Ver Figura 14) con el cual se realiza la lectura de tarjetas de tipo Mifare 1k (Algunos de los carnets de la Universidad distrital cuentan con comunicación RFID esto quiere decir que pueden ser registrados en el sistema como una tarjeta normal).



- Modelo: MF522-ED.
- Corriente de operación: 13-26mA a 3.3V.
- Isb de stand by: 10-13mA a 3.3V.
- Ism de sleep-mode: <80uA.
- Im máxima: 30mA.
- Frecuencia de operación: 13.56Mhz.
- Distancia de lectura: 0 a 60mm.
- Protocolo de comunicación: SPI.
- Velocidad de datos máxima: 10Mbit/s.
- Dimensiones: 40 x 60 mm.
- Temperatura de operación: -20 a 80°C.
- Humedad de operación: 5%-95%.
- Máxima velocidad de SPI: 10Mbit/s.

Figura 14: Lector RFID-RC522 y tabla de datos. [14]

La raspberry se encarga se encarga de ejecutar un código llamado Control.py, este es el encargado de inicializar la LCD la cual muestra un mensaje de bienvenida e indica que el sistema está iniciando, en ese momento la raspberry configura los parámetros de conexión con la base de datos Firebase y posteriormente se realiza una copia de los usuarios habilitados a ingresar desde Firebase.

Luego de configurada la base de datos se crea un ciclo While el cual se encarga de esperar que el usuario acerque una tarjeta al lector RC 522, cuando esto sucede se pide leer el número de UID de la tarjeta que se usó, después se hace una verificación a la base de datos, si el programa detecta una modificación, este borra la copia de usuarios en el sistema y crea una nueva, actualizando así los usuarios eliminados o añadidos instantáneamente, esto con

el fin de reducir tiempos de comparación entre el usuario leído y la base de datos, pero al mismo tiempo se agregan y se eliminan usuarios de forma instantánea.

Después que se ha realizado la verificación de cambios en la base de datos, se procede a comparar cada UID que se encuentra almacenado y relacionado a un usuario en la base datos, con el UID que entrega la tarjeta por medio del lector RC 522, esto se hace por funciones repetitivas FOR como se muestra en la figura 15. Si se encuentra alguna coincidencia se activa una bandera llamada “FLAG” esta se encarga de tomar la posición del UID dentro de la base de datos y buscar esa misma posición el nombre del usuario relacionado. La bandera FLAG también tiene la función de tomar nombre del usuario, número de tarjeta (UID), la fecha y la hora para así publicarla a la base de datos y saber quién y en qué hora se presentó el acceso a la sala.

```
for usuarios in listaUsuarios:

    if (f==listaUsuarios[e])&(flag==False):
        flag=True
    if (f!=listaUsuarios[e])&(flag==False):
        flag=False

    if flag==False:
        e=e+1


if flag:
    print("ACCESO PERMITIDO A USUARIO :",listaNombres[e])
    print ("Hora y Fecha del ingreso: ",time.strftime('%l:%M %p en %b %d, %Y'))
    data2={"Nombre":listaNombres[e],
           "Tarjeta":listaUsuarios[e],
           "Hora y Fecha del ingreso":time.strftime('%l:%M %p en %b %d, %Y')}
    db.child("/Registro/Accesos").push(data2)
```

Figura 15 : verifiacion de usuarios por medio de codigo en Python.

Por último, el código después que ha realizado la actualización de los registros de ingresos a la sala se procede a activar un módulo relé por medio de un pulso lógico proveniente del GPIO de la raspberry, este lo único que hace es enviar un pulso en alto durante 2 segundos hacia la base de un transistor que activa la bobina la de un relé y a su vez este habilita la bobina de una chapa electromagnética como la de la figura 16.

Cabe aclarar que parte necesaria de este proyecto se basa en una conexión estable a internet por parte de la Raspberry, esta se precisa conectada a un punto Ethernet de la red de internet de la Universidad Distrital. A continuación se muestra un plano detallado de la conexión del hardware del proyecto.

