Original research / Artículo original / Pesquisa original - Tipo 1

Embedded system for staff access control using NFC and MIFARE technologies

Rodrigo Andrés Góngora Herrera / ragongorah@correo.udistrital.edu.co

Brayan David Ruiz Rubiano / bdruizr@correo.udistrital.edu.co

Darin Jairo Mosquera Palacios, MSc / djmosquerap@udistrital.edu.co

Universidad Distrital Francisco José de Caldas - Grupo de Investigación Orión

ABSTRACT This paper presents the analysis and performance evaluation of an embedded prototype to control the access of people to companies or institutions by using short range wireless technologies, like NFC and RFID. The developed system proposes a hybrid identification method between MIFARE cards and smartphones with Android operating system. It integrates a web platform in charge of the processing of the system data and increase the use of the technology through services where the gathering of people and objects register and authentication is required. With this proposal, we seek to optimize the time in the identification transactions and improve the security in places where the manual access is carried out. This work is an answer to the need of an adequate management of the access control of the Technological Faculty personnel in the Universidad Distrital Francisco José de Caldas in Bogotá: the chosen scenario for testing our proposal.

KEYWORDS Access control; Android; contactless communications; embedded system; personal identification; NFC; RFID.

Sistema embebido para el control de acceso a personal utilizando tecnologías NFC y MIFARE

RESUMEN El artículo presenta el análisis y la comprobación de un prototipo embebido para controlar el acceso de personal a empresas o instituciones utilizando tecnologías inalámbricas de corto alcance NFC y RFID. El sistema desarrollado plantea un método de identificación híbrido entre tarjetas MIFARE y teléfonos inteligentes con sistema operativo Android; integra una plataforma web que se encarga de procesar los datos del sistema y extender el uso de la tecnología a través servicios en los que se requiere obtener el registro y la identificación de personas y objetos. Con este desarrollo se busca optimizar el tiempo en las transacciones de identificación y mejorar la seguridad en lugares donde se realiza el control manual del acceso de personas. Este desarrollo responde a la necesidad de un adecuado manejo para el control de acceso del personal de la Facultad Tecnológica de la Universidad Distrital Francisco José de Caldas de Bogotá, la cual se ha tomado como escenario de pruebas y comprobación.

PALABRAS CLAVE Control de acceso; Android; comunicaciones sin contacto; sistemas embebidos; identificación de personas; NFC; RFID.

Sistema embarcado para controle de acesso de pessoal usando tecnologias NFC e MIFARE

RESUMO O artigo apresenta a análise e teste de um protótipo embarcado para controlar o acesso de pessoal para empresas ou instituições usando tecnologias sem fio de curto alcance NFC e RFID. O sistema desenvolvido apresenta um método híbrido de identificação entre cartões MIFARE e smartphones com sistema operacional Android; integra uma plataforma web encarregada de processar os dados do sistema e de estender o uso da tecnologia por meio de serviços nos quais é necessário obter o registro e identificação de pessoas e objetos. Este desenvolvimento visa otimizar o tempo em operações de identificação, bem como melhorar a segurança em lugares onde é feito o controle manual de acesso de pessoas. Ainda reflete a necessidade de uma gestão adequada do controle de acesso do pessoal da Faculdade Tecnológica da Universidade Francisco José de Caldas de Bogotá, que tem sido tomada como cenário para testes e verificação.

PALAVRAS-CHAVE Controle de acesso; Android; comunicações sem contato; sistemas embarcados; identificação de pessoas; NFC; RFID.

Received / Recepción: December 23, 2016 - Accepted / Aceptación: February 10, 2017 *doi: 10.18046/syt.v15i40.2403*

I. Introduction

The access control systems consist of the verification of an entity (either a person or a computer) that needs to access a resource when it has the necessary rights to do it; these resources can be physical or logical (Kim & Solomon, 2012). Generally, these systems include three components: the authentication of the entity using some mechanism —a password or a tag—, the authorization, and the traceability (Whitman & Mattord, 2013) and they focus the study in such mechanisms that guarantees the access control system handles the three key components. The use of new technologies that ease their use in several areas such as the Near Field Communication [NFC] is trending nowadays and this work will assess that technology in an access control system.

This article is composed by four sections: a theoretical background where we describe some concepts involving NFC technology, we compare some aspects of another short range communication technologies, and we present the study case detailing the embedded system. In the methodology section, we explain —in a technical way— the development of the prototype and how we worked in each module of the project by considering software and hardware aspects; the integration and testing section presents the performed tests and the achieved results with the system, and the article summarizes some conclusions and recommendations when developing systems with the employed technologies.

II. Theoretical background

A. NFC

NFC is an extension of the ISO 14443 Radio Frequency IDentification [RFID] standard, the basis for most part of its technology. With the enhancements in the radiofrequency communication, it operates in the 13.56 MHz band and NFC was able to be involved in some common habits with the growing of the mobile technology. This caused that the inclusion of the RF communications in mobile phones to be a de-facto standard nowadays, refining some features as the reduction of its reach or the storage type of certain type of data. In 2002, the first standard for NFC was presented with the name of Mobile RFID and a year later, it was approved under the ISO standards with the ISO/IEC 18092 denomination (including the ISO 14443 type A and B and its Felicity Card [FeliCa]).

I. Introducción

Los sistemas de control de acceso consisten en la verificación de una entidad (una persona, un ordenador) que desea acceder a un recurso cuando tiene los derechos necesarios para hacerlo, estos recursos pueden fisicos o lógicos (Kim & Solomon, 2012); generalmente incluyen tres componentes: la autenticación de la entidad por medio de algún mecanismo, –una contraseña, el uso de un *tag*–, la autorización; y la trazabilidad (Whitman & Mattord, 2013). Enfocando el estudio en el mecanismo que garantice que el sistema de control de acceso maneje los tres componentes que lo caracterizan, sumado a la opción de usar nuevas tecnologías que facilitan su uso en determinadas áreas, la tecnología *Near Field Communication* [NFC] será usada para el manejo de un sistema de control de acceso y se verificará que la tecnología es efectiva para su uso en este tipo de procedimientos.

El artículo está compuesto por cuatro secciones adicionales: *Marco teórico*, donde se describen algunos conceptos que involucran la tecnología NFC, se comparan algunos aspectos con otras tecnologías de comunicación de corto alcance y se presenta el caso de estudio en el cual se desarrolló el sistema embebido; *Metodología*, en donde se explica de manera técnica el desarrollo del prototipo y cómo se trabajó cada uno de los módulos del proyecto, tomando en cuenta aspectos de hardware y software; *Integración y pruebas*, donde se plasman las pruebas realizadas y los resultados alcanzados con el sistema en general y, de manera específica, con cada uno de sus componentes; y por ultimo *Conclusiones y recomendaciones*, donde se describen los resultados finales del uso de NFC y el desarrollo del prototipo, y se presentan algunas limitaciones a la hora del desarrollo de un sistema con la tecnología aplicada, y recomendaciones para trabajos o proyectos que se quieran trabajar con la misma.

II. Marco teórico

A. NFC

NFC es una extensión del estándar ISO 14443 *Radio Frequency IDentification* [RFID], en el cual se basa la mayor parte de su tecnología; con el avance de la comunicación por radiofrecuencia, funciona en la banda de los 13.56 MHz. Esta tecnología logro involucrarse en algunos ámbitos de la vida cotidiana con el crecimiento de la tecnológica móvil, por lo que se buscó la forma de incluir las comunicaciones por radiofrecuencia en teléfonos celulares, depurando algunas de sus características como la reducción de su alcance o el diseño de almacenamiento de ciertos tipos de datos. En 2002 nace el primer estándar bajo el nombre de Mobile RFID o NFC, y en 2003 se aprueba bajo los estándares ISO con la denominación ISO/IEC 18092 que incluyen los estándares ISO 14443 (tipos A y B) y FeLica abreviación de *Felicity Card*.

Para 2004 empresas relacionadas con las comunicaciones móviles, como Nokia, Phillips y Sony, se interesan en una mejor estandarización y especificación de NFC, y fundan NFC fórum, basándose para ello en la ISO/IEC 18092. Entre sus

Table 1. Comparison of wireless technologies / Comparación de tecnologías inalámbricas

	NFC	RFID	IrDA	Bluetooth	ZigBee
Boot time / *Tiempo de inicialización*	< 0.1 s	< 0.1 s	0.5 s	6 s	> 1 s
Network type / *Tipo de red*	Point-to-point / *Punto a punto*	Point-to-point / *Punto a punto*	Point-to-point / *Punto a punto*	Point-to-multipoint / *Punto a multipunto*	Point-to-multipoint / *Punto a multipunto*
Maximum reach / *Alcance máximo*	10 cm	3 cm	1m	10 m (depending on the version)	70 m
Transmission speed / *Velocidad de transmisión*	424 kbps	424 kbps	115 kbps	2,1 Mbps, V. 3.0 up to 24 Mbps	250 kbps
Battery consumption / *Consumo de batería*	Low / *Bajo*	Low / *Bajo*	High / *Alto*	High / *Alto*	Low / *Bajo*
Cost of devices / *Costo de los dispositivos*	Medium / *Medio*	Medium / *Medio*	Low / *Bajo*	Low / *Bajo*	Low / *Bajo*
Security / *Seguridad*	High, s/n distance between devices / *Alta, s/n distancia entre dispositivos*	Vulnerable	Vulnerable (except IFRM)	Determined by the encryption mechanisms / *según los mecanismos de encriptación*	Determined by the encryption mechanisms/ *según los mecanismos de encriptación*
User experience / *Experiencia de usuario*	Only one touch / *Solo un toque*	No configuration / *Sin configuración*	Configuration required / *Requiere configuración*	Configuration required / *Requiere configuración*	No configuration/ *Sin configuración*

logros se encuentran las especificaciones NFCIP-1 y NFCIP-2 que permiten la comunicación entre dos dispositivos NFC; en 2007 salen al mercado los primeros teléfonos móviles que incluyen la tecnología NFC; para 2012 las grandes compañías involucradas en el desarrollo de teléfonos celulares –sumado al esfuerzo de desarrolladores de sistemas operativos para estos terminales– logran la incorporación de NFC en la mayoría de equipos de las gamas media y alta (NFC World, 2016), para los próximos años se espera una mayor expansión de esta tecnología (INTECO, 2013).

Frente a otras tecnologías de corto alcance NFC trae mejoras en aspectos como la seguridad, la velocidad y el tiempo de conexión entre dispositivos (**Tabla 1**); su corto alcance de operación brinda una ventaja de seguridad, por lo que implica que la interceptación de datos en las transacciones, por parte de agentes externos, sea difícil de realizar (Pulipati & Srinivas, 2013). La comunicación entre dispositivos que maneja NFC se realiza de manera rápida, lo que permite transacciones en tiempo real (Chavarría, 2011); el consumo de energía por parte de los dispositivos que la usan es muy bajo; y no necesita una configuración previa para su uso, lo que ayuda a que la experiencia de usuario con la tecnología sea fácil y sencilla, y no que se requiere de conocimientos previos para poder aprovechar sus capacidades. Sus tres modos de comunicación –lectura/escritura, punto a punto y emulación de tarjeta NFC– permiten que pueda ser usada en infinidad de aplicaciones y escenarios, además de ser integrada en múltiples elementos y dispositivos; además, es compatible con infraestructuras RFID y con tarjetas inteligentes (Anaya

In 2004, some companies related to the mobile communications area such as Nokia, Phillips, and Sony were interested in a better standardization and specification of NFC; together, they found the NFC Forum based on the ISP/IEC 18092 norm. Their considerable achievements were the NFCIP-1 and NFCIP-2 specifications, which allowed the communication between two NFC devices. In 2007, the first mobile phones with this technology were out in the market and by 2012, the largest companies involved in the mobile phones industry made the incorporation of the technology in the medium and high-end devices (also thanks to the effort of the developers working on the dominating operating systems) (NFC World, 2016). For the upcoming years, a possible expansion of this technology is expected (INTECO, 2013).

With respect to another short range technologies, NFC has improvements in aspects as security, speed, and connection time between devices (see **Table 1**); its short range presents an advantage in security, since the interception of data in the transactions coming from external agents is difficult to perform (Pulipati & Srinivas, 2013). The communication between the devices that mount NFC is performed in a quick way, which allow real-time transactions (Chavarría, 2011) and the

Table 2. Comparison of technologies implemented in access control systems / Comparación de tecnologías implementadas en sistemas de control de acceso

		Cost / *Costo*		Diffusion in the market / *Difusión en el mercado*	Diffusion in the market / *Difusión en el mercado*	Equipment / *Equipo*	Usage / *Uso*
Magnetic cards / *tarjetas magnéticas*		Low, but the maintenance cost increases with time / *Bajo pero con costos de mantenimiento crecientes.*	Low / *Baja*	Non-invasive / *No invasiva*	Medium / *Media*	Reader / *Lector*	Offices and administrative locations / *Oficinas y lugares administrativos*
Biometrics / *Biometría*	Fingerprint / *huella dactilar*	Low / *Bajo*	High / *Alta*	Invasive / *Invasiva*	High / *Alta*	Biometric reader for fingerprint / *Lector biométrico de huellas dactilares*	Governmental buildings / *Edificios de gobierno*
	Eye/*retina (scanning)*	High / *Alta*	Very high / *Muy alta*	Invasive / *Invasiva*	High / *Alta*	Biometric reader for eye scanning / *Lector biométrico de retina*	Military bases, governmental buildings, high confidentially locations / *Bases militares, edificios de gobierno*
	Hand / *Mano (scanning)*	High / *Alta*	High / *Alta*	Non-invasive / *No invasiva*	High / *Alta*	Biometric reader for hand scanning / *Lector de la palma de la mano*	Military bases, governmental buildings / *Bases militares, edificios de gobierno*
RFID		Low / *Alto*	Low / *Baja*	Non-invasive / *No invasiva*	High / *Alta*	Proximity cards reader / *Lector de tarjetas de aproximación*	Public places with high affluence of people / *Lugares públicos con alta concurrencia de personas*
NFC		Medium / *Medio*	High / *Alta*	Non-invasive / *No invasiva*	Low / *Baja*	Proximity cards reader, mobile phones / *Lector de tarjetas de aproximación, dispositivos móviles*	Public places with high affluence of people, conferences / *Lugares públicos con alta concurrencia de personas, conferencias*

& López, 2014), características que hacen un común denominador para aplicaciones del tipo de pago, identificación, sincronización, control de acceso, educación, transporte, entre otras; NFC, enfocada en ambientes específicos, puede brindar interfaces amigables en procesos operativos que normalmente no se apoyan en ninguna tecnología, como lo muestran Racero, López, Hernández y Salas (2015) en un contexto universitario.

Al hablar de sistemas de control de acceso (**Tabla 2**) NFC es una tecnología que ha incursionado en sistemas sin contacto, en los últimos cinco años ha atraído la atención de los desarrolladores y se estima que pueda ser usado en variedad de campos, ya que tiene grandes ventajas en seguridad y experiencia con el usuario, además de la portabilidad que posee al estar incluida en dispositivos móviles; su costo medio y velocidad en las transacciones la hace candidata a ser usada en lugares donde la cantidad de ingresos es alta (lugares públicos, sistemas de transporte masivo, conferencias). Como en el caso anterior, cada tecnología tiene sus ventajas y desventajas al ser implementada, todo depende de las necesidades que tengan el sistema de proteger-restringir en diversos casos (Arriagada, 2014).

B. Mifare

Tecnología de tarjetas inteligentes sin contacto basada en la norma ISO 14443A, maneja un tipo de memoria, *Electrically Erasable Programmable Read-Only Memory* [EEPROM]. Las tarjetas Mifare Classic tienen 1KB o 4KB de memoria EEPROM, cada bloque de memoria puede ser configurado con diferentes condiciones de acceso, con dos claves de autenticaciones separadas, presentes en cada bloque. Estas tarjetas suelen tener una NUID–identificador de Usuario– de 4 bytes que de forma única identifica la tarjeta que viene pregrabada de fábrica. Es posible tener un ID de 7 bytes también, pero los modelos de 4 bytes son mucho más comunes en las tarjetas Mifare Classic (NXP, 2014).

La memoria se divide en secciones, llamadas sectores y bloques, cada sector tiene derechos de acceso individuales y contiene un número fijo de bloques que son controlados por estos derechos de acceso; cada bloque contiene 16 bytes, y los sectores comúnmente tienen 4 bloques para un total de 64 bytes por sector o 16 bloques solo para las tarjetas de 4K, para un total de 256 bytes por sector. En ese sentido los tipos de tarjetas se organizan así:

- tarjetas de 1K: 16 sectores de cuatro bloques cada uno(-del sector número 0 al 15); y
- tarjetas de 4K: 32 sectores de cuatro bloques cada uno (del sector número 0 al 31) y ocho sectores de 16 bloques cada uno (del sectores número 32 al 39).

Estos sectores individuales de cuatro bloques tienen funciones de seguridad básicas, es decir, cada uno puede ser configurado para funciones de lectura/escritura independientes con dos claves de autenticación de 6 bytes diferentes (las claves pueden ser diferentes para cada sector); las claves de autentificación están almacenadas en el último bloque, llamado el *sector tráiler* (Adafruit, 2015). En la **Figura 1** se puede ver la organización de un bloque.

energy consumption of the devices is low; they also do not need a previous set-up for their usage. This latter helps that the user experience with the technology to be easy and simple and no previous technical requirements are needed to work with NFC devices. Its three communication modes (i.e., reading/writing, point-to-point, and NFC card emulation) allow the use in multiple applications and scenarios, besides of its integration in multiple elements and devices. NFC devices are also compatible with RFID infrastructures and with intelligent cards (Anaya & López, 2014), features that make it a common denominator for payment, identification, synchronization, access control, education, and transport applications. NFC focused in specific environments can present friendly interfaces in operative process that —normally— are not supported in other technologies, as Racero, López, Hernández & Salas (2015) show for a university context.

Regarding the access control systems (see **Table 2**), NFC is a technology that has made its way in contactless systems and in the latest years has brought the attention of the developers, it is expected that NFC to be used in several fields, since it has considerable advantages in security and user experience, besides of the portability of being included in mobile devices. Its medium cost and speed in the transactions made NFC a strong candidate to be used in places where the ingress amount is higher (i.e., public places, massive transportation systems, conferences, and more). Each technology has its own advantages and disadvantages at the implementation time, all depends of the necessities the system has to protect and restrict in several cases (Arriagada, 2014).

B. MIFARE

MIFARE is a technology of contactless intelligent cards based on the ISO 14443A norm and it uses an Electrically Erasable Programmable Read-Only Memory [EEPROM]. The MIFARE classic cards have 1 or 4 kB or EEPROM, each memory block can be configured with different access conditions with two separated authentication keys within each block. These cards usually have a NUID —user ID— of 4 bytes that comes factory preset and it is possible to have a 7 bytes ID, but the 4-byte models are more common in the MIFARE classic cards (NXP, 2014).

The memory is divided in sections called sectors and blocks, each sector has individual access rights and it has a fixed number of blocks controlled by these access

rights. Each block has 16 bytes and the sectors —usually— have 4 blocks, for a total of 64 bytes per sector or 16 blocks only for the 4K cards; hence, a grand total of 256 bytes per sector is the final sum. In this sense, the types of cards are organized as follow:

- 1K cards: 16 sectors of 4 blocks each one (from sector 0 to the 15); and
- 4K cards: 32 sectors of 4 blocks each one (from sector 0 to the 31) and 8 sectors of 16 blocks each one (from sector 32 to the 39).

These individual 4-block sectors have basic security functions, i.e., each one can be configured for independent reading/writing functions with two different authentication keys of 6 bytes (the keys might be different for each sector); the authentication keys are stored in the latest block, called the trailer sector (Adafruit, 2015). **Figure 1** presents the organization of a single block.

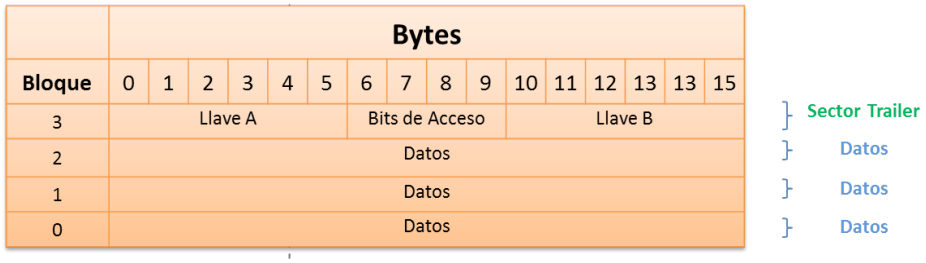

Figure 1. Sector 0 of a MIFARE classic card / Sector 0 de una tarjeta Mifare Classic

C. Host Card Emulation

In most of the cases, to emulate a NFC card, a chip (called secure element) separated from the device is required to correctly operate. Most of the SIM cards provided by telecommunications providers have this secure element.

From the API 19 and version 4.4 of Android and version 10 of the BlackBerry operating system, a new emulation method that does not requires a secure element was public, it was called Host Card Emulation [HCE]. This allows that any Android application can emulate a card and communicate directly to the CPU of its terminal where the application is being executed, instead of route the NFC frames to a secure element. This technology allows total independency of the mobile operators and a broader control of the device for the developers, which opened the gates towards payment applications and cases where a card emulation is required (Android Developers, 2013).

III. Method

The entrance to administrative places, either public or private, has suffered a series of modifications that have allowed some technologies to be implemented to increase the efficiency in security topics. RFID is the clearest example of this (Herrera, Pérez, & Marciano 2009) and its use has been growing with time, probably it is the most implemented technology for access control systems.

C. Host Card emulation

En la mayoría de los casos, para emular una tarjeta NFC se necesitaba un chip separado del dispositivo (llamado un elemento seguro), para poder funcionar. Muchas de las tarjetas SIM proporcionadas por proveedores de telecomunicaciones tienen este elemento seguro.

A partir del API 19 versión 4.4 de Android y la versión 10 de BlackBerry, se dio a conocer un nuevo método de emulación de tarjeta que no implica un elemento seguro, llamado *Host Card Emulation* [HCE], el cual permite que cualquier aplicación de Android pueda emular una tarjeta y comunicarse directamente con el lector NFC. Cuando una tarjeta NFC se emula a través de HCE, los datos son enviados directamente a la CPU de la terminal en la que se está ejecutando la aplicación, en lugar de encaminar las tramas del protocolo NFC a un elemento seguro. Esta tecnología permite total independencia de los operadores móviles y un mayor control del dispositivo por parte de los desarrolladores, lo que abre paso a aplicaciones de pago y a casos donde se necesite emular una tarjeta (Android Developers, 2013).

III. Método

El ingreso a lugares administrativos, sean públicos o privados, ha sufrido una serie de modificaciones, ello ha permitido que algunas tecnologías puedan ser implementadas para aumentar la eficacia de la seguridad. RFID es el ejemplo más claro del tema (Herrera, Pérez, & Marciano 2009), su uso se ha masificado y se podría decir que es la tecnología que más se implementa a la hora de desarrollar un sistema de control de acceso.

En ocasiones por falta de presupuesto, poca atención al tema u otros motivos, el control de personal queda limitado a un equipo de seguridad que, puede ser eficiente pero en algunos casos puede traer inconvenientes, como ejemplo el cambio de turno entre personal de vigilancia; presentar un identificador no garantiza que se restringa el acceso a un individuo que este suplantando la identidad de otro, por lo que puede existir una vulnerabilidad en la seguridad de un lugar, que deja expuestos elementos de la zona para ser tomados por agentes externos o afectar la integridad de las personas.

Las universidades son un claro ejemplo de lo anteriormente mencionado; manejan accesos de todo tipo de personal (estudiantes, docentes, administrativos) de manera manual, como es el caso de la institución seleccionada; en ella, el personal de vigilancia asignado debe estar presente, tanto a la entrada, como a la salida. A la entrada solo basta con mostrar el respectivo

carné de identificación, lo que dejan en "manos" de ese elemento la validación de ingreso a la institución educativa; a la salida basta con que el vigilante verifique qué objetos lleva una persona, en caso de que ella porte un utensilio –maleta, bolso, etc.– donde algunos elementos se puedan albergar.

El método que siguió esta investigación está basado en el análisis de metodologías para el desarrollo de sistemas embebidos, según el Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, INFOTEC (Chapela, 2014). De acuerdo con él, el proyecto se desarrolló en las fases que se describen a continuación.

A. Análisis y diseño

Para que el desarrollo del sistema tuviera los resultados esperados se tomaron en cuenta tres requerimientos fundamentales para que este cumpliera su función:

- Respuesta tiempo real. Fue uno de los mayores requerimientos considerados, la respuesta oportuna en tiempo real a la hora de realizar las transacciones con los *tag* RFID/NFC, facilita el acceso de personal en tiempos muy cortos.
- Sistema escalable. Además del control de acceso de personal, el proyecto propone ser escalable y aprovechar la tecnología RFID/NFC para optimizar otros procesos internos de la institución, como: enfermería, carnetización y préstamos de activos y salones.
- Alta disponibilidad. El sistema propuesto debe estar disponible en todo momento y debe funcionar de manera continua, por eso se propone aplicar técnicas de fiabilidad, tanto en el hardware, como en el software.

Arquitectura del sistema

Como objetivo del sistema es controlar y validar el acceso a la institución, el miembro de la comunidad universitaria podrá utilizar el carné o su teléfono inteligente para identificarse ante el lector, este realizará una consulta en la base de datos, hará las validaciones pertinentes de seguridad y, si todo es correcto, enviará un mensaje al torniquete que permitirá que la persona pueda ingresar (**Figura 2**). Se implementó un servidor web Apache y un motor de base de datos relacional MySQL.

Sometimes, due to limitations in budget, low attention to the topic, or another reasons, the personnel control is limited to a security team that might be efficient, but in some cases, this can carry inconveniences; for instance, in the shift change of the security personnel the presentation of an identity card does not guarantee that the access to a certain individual spoofing the identity of someone authorized is denied. This implies that there might be some vulnerabilities in the safety of certain place, exposing elements of the zone to be taken by external agents or affect the integrity of the people.

The universities are a clear example of the aforementioned, they handle several types of personnel (students, professors, administrative personnel) generally in a manual way —as it is in the case of the mentioned college for doing the tests—. There, the assigned security personnel must be present both in entrances and exits. In the entrances, showing the respective ID is enough to pass through; hence, that is the only security filter to enter the university. Whilst, on exit, a quick revision of the backpack to check there are no forbidden items is enough.

The method we followed in this research is based on the analysis of methodologies for the development of embedded systems, given by the Research and Innovation Center in Information and Communication Technologies [INFOTEC] (Chapela, 2014). According to that, the project was developed in the phases described below.

A. Analysis and design

Pursuing that the development of the system had the expected results, we considered three fundamental requirements to ensure it complies with its functions:

- Real-time response. It was one of the biggest considered requirements, the opportune real-time response when performing the transactions with the RFID/NFC tags eases the access of personnel in short time intervals.
- Scalable system. Besides of the personnel access control, the project proposes scalability and consider the RFID/NFC technology to optimize another internal processes of the institution as nursery, ID cards manufacturing, and loan applications for classrooms.

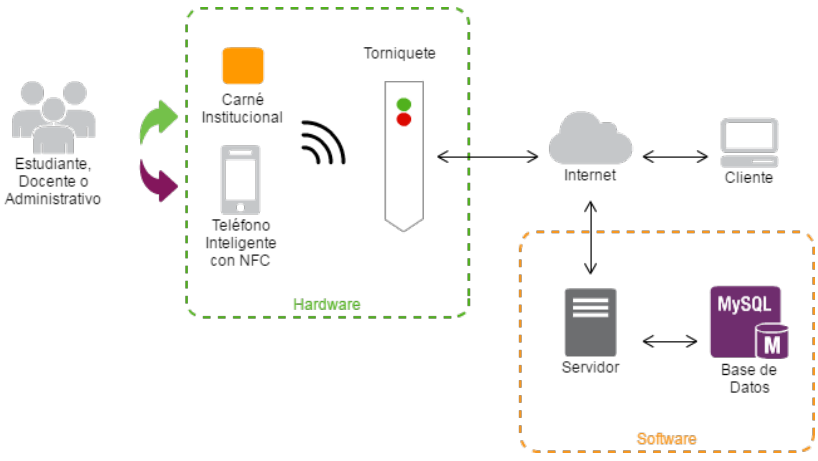

Figure 2. General schematic of the system / Esquema general del sistema

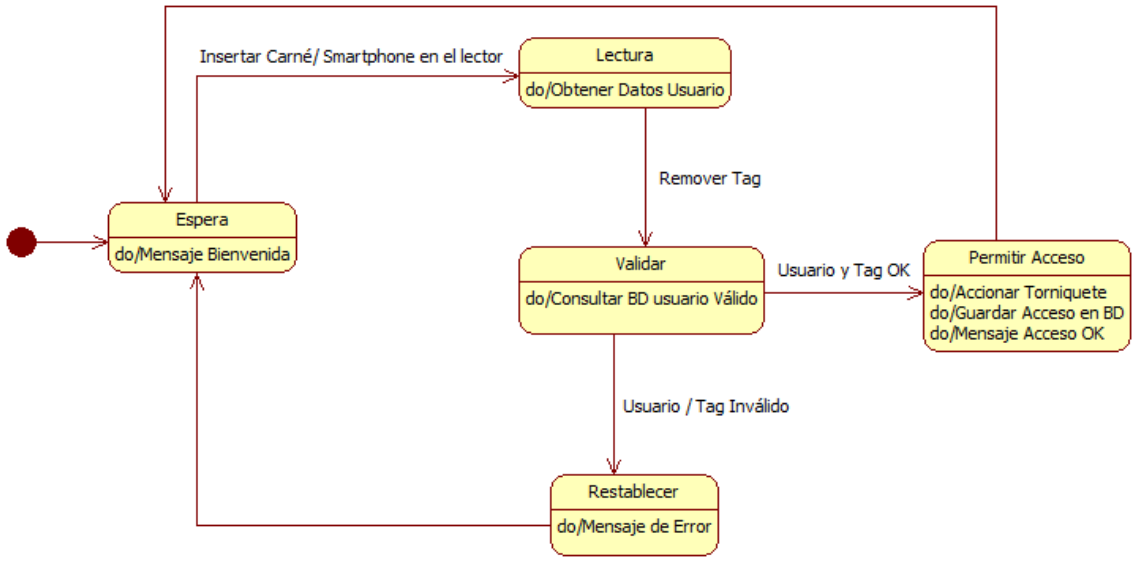

Figure 3. Model of states in the access system / Modelo de estados del sistema de acceso

- High availability. The proposed system should be available always —ideally— and it must operate in a continuous way; for these reasons, we propose to use trustworthiness techniques both in the hardware and in the software.

System architecture

As the main objective of the system is to control and validate the access to the institution, the members of the college might be able to use either their ID or smartphone to gain permission in the reader. These elements will launch a consult to the database and if everything is clear, will perform the pertinent security validations and will send a message to the turnstile, allowing the entrance of the people (**Figure 2**). We implemented an Apache web server and a relational MySQL database engine.

Currently, the university personnel employ a MIFARE 4K ID card that is used only for the Public Transportation Integrated System of Bogotá, for a task where only a few sectors in the memory are used. This lets available sectors that will be used for the proposal objective. Following this, we propose a hybrid access control where both the ID and the smartphone are valid for anyone of the above-mentioned transactions.

Design of the hardware and software

An expected feature in the embedded systems is the ability to be reactive and respond to events on its environment (Sommerville, 2011). **Figure 3** describes the model of states in stimulus responses of the access control system.

Actualmente la Universidad usa un carné del tipo Mifare 4K, que es utilizado solo para el Sistema Integrado de Transporte Público [SITP] de Bogotá, para una tarea donde solo se ocupan unos pocos sectores de la memoria, lo que deja sectores disponibles que se utilizarán para el objetivo del proyecto. De este modo se propone un control de acceso hibrido, en el cual, tanto el carné, como el teléfono inteligente, son válidos para cualquiera de las transacciones.

Diseño de hardware y software

Una característica esperada en los sistemas embebidos es que sean reactivos y respondan a eventos en su entorno (Sommerville, 2011). En la **Figura 3** se describe el modelo de estados en respuesta de estímulos del sistema de control de acceso.

Como respuesta a la necesidad de contar con un sistema escalable y aprovechando que tecnología NFC puede habilitar información ubicua (Córdoba et al., 2013), se diseñó una base de datos en la que los servicios se pudieran extender fuera de los de acceso, solo con obtener la referencia del usuario se podría adaptar cualquier servicio a la base de datos. La **Figura 4** muestra el modelo de datos utilizado, con algunos de los servicios, como es el caso del préstamo de salones.

B. Desarrollo del hardware

El sistema utiliza una placa de expansión [*shield*] en la que viene integrado un chip de referencia PN532 con funcionalidades de lectura y escritura en *tags* pasivos tipo Mifare y NFC (Adafruit, 2011); el modulo facilita la comunicación con dispositivos NFC, gracias a lo cual se puede acceder a la memoria del carné institucional sin problema, ya que la placa está diseñada para su uso en la placa de Hardware libre Arduino, la que tiene la tarea de interpretar los datos que envía o recibe el *shield* vía SPI [*Serial Peripheral Interface*]; también para el desarrollo del sistema se usa la placa computadora conocida como Raspberry Pi, la cual lee la información que envía el Arduino

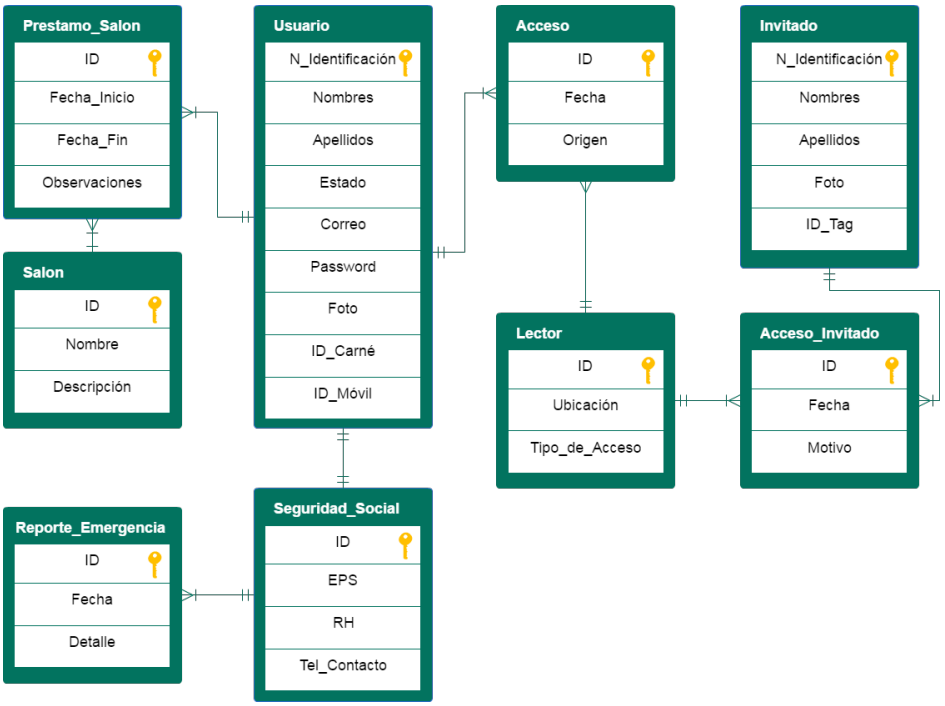

Figure 4. Part of the relational diagram of the system / Parte del diagrama relacional del sistema

por el puerto serial; gracias al uso del lenguaje Python y su librería serial.py, él obtendrá los datos y accederá al servidor, en concreto a la base de datos vía TCP/IP, y por medio de validaciones retornará la respuesta, indicando si el usuario puede o no acceder al recinto educativo (**Figura 5**).

Para el caso del hardware en los módulos de los servicios no es necesaria la Raspberry Pi, solo se necesitará un computador que tenga conexión a la red, para realizar la conexión con la plataforma web; además, en algunos servicios como el de carnetización, el *shield* actuará en modo escritura, dado que en los ubicados para el acceso a personal solo estaría habilitada la función de lectura.

Utilizando los sectores que brinda el carné institucional, gracias al uso de Mifare 4K, se organizó la información almacenada para los miembros de la comunidad universitaria, en primer lugar, su número de identificación y el rol que tiene

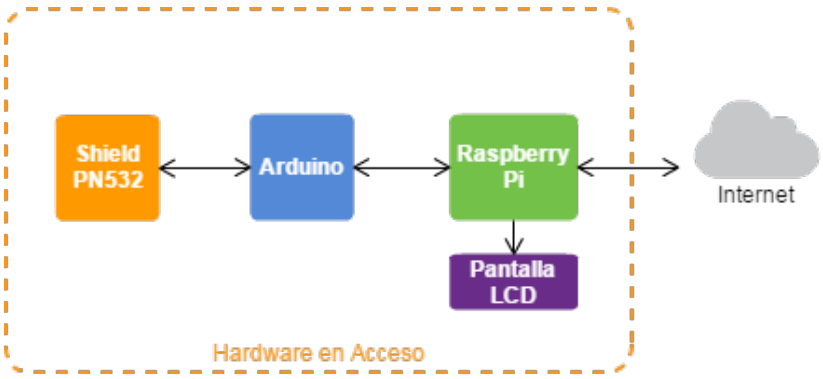

Figure 5. Hardware prototype / Prototipo de Hardware

As a response to the need to have a scalable system and considering that the NFC technology can enable ubiquitous information (Córdoba et al., 2013), we designed a database where the services might be extended out of the access ones, only with the gathering of the user reference, an adaptation of any service to the database would be possible. **Figure 4** presents the used data model with some of the services (e.g., the loan of classrooms).

B. Hardware development

The system uses an expansion shield where a PN532 reference chip is integrated; it allows reading and writing functionalities in passive tags as the MIFARE and NFC ones (Adafruit, 2011). The module eases the communication with NFC devices and the access to the memory where the institutional ID information is stored has no issues. This, since the shield is designed to be used in the Arduino open hardware platform by process the data coming from the shield via Serial Peripheral Interface [SPI]. Besides, for the development of our proposal, we used the minicomputer known as Raspberry Pi, which reads the information the Arduino sends via SPI and using a Python script (serial.py), the gathering of the data is granted, together with the access to the server. This access is via TCP/IP and it is pointed to the database; besides, via validations, it will return the answer indicating if the user is granted to access the location or not (see **Figure 5**).

For the hardware case, punctually in the service modules, the use of the Raspberry Pi is not necessary, only needed is a computer with Internet connection to execute the connection with the web

Table 3. Information stored by user type of the MIFARE card / Información almacenada por tipo de usuario la tarjeta MIFARE

Block / *bloque*	Users / *Usuario*	Guests / *Invitado*
8	ID number	ID number
9	Role / *Rol*	Role / *Rol*
10	-	Reason to enter / *Motivo de visita*

platform. Besides, in some services as the ID cards manufacturing, the shield will act in writing mode, since the ones located for the personnel access will have only enabled the reading function.

Using the sectors that the institutional ID provides and thanks to the use of the MIFARE 4K cards, we organized the stored information for the members of the university with his/her identification number and the role within the college (e.g., student, professor, administrative personnel). For the guests, some white tags of the same reference are used, where their ID number and the reason of the visit to the place are stored (see **Table 3**).

Regarding the security, the access conditions for each one of the blocks containing data were changed in the tags; hence, the reading of a tag is only possible if it has the corresponding key. Besides, we configured the tags forcing that after the first information recording, they cannot be modified in the future, avoiding vulnerabilities related with the cloning of tags.

C. Software development

This phase implied work in two platforms: we developed a web and a mobile application.

Web application

Web applications for a custom-made control access system are already a studied field (Olivares, & Bautista, 2008), which offer advantages related to the existing ones in the market. For that reason, we created a web platform, where it is possible to process, store, and manage the personnel access and their requests in the corresponding areas of the institution. All of the monitored areas are linked with processes where the institutional ID might have an expansion on its usage —as the use of the ID to sedentro de la comunidad universitaria (e.g., estudiante, docente, administrativo). Para los invitados se utilizan *tags* en blanco de la misma referencia Mifare 4K, en los que se graba su número de identificación y el motivo de su visita al lugar (**Tabla 3**).

Respecto de la seguridad, a los *tags* se les cambiaron las condiciones de acceso a cada uno de los bloques que contienen datos, de manera que solo se puede hacer la lectura a un *tag* si se cuenta con la clave correspondiente; además, se configuró de manera tal que después de la primera grabación la información de usuario no puede ser modificada a futuro, con lo que se logra evitar vulnerabilidades como la clonación de los *tags*.

C. Desarrollo del software

Esta fase implicó trabajo en dos plataformas, se desarrollaron dos aplicativos, uno para Web, otro para móviles.

Aplicativo Web

Ya se han visto aplicaciones web para sistemas de control de acceso a la medida (Olivares, & Bautista, 2008), que ofrecen ventajas con respecto a los existentes en el mercado; por tal motivo se creó una plataforma web en la cual se pueden procesar, almacenar y administrar los accesos de personal y las solicitudes en las dependencias existentes de la institución, todas ellas vinculadas con procesos donde el carné institucional puede tener una expansión en su uso –como la obtención de la credencial universitaria, el préstamo de elementos que brinda la comunidad educativa son dos modelos que tiene el sistema y que interactúan con el desarrollo del proyecto en general, demostrando su escalabilidad–, además de administrar a los usuarios que acceden al lugar. El aplicativo web se dividió en módulos, así: Administración, Enfermería, Deportes, Activos, Salones, Carnetización, Seguridad y Pérdida de identificador. En la **Figura 6** se puede ver una captura de pantalla del módulo de Enfermería en el que se utiliza un *tag* para consular la información de un paciente y crear un reporte.

Figure 6. Module involving a tag reader / Módulo que involucra una lectura del tag

Para su desarrollo se utilizó el lenguaje de programación PHP por medio del framework symfony2, gracias a su serie de herramientas, redujo el tiempo de creación de la plataforma, además de su integración con JavaScript por medio de la librería JQuery que es la que permite la comunicación del lector con la plataforma.

Aplicación móvil

Se desarrolló una aplicación en el sistema operativo Android en la que se puede hacer uso de los servicios institucionales vía NFC. La aplicación integra un módulo de registro e información, en el cual se valida la información de entrada en la base de datos y se carga la información de cada usuario para que pueda ser utilizada por los servicios NFC. Además, tiene un módulo de servicios NFC que utiliza la tecnología HCE, lo que hace que la terminal se pueda comportar como un *tag* NFC y de esta manera ser transparente para el lector.

Para la identificación única del dispositivo se utiliza el *International Mobile Station Equipment Identity* [IMEI] de la terminal. Con ello se garantiza que la relación entre usuario y dispositivo es uno a uno, y se asegura que no se haga un inicio de sesión desde diferentes cuentas en un mismo dispositivo, ni que se utilice una misma cuenta en diferentes dispositivos. Solo basta estar situado en cualquier aplicación para que el usuario acerque el Smartphone al lector para que se active la aplicación. A continuación se describen dos funciones en las que la aplicación Android establece comunicación con el lector.

```
@Override
public byte[ ] processCommandApdu(byte[ ] apdu, Bundle extras) {
    if(User.getCodigo(this).length() != 0) {
      if (selectAidApdu(apdu)) {
        Intent dialogIntent = new Intent(this, AccesoActivity.class);
        dialogIntent.addFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
        startActivity(dialogIntent);
        return getWelcomeMessage();
      }else {
        return null;
      }
    }
    return null;
}
private byte[ ] getWelcomeMessage( ) {
return(Dispositivo.getIMEI(this)+";"+User.getId(this)+";"+User.getRol(-
this)+(";2")).getBytes( );
}
```

La función *"processCommandApdu"*, que activa el proceso de escucha del servicio, es de tipo *override*, así que es un método sobrescrito de una clase abstracta estándar que provee Android para HCE. En la función se hace una verificación con el ID del lector corresponde al ID configurado en la aplicación, si los parámetros son correctos, inicia la actividad que muestra la foto (**Figura 7**) y se envían los datos de usuario a través de NFC en la función *"getWelcomeMessage"*, en bytes, como tipo de dato.

veral services and the loan of a variety of elements—, demonstrating the system scalability. The web application was divided in two modules: management, nursery, sports office, assets, classrooms, ID manufacturing, and safety/loss of ID. In **Figure 6**, we present a screen capture of the nursery module, where the tag is used to consult the information of a patient and create a report.

For its development, we used the PHP programming language and we used the symfony2 framework. Thanks to a series of tools this framework has, it helped us reduce the creation time of the platform, besides of its integration with JavaScript through the use of the JQuery library, which is the one that allows the communication of the reader with the platform.

Mobile application

We developed an application in the Android operating system, where we can use the institutional services via NFC. The application integrates registering and information modules, where the information for the entrance to the database is validated, if this is correct, the information of each user is loaded so that the NFC services can use it. Besides, it has a NFC services module that uses the HCE technology, which allows the terminal can behave like a NFC tag and be transparent to the reader.

For the unique identification of the device, we used the International Mobile Station Equipment Identity [IMEI] of the terminal. With that, we guarantee that the relation between the user and the device is one-to-one, and we certify that neither a multiple login from different accounts, nor the usage of a single account in several devices are not performed. It is only necessary that the user puts the smartphone near the reader in order the application automatically launches. In the next paragraphs, we describe two functions where the Android application establishes communication with the reader.

```
@Override
public byte[ ] processCommandApdu(byte[ ] apdu, Bundle extras) {
    if(User.getCodigo(this).length() != 0) {
      if (selectAidApdu(apdu)) {
        Intent dialogIntent = new Intent(this, AccesoActivity.class);
        dialogIntent.addFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
        startActivity(dialogIntent);
        return getWelcomeMessage();
      }else {
        return null;
      }
```

```
        }
        return null;
    }
    private byte[ ] getWelcomeMessage( ) {
    return(Dispositivo.getIMEI(this)+";"+User.getId(this)+";"+User.getRol(-
this)+(";2")).getBytes( );
    }
```

The "processCommandApdu" function, that activates the service listening process is from the override kind; hence, it is an overwritten method of a standard abstract class that provides Android for HCE. In the function, a verification with the reader ID is performed, in order to confirm that the ID corresponds to the configured in the application; if the parameters are correct, the activity is started that **Figure 7** shows and the user data is sent through NFC in the "getWelcomeMessage" function. This latter is sent in bytes as the data type.

IV. Integration and testing

By creating a series of applications in several platforms, it is important to consider on how to achieve that everything connects in a correct way, no matter what tool handles each application. For this case, we have as a common element the database for the access system. In this phase, we performed the integration of the software components build in several environments or programming languages; also, we did the communication between the system software and hardware. In the next paragraphs, we present a brief description on how this was performed.

Integration between hardware and software

For the modules that involved the reading and writing, we used a desktop application coded in Python that served as a bridge between the reader and the web platform. Given the fact that the hardware is in a different environment than the web platform, we required to have a common element. In this case, we used the web-socket technology that implements a bidirectional and full-duplex communication over a single TCP socket, allowing to communicate the reader with the web application (Mozilla Developer Network, 2016). **Figure 8** presents this communication process.

Serial communication

The communication between the RFID/NFC reader and the software is done via the serial port of the Raspberry Pi, reading a separated text line with a semicolon with data of the personnel type to enter the location (see **Table 4**).

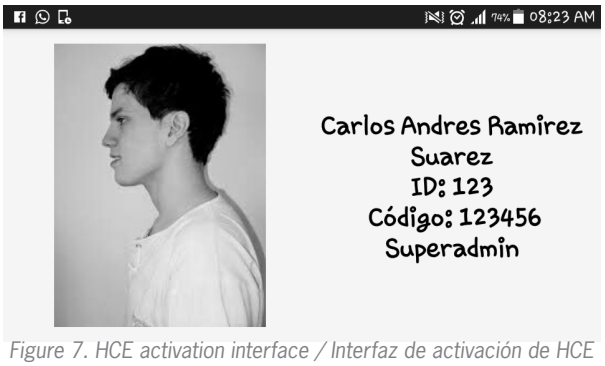

Figure 7. HCE activation interface / Interfaz de activación de HCE

IV. Integración y pruebas

Al crear una serie de aplicaciones en diferentes plataformas se debe tener en cuenta cómo lograr que todo se conecte adecuadamente, sin importar qué herramienta maneja cada aplicación, en este caso, se tiene como elemento común la base de datos del sistema de acceso. En esta fase se realizó la integración de los componentes de software que están en diferentes entornos o lenguajes de programación, así como la comunicación entre el Hardware y Software del sistema, a continuación se describe brevemente cómo se logró la comunicación entre todos los procesos.

Integración entre hardware y software

Para los módulos que involucraron la lectura y escritura se utilizó una aplicación de escritorio codificada en Python que sirve como puente entre el lector y la plataforma web. Dado que el hardware se encuentra en un entorno diferente al de la plataforma web, se requiere tener un elemento en común; en este caso se aplicó la tecnología Websocket que implementa una comunicación bidireccional y full-dúplex sobre un único

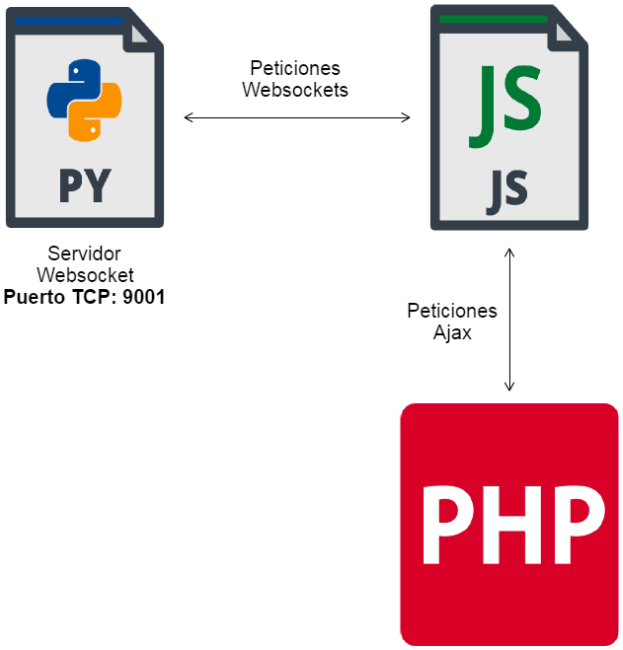

Figure 8. Communication process between hardware and software / Proceso de comunicación entre hardware y software

Table 4. Data scheme of a user and a guest / Esquema de datos de un usuario y de un invitado

Users / *Usuario*	Guests / *Invitado*
ID of the MIFARE/*NFC card*	ID of the MIFARE card
Identification number	Identification number
Role / *Rol*	Role / *Rol*
Device type / *Tipo de dispositivo*	Reason to enter / *Motivo de visita*

socket TCP, de este modo se puede comunicar el lector con la aplicación web (Mozilla Developer Network, 2016). En la **Figura 8** se ilustra este proceso de comunicación.

Comunicación serial

La comunicación entre el lector RFID/NFC y el software se hace desde el puerto serial de la Raspberry Pi o computador, leyendo una línea de texto separada con punto y coma con datos del tipo de personal que va entrar (ver **Tabla 4**).

Comunicación Android - base de datos

Dado que es necesario obtener la información correspondiente a cada usuario en la aplicación móvil se implementó un servicio web en el que se realiza la comunicación con el servidor de base de datos; esta conexión se realizó haciendo una solicitud HTTP a un script PHP que consulta la base de datos y obtiene el resultado en formato JSON (**Figura 9**).

Resultados

En el caso del sistema de control de acceso se utilizó una pantalla LCD que muestra los resultados en cada uno de los casos que se contemplaron (ver **Tabla 5**) para los dos tipos de personal que pueden ingresar a la universidad (usuarios e invitados); se contempló una serie de excepciones que puede tener el sistema (ver **Tabla 6**), dando solución a cada una de ellas, con el objetivo de que el sistema no sufra ningún tipo de vulnerabilidad y afecte la principal tarea que tiene, manteniendo así el servicio activo. Además, el sistema utiliza un mecanismo que simula un torniquete, el cual, en caso de tener una respuesta efectiva –que el usuario pueda ingresar–, se activa.

La integración del lector con la plataforma web también tuvo en cuenta los resultados esperados del sistema en los aspectos de lectura y escritura de *tags* (ver **Tabla 7**) y sus respectivas excepciones (ver **Tabla 8**), la plataforma misma muestra los resultados respectivos gracias al uso de las alertas que usa JavaScript y que pueden informar qué sucede en el sistema cuando ocurre algún evento en la interacción lector-plataforma.

Android - database comunication

Given the fact that it is necessary to obtain the corresponding information for each user in the mobile application, we implemented a web service that performs the communication with the database server. This connection was performed by doing an HTTP request to a PHP script that consults the database and gathers the results in JSON format (see **Figure 9**).

Results

In the case of the access control system, we used an LCD screen that shows the results on each of the considered cases (see **Table 5**) for the two types of personnel that might enter the university (either users or guests). We considered a series of exceptions that the system might have (see **Table 6**), solving each one of them with the objective the system does not suffer any vulnerability affecting its main task, ensuring availability. Furthermore, the system uses a mechanism simulating a turnstile which, in case of having a positive response —the user can enter the place—, it is activated.

The integration of the reader with the web platform also considered the expected results of the systems in the topics related to the reading and writing of tags (see **Table 7**) and their respective exceptions (see **Table 8**). The platform itself shows the respective results thanks to the use of alerts that JavaScript employs and that are usable to inform the current state of the system when some event in the reader-platform interaction occurs.

V. Conclusions

After the obtained results in this project, we recognize the following limitations:

- The mobile application can only be used in mobile devices running the Android operating system, since the development was only focused in that platform; and
- For the modules of the web platform involving the use of the card, there always exists the need of

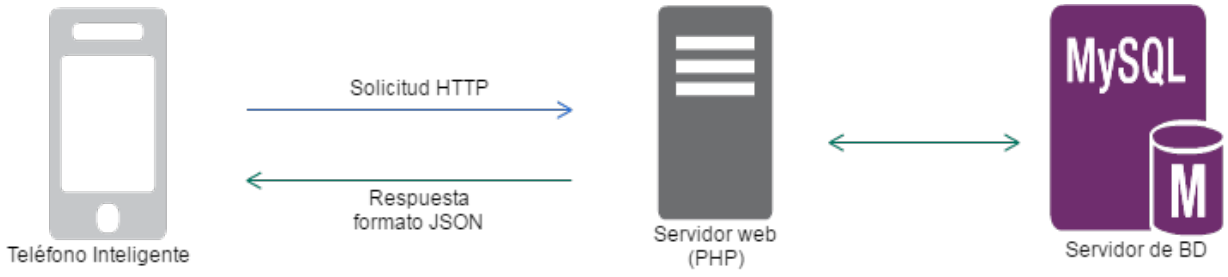

Figure 9. Communication process between the Android application and the database / Proceso de comunicación entre la aplicación Android y la base de datos

Table 5. System responses to the access module / Respuestas del sistema en el módulo de Acceso

Users / *Usuario*	Guests / *Invitado*	Trigger / *Iniciador*	Parameters / *Parámetros*	Response / *Respuesta*
Read of the user mobile tag / *Lectura del tag-móvil del usuario*	The reader sends the information to the database / *El lector envía los datos a la base de datos*	User / *Usuario*	Tag ID, user ID, and user role / *Id del tag, id del usuario y rol del usuario*	An alert will be send depending on the records found in the database / *Dependiendo de lo encontrado en la base de datos se enviará una alerta*
Read of the guest tag / *Lectura del tag del invitado*	The reader sends the information to the database / *El lector envía los datos a la base de datos*	Guest / *Invitado*	Tag ID, user ID, and reason to enter / *Id del tag, id del usuario y motivo de ingreso*	An alert will be send depending on the records found in the database / *Dependiendo de lo encontrado en la base de datos se enviará una alerta*
Introducing an entrance event / *Inserción de una entrada*	The reader confirms the user data and writes an entrance event in the system / *El lector confirma los datos del usuario e inserta una entrada en el sistema*	Reader / *Lector*	User/guest ID and date of entrance/ *Id del usuario/invitado y fecha de entrada*	The entrance is granted to the user and the record is saved in the database / *Se concede la entrada al usuario y se inserta el registro en la base de datos*
Introducing an exit event / *Inserción de una salida*	The reader confirms the user data and writes an exit event in the system / *El lector confirma los datos del usuario e inserta una salida en el sistema*	Reader / *Lector*	User/guest ID and date of exit / *Id del usuario/invitado y fecha de salida*	The exit is granted to the user and the record is saved in the database / *Se concede la salida al usuario y se inserta el registro en la base de datos*

Table 6. Exceptions in the access module / Excepciones en el módulo de Acceso

Exception / *Excepción*	Description / *Descripción*	Event /*Evento*
Different identifier /*Identificador diferente*	The user uses a tag type different than the university one / *El usuario pasa en el lector un tipo de tag diferente al institucional*	The system informs the user does not exist / *El sistema informa que el usuario no existe*
Duplicated access / *Doble acceso*	The user tries to pass more than once the tag through the entrance reader / *El usuario pasa más de una vez el tag por el lector de ingreso*	The system indicates the user already acceded/exit the place / *El sistema informa que el usuario ya accedió o salió del lugar*
User not valid / *Usuario no validó*	User identified as "not registered" in the database / *Usuario con "no registrado" en la base de datos*	The system informs the user does not exist / *El sistema informa que el usuario no existe*
Identifier ID does not exist / *Id del identificador no existe*	User with tag ID or mobile not valid / *Usuario con ID del tag o móvil no válido*	The system informs the user is not valid / *El sistema informa que el usuario no es válido*
Inactive user / *Usuario inactivo*	Inactive user in the system / *Usuario activo en el sistema*	The system informs the user is inactive in the database / *El sistema informa que el usuario está inhabilitado*

Table 7. System responses in the web application / Respuestas del sistema en la aplicación web

Event / *Evento*	Trigger / *Iniciador*	Trigger / *Iniciador*	Parameters / *Parámetros*	Response / *Respuesta*
Read of the user tag/ mobile / *Lectura del tag-móvil del usuario*	The application is capable to read the data in the tag for its processing / *La aplicación es capaz de leer los datos del tag para su manipulación*	User / *Usuario*	User ID and tag/mobile ID / *Id del usuario e id del tag/móvil*	The application will consult the user ID in the system, depending on that result, it will trigger the desired action / *La aplicación hará la consulta del usuario al sistema y, dependiendo del resultado, efectuará la acción deseada*
Write of the user tag / *Escritura del tag del usuario*	The application is capable to do a write action in the tag in order the user/guests grants the correct authentication / *La aplicación es capaz de hacer una escritura al tag para que el usuario/invitado quede plenamente identificado*	User-ID manufacturing module / *Usuario-módulo de carnetización*	User ID / *Id del usuario*	The application sends the user ID and the role she/he has in the platform to the tag, then it records the data in the identifier / *La aplicación envía al tag el id del usuario y el rol que tiene en la plataforma, y graba los datos en el identificador*

Table 8. Exceptions in Web App. / Excepciones en la aplicación Web

Exception / *Excepción*	Description / *Descripción*	Event / *Evento*
Reader not connected / *Lector no conectado*	The reader has no communication with the application / *El lector no tiene comunicación con la aplicación*	The application sends an alert indicating the reader is not present / *La aplicación envía una alerta informando que no está presente el lector*
Tag/mobile not detected / *Tag/móvil no detectado*	The reader activates itself without presence of the tag/mobile / *El lector se activa sin que el tag/móvil esté presente*	The application sends an alert informing there is no tag in the reader / *La aplicación envía una alerta informando que no hay un tag presente en el lector*
Tag/mobile ID not found in the database / *Id del tag/móvil no encontrado en la base de datos*	The tag ID is not related to the current user tag ID in the database / *El id del tag no se relaciona con id del tag del usuario presente en la base de datos*	The application sends an alarm indicating the user with the current credentials does not exist / *La aplicación envía una alerta informando que el usuario con las credenciales entradas no existe*

V. Conclusiones

Luego de los resultados obtenidos con este proyecto, se reconocen las siguientes limitaciones:

- la aplicación móvil solo puede ser utilizada en dispositivos móviles con sistema operativo Android, ya que el desarrollo solo se enfocó en dicha plataforma; y
- para los módulos de la plataforma web que involucren el uso de la tarjeta siempre se debe tener algún administrador que valide la información del usuario y verifique que sea correcta, con el fin de que las transacciones sean totalmente correctas, tanto del lado del sistema, como del usuario.

A partir de los resultados obtenidos, se recomienda:

- para evitar que la aplicación móvil sea exclusiva de un solo sistema operativo –y romper así las barreras de la multiplataforma–, se recomienda el desarrollo en otras plataformas móviles, como Windows 10 Mobile y iOS haciendo uso de herramientas para aplicaciones hibridas en HTML5 y JavaScript;
- el sistema de control de acceso siempre deberá tener comunicación con la base de datos, para realizar las respectivas validaciones y permitir así el acceso a los usuarios, para ello se recomienda implementar mecanismos de redundancia y alta disponibilidad en los servidores donde se aplique la solución;
- para la realización del proyecto se usó un *shield* conjunto a la placa Arduino el cual tiene un chip del tipo PN532, se recomienda el uso de un lector que posea este chip ya construido y ensamblado, que realice estas tareas de la misma forma.

En conclusión, con los resultados obtenidos se presentó el desarrollo de un sistema de control de acceso que cumplió con todas las necesidades y características que poseen este tipo de sistemas, usando como mecanismo un prototipo que funciona correctamente con la tecnología NFC. La implementación de este sistema es capaz de solucionar una gran parte del problema de acceso y seguridad en sitios de características similares a las mencionadas en el caso de estudio. Cabe resaltar que los usuarios prefieren utilizar su dispositivo móvil en lugar del carné para identificarse, por motivos de comodidad y practicidad.

an administrator that validates the user information and verifies if it is correct, in order to ensure the correctness of the transactions either in the system side or in the user one.

From the obtained results, we recommend:

- In order to avoid that the mobile application to be exclusive of a unique operating system —breaking the multiplatform barriers—, we recommend the development in another mobile platforms as Windows Mobiles and iOS, by using hybrid tools in HTML5 and JavaScript
- The access control system always should have communication with the database, in order to perform the respective validations and allow the access to the users; for that, we recommend to implement redundancy and high availability mechanisms in the servers where the application is nested
- For this project, we used a shield together with an Arduino development board, which has a PN532 chip, we recommend the use of a reader with this chip already built and assembled, that performs these tasks in a similar way.

Summarizing, with the obtained results, we presented the development of an access control system that complied with all the needs and features these kind of systems have, using as the mechanism a prototype that correctly operates with the NFC technology. The implementation of this system is capable to solve a large part of the access and security problem in places of similar features as the ones mentioned in the studied case. It is important to focus that the users prefer to use their mobile device instead of the ID to identify themselves by comfort and practicality reasons.

NFC presents interesting advantages in relation to other short range communication technologies for the access control. Used in specific scenarios, it can improve subs-

tantially the ease, efficiency, speed, and security of process where transactions with personnel, objects, and zones are involved. With the development of this project, we achieved to use an efficient use of this technology, carry on practice some theoretical concepts, and implement them in a set of applications that were able to take advantage of its features, demonstrating that the technology is scalable given the particular needs —both of the users and of the location—.

Acknowledgement

The authors would like to thank the ORION research group of the Universidad Distrital Francisco José de Caldas for the support received in this project. ST

NFC presenta notables ventajas frente a otras tecnologías de comunicación de corto alcance y control de acceso, dispuesta en escenarios específicos puede mejorar sustancialmente la facilidad, eficacia, rapidez y seguridad de procesos en los que se involucren transacciones de personal, objetos y zonas. Con el desarrollo de todo el proyecto se logró dar un uso eficiente a la tecnología NFC, llevar algunos de sus conceptos a la práctica e implementarla en un conjunto de aplicaciones que pudieron aprovechar sus ventajas, demostrando que la tecnología permite ser escalable según las necesidades, tanto de los usuarios, como del sitio.

Agradecimientos

Los autores agradecen al grupo de investigación ORION de la Universidad Distrital Francisco José de Caldas, por su apoyo en este proyecto. ST

References / Referencias

Adafruit Industries (2011). *PN532/C1 NFC controller*. Retrieved from: https://cdn-shop.adafruit.com/datasheets/pn532ds.pdf

Adafruit Learning System (2015). *MiFare Cards & Tags | Adafruit PN532 RFID/NFC Breakout and Shield. Retrieved* from: https://learn.adafruit.com/adafruit-pn532-rfid-nfc/mifare

Anaya, A. & López, I. (2014). La tecnología NFC en teléfonos celulares, sus retos y aplicaciones. *Research in Computing Science, 77, 97-107.* Available at: http://www.rcs.cic.ipn.mx/rcs/2014_77/La%20tecnologia%20NFC%20en%20telefonos%20celulares_%20sus%20retos%20

Android Developers (2013). *Android KitKat.* Retrieved from: https://developer.android.com/about/versions/kitkat.html

Arriagada, C. (2014). *Análisis de la tecnología de comunicación de campo cercano (NFC) y sus aplicaciones* [thesis]. Universidad Austral de Chile: Valdivia. Available at: http://cybertesis.uach.cl/tesis/uach/2014/bmfcia775a/doc/bmfcia775a.pdf

Chapela, L. (2014). *Proceso de desarrollo de sistemas embebidos y aseguramiento de calidad* [Infotec - Cuadernos de trabajo, No. 6]. Retrieved from: https://www.infotec.mx/work/models/infotec/cuadernos/9/9.pdf

Chavarría, D. (2011) *Tecnología de comunicación de campo cercano (NFC) y sus aplicaciones* (thesis). Universidad de Costa Rica: San Pedro, Costa Rica. Available at: http://eie.ucr.ac.cr/uploads/file/proybach/pb2011/pb2011_012.pdf

Córdoba, C., Burbano, M., Lame, H., Salazar, M., Ramírez, G., Solarte, M., & Herrera, O. (2013). Valoración de sistemas ubicuos basados en e-Campus y Near Field Communication en un ambiente universitario. *Sistemas & Telemática, 11*(27), 55-76. doi:http://dx.doi.org/10.18046/syt.v11i27.1695

Herrera, J. C., Pérez, P., & Marciano, M. (2009). Tecnología RFID Aplicada al Control de Accesos. *Polibits, 40,* 57-62. Available at: http://www.gelbukh.com/polibits/2009_40/40_08.pdf

Instituto Nacional de Tecnologías de la Comunicación [INTECO]. (2013). *La tecnología NFC: aplicaciones y gestión de seguridad.* Retrieved from: http://www.egov.ufsc.br/portal/sites/default/files/cdn_nfc_final.pdf

ISO/IEC 14443-3:2016. Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision. Retrieved from: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=70171

ISO/IEC 18092:2013. Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1). Retrieved from: http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=56692

Joya, I. & Rondón, L. (2008). Control de acceso basado en tecnología RFID. *Ingeniería y Región, 5,* 67-72. Available at: https://www.journalusco.edu.co/index.php/iregion/article/view/825

Kim, D. & Salomon, M. (2012). *Fundamentals of information systems security.* London, UK: Jones & Barlett Learning.

Mozilla Developer Network (2016). *Escribiendo aplicaciones con WebSockets.* Retrieved from: https://developer.mozilla.org/es/docs/WebSockets-840092-dup/Writing_WebSocket_client_applications

NFC World. (November, 2016). *List of NFC phones.* Retrieved from: https://www.nfcworld.com/nfc-phones-list/

NXP Semiconductors. (2014). *MIFARE Classic EV1 4K - Mainstream contactless smart card IC for fast and easy solution development.* Retrieved from: http://www.nxp.com/documents/data_sheet/MF1S70YYX_V1.pdf

Pulipati, M. Srinivas, K. P. (2013). Comparison of various short range wireless communication technologies with NFC. *International Journal of Science and Research (IJSR), 2* (4), 87-91. Available at: http://www.ijsr.net/archive/v2i4/IJSRON2013728.pdf

Racero, A., López, L., Hernández, M., & Salas, D. (2015). Internet de objetos para el apoyo de procesos de enseñanza/aprendizaje en estudiantes de ingeniería. *Revista GTI, 13*(37), 97-105. Available at: http://revistas.uis.edu.co/index.php/revistagti/article/view/4694/5696

Sommerville, I. (2009). *Ingeniería de software* (9th ed). Madrid, Spain: Pearson Educación.

Whitman, M. & Mattord, H. (2013). *Management of information security,* (4th ed.). Boston, MA: Cengage Learning.

CURRICULUM VITAE

Rodrigo Andrés Góngora Herrera Technologist in Data Systematization from the Technological Fa¬culty of the Universidad Distrital Francisco José de Caldas (Bogotá, Colombia), and member of ORION research group. His broader interest areas are the design and development of web applications / Tec¬nólogo en Sistematización de Datos egresado de la Facultad Tecnológica de la Universidad Distrital Francisco José de Caldas (Bogotá, Colombia), y miembro del grupo de investigación Orión. Su mayor área de interés es el diseño y desarrollo de aplicaciones web.

Brayan David Ruiz Rubiano Technologist in Data Systematization from the Technological Faculty of the Universidad Distrital Francisco José de Caldas (Bogotá, Colombia), and member of ORION research group. His broader interest areas are the development of Mobile applications and the Internet of Things [IoT] / Tecnólogo en Sistematización de Datos, egresado de la Facultad Tecnológica de la Universidad Distrital Francisco José de Caldas (Bogotá, Colombia), y miembro del grupo de investigación Orión. Sus áreas de interés son el desarrollo de aplicaciones móviles y el Internet de las cosas [IoT].

Darin Jairo Mosquera Palacios, MSc. Systems Engineer, Specialist in Tele-informatics and Master in Tele-informatics; full-time professor at the Technological Faculty of the Universidad Distrital Francisco José de Caldas and Director of ORION research group (emphasis in telematics) / Ingeniero de Sistemas, Especialista en Teleinformática, Máster en Teleinformática; profesor de tiempo completo de la Facultad Tecnológica de la Universidad Distrital Francisco José de Caldas y Director del grupo de investigación Orión [énfasis en telemática].