CARÁTULA

Implementación de un sistema de seguridad de acceso y registro biométrico basado en tecnología arduino para domicilio privado.

Enríquez Cuenca, Niza Solange

Departamento de Eléctrica y Electrónica

Carrera de Tecnología en Electrónica mención Instrumentación y Aviónica

Monografía, previo a la obtención del título de Tecnólogo en Electrónica mención Instrumentación & Aviónica

Ing. Calvopiña Osorio, Jenny Paola

09 de marzo de 2021

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE TECNOLOGÍA EN ELECTRÓNICA MENCIÓN INSTRUMENTACIÓN Y AVIÓNICA

CERTIFICACIÓN

Certifico que la monografía, "**IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD DE ACCESO Y REGISTRO BIOMÉTRICO BASADO EN TECNOLOGÍA ARDUINO PARA DOMICILIO PRIVADO**" fue realizado por la señorita Enríquez **Cuenca, Niza Solange**, la cual ha sido revisada y analizada en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

09 de marzo de 2021

Firma:

JENNY PAOLA CALVOPINA OSORIO

Ing. Calvopiña Osorio, Jenny Paola

C.C.: 0503390239

Reporte de verificación

URKUND

Document Information

Analyzed document	ENRÍQUEZ CUENCA NIZA SOLANGE.pdf (D97383758)
Submitted	3/5/2021 9:01:00 PM
Submitted by	
Submitter email	nsenriquez@espe.edu.ec
Similarity	6%
Analysis address	jpcalvopina1.espe@analysis.urkund.com

Sources included in the report

SA	**PROYECTO-TITULACION-ORTEGA.docx** Document PROYECTO-TITULACION-ORTEGA.docx (D47427652)	1
W	URL: https://docplayer.es/59879081-T-e-s-i-s-universidad-nacional-autonoma-de-mexico.html Fetched: 4/15/2020 4:54:49 PM	3
SA	**Tesis final Freddy Cali Rivera.docx** Document Tesis final Freddy Cali Rivera.docx (D63108127)	2
W	URL: https://docplayer.es/19520760-Escuela-politecnica-nacional.html Fetched: 11/27/2019 5:11:07 PM	3
SA	**Marlon Acebo 1.docx** Document Marlon Acebo 1.docx (D41205997)	1
SA	**Sistema de registro de asistencia final.docx** Document Sistema de registro de asistencia final.docx (D77714487)	3
W	URL: https://bibdigital.epn.edu.ec/bitstream/15000/5487/1/T2349.pdf Fetched: 11/22/2020 9:04:35 AM	1

JENNY PAOLA CALVOPIÑA OSORIO

Ing. Calvopiña Osorio, Jenny Paola
C.C.: 0503390239

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELECTRICA Y ELECTRÓNICA

CARRERA DE TECNOLOGÍA EN ELECTRÓNICA MENCIÓN INSTRUMENTACIÓN Y AVIÓNICA

RESPONSABILIDAD DE AUTORÍA

Yo, **Enríquez Cuenca, Niza Solange**, con cédula/cedulas de ciudadanía n° **1718854852**, declaro que el contenido, ideas y criterios de la monografía: **"Implementación de un sistema de seguridad de acceso y registro biométrico basado en tecnología arduino para domicilio privado"** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

09 de marzo de 2021

Firma

.....

Enríquez Cuenca, Niza Solange

C.C.: 1718854852

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE ELECTRÓNICA MECIÓN INSTRUMENTACIÓN Y AVIÓNICA

AUTORIZACIÓN DE PUBLICACIÓN

Yo Enríquez Cuenca, Niza Solange, con cédula/cedulas de ciudadanía n° 1718854852, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar la monografía **"Implementación de un sistema de seguridad de acceso y registro biométrico basado en tecnología arduino para domicilio privado** "en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

09 de marzo de 2021

Firma

.....

Enríquez Cuenca, Niza Solange

C.C.: 1718854852

Dedicatoria

El presente trabajo va dedicado a mi madre la Sra. Cuenca Loaiza, Agustina Irene y a mi abuelita la Sra. Loaiza Soto Olga Isabel, a mi familia y amigos quienes tuvieron un apoyo incondicional para la culminación de mis estudios.

A el Sr. Fulvio Sánchez y la Sra. Mercedes Cuenca quienes siempre han confiado en mí y han apoyado cada una de mis decisiones.

En especial a mi madre una persona que ha estado a lo largo de mi vida apoyándome para ser un mejor ser humano y una excelente profesional, quien desde pequeña ha guiado mis pasos y ha estado en cada caída y victoria, a ella que es mi mayor motivación para seguir adelante y siempre mejorar, las palabras no bastan para expresar mi gratitud.

ENRÍQUEZ CUENCA, NIZA SOLANGE

Agradecimiento

Principalmente a Dios por su inmenso amor y por guiarme en el camino brindándome el valor, la constancia para alcanzar cada objetivo propuesto.

A la Universidad de las Fuerzas Armadas “ESPE” junto a sus docentes quienes me ofrecieron la oportunidad de realizar mi formación profesional.

ENRÍQUEZ CUENCA, NIZA SOLANGE

Tabla de contenido

Índice de tablas

Índice de figuras

Resumen

En la presente monografía se describe la implementación de un sistema de seguridad de acceso y registro biométrico basado en tecnología arduino para un domicilio privado, ubicado en la Cdla. Hospitalaria de la ciudad de Quito. El sistema de acceso biométrico posee un sensor de huella dactilar, para detectar los rasgos característicos, presentes en las crestas papilares de un dedo de la mano de cada persona registrada. La imagen captada, es comparada con un banco de imágenes de los usuarios autorizados, siendo necesario tener mínimo 2 imágenes por cada individuo, si existe coincidencia; se activará un puerto de la placa de desarrollo, que a su vez enviará un pulso eléctrico para que la cerradura entre en funcionamiento permitiendo el acceso al usuario. En caso de que el sistema detecte 3 lecturas erróneas de forma consecutiva se enviará un mensaje de texto al usuario principal alertando de los intentos fallidos. Para registrar nuevos usuarios, se tiene un pulsador y una pantalla LCD 16X2 que refleja las instrucciones a seguir, además se requiere de la huella del administrador como parámetro de seguridad del sistema para continuar con el proceso. Al registrar el acceso de un usuario, los datos del mismo serán almacenados en una tarjeta MicroSD.

Palabras clave:

- **CERRADURA BIOMÉTRICA**
- **HUELLA DACTILAR**
- **REGISTRO BIOMÉTRICO**
- **SISTEMA DE SEGURIDAD DOMICILIARIA**

Abstract

This monograph describes the implementation of a biometric registry and access security system based on Arduino technology for private domicile, located at the Cdla. Hospitable of the city of Quito. The biometric access system has a fingerprint sensor to detect the characteristic features, present in the papillary ridges of a finger of each person's hand. The image captured, is compared with a bank of images of authorized users, being necessary to have minimum 2 images for each individual, if there is coincidence; a port of the development plate will be activated, which in turn will send an electric pulse for the lock to come into operation allowing access to the user. In case the system detects three erroneous readings consecutively a text message will be sent to the main user warning of failed attempts. To register new users, you have a pushbutton and a 16X2 LCD screen that reflects the instructions to follow, and the administrator's footprint is required as a system security parameter to continue the process. When registering a user's access, the user's data will be stored on a MicroSD card.