Fecha de envío:
Fecha de recepción:
Fecha de aceptación:

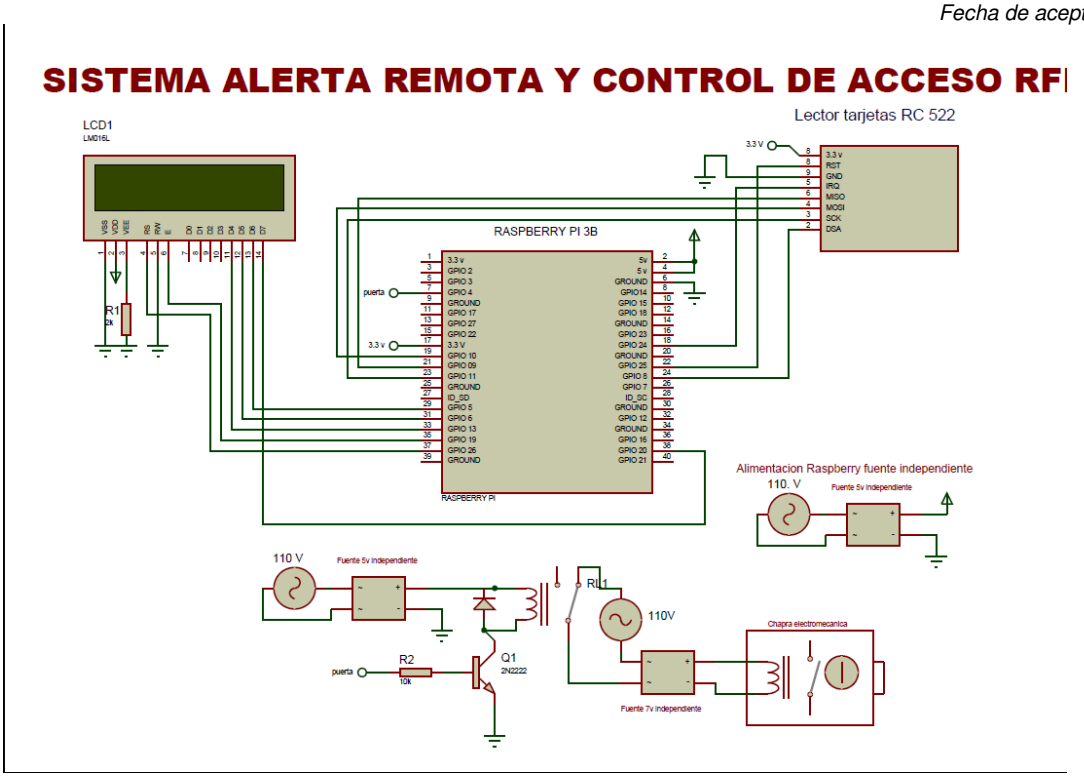


Figura 16: Chapa electromecánica Yale



Figura 17: Chapa electromecánica Yale

La chapa Yale (Figura 17) cuenta con un sistema de accionamiento mecánico mediante llave como cualquier chapa del común esto facilita su apertura en caso de falla eléctrica o emergencia. Por otro lado cuenta con un sistema de accionamiento electrónico, este se activa con una señal de voltaje de entre 7 y 12 voltios a 1,2 amperios, al momento que se recibe esta señal, la chapa internamente suelta un resorte que hala el pestillo de la chapa permitiendo abrir la puerta.

Fecha de envío:
Fecha de recepción:
Fecha de aceptación:

A continuación se muestra en la Figura 17 la parte exterior del salón, ahí se puede observar al lado izquierdo una caja metálica de color negro la cual contiene el lector Rc 522 y la lcd, y en el lado derecho la parte exterior de la chapa en color dorado.



Figura 17: Caja metálica y chapa ya instaladas en la puerta de INTEGRA

En la figura 18 se observa la caja con la lcd de color azul y en la Figura 19 el sistema ya en funcionamiento indicando un acceso denegado a un carnet de la universidad no registrado

