Capítulo 3 Cerradura con Seguridad Biométrica y Móvil con Bluetooth

Chapter 3 Biometric Security and Mobile Security Lock with Bluetooth

HERNÁNDEZ-LEYVA, Jovanny del Rosario†*, LUGO-LUGO, Juan De Dios, PEÑA-BOJORQUEZ, Dania Esther y MONTIEL-VILLA, Christhian Allan

Instituto Tecnológico de Nogales-Tecnológico Nacional de México

ID 1er Autor: *Jovanny del Rosario, Hernández-Leyva* / **ORC ID**: 0000-0001-6019-9996, **arXiv Author ID**: jovanny_hernandez, **CVU CONACYT-ID:** 904332

ID 1er Coautor: *Juan De Dios, Lugo-Lugo* / **ORC ID**: 0000-0001-5980-3607, **Researcher ID Thomson**: I-2888-2018, **CVU CONACYT-ID:** 665853

ID 2do Coautor: *Dania Esther, Peña-Bojorquez* / **ORC ID**: 0000-0003-4146-4867, **Researcher ID Thomson**: I-2797-2018, **CVU CONACYT-ID:** 904344

ID 3er Coautor: *Christhian Allan, Montiel-Villa* / **ORC ID**: 0000-0001-8118-5956, **Researcher ID Thomson**: I-3328-2018, **CVU CONACYT-ID:** 903675
.

Abstract

Society is advancing by leaps and bounds, which makes the issue of security, vital, therefore new ways of protecting belongings and new ways of circumventing them, are created every day. Biometric locks are no exception, most systems are based solely on fingerprint reading. This works propose the implementation of a second layer of security: to use also a mobile device registering the MAC address by reading it from the Bluetooth module, this is possible because you can associate it with a user. The algorithm works this way: the user fingerprint is registered in the computer, the mobile is connected using Bluetooth, then a fingerprint sample is taken, and this way the system checks its registration, the connection of the associated mobile device is requested and access is granted or denied. The system has been tested using an Arduino component and has had 99.5% of accuracy when implementing the system in a safe box prototype.

Lock, Biometric, Bluetooth

Introducción

Un sistema biométrico es un método de identificación y verificación de un individuo utilizando biometría estática, en este trabajo, la huella dactilar, ya que esta característica es inherente a la persona, tiene la ventaja de la comodidad del usuario, y que las características siempre están con la persona sin la posibilidad de olvidar o perder. También en el aumento de la seguridad, estas no se pueden trasmitir de forma deliberada (Marquez Moreno, Niño Garzón, & Luengas Contreras, 2017).

Con la llegada de los dispositivos móviles y la convergencia de las tecnologías inalámbricas e Internet, tanto el contenido como la calidad de la investigación en este campo está sujeta a cambios regulares (Hae-Duck J.Jeong, 2015). Se han producido una *variedad de dispositivos informáticos de última generación que son compatibles entre sí, que tienen la capacidad de interactuar con las personas, lo que se conoce como computación generalizada (Hae-Duck J.Jeong, 2015).

Debido al medio social, la seguridad es un tema de vital importancia, simplemente hablando de robo a casas – habitación sin violencia, en un año ha aumentado casi un 3%, pasando de 75,140 a 77296 de 2016 a 2017, según cifras de (SESNSP, 2018), por lo cual, nuevas formas de proteger las pertenencias y también nuevas formas de burlar dichas protecciones son creadas día con día. Las cerraduras biométricas no son la excepción, ya que la mayoría de los sistemas de este tipo, están basados en la lectura de huellas digitales, password y pestillos mecánicos (SignTech, 2016).

Aunque existen diversos dispositivos móviles que utilizan Bluetooth en el mercado, la mayoría de los sistemas biométricos de cerraduras existentes se basan en la adaptación de dispositivos que se encuentran en el mercado, que les permite construir los prototipos a los que hacen mención (Aguirre & Luzuriaga Hidalgo, 2015), algunos se basan en la implementación de la cerradura desde cero pero sin utilizar Bluetooth (Pérez García, 2014).

No encontramos dispositivos que implementen una cerradura igual a la que se propone, una Cerradura con Seguridad Biométrica y Seguridad Móvil con Bluetooth que cuenta con una segunda capa de seguridad que consiste en incluir a la seguridad biométrica la utilización de un dispositivo móvil.