Key words:

- **BIOMETRIC LOCK**
- **FINGERPRINT**
- **BIOMETRIC RECORD**
- **HOME SECURITY SYSTEM**

1. Introducción

1.1. Tema

Iimplementación de un sistema de seguridad de acceso y registro biométrico basado en tecnología arduino para domicilio privado.

1.2. Antecedentes

Hace varios años no se podía imaginar cerraduras electrónicas, ya que las más seguras para el hogar eran las cerraduras tradicionales como son las cerraduras cilíndricas, cerraduras de pistón, cerraduras con llave, entre otras, al pasar el tiempo junto con los avances tecnológicos se ha evidenciado un cambio agitando ya que se ha pasado de las cerraduras tradicionales a las cerraduras eléctricas y finalmente a las cerraduras electrónicas, todas ellas con el fin de brindar seguridad en el hogar, las mismas se han visto respaldadas en distintas investigaciones, por ejemplo:

- En el proyecto titulado: Sistema de monitoreo integral para casa habitación. Donde su objetivo principal era el monitoreo de sensores instalados dentro de una habitación o a lo largo de una casa para tener un control de la misma mediante el uso del internet, ayudado de cámaras que brindaban una imagen en tiempo real. (Serrano, 2006)
- En la investigación titulada: Sistema de control de acceso por biometría. Donde describe un prototipo para el control de acceso de individuos a una instalación, el prototipo pretende validar el reconocimiento de huella dactilar, así como el reconocimiento facial para permitir el ingreso a personal previamente registrado. (Marquez, Niño, & Luengas, 2017)

- En el proyecto donde se expone el diseño y construcción de un prototipo para el acceso de usuarios a sus hogares utilizando un sistema electrónico mediante arduino, lector de huella digital, una tarjeta RFID y un módulo bluetooth, logrando así atender diferentes necesidades con múltiples opciones. (Rugarcía, 2019)

En la actualidad se puede encontrar cerraduras electrónicas con lectores de código de barras, cerraduras con llaves magnéticas, cerraduras biométricas como es el caso del presente proyecto donde se realizará una cerradura biométrica de lectura de huella dactilar con el registro de datos de ingreso al igual que con una notificación mediante mensajes de texto al exceder los intentos permitidos, asegurando así el ingreso únicamente de usuarios registrados.

1.3. Planteamiento del problema

En la actualidad se vive una sensación muy grande de inseguridad que amenaza constantemente a las personas, uno de los lugares más comunes donde se evidencia esto son los domicilios ya que uno de sus puntos débiles son las cerraduras tradicionales, puesto que las llaves usadas para las mismas se pueden perder o clonar permitiendo el acceso a los domicilios de personas ajenas o no autorizadas.

La posibilidad del libre ingreso de una persona indeseable a los domicilios, pone en riesgo no solo las cosas materiales sino también la vida de quien habita en el lugar, por esta razón es muy importante tomar acciones con las cuales se pueda disminuir en gran parte los peligros que puedan presentarse. Existen varias medidas a tomar en cuenta para solucionar este problema como, por ejemplo: la implementación de una

contraseña para el ingreso a propiedades, tarjeta de identificación o código de barras; cabe recalcar que estas propuestas también pueden presentar fallas por suplantación, pérdida de identificación o a su vez compartir la contraseña con personas indebidas por error, sí no se implementa un sistema de acceso con las respectivas seguridades y respaldos.

Al implementar un sistema de acceso por seguridad biométrica se verifican características únicas de cada persona como la huella dactilar, la retina del ojo o a su vez todo el rostro, estas características son intransferibles e imposibles de perder, así como el reconocimiento y autentificación digital para tener acceso a un domicilio será una medida de seguridad que presentaría menores problemas.

Al no implementar un sistema de seguridad basado en reconocimiento biométrico se corre el riesgo de que ingresen al domicilio personas no autorizadas, que pudiesen obtener la llave de ingreso de una cerradura tradicional.

1.4. Justificación

En el desarrollo de este proyecto se implementarán conocimientos adquiridos a lo largo de la carrera de Tecnología Electrónica Mención Instrumentación y Aviónica, consiguiendo de esta forma resaltar la imagen institucional de la Universidad y sentando una base de posibles mejoras de este trabajo para la carrera de Tecnología Superior en Automatización e Instrumentación.

El propósito general del presente trabajo de titulación, tiene la intención de mostrar que tener el control de ingreso hacia personas que puedan afectar la integridad de los integrantes de un hogar es primordial, y que no solamente existen las llaves tradicionales para abrir cerraduras, tarjetas magnéticas, contraseñas o códigos de

barras que en todos sus casos pueden adulterarse, copiarse o extraviarse causando molestias e incumpliendo su principal función de proteger.

Para evitar contratiempos que puedan presentarse se ha propuesto un sistema de seguridad biométrico basado en la huella dactilar de las personas, la cual es única para cada ser humano lo que la hace intransferible e inviolable evitando así los problemas ya mencionados y reduciendo el nivel de riesgo de una invasión a la propiedad privada, esto gracias a que la tecnología brinda cada vez más y mejores seguridades.

En el reconocimiento de rasgos biométricos se ha visto un gran avance tecnológico en los últimos años que ha hecho posible que se pueda utilizar en lo que antes ni siquiera se imaginaba como son en tecnologías de acceso a domicilios. Usando este tipo de tecnología accesible para personas de diferente nivel social se puede limitar el clonar llaves o tarjetas de acceso, el robo de claves para el ingreso a domicilios, brindando así seguridad para el usuario.

1.5. Objetivos

1.5.1. Objetivo general

- Implementar un sistema de seguridad de acceso y registro biométrico basado en tecnología Arduino para domicilio privado.

1.5.2. Objetivos específicos

- Investigar qué módulos compatibles con arduino existen y cómo funcionan para el desarrollo de sistemas de seguridad en páginas oficiales, libros, proyectos de grado, artículos académicos y repositorios digitales.

- Definir los comandos de configuración en Arduino para el reconocimiento de huellas dactilares mediante investigación en páginas oficiales del sensor.
- Levantar información de las necesidades del domicilio para definir el modo de funcionamiento del sistema de seguridad en base a los módulos compatibles con arduino disponibles en el mercado.
- Implementar y verificar el sistema de seguridad de acceso y registro biométrico mediante pruebas para tener un correcto funcionamiento.

1.6. Alcance

El proyecto está dirigido a las personas que habitan en un domicilio privado en la ciudad de Quito en el sector del valle de los chillos donde será instalado el sistema de seguridad, y además a personas que deseen tener un mayor control de seguridad en sus domicilios mediante el uso de avances tecnológicos.

El presente proyecto constará de un sistema de seguridad de acceso y registro biométrico, ya que en el actual domicilio se refleja la ausencia de un sistema que brinde la seguridad necesaria por la ubicación del mismo. Al no contar con un sistema de acceso restringido personas con malas intenciones pueden ingresar al domicilio y afectar tanto física como mentalmente a los ocupantes del lugar. Con la implementación del sistema de seguridad de acceso y registro biométrico se busca solucionar de manera definitiva estos incidentes.

El impacto de este tema pretende dar a conocer que un sistema de seguridad con huella dactilar es menos vulnerable en la sociedad actual, ya que no depende de instrumentos físicos para su funcionamiento como son llaves o tarjetas de acceso, las

cuales pueden sufrir desperfectos o perdidas, mientras que al usar seguridad biométrica el acceso únicamente puede ser a la persona portadora de la huella autorizada.

2. Marco teórico

2.1. Sistema de Seguridad

Un sistema de seguridad es la unión de varios elementos que guardan una relación entre ellos, que en este caso es de establecer protección ante posibles peligros, riesgos o delitos que afecten negativamente a una persona, hogar o negocio. Para obtener el sentimiento de tranquilidad ante cualquier acto mencionado, se logra mediante alarmas, controles de acceso, entre otros. (SEGURIDAD, 2017)

2.1.1. Control de acceso

Un control de acceso es el uso de un dispositivo cuyo objetivo es impedir el libre acceso del público a ciertas instalaciones. En primer lugar, se debe justificar por qué se desea tener un control de acceso, por ejemplo, la existencia de componentes humanos como materiales que se desean proteger.

En un lugar de trabajo los componentes a proteger pueden ser fácilmente identificables, como son las zonas donde se manipula dinero, donde se guardan los registros del personal y propiedad intelectual. Hay que considerar que al tener un control de acceso un espacio se dividirá en varias zonas o subáreas como son la interna (área protegida) y externa o sin protección.

Las barreras a utilizar serán físicas tal como puertas, barreras vehiculares u otros dispositivos físicos que impidan el libre ingreso a un área interna. Asimismo, se debe definir las reglas o privilegios de cada uno de los usuarios que podrán acceder a determinada zona protegida. Estos privilegios podrán depender de la categoría o rango de la persona dentro de la empresa, de su función, de un determinado horario en el que puede ingresar o salir, del día de la semana, si es un feriado, etc. (COSETINO, 2016)

Los elementos que con mayor frecuencia son utilizados en la actualidad para controlar el acceso a un determinado lugar son las cerraduras ya sean eléctricas, magnéticas, electromagnéticas, mecánicas entre otras.

2.1.2. Tipos de cerraduras

Las cerraduras son comunes en hogares y en sitios concurridos, se las puede apreciar en puertas principales, son dispositivos mecánicos cuya función es la de controlar el acceso a un sitio y brindar seguridad a los mismos, este dispositivo comúnmente es usado mediante una llave para abrir y cerrar. (Madrid, 2018)

a) **Cerraduras cilindricas**. El componente principal es una caja cilíndrica con un eje de rotación perpendicular a la hoja de la puerta, el mecanismo central de la cerradura se encuentra al interior de la puerta, la misma puede usar o no llave, como se ve en la Figura 1. Las que no utilizan llave reciben el nombre de cerraduras de simple paso, pueden combinar seguro por dentro y llave por la parte exterior, o utilizarla por ambos lados. Se utilizan principalmente en puertas de interior. (Alvarado, 2010)

Figura 1

Cerradura cilíndrica

Nota. Recuperado de “Análisis, diseño e implementación de un sistema de inmótica para el edificio administrativo de la facultad técnica para el desarrollo de la universidad católica de Santiago de Guayaquil”, (p. 12), 2010 (Alvarado, 2010)

b) **Cerradura sin llaves**. Existen varias formas de activación como es con una clave que puede ser digitado manualmente, utilizando una tarjeta magnética, o por medio de una combinación de las dos, como se muestra en la Figura 2.

Existen cerraduras de seguridad que poseen sensor óptico que funcionan de la siguiente manera: el espejo que da claridad en el dedo es desigual por la humedad distinta que hay entre cada minúscula ranura, a película reflexiva nítidamente la señal digital que es captada por una operadora Ccd que digitaliza los números reputados. Estos son comparados con los datos previamente guardados, solo si coinciden el usuario es autorizado y la cerradura se acciona. (Acebo, 2018)

Figura 2

Cerradura sin llaves

Nota. Recuperado de " Implementación de acceso inteligente a las oficinas de coordinación y sala de docentes en la carrera de ingenierías en sistemas computacionales", 2018 (Acebo, 2018)

c) **Cerradura electrónica.** La cerradura electrónica es la más actual en la historia de las cerraduras, ya que posee un bloqueo electrónico, como se muestra en la Figura 3. Es un dispositivo que funciona en base a la corriente eléctrica, en ocasiones son completamente independientes y en otros casos son conectadas a un sistema de control de acceso remoto. (Cadillo, 2018)

Figura 3

Cerradura electrónica

Nota. Recuperado de “Modelo de sistema biométrico de interfaz híbrida para cerraduras de seguridad electrónicas”, 2018 (Cadillo, 2018)

d) **Cerraduras Inteligentes**. Con los avances tecnológicos de hoy en día se puede implementar cerraduras inteligentes que tienen un registro o código de acceso el cual permite activar o desactivar la cerradura. Existen varios modelos de cerraduras y pueden ser independientes o también pueden ser parte de un sistema de seguridad donde los accesos son monitoreados remotamente. (Madrid, 2018)

e) **Cerraduras Biométricas** Este tipo de cerraduras son personalizadas ya que se abren simplemente al tocarlas. Algunas cerraduras poseen un lector de huellas, como se muestra en la Figura 4. Existen distintos modelos que pueden funcionar con clave, con huella o con llave, y es capaz de almacenar hasta 138 huellas dactilares diferentes. (Alvarado, 2010)

Figura 4

Cerradura biométrica

Nota. Recuperado de “Análisis, diseño e implementación de un sistema de inmótica para el edificio administrativo de la facultad técnica para el desarrollo de la universidad católica de Santiago de Guayaquil”, (p. 51), 2010 (Alvarado, 2010)

2.2. Biometría

Es el estudio de métodos utilizados para el reconocimiento de uno o más rasgos conductuales o físicos en los humanos. Se deriva de las palabras griegas "BIOS" de vida y "metrón" de medida. En las tecnologías de la información (TI), se refiere a las tecnologías para calcular y examinar características físicas del comportamiento humano para el propósito de autentificación. (Alvarado, 2010)

2.2.1. Funcionamiento de la Biometría

La persona se registra en el sistema cuando una o más de sus características físicas es obtenida, a continuación, es procesado mediante un algoritmo numérico y es almacenado en una base de datos. Entre las tecnologías actuales se encuentra tasas de error que varían desde 60% al 99,9%. (Alvarado, 2010)

2.2.2. Estándares relacionados a tecnología biométrica

Los principales comités que son encargados de coordinar a nivel mundial los estándares biométricos son:

- El Sub-Comité 17 (SC17) es encargado a nivel mundial de coordinar las actividades de estandarización biométrica es del Joint Technical Committee on Information Technology (ISO/IEC JTC1), del International Organization for Standardization (ISO) y el International Electrotechnical Commission (IEC). (Alvarado, 2010)
- El Comité Técnico M1 del INCITS (InterNational Committee for Information Technology Standards), el National Institute of Standards and Technology (NIST) y el American National Standards Institute (ANSI) son

encargados de desempeñar un papel similar en Estados Unidos. (Alvarado, 2010)

Entre los estándares más importantes utilizados en la actualidad se encuentran:

- **Estándar ANSI X.9.84:** creado en 2001, por la ANSI (American National Standards Institute) y actualizado en 2003, define las condiciones de los sistemas biométricos para la industria de servicios financieros. (Alvarado, 2010)
- **Estándar ANSI / INCITS 358:** creado en 2002 por ANSI y BioApi Consortium garantiza que los productos y sistemas que cumplen este estándar son interoperables entre sí mediante una interfaz de programación. (Alvarado, 2010)
- **Estándar ISO 19794-2:** fue creado en 2005 por la ISO/IEC con propósitos similares a la norma ANSI 378, respecto a la que guarda mucha similitud. (Alvarado, 2010)
- **Estándar PIV-071006:** establece los criterios de calidad de imagen que deben cumplir los lectores de huellas dactilares para poder ser usados en procesos de verificación de identidad en agencias federales. (Alvarado, 2010).

2.2.3. Sensores biométricos

Entre los sensores biométricos se utiliza el mismo sistema de captación, por ejemplo, para el reconocimiento visual se capta el iris mediante una cámara, mientras que para el reconocimiento de voz se utiliza un micrófono. (BORJA, 2008)

Los más utilizados se detallan a continuación:

- **Sensores Ópticos:** Es uno de los más comunes suele estar formado por cámaras de vídeo de tipo CCD. Este dispositivo consiste de varios miles de píxeles localizados en la superficie de un diminuto CI. Cada píxel se ve afectado con la luz que incide sobre él almacenando una carga de electricidad.

  Los píxeles se encuentran distribuidos en forma de malla con registros de transferencia verticales y horizontales que trasladan las señales a los circuitos de procesamiento de la cámara (convertidor analógico-digital y circuitos adicionales). La transferencia de señales se realiza 6 veces por segundo. (BORJA, 2008)

- **Sensores Termoeléctricos**: Utiliza un sistema único para reproducir el dedo completo "arrastrándolo" a mediante del sensor. Durante el movimiento se realizan tomas sucesivas y se pone en marcha un software especial que reconstruye la imagen del dedo.

  El sensor captura la temperatura diferencial entre las crestas papilares y el aire retenido en los surcos, este método brinda una imagen de buena calidad. (BORJA, 2008)

- **Sensores de campo eléctrico:** Mediante una antena mide el campo eléctrico existente entre dos capas conductoras como es en la capa subcutánea de la piel generando y detectando campos lineales geométricos, se utiliza un amplificador para medir la señal, los sensores imitan una imagen clara de la huella dactilar de una forma más nítida que con otro tipo de sensores. Una desventaja se puede ver reflejada en la baja resolución de la imagen y el área pequeña la misma. (BORJA, 2008)

- **Sensores sin contacto**: Posee un cristal de precisión óptica de distancia de dos pulgadas de la huella dactilar. Al utilizar este tipo de sensores hay que tener en cuenta que las huellas escaneadas son esféricas por lo que se origina un algoritmo mucho más complejo. (BORJA, 2008)
- **Micrófonos ópticos unidireccionales:** Es comúnmente utilizada en el reconocimiento por voz**,** su funcionamiento se da cuando la luz de un diodo es emitida sobre una membrana reflectora a través de fibra óptica, al momento que las ondas de sonido golpean a la membrana, ésta vibra; cambiando así las tipologías de la luz reflejada. Un foto-detector reconoce la luz reflejada que con la ayuda de una electrónica de procesamiento obtiene una representación precisa de las ondas de sonido. (BORJA, 2008)

2.2.4. Biometría de la huella dactilar

Los patrones dentro de una huella dactilar se pueden clasificar según el arco, lazo y espiral, adicional las líneas de la huella dactilar se cortan bruscamente de una manera única. La probabilidad de que dos individuos posean las mismas huellas dactilares es de 1 en 64.000 millones. (BORJA, 2008)

2.2.5. Sensores de huella dactilar

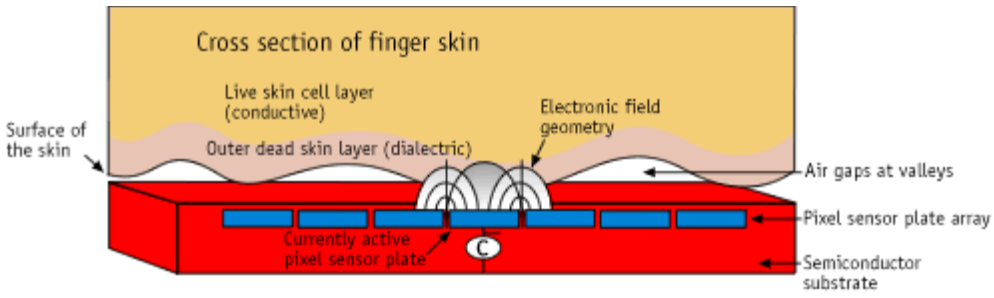
Los sensores de huella dactilar son dispositivos que poseen varias funciones integradas como son la lectura, identificación y almacenamiento de huellas dactilares, todos los procesos se logran mediante el uso de una pieza sensible al tacto que poseen todos los sensores biométricos, el funcionamiento de esta placa marca la diferencia entre los tipos de sensores como lo son:

- **Sensor de matriz capacitivo:** La capacitancia en cada pixel es medida individualmente ya que se deposita en cada pixel una carga fija. La capacitancia del pixel debe der proporcional al voltaje estático que es generado por la carga. Por la forma del dedo, las líneas que definen la huella dactilar se inducen en cada porción de la piel adyacente a esta superficie, como se puede apreciar en la Figura 5.

  La desventaja existente en este diseño es que se puede tener el efecto soplamiento reduciendo la resolución de la imagen por la geometría esférica del campo generado. (Alvarado, 2010)

Figura 5

Sección diagonal de la huella dactilar



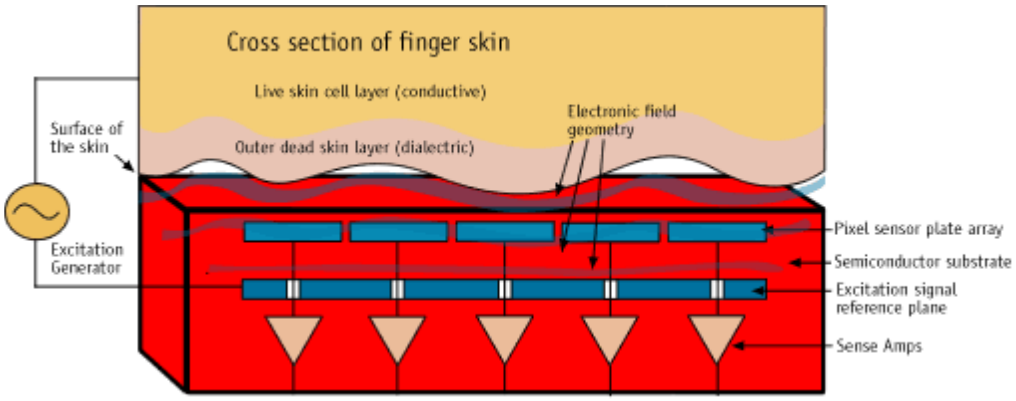
Nota. Recuperado de “Análisis, diseño e implementación de un sistema de inmótica para el edificio administrativo de la facultad técnica para el desarrollo de la universidad católica de Santiago de Guayaquil”, (p. 56), 2010 (Alvarado, 2010)

- **Sensor de matriz de antena**: Mediante un campo RF aplicado entre un chip de silicón y otro ubicado por debajo de la piel del dedo, como muestra la Figura 6, existen sensores que miden el campo que junto con

amplificadores conectados a cada plato convierten estos en voltajes potenciales y así se representa el patrón de huella. En este modelo no se depende de las características geométricas de la superficie. (Alvarado, 2010)

Figura 6

*Modelo sensor matriz a*ntena



Nota. Recuperado de “Análisis, diseño e implementación de un sistema de inmótica para el edificio administrativo de la facultad técnica para el desarrollo de la universidad católica de Santiago de Guayaquil”, (p. 57), 2010 (Alvarado, 2010)

2.2.6. Arquitectura de un sistema biométrico para identificación personal

Existen tres componentes básicos en un dispositivo biométrico que se detallan continuación:

- El primero es el encargado de la adquisición digital o análoga del indicador biométrica del usuario.

- El segundo es encargado de la compresión, procesamiento, almacenamiento y comparación de los datos recibidos con los datos registrados.
- El tercer componente crea una interfaz con aplicaciones en el mismo sistema u otro.

Toda la arquitectura se puede representar conceptualmente como dos módulos:

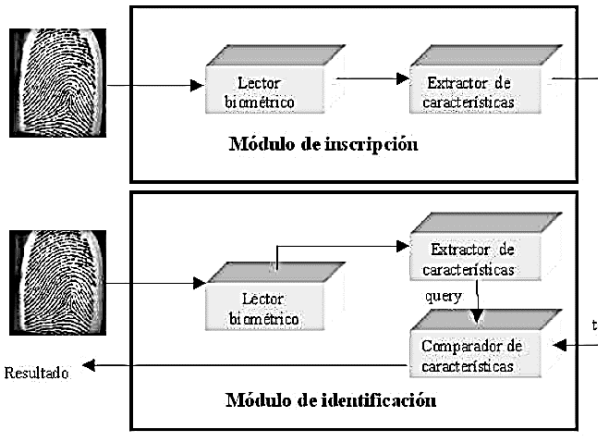
1. Módulo de inscripción
2. Módulo de identificación

En el módulo de inscripción se encuentra el proceso de adquirir y almacenar la información que brinda el indicador biométrico para después comprar con la información registrada anteriormente. Como se puede apreciar en la Figura 7. Los componentes principales del módulo de inscripción son el lector biométrico y el extractor de características. (Alvarado, 2010)

El lector biométrico adquiere los datos relativos y los entrega en un formato digital, mientras que el extractor de características realiza la extracción de características más representativas. Al estar en conjunto se almacena en una base de datos que recibe el nombre de template. (Alvarado, 2010)

Figura 7

Arquitectura de un sistema biométrico



Nota. Recuperado de “Análisis, diseño e implementación de un sistema de inmótica para el edificio administrativo de la facultad técnica para el desarrollo de la universidad católica de Santiago de Guayaquil”, (p. 51), 2010 (Alvarado, 2010)

2.2.7. Carácteristicas de las cerraduras biométricas

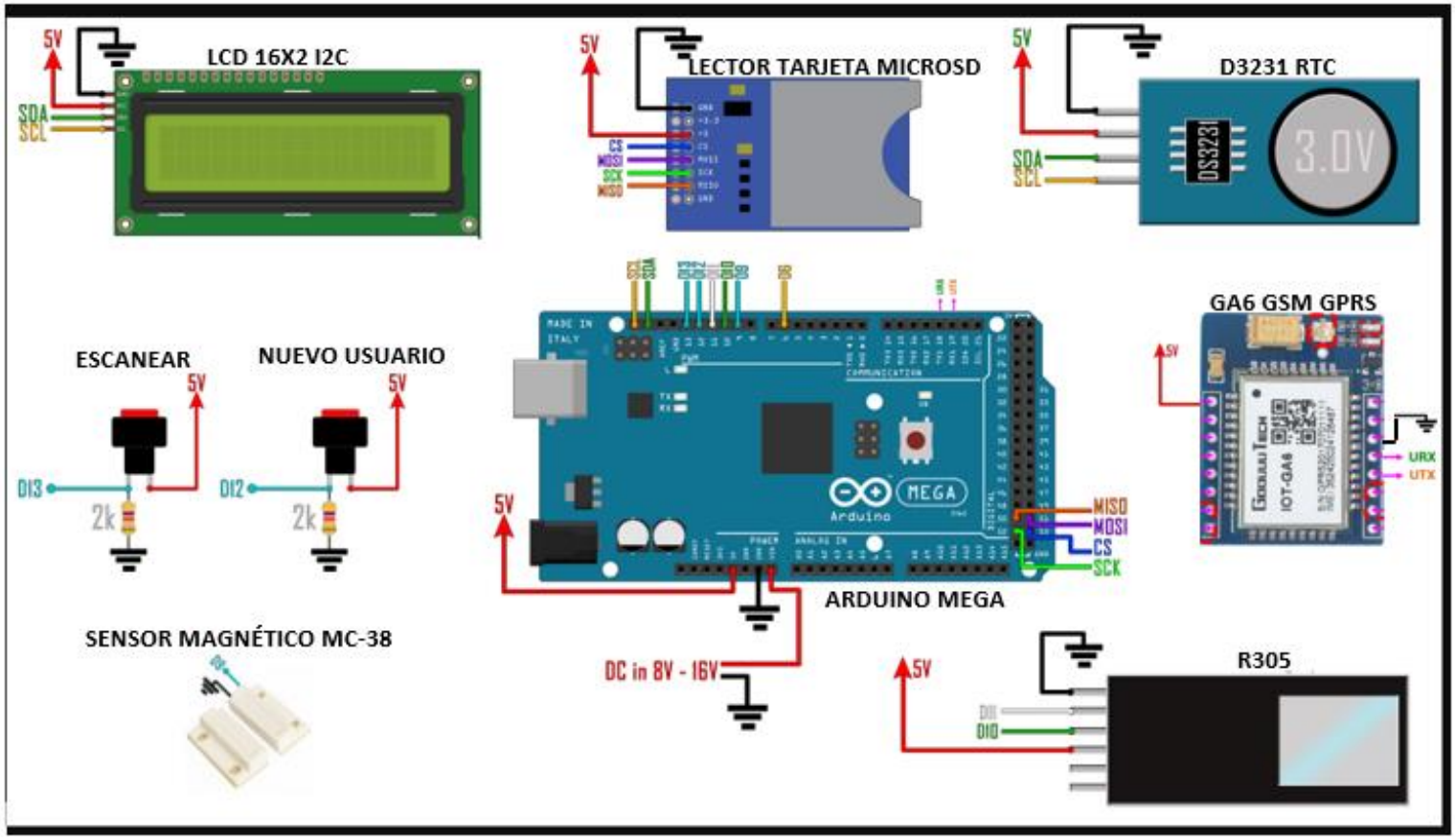
- Modo de apertura: mediante la hulla digital, escaneo de un rasgo físico como retina o comando de voz.
- Fácil ubicación
- Almacena más de 99 usuarios con un Master
- Alimentación de 12 V
- Didáctico con usuarios

3. Desarrollo

El presente proyecto se implementó en la puerta frontal de un domicilio privado, el cual cuenta con un sensor de huella dactilar R305 ubicado a 1.2m del suelo, conectado una placa de desarrollo Arduino mega donde mediante código de programación se compara la huella dactilar adquirida por el sensor R305 con la base de datos activando el pin 8 de salida del arduino, el mismo que envía una señal para que entre en funcionamiento la cerradura eléctrica Travex, al mismo tiempo se registra en una memoria MicroSD mediante el módulo de interfaz conectada a arduino los datos de ingreso, como son la huella dactilar que activo la cerradura, los datos de hora y fecha proporcionados por el módulo D3231. Mediante el sensor magnético MC-38 se controla que cuando la puerta se encuentre abierta no se pueda realizar el ingreso de huellas para la reapertura. En caso de exceder los tres intentos seguidos erróneos de ingreso al domicilio se envía una alerta al usuario principal, mediante el módulo GA6 GSM GPRS que nos proporciona la opción de enviar mensajes de texto. Para la activación del lector de huella digital R305 y para agregar a un nuevo usuario se realiza siguiendo las instrucciones reflejadas en el LCD 16X2 I2C. El esquema se puede apreciar en la Figura 8 para realizar una cerradura biométrica.

Figura 8

Esquemático general



Nota. Diagrama para la conexión de los módulos con el Arduino mega

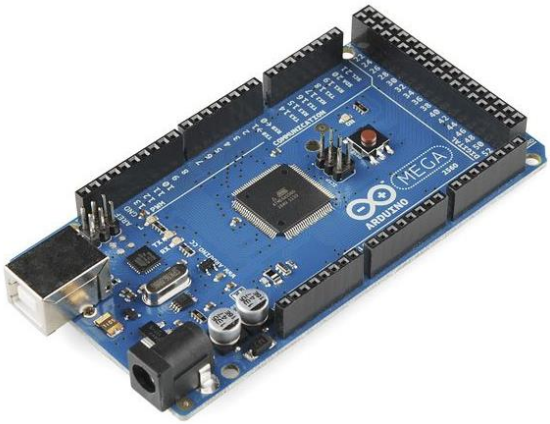
3.1. Componentes físicos

3.1.1. Arduino Mega

En el presente proyecto se utiliza un arduino mega es utilizado por ser una placa con mayor capacidad de memoria, como se muestra en la Tabla 1 y por ser compatible con la mayoría de placas de expansión (shields), la cantidad de puertos que posee es mayor comparado con otras placas de arduino, como se ve en la Figura 9 y la Figura 10. Para más información referirse al Anexo A.

Figura 9

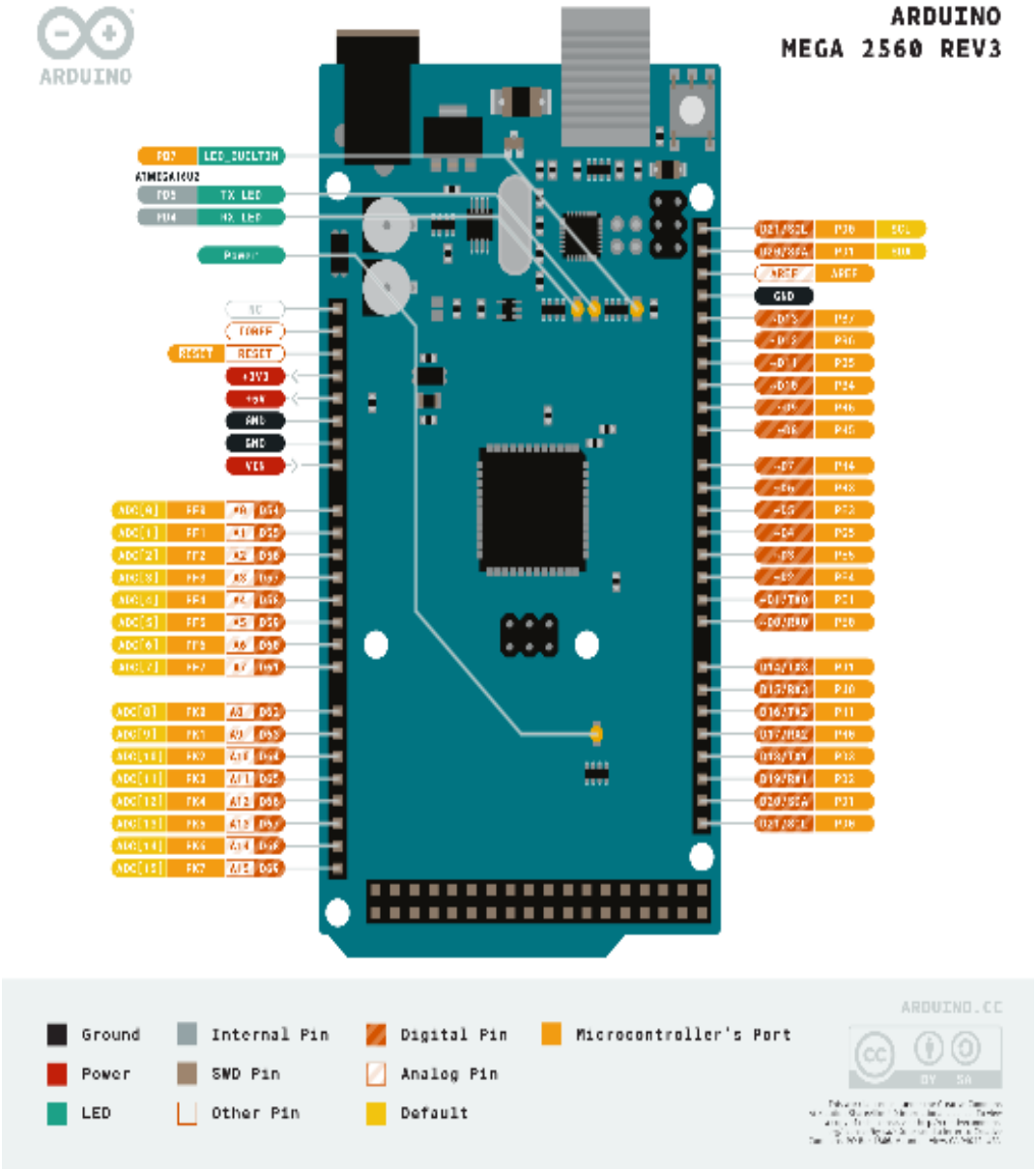
Arduino Mega



Nota. El número de puertos que posee el arduino mega es de 52.

Figura 10

Pin out Arduino Mega



Nota. Recuperado de Arduino mega, (Página Oficial de Arduino, 2020).

Tabla 1

Características de Arduino Mega

Características	Arduino Mega	Arduino Nano	Arduino Uno
Microcontrolador:	ATmega2560.	ATmega328	ATmega328
Tensión de Funcionamiento:	5V.	5V	5V.
Memoria flash.	256Kb – 8Kb usados en el gestor de arranque.	32Kb-2Kb usados en el gestor de arranque	32Kb-0.5Kb usados en el gestor de arranque.
SRAM.	8Kb.	2Kb	2Kb
Reloj.	16Mhz.	16Mhz	16Mhz
Entradas Analógicas.	16.	8.	6.
EEPROM.	4 Kb.	1Kb	1Kb
Corriente por pines de E/S.	40 mA.	40mA	40mA
Voltaje de entrada .	7-12V.	7-12V	7-12V.
Pines digitales de E/S.	54.	22	14
Salidas PWM.	15.	6	6

Nota. Recuperado de Especificaciones Técnicas del Arduino, (Página Oficial de Arduino, 2020)

3.1.2. Sensor de huella biomético R305

Utiliza un DSP para realizar el procesamiento digital de imágenes interno, incluye la capacidad de comparación en una base de datos. Para más información referirse al Anexo B. Una característica especial que posee el dispositivo es su capacidad de almacenar 162 huellas dactilares en su memoria Flash interna a pesar de su tamaño compacto, como se puede observar en la Figura 11

Figura 11

Sensor R305

Nota. Recuperado de ElectroStore 2019. (Electrostore, 2019)

3.1.3. Módulo de interfaz tarjeta MicroSD

Este módulo permite la conexión a un microcontrolador para el almacenamiento de datos de ingreso como son la hora y el usuario. El uso de este módulo es únicamente con tarjetas MicroSD por su singular tamaño, como se aprecia en la Figura 12. Para más información referirse al Anexo C.

Figura 12

Módulo MicroSD

Nota. En el módulo ingresa únicamente con el tamaño de tarjetas MicroSD, sin importar la capacidad de almacenamiento.

3.1.4. Módulo D3231 RTC

Posee un oscilador de cristal con compensación de temperatura, lo que permite ser un reloj entiempo real de alta precisión que refleja el registro de año, mes, día, hora, minutos y segundos. Para más información referirse al Anexo D. El módulo debe ser programado una vez ya que posee una batería de respaldo que le permite seguir con su funcionamiento, como se ve en la Figura 13

Figura 13

Módulo RTC

Nota. Recuperado de Programar Fácil, 2020. (Valle, 2020)

3.1.5. Patalla de cristal líquido I2C

Su conexión con el módulo I2C permite que su ejecución sea más rápida a comparación con otras pantallas LCD, además de ser compatible con cualquier placa de arduino y al ser más sencilla su conexión al utilizar cuatro pines, como se aprecia en la Figura 14, para más información referirse al Anexo E. Es usado en el presente proyecto para reflejar las instrucciones que el usuario debe seguir para la activación de la cerradura eléctrica.

Figura 14

LCD I2C

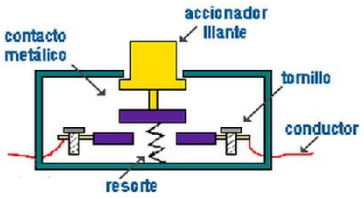
Nota. Recuperado de Programar Fácil, 2020. (Valle, 2020)

3.1.6. Pulsadores

Los pulsadores “NO” tienen la función de activar o desactivar varios comandos como son el registro de nuevas huellas dactilares y de activar la lectura del sensor, como muestra la Tabla 2. Estos dispositivos poseen un contacto que al ser presionado se activa, como se puede observar en la Figura 15

Figura 15

Pulsador “NO”



Nota. Recuperado de Mundo Eléctrico Residencial, 2019 (Castillo, 2019)

Tabla 2

Funcionamiento de pulsadores

Pulsador	Detalles
Pulsador A	Activa la lectura del sensor de huella dactilar.
Pulsador B	Añadir nuevo Usuario

Nota. Los pulsadores se encontrarán con acceso al usuario

3.1.7. Cerradura eléctrica

En la Figura 16 se aprecia la cerradura eléctrica Travex posee varias características como se indica en la Tabla 3.

Figura 16

Cerradura Eléctrica

Nota. Recuperado de Travex. (S.A.C, 2020)

Tabla 3

Características de cerradura eléctrica

Característica	Detalles
Tipo de puerta	Exterior e Interiores.
Voltaje	9- 12 V
Tipo de corriente	CA
Potencia	12 Watts
Grosor de placa de acero	1,50mm
Material de puertas	Metálicas o madera

Nota. Información recuperada de Travex. (S.A.C, 2020)

3.1.8. Módulo Iot GA6 Gsm Gprs

Módulo capaz de enviar y recibir mensajes, llamadas de voz e intercambio de datos a través de internet, posee una ranura en la parte posterior para conectar un Micro SIM, adicional tiene pines para conexión de micrófono y auricular, como muestra la Figura 17. Para más información referirse al Anexo F.

En el proyecto es utilizado para enviar al usuario principal una alerta del intento de ingreso al domicilio, al cumplir una condición de tres intentos consecutivos fallidos el módulo enviara un mensaje de texto “Alerta Intento de Ingreso”.

Figura 17

Módulo GA6

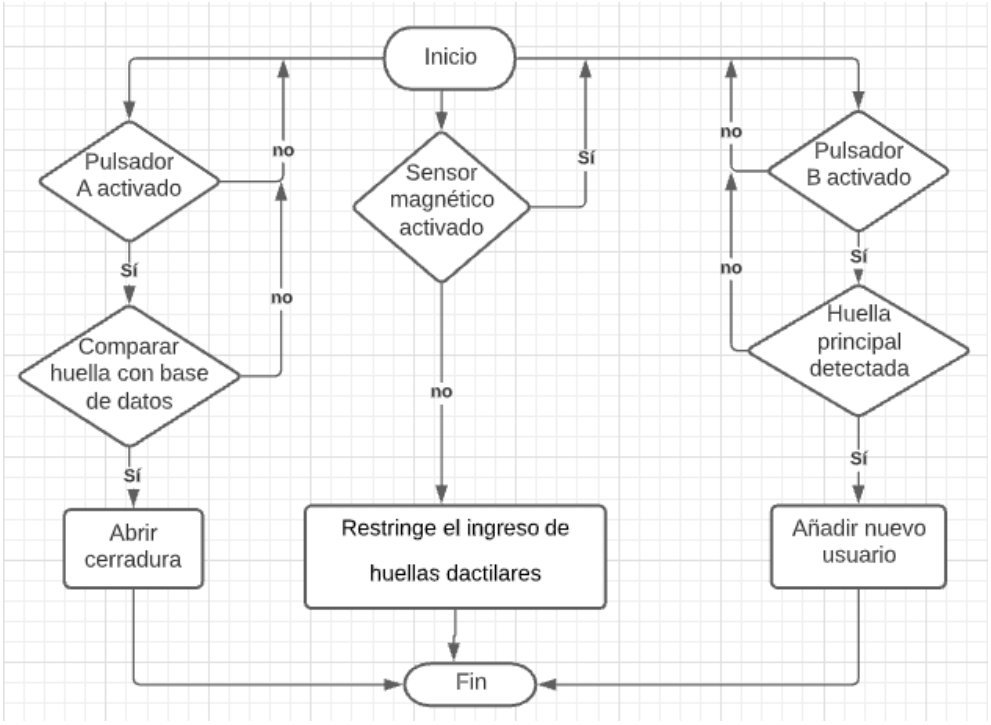
Nota. Se comunica mediante interfaz UART y es compatible con Arduino, Rasperry

3.2. Algoritmo de control

El lenguaje de programación fue código C++, desarrollado en IDE de Arduino. Todo el algoritmo se incluye en el Anexo G y a continuación se explica lo más relevante para el funcionamiento de cada módulo mediante la Figura 18.

Figura 18

Diagrama de flujo



Nota. Al añadir usuario se deberá seguir las instrucciones reflejadas en el LCD 16X2 I2C, como es la asignación de usuario y el registro de huella en la base de datos.

3.3. Librería Adafruit_Fingerprint

En la Figura 19 se muestra las líneas de programación utilizados de la Librería Adafruit_Fingerprint para sensores biométricos. Este código iniciará una vez que el pulsador de escaneo haya sido activado, mediante la función **FINGER.GETIMAGE()** si el sensor de huella dactilar detectó la presencia de una, la comparará con la base de datos existente en la memoria del sensor, en caso de haber coincidencias se mostrara un mensaje de error en el LCD. Mientras que la función **FINGER.IMAGE2TZ** solicita al sensor que convierta la imagen registrada en un modelo de características.

Figura 19

Instrucciones principales de Adafruit_Fingerprint

```
uint8_t getFingerprintID()
{
  uint8_t p = finger.getImage();
  switch (p)
  {
    case FINGERPRINT_OK:
    break;
    case FINGERPRINT_NOFINGER: return p;
    case FINGERPRINT_PACKETRECIEVEERR: return p;
    case FINGERPRINT_IMAGEFAIL: return p;
    default: return p;
  }


  p = finger.image2Tz();
  switch (p)
  {
    case FINGERPRINT_OK: break;
    case FINGERPRINT_IMAGEMESS: return p;
    case FINGERPRINT_PACKETRECIEVEERR: return p;
    case FINGERPRINT_FEATUREFAIL: return p;
    case FINGERPRINT_INVALIDIMAGE: return p;
    default: return p;
  }
```

Nota: Código para escanear y convertir la huella registrada por el sensor.

Para habilitar el registro de un nuevo usuario es importante el escaneo de huella dactilar del usuario principal como se muestra en la Figura 20, ya que sin ella el proceso no se puede completar, a continuación, pide seleccionar el ID de la huella nueva que se podrá guardar hasta 16 usuarios, acto seguido se debe registrar dos veces seguidas la misma huella dactilar.

Figura 20

Instrucción de comparación de usuario principal

```
p = finger.fingerFastSearch();

if (p == FINGERPRINT_OK)
{
  scanning = false;
  counter = 0;
  if(add_new_id)
  {
    if(finger.fingerID == main_user_ID)
    {
      main_user = true;
      id_ad = false;
    }
    else
    {
      add_new_id = false;
      main_user = false;
      id_ad = false;
    }

  }
```

Nota. Código de programación para comparar usuario principal en el registro de nueva huella dactilar.

3.4. Librería DS3231

Para el registro de acceso se utilizan las instrucciones **RTC.GETTIMESTR** y **RTC.GETDATESTR** como se muestra en la Figura 21, de esta forma se consigue obtener los datos precisos de hora y fecha al momento de ingreso o de ingreso fallido de un usuario.

Figura 21

Instrucciones para la adquisición de fecha y hora

```
myFile.print("Door lock system started at ");
myFile.print(rtc.getTimeStr()); myFile.print(" and day ");  myFile.print(rtc.getDateStr());
myFile.println(" ");myFile.println(" ");
myFile.close();
```

Nota. Los datos adquiridos se registran en la MicroSD para el uso de los mismos.

3.5. Estructura

El domicilio donde se realizó la implementación del proyecto está ubicado en Quito- Cdla. Hospitalaria, específicamente en la puerta del acceso frontal cuyas dimensiones son 1.94m de alto y 0.81m de ancho, como se puede apreciar en la Figura 22.

Figura 22

Puerta con cerradura anterior

Nota. La cerradura fue remplazada por una cerradura eléctrica para su correcto funcionamiento.

Por la integridad de los elementos han sido colocados en dos cajas de madera, la primera caja cuenta con dimensiones de 10cm de alto, 10cm de ancho y 10 cm de profundidad, es utilizada para el almacenamiento del sensor dactilar, pulsadores de registro de usuario y lectura de huella, junto con el LCD 16X2 I2C, como muestra la Figura 23. La segunda caja de madera cuyas dimensiones son 20 cm la largo, 10 cm de ancho 12 cm de profundidad, fue utilizada para resguardar los módulos y el arduino de distintos factores externos como es la humedad y la corrosión de los elementos, como se puede visualizar en la Figura 24.

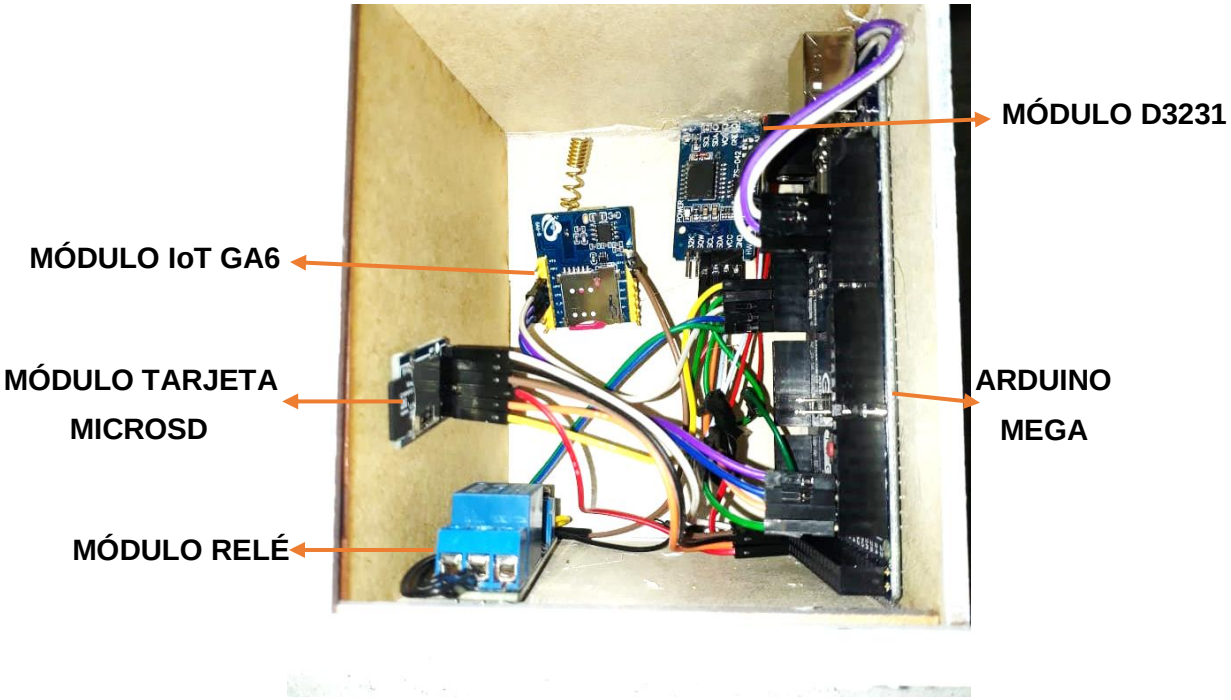
Figura 23

Caja exterior del domicilio

Nota. La caja exterior será ubicada a 1.20m del suelo para su fácil acceso.

Figura 24

Caja interior del domicilio



Nota. Los módulos fueron ubicados en posición estratégica para su correcta conexión.

Por seguridad de los elementos la caja que contiene los módulos y el arduino fue ubicada en la parte interior de la casa a una altura de 2.5m, como se puede apreciar en la Figura 25, para evitar la manipulación constante de la misma.

Figura 25

Ubicación de la caja interior

Nota. La caja interior es ubicada a una altura considerable para evitar la manipulación de niños.

3.6. Pruebas y Resultados

Antes de utilizar el sistema implementado se recomienda verificar las instrucciones proporcionadas en el manual de usuario mostrado en el Anexo I, donde se indica cómo activar el lector de huellas, el registro de un usuario, la lectura del almacenamiento de la MicroSD, cambio de número telefónico para la alerta de mensaje de texto y el número de contacto en caso de existir dudas.

Figura 26