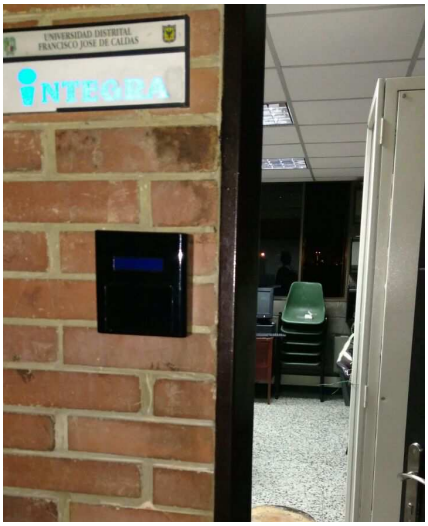


Figura 18: Caja en la puerta de INTEGRA



Figura 19: Control de acceso funcionando

5. CONCLUSIONES

- Android Studio es una plataforma bastante cómoda para el desarrollo de aplicaciones móviles, Los métodos nos ayudan a crear un programa modular, legible y manejable por parte del programador. El uso de estructuras llamadas Splits en los archivos de configuración de la aplicación, son de bastante utilidad para crear una aplicación compatible con cualquier

tamaño y densidad de pantalla, deben incluirse siempre que sea necesario para una correcta visualización.

- El diseño de una aplicación móvil siempre debe hacerse con una interfaz simple pero útil. Para aplicaciones en Android Studio donde se deba mostrar una gran cantidad de información en listas no es recomendable el uso de ListView, en este caso se observó que el uso de RecyclerView dentro de la aplicación consume menor cantidad de recursos, ya que este último va eliminando los ítems de la lista a medida que el usuario deja de verlos, es decir los va reciclando para ahorrar recursos.

- Aplicaciones que conlleven un grado de responsabilidad como lo es el caso, siempre deberán contar con un sistema de autentificación el cual inhabilite el uso de la aplicación a personas no deseadas. Si no se contara con esta característica cualquier persona podría modificar la base de datos. En la aplicación anteriormente descrita se hizo muy necesaria la opción de ver cual moderador ha agregado un usuario nuevo, esto aporta un poco más de seguridad y confiabilidad a la aplicación.

- Firebase es actualmente una herramienta de Google con gran utilidad, esta originalmente fue diseñada para el uso con aplicaciones móviles, pero como se pudo observar ofrece un gran repertorio de compatibilidad con leguajes de programación y plataformas de desarrollo. Para el presente proyecto se usa la autentificación y la base de datos en tiempo real, estas dos herramientas presentan una alta estabilidad y confiabilidad en términos de seguridad, por esto se concluye que para proyectos académicos o relacionados con IoT donde el tráfico de datos sea pequeño, Firebase es la herramienta más recomendada ya que además de bridar ventajas como su facilidad de uso, alta compatibilidad, buena estabilidad también es de carácter gratuito. No está por demás decir que si se presenta la necesidad de un tráfico de datos mayor se pueden optar por otras alternativas en bases de datos de tipo JSON o contratar un plan pago de Firebase el cual otorga utilidades Premium y mayor capacidad pero así mismo con costos un poco elevados.

- Raspberry pi es una excelente plataforma de desarrollo para todo tipo de proyectos, su conexión a internet, Bluetooth, sistema operativo y software libre hacen posible la implementación de sistemas de control de complejidad media, esta ofrece una alta

estabilidad y bajo consumo de energía, es bastante flexible ante las necesidades de programación que se tengan y posee un bajo costo frente a otras plataformas.

- En sistemas de seguridad el RFID puede ser una de las mejores opciones para el control de acceso, esto basado en su baja complejidad y costo de mantenimiento. Respecto a sistemas biométricos presenta ventajas como lo es la capacidad de almacenamiento de usuarios, muchos de estos sistemas biométricos limitan la cantidad de usuarios que pueden ser leídos o registrados. El uso de tarjetas o tags RFID es bastante cómodo, ocupa poco espacio y no genera un desgaste al sensor como otros sistemas si lo hacen, estas tarjetas pueden ser personalizables y también representan un bajo costo junto al sistema. Como anteriormente se dijo los controles de acceso de RFID son poco complejos, y sus tarjetas o tags usan un UID único de difícil clonación, para las necesidades planteadas de este proyecto RFID es la mejor opción, ya que permite el registro de usuarios solo sabiendo el UID, pero sí de mayor seguridad y mayor responsabilidad de un sistema se habla, se puede optar por otros tipos de identificación.

- La unión de sistemas de seguridad con aplicaciones móviles actualmente es imprescindible ya que desde los últimos años el uso de Smartphone y la conexión constante a internet ha crecido de forma incalculable permitiendo llevar un control total de propiedades y demás según sea necesario. A pesar de que este avance tecnológico genera altos niveles de confiabilidad, también se hace necesario tener alternativas en caso de fallas el sistema, en este caso una llave para la apertura de la puerta marca una diferencia importante al momento de una emergencia o algún problema con el tendido eléctrico.

REFERENCIAS

[1] E. Vicente, G. Tutor, and M. M. Organero, “DESARROLLO DE UNA APLICACIÓN DE CONTROL DE ACCESO Y SISTEMAS DE IDENTIFICACIÓN MEDIANTE LA TECNOLOGÍA NFC,” 2011.

[2] P. Korshunov and S. Marcel, “Impact of score fusion on voice biometrics and presentation attack detection in cross-database evaluations,” *IEEE J. Sel. Top. Signal Process.*, pp. 1–1, 2017.

[3] M. W. Diaz Saravia, “Access control system using NFC and Arduino,” *Proc. 2015 IEEE 35th Cent. Am. Panama Conv. CONCAPAN 2015*, no. Concapan Xxxv, 2016.

[4] M. Devices Team and J. Belostock, “Way We Live Next interview with NFC man, Jeremy Belostock - Microsoft Devices BlogMicrosoft Devices Blog,” *october 2*, 2015. [Online]. Available:

https://blogs.windows.com/devices/2008/11/03/way-we-live-next-interview-with-nfc-man-jeremy-belostock/#Lta1SHFqHu7UekFo.97. [Accessed: 14-Apr-2017].

[5] C. Leckness, "Nokia is Working on NFC and Wireless Charging for the Lumia Lineup," *31 enero*, 2012. [Online]. Available: http://www.gottabemobile.com/nokia-is-working-on-nfc-for-the-nokia-lumia-series/. [Accessed: 14-Apr-2017].

[6] C. Acosta, "NFC en la vida cotidiana, lo que hace y lo que podría hacer," *16 julio*, 2013. [Online]. Available: http://www.luisgyg.com/usos-y-predicciones-del-nfc/#.WPD5FvmGPIU. [Accessed: 14-Apr-2017].

[7] I. Hwang and J. Baek, "Wireless access monitoring and control system based on digital door lock," *IEEE Trans. Consum. Electron.*, vol. 53, no. 4, pp. 1724–1730, 2007.

[8] P. J. Sousa, R. Tavares, P. Abreu, M. Quintas, A. Reis, and M. T. Restivo, "Wireless control and network management of door locks," *exp.at 2015 - 3rd Exp. Int. Conf. Online Exp.*, pp. 141–142, 2016.

[9] "Asensio Sistemas S.A. - GS4." [Online]. Available: http://www.asensiosistemas.net/GS4.php. [Accessed: 11-Apr-2017].

[10] Y. Nobu, K. Takeda, and H. Yamaki, "Implementation of a User Account Provisioning System Based on NFC for Public Wi-Fi Services," *2015 Int. Conf. Comput. Appl. Technol.*, pp. 114–117, 2015.

[11] Solucione Vodafone, "Control de Accesos por NFC | Vodafone empresas," 2012. [Online]. Available: https://www.vodafone.es/c/empresas/es/soluciones-para-pymes/digitaliza-tu-negocio/control-acceso-NFC/. [Accessed: 12-Apr-2017].

[12] Penalva Javier, "NFC: qué es y para qué sirve," *25 enero*, 2011. [Online]. Available: https://www.xataka.com/moviles/nfc-que-es-y-para-que-sirve. [Accessed: 11-Apr-2017].

[13] C. J. Date Departamento de ciencias de la computación e I.A, "Introducción a las bases de datos."pp. 142-145.

[14] S. Gestor, E. Sgbd, and M. Relacional, "Teoría de Bases de Datos."

[15] A. Lee, "OverView Firebase" [Online]. Available: https://www.crunchbase.com/organization/firebase

[16] A. Lee, Google Analytics para Firebase [Online]. Available: https://firebase.google.com/docs/Analytics/

[17] A. Lee, Firebase Realtime Database [Online]. Available: https://firebase.google.com/docs/database/

[17] A. Lee, Firebase Service [Online]. Available: https://firebase.google.com/docs/services/