En éste documento encontrará una descripción de los elementos utilizados para la construcción del prototipo: el funcionamiento del módulo Arduino utilizado, el Servomotor que abre la puerta de la caja fuerte del prototipo y dispositivo de lectura de huella digital utilizado. Asimismo se explica la parte de software que controla los accesos al programa, registro y validación. Al final se presenta la metodología, resultados, agradecimientos, conclusiones y referencias utilizadas.

Funcionamiento Arduino UNO

Para hacer funcionar el prototipo se utilizó un dispositivo llamado Arduino UNO (figura 3.1), el cual es una placa electrónica basada en el microprocesador Atmega328. Contiene lo necesario para apoyar el microcontrolador (Arduino, 2014).

Figura 3.1 *Arduino UNO*

Fuente: Recuperado de https://www.arduino.cc/en/uploads/Main/ArduinoUno_R3_Front.jpg

El Arduino UNO recibirá una señal enviada desde el programa, una vez hayan sido comprobado que los datos de la huella y la MAC Address coinciden con los que están guardados en la base de datos, lo cual hará que se active un servomotor dándonos acceso al contenido o lugar en el que haya sido instalada nuestra cerradura.

Funcionamiento del servomotor

Un servomotor (figura 3.2) es un motor eléctrico al que podemos controlar tanto la velocidad, como la posición del eje que gira.

Figura 3.2 Servomotor MicroServo

Fuente: Recuperado de https://circuitdigest.com/article/servo-motor-basics

Las características principales de un servomotor son el par y la velocidad. (Tecnología, 2017).

Una vez activado el servomotor por el Arduino UNO, este hará una rotación de 90°, en este prototipo se simula la acción de abrir una cerradura en una caja fuerte prototipo (figura 3.3) que contiene en su interior el servomotor que apertura la cerradura, permitiendo acceder al contenido o lugar y una vez que se haya salido del programa, el servomotor regresará a su posición original para cerrarse.

Figura 3.3 Prototipo de caja fuerte

Funcionamiento del Lector de Huella

El lector U.are.U 4500 (figura 3.4) es un lector de reconocimiento huellas digitales USB (Seat, 2017).

Figura 3.4 Lector U.are.U® 4500

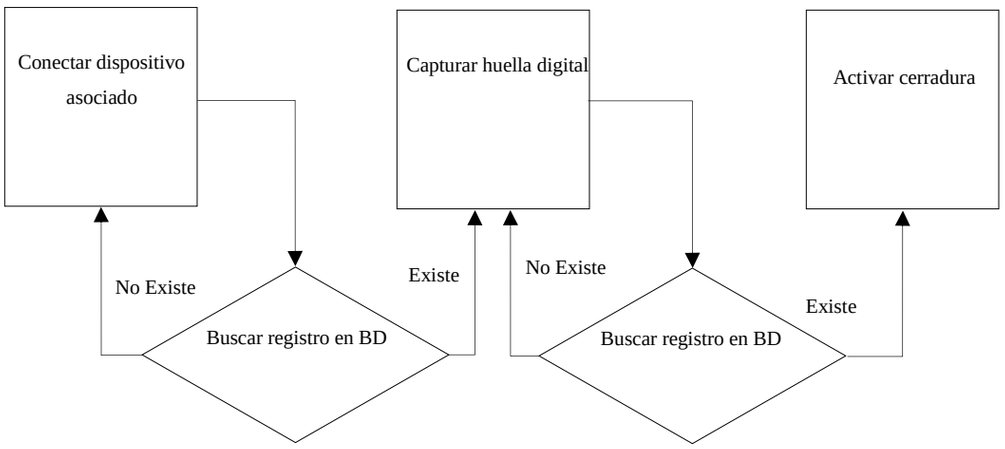
Fuente: Recuperado de http://www.siasa.com/productos/imagenes/medianas/uareu4500.jpg

En el sistema se lee una vez la huella digital para comprobar que la persona que intenta ingresar, es la que está registrada en la base de datos del programa, al cual se le identificará como el administrador y tendrá acceso a las acciones dentro la interfaz del programa.

Algoritmos utilizados y Arquitectura

El diagrama (Gráfico 3.1) muestra cómo es el proceso por el que se debe pasar para poder acceder a la apertura del cerrojo de la caja fuerte.

