

Control de Acceso con Tecnologías NFC y Arduino

Morris William Díaz Saravía

Ingeniero Electricista, Docente Investigador, Escuela de Eléctrica y Electrónica, ITCA - FEPADE Sede Central. Email: wsaravia@itca.edu.sv

Resumen

En este artículo se explica el desarrollo de un sistema de control de acceso mediante el uso de tecnología NFC (Near Field Communication o Comunicaciones por campo cercano), que mediante la potencia de un sistema informático, adquiere una versatilidad en lugares en los cuales se manejan múltiples locales con múltiples locales accediendo, mediante horarios específicos, como lo pueden ser las aulas de un campus, las habitaciones en un hotel, sistema de alquiler de bodegas, etc. En los sistemas de control de acceso se han utilizado una gran cantidad de tecnologías: de control biométrico, como lectores de iris y lectores de huellas dactilares; lectores de códigos de barras y acceder mediante un código digitado en un teclado, entre otros.

La más reciente tecnología, es el acceso mediante un 'tag' NFC, el cual establece una conexión inalámbrica para validarse con una base de datos centralizada. Entre sus ventajas tenemos su relativo bajo costo en comparación de tecnologías como scanner ópticos y lectores de huella, además de ofrecer un alto nivel de seguridad en comparación de los lectores de código de barras, RFID o teclados. Una gran gama de teléfonos inteligentes, tanto en la gama media como alta, incorporan tecnología NFC, la cual se vislumbra con un futuro muy prometedor, con docenas de posibles aplicaciones, como son: monedero electrónico, pago automático en "vending machines", llave electrónica y compra de boletos.

Palabras clave

Sistemas de control, Arduino, RFID, sistemas de control digital, controladores Lógicos programables.

Abstract

This document describes the development of an access control system using NFC (Near Field Communications), and using the power of a computer system. This system offers versatility in places where handled multiple locations with multiple local accessing, by specific times, like a campus with multiple classrooms, rooms in a hotel, rental systems of warehouses, etc. In the access control systems are available many technologies: biometric control as the retina readers and fingerprint readers; bar code readers, access code typed on the keyboards, and others.

The latest technology is the access through a NFC tag, which establishes a connection with a centralized database for validation. Some advantages have their relatively low cost compared to technologies such as optical scanners and fingerprint readers, and offer a high level of security compared to the barcode readers, keyboards or RFID. A wide range of smart phones incorporate NFC technology, which is seen with a very promising future, with dozens of potential applications, including: electronic wallet, automatic payment vending machines, electronic door key and getting tickets or boarding passes.

Keywords

Control systems, Arduino, RFID, digital control systems, programmable logic controllers.

Recepción: 29/01/2016 - Aceptación: 15/06/2016

Introducción

En lugares donde hay muchos locales con acceso restringido, con múltiples usuarios que usan simultáneamente dichos locales, se tienen fuertes gastos administrativos para permitir el acceso.

Ejemplo de estos lugares son campus universitarios, escuelas, hoteles, bodegas, etc. y la solución común es utilizar una llave por local, las cuales están centralizadas en un lugar específico; para ello se necesita tener una persona encargada de entregar y recibir las llaves y en ocasiones hasta dos personas encargadas, cuando dichos locales son usados todos los días de la semana, desde las 6:00 AM hasta las 8:30 PM.

Además, es necesario implementar un sistema de control para generar reportes de uso de las llaves, saber quién estuvo en cuál local, si hay algún daño al local.

Ante esta situación y buscando una solución informática, se analizaron diferentes alternativas considerando costos, facilidad de uso, seguridad, versatilidad y facilidad de instalación.

En la figura 1 se muestra el sistema a implementar en diagrama de bloques.

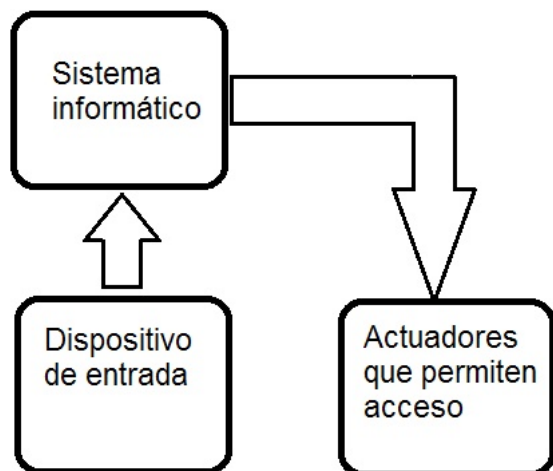


Fig. 1. Diagrama de bloques del Sistema de Control de Acceso para el campus de la Escuela Especializada en Ingeniería ITCA-FEPADE

VENTAJAS

Los sistemas de control de acceso son tecnologías que tienen mucha demanda actualmente; estos han evolucionado desde sistemas mecánicos hasta sistemas de entrada y salida completamente automatizados, utilizando diferentes tipos de tecnologías y dispositivos,

introduciendo la funcionalidad que sólo un sistema con microprocesador puede dar. Un Sistema de Control de Acceso se integra a un sistema de control de personal y uso de locales; permite el control de la entrada de los usuarios; restringe las zonas sólo al personal autorizado; da seguimiento de horarios y en general, se obtiene mediante la administración adecuada, un mejor aprovechamiento de las instalaciones.

Las ventajas que se pueden obtener con los sistemas de control de acceso son:

1. Mayor seguridad
2. Mejora en la puntualidad y cumplimiento del personal
3. Mejora la productividad
4. Reportes personalizados de entrada/salida
5. Ahorro en costos en personal que lleve los controles de acceso
6. Mejor control de visitantes
7. Integración con otros sistemas para el control y gestión del personal

DISPOSITIVOS DE ENTRADA

Es la tecnología utilizada para ingresar la entrada que activará los actuadores para permitir el acceso al local o aula. Entre las tecnologías consideradas, se tienen:

A) Teclado Numérico

El usuario del aula, en este caso el docente, introduce un código numérico proporcionado por la administración, el cual habilita al activador y abre la puerta, siempre y cuando esté registrado en el sistema informático. En comparación con otras alternativas, tiene un costo bajo, pero parece la solución con menos seguridad, ya que cualquiera que esté cerca puede captar las teclas presionadas para luego ingresar.



Fig. 2. Control de acceso mediante teclado numérico.

B) Lector RFID

El usuario porta una etiqueta con un código RFID (Identificación por Radio Frecuencia), la cual, al recibir el campo electromagnético del lector, genera un campo nuevo con el código de la etiqueta que es leído por el lector. Esta etiqueta puede estar adherida en una tarjeta o formar parte de un carné, el cual al ser pasado frente del lector a corta distancia, es leído por el sistema informático y permite que el actuador abra la puerta, si el usuario está autorizado.

El costo es medio, pero su principal desventaja es que tiene conocidas fallas de seguridad.



Fig. 3. Lector de etiqueta RFID



Fig. 4. Etiqueta con dispositivo RFID

C) Lector NFC (Near Field Communication)

El NFC o Comunicación de Campo Cercano es una tecnología innovadora, con el mismo principio del código RFID, sólo que en este caso puede haber interacción entre la etiqueta y el lector, además de transmitir mayor información, lo cual lo vuelve una tecnología segura.

El costo de los lectores es de gama media en comparación con otras tecnologías; tiene la ventaja que el costo de los carnés con la etiqueta es relativamente bajo y presenta un nivel alto de seguridad. Además, en la actualidad hay muchos teléfonos inteligentes que incorporan la tecnología NFC, que mediante programación, pueden funcionar como etiquetas activas que interactúen con los lectores de NFC.



Fig. 5. Lector de etiquetas NFC

D) Lector de huella dactilar

Como su nombre lo indica, el usuario coloca la huella sobre la ventanilla de lectura y ésta es digitalizada y buscada por el sistema informático en una base de datos. Si está registrada permite el acceso al local o aula.

Esta alternativa es de costo medio, presenta un alto nivel de seguridad y el usuario no necesita portar ninguna etiqueta, basta con su huella para ingresar. La principal desventaja que tiene esta tecnología es la dificultad para leer algunas huellas, lo que lleva a utilizar sistemas alternativos, como el lector RFID o la introducción de código por un teclado, elevando los costos de implementación.



Fig. 6. Lector de huellas dactilares

El lector de huellas dactilares pertenece a los sensores biométricos, estos utilizan alguna característica física del usuario para ser detectada y utilizada para verificación. Una de sus ventajas es que no hay una llave, tag o dispositivo electromagnético que pueda extraviarse y luego ser utilizada por otras personas no autorizadas.

Entre los lectores biométricos más usados se tienen:

1. *Lector de huellas dactilares*: utiliza la huella dactilar del usuario para verificar el acceso.
2. *Scanner de iris*: lee el iris del ojo del usuario para permitir el acceso.
3. *Reconocimiento facial*: en base al rostro del usuario, permite o no el acceso.

Los sistemas biométricos tienen algunas desventajas:

- Son tecnologías de mayor costo que las tecnologías electromagnéticas, como RFID o NFC.
- Necesitan de un sistema alternativo de autenticación, en caso que el usuario tenga dañada la característica física, como por ejemplo la huella dactilar.
- Los lectores biométricos tienden a ser frágiles al vandalismo, por lo cual limita su uso a interiores en zonas de máxima seguridad, bajo vigilancia.
- La característica física del usuario debe estar almacenada en un formato digital para compararla con la característica física detectada por el dispositivo.

Este almacenamiento puede ser de diferentes formas:

- a) En una tarjeta o llavero magnético que porta el usuario del sistema, contra el cual se autentica.
- b) En una memoria de almacenamiento interna del dispositivo donde se guardan los patrones de huellas, iris o rostros de los usuarios; esto incrementa el costo del dispositivo y limita la cantidad de usuarios, ya que la memoria es finita.
- c) En una base de datos que exige un sistema informático que la administre. También debe existir conectividad del dispositivo con dicho sistema. Además pueden generarse altos tiempos de respuesta, ya que es necesario hacer una búsqueda en la base de datos.

Al revisar las diferentes tecnologías utilizadas para permitir acceso, se ha desarrollado una tabla donde se hace un análisis comparativo, indicando los costos económicos de la tecnología, la dificultad de instalación,

el tipo de conectividad que presentan, la confiabilidad, la posibilidad de escalar a mayor cantidad de sistemas y el tipo de seguridad que ofrecen.

Fig. 7. Tabla comparativa de diferentes tecnologías de control de acceso.

Tecnología	Costos iniciales	Instalación	Conectividad	Confiabilidad	Escalabilidad	Seguridad
RFID	Intermedio	Medio	USB, Ethernet	Alta	Posible	Alta
NFC	Alto	Medio	USB, Ethernet	Alta	Posible	Muy baja
Código de barra	Alto	Alta	USB, Ethernet	Alta	Posible	Baja
Código QR	Bajo	Muy alta	USB, WIFI	Media	Posible	Media
Scanner de iris	Muy alto	Baja	USB, Ethernet	Muy baja	Posible	Muy alta
Lector de huella dactilar	Intermedio	Media	USB, Ethernet	Alta	Posible	Alta
Reconocimiento Facial	Muy alto	Baja	USB, Ethernet	Muy alta	Posible	Muy alta
Teclado	Intermedio	Media	USB, Ethernet	Media	Posible	Media

SISTEMAS INFORMÁTICOS

Para procesar la entrada desde el sensor, es necesario un sistema basado en un procesador. Entre las opciones consideradas se tienen:

A) *Computador personal*

Este puede ser un equipo que conste de un CPU, teclado, ratón, monitor, puertos USB y de red. Se hace especial énfasis que este equipo debe estar energizado los 7 días de la semana, 24 horas al día, además debe contar con un sistema de respaldo de energía para que tenga autonomía en caso de cortes energéticos.



Fig. 8. Equipo de cómputo

B) Raspberry PI

Raspberry PI es un computador de placa reducida (SBC: Single Board Computer). Este fue desarrollado en Inglaterra por la Fundación Raspberry PI para promover la enseñanza de las ciencias de la computación; contiene un procesador ARM hasta de 1 Ghz, un procesador de video VIDEOCORE IV, 512 Mb en RAM, no posee disco sino que se utiliza una memoria SD para cargar el sistema operativo. El modelo B contiene dos puertos USB, puerto de red Ethernet, puerto de video HDMI, puerto de audio de salida miniplug 3.5 mm y almacenamiento integrado SSD y MMC.

Una de las principales ventajas de éste es su bajo consumo de energía: 3.5W.

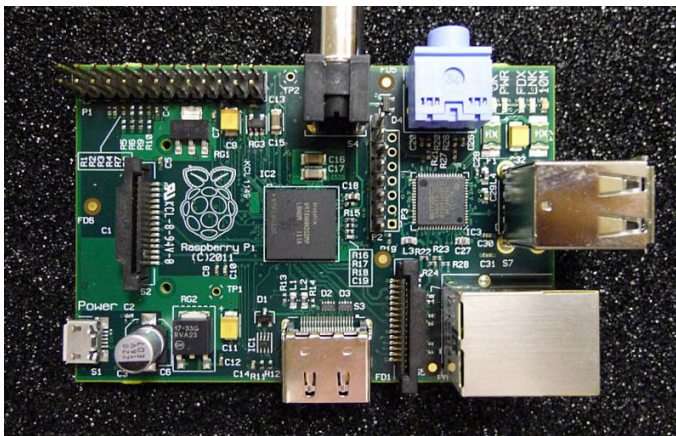


Fig. 9. Raspberry PI (SBC)

El propósito original de este computador SBC es para fines didácticos: la enseñanza de las ciencias de la computación a los estudiantes, aunque cuenta con una potencia que es capaz de ejecutar video HD 1080 perfectamente.

C) Sistema Arduino

Similar al Raspberry PI es un computador modular, fue diseñado en el Instituto IVRAE en Italia por Massimo Banzi y Hernando Barragán y se ideó para la enseñanza, aunque con un enfoque orientado a desarrollar proyectos electrónicos multidisciplinarios; es capaz de controlar luces, sensores, motores y diversos tipos de actuadores.

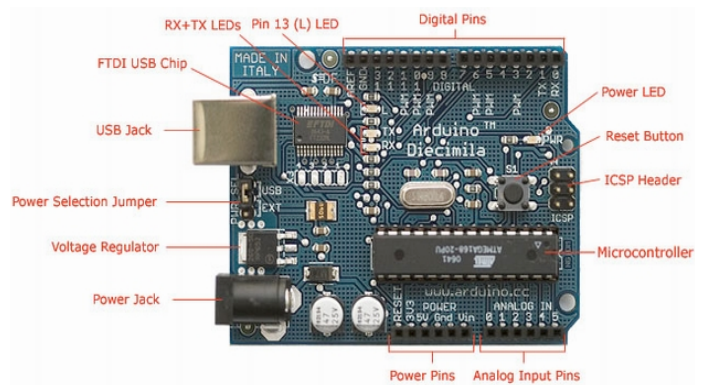


Fig. 10. Sistema Arduino

Arduino cuenta con un procesador Atmel AVR, puertos de entrada-salida y un Entorno de Desarrollo Integrado (IDE). Puede trabajar conectado a otros subsistemas (computadores y equipos con OS Android) o puede trabajar de forma autónoma. A diferencia de Raspberry PI, Arduino es modular y el módulo base comprende el procesador, un puerto USB, puertos digitales y analógicos de entrada-salida; si se necesita tarjeta de red, se agrega otro módulo; si se desea conectar un monitor, se agrega el respectivo módulo; de igual manera controladores RFID, NFC y otros módulos disponibles para Arduino.

ACTUADORES

Se denomina actuadores a los dispositivos encargados de realizar una operación mecánica.

Entre los actuadores que pueden ser utilizados están:

- Chapa eléctrica.
- Electroimanes.
- Cantonera eléctrica.

ANÁLISIS DE UNA SOLUCIÓN

La Escuela Especializada en Ingeniería ITCA-FEPADE en función de la seguridad, realizó una revisión de diferentes sistemas de acceso para el público, estudiantes y el personal, considerando una forma única y portable que les permita el acceso a diferentes espacios del campus.

A) Sistema de Entrada

El sistema NFC proporcionaría una identificación única a cada usuario; el tag de acceso NFC puede estar integrado en el carné de identificación y además contar con un sistema de encriptación que dificulta su duplicación.

El sistema RFID, aunque similar al NFC, no es conveniente por problemas de seguridad comprobados; además la tecnología NFC y RFID tienen costos similares.

En cuanto a los lectores de huella, para el sistema preexistente de marcaje de entrada y salida, se observó dificultades con la lectura de huellas dactilares de algunos miembros del personal. Los sistemas biométricos, como scanner lector de iris u otros, se descartaron por su alto costo y vulnerabilidad al vandalismo.

B) Sistema Informático

Entre las opciones revisadas, la que mejor se acoplaría a las necesidades del sistema de acceso es el Arduino, el cual permite conectividad Ethernet con otros equipos, programación de bases de datos, bajo consumo de potencia. Cuenta con puertos analógicos y digitales para controlar los actuadores; cuenta con módulos con tecnología NFC que pueden ser integrados en una caja como un sistema todo en uno.

C) Actuadores

El Sistema de Control de Acceso NFC con Arduino, podría utilizar cantoneras o chapas eléctricas, siendo otra opción el uso de electroimanes.

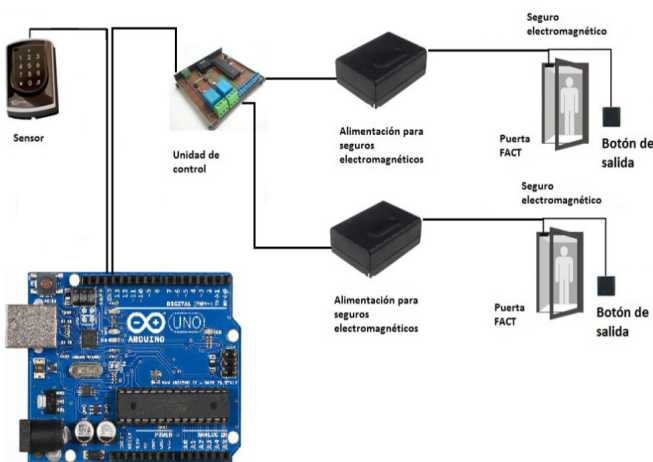


Fig. 11. Sistema de Control de Acceso con Arduino.

FUNCIONAMIENTO ESPERADO

El usuario: cada usuario tendrá un tag NFC incorporado en su carné de la institución; además existirán tags independientes para personas que no cuentan con éste. Cada tag contiene un código el cuál es leído por el lector NFC.

El programa: el sistema Arduino ejecutará el programa y leerá el código que se introduzca en el lector NFC; buscará este código en la base de datos almacenada en la SD card del sistema Arduino, si no hay coincidencia avisará con un beep, si hay coincidencia, el programa verificará que el horario permitido de acceso coincida con la hora del sistema, si es así, activará el actuador para abrir los accesos respectivos.

Los actuadores: el sistema Arduino, mediante puertos digitales, mantendrá los electroimanes en posición de cierre y los habilitará para que permitan el acceso cuando se cumplan las condiciones antes enunciadas.

En caso de pérdida del suministro eléctrico, el sistema tendrá un sistema de respaldo con batería, el cual permitirá el acceso mediante el tag NFC. Si la pérdida de energía es prolongada, el sistema tendrá un botón para desactivarlo y volver a la modalidad de llave manual.

VENTAJAS DEL CONTROL DE ACCESO NFC UTILIZANDO ARDUINO


En general algunas ventajas del Sistema de Control de Acceso son:

- Aumenta la seguridad.
- Mejora la productividad.
- Se integra con otros sistemas de gestión y control del personal.
- Genera reportes personalizados de entrada.
- Ahorra tiempo en el personal que lleva control de acceso.
- Mejora el control de los usuarios.

Referencias


LIBROS

- [1] T. Kosch, C. Schrotg, M. Strassberger and M. Bechler Villar, Automotive Internetworking, London: Wiley, 2012.
- [2] M. Benantar, Access Control Systems: Security, Identity Management and Trust Models, New York: Springer, 2006.
- [3] B. Ballard, T. Ballard y E. K. Banks, Access Control, Authentication, and Public Key Infrastructure, Jones & Barlett Learning, 2011.
- [4] J. M. Huidobro Moya, Radiocomunicaciones: viajando a través de las ondas, España: Creaciones Copyright, 2011.
- [5] M. Changshe y J. Weng, «Radio Frequency Identification System Security,» de Criptology and Information Security Series, Amsterdam, 2013.
- [6] H. Kazmi, Security and Privacy Issues in Near Field Communication (NFC) Systems: Contactless Communication in Digital World, Publishing LAP Lambert Academic, 2012.
- [7] D. A. Chavarría, «Tecnologías de campo cercano y sus aplicaciones,» Universidad de Costa Rica, San José, 2011.
- [8] W. Stalling, Cryptography and Network Security, Prentice Hall, 2011.
- [9] R. Hernández Sampieri, Metodología de la investigación, McGraw-Hill Education, 2003.
- [10] B. Schneier, Applied Cryptography, New York: John Wiley & Sons, 2015.
- [11] V. Coskum, K. Ok y B. Ozdenizci, Professional NFC Application Development for Android, Ankara: Wrox, 2013.



Escuela Especializada en Ingeniería
ITCA FEPADE

PROGRAMACIÓN DE CURSOS ACADEMIA CISCO



CURSO	HORARIO
CCNA 1	Domingos de 7:00 am. a 12:00 m.
CCNA 3	Sábados de 1:00 a 6:00 pm.
CCNA 4	Domingos de 7:00 am. a 12:00 m.
CCNA SECURITY	Sábados de 7:00 am. a 12:00 m.
CCNA VOICE	Sábados de 1:00 a 6:00 pm.

PARA MÁS INFORMACIÓN.

Puede contactarnos a los teléfonos: 2132-7537 y 2132-7570
o a las direcciones de correo: eguillen@itca.edu.sv y cescobar@itca.edu.sv

TODOS LOS CURSOS CUENTAN CON APOYO DE INSAFORP PARA EMPLEADOS DE EMPRESAS COTIZANTES