Gráfico 3.1 Diagrama de registro y validación



El cual funciona de la siguiente manera: registrar la dirección de control de acceso del dispositivo (MAC Address), extrayéndolo del módulo Bluetooth, este dato se puede asociar a los datos de un determinado usuario.

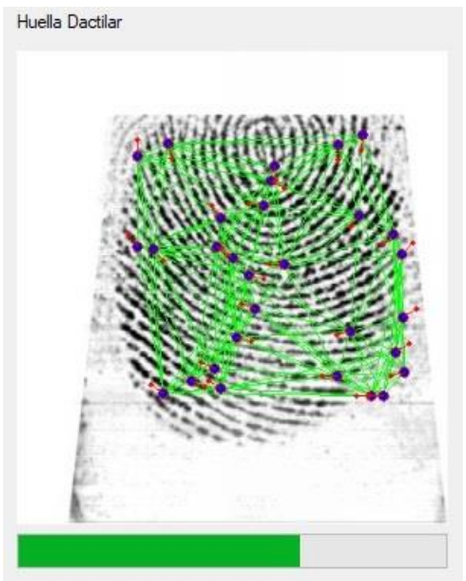
De esta forma se registra la huella dactilar del usuario en la computadora, se conecta el móvil a través del Bluetooth, se toma una muestra de huella dactilar, en el sistema se verifica su registro, se solicita la conexión del dispositivo móvil asociado y se concede o niega el acceso.

Para hacer la programación del sistema se utilizó C# con base de datos MySQL, en el módulo del dispositivo móvil, se utilizó Android Studio.

Módulo de Registro

Al iniciar el registro el sistema pide al usuario que ingrese su huella dactilar (figura 3.5), esta es captada por un dispositivo conectado a la computadora (en nuestro caso el lector de huellas para posteriormente analizar sus características. Si la cantidad de minucias captadas es suficiente el usuario podrá proceder al siguiente paso.

Figura 3.5 Minucia de la huella digital solicitada



Posteriormente se asocia la huella digital con un dispositivo móvil (figura 3.6), para esto el sistema se vale del módulo Bluetooth presente en la gran mayoría de los teléfonos de hoy en día, el sistema le pide al usuario que active dicho modulo para posteriormente hacer un escaneo, una vez terminado, el usuario tendrá que seleccionar de una lista el dispositivo que desea asociar.

Figura 3.6 Dispositivo móvil asociado

Por último se le pedirá al usuario que ingreso su nombre y apellido (figura 3.7) para su registro.

Figura 3.7 Datos de usuario

Una vez finalizados todos los pasos el sistema procederá a registrar en una base de datos toda la información ingresada por el usuario.

Módulo de Validación

Al iniciar el módulo de validación (figura 3.8) el sistema le pedirá al usuario que conecte el dispositivo móvil que asocio durante el registro, una vez hecho esto la aplicación buscará en una base de datos si el dispositivo conectado se encuentra registrado y de ser así lanzara un mensaje confirmándolo.

Figura 3.8 Conectar dispositivo

Después de validar el dispositivo el sistema esperara a que el usuario coloque su huella digital para proceder a escanearla. Si el escaneo coincide con la información capturada en la base de datos el sistema lanzara un mensaje de bienvenida (figura 3.9) y enviara una señal a un microcontrolador para ejecutar un actuador, en nuestro caso un servomotor, que permitirá el acceso.

Figura 3.9 Bienvenida al sistema

Metodología

Se construyó una caja fuerte prototipo, en la que se hicieron pruebas de desempeño, los usuarios que utilizaron el dispositivo, un total de 20, observaron cómo se abría la caja fuerte cuando proporcionaban los datos de manera correcta y cómo se negaba el acceso al contenido de la misma cuando los datos eran incorrectos.

Se utilizó para su construcción un dispositivo Arduino UNO, que es el que se tenía a disposición, además de ser suficiente para realizar las tareas de enviar la señal al siguiente dispositivo, el Servomotor para que se moviera y abriera la caja fuerte, el cual tiene la rotación adecuada para abrir en un ángulo de 90º. Para proporcionar la huella digital se utilizó un lector UareU modelo 4500, que tiene una precisión de 99% para capturar las muestras de las minucias de las huellas digitales.

Para la programación del módulo se realizó una aplicación Web en C# con base de datos MySQL, en el módulo del dispositivo móvil, se utilizó Android Studio, sin embargo es posible en una implementación realizar la programación para dispositivos móviles al pasar el prototipo a la realidad.

Toda vez construido el prototipo se procedió a realizar las pruebas de desempeño, que permitieron llegar a los resultados descritos en este trabajo.

Resultados

Se hicieron muchas pruebas de acceso a la caja fuerte prototipo y en todas, excepto una, el prototipo funcionó apropiadamente, dando un 99.5% de confiabilidad, a los diferentes tipos de usuarios, de diferentes usuarios les tomó 1 minuto en promedio abrir la caja fuerte, quienes opinaron que les parece muy bueno el sistema, lo que hace pensar que el prototipo es factible.

El Hardware utilizado resultó ser apropiado para el prototipo construido, ya que el Arduino UNO contiene las características apropiadas para realizar las tareas que se requieren para controlar la apertura de la caja fuerte, el servomotor contiene los movimientos que asemejan los realizados al realizar la apertura un dispositivo de seguridad como el mencionado, y el Lector de Huella permitió autenticar con confiabilidad suficiente a los usuarios registrados. Los módulos del programa realizaron el Registro apropiado de los usuarios con permiso de abrir la cerradura y la Validación de los datos se realizó con éxito.

Con lo cual se ha podido construir el sistema utilizando un Arduino y se ha tenido éxito al implementar el sistema en una caja fuerte prototipo.

Agradecimiento

Agradecemos al Tecnológico Nacional de México, en especial al plantel: Instituto Tecnológico de Nogales, por las facilidades brindadas, tanto para la construcción del prototipo, como para el financiamiento para la presentación del artículo.

Conclusiones

Tras haber realizado múltiples pruebas se obtuvo como resultado que el sistema valida de forma correcta la huella digital de un usuario y el dispositivo móvil asociado al mismo, impidiendo de esta manera el ingreso a quienes no cumplan con las características registradas.

En conclusión, al combinar con éxito en el sistema que lee algo que el usuario es, es decir la minucia de su huella digital y controla algo que el usuario tiene, es decir los dispositivos que conforman el prototipo, se ha logrado mejorar de una manera eficiente y económica la seguridad en un circuito digital de acceso.

Todavía quedan muchos detalles que mejorar, como el implementar el dispositivo en una caja fuerte real, y quizá embeber el sistema completamente en el dispositivo portátil, sin embargo se piensa que se sientan las bases para lograr construir mejores herramientas para una nueva capa de seguridad en dispositivos para resguardar pertenencias.

Referencias

Aguirre, O., & Luzuriaga Hidalgo, G. E. (2015). *Caja de seguridad electrónica biométrica.* Quito: Repositorio Quito.

Arduino. (01 de Enero de 2014). *Especificaciones técnicas Arduino UNO*. Obtenido de http://arduino.cc/en/Main/arduinoBoardUno

Hae-Duck J.Jeong, W. L. (2015). Utilizing a Bluetooth remote lock system for a smartphone. *Pervasive and Mobile Computing Elsevier* , 150-165.

Marquez Moreno, I. J., Niño Garzón, M. J., & Luengas Contreras, L. A. (2017). Sistema de Control de Acceso por Biometría. *Visión Eletrónica* , 1-25.

Pérez García, D. (2014). *Diseño y construcción de un cierre electrónico inteligente para armarios.* Oviedo: Repositorio Institucional.

Seat, S. (01 de Noviembre de 2017). *SEAT Seguridad y Equipos de Alta Tecnología*. Obtenido de http://seguridadseat.com/pdf/files-pdf/LectorHuella-UareU_4500.pdf

SESNSP. (1 de MAyo de 2018). *Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública*. Recuperado el 6 de Junio de 2018, de http://secretariadoejecutivo.gob.mx/incidencia-delictiva/incidencia-delictiva-fuero-comun.php

SignTech. (1 de Enero de 2016). *Sign Tech Biometric*. Recuperado el 7 de Junio de 2018, de http://signtechbiometric.com/cerraduras-biometricas/

Tecnología, Á. (09 de Noviembre de 2017). *Área Tecnología*. Obtenido de http://www.areatecnologia.com/electricidad/servomotor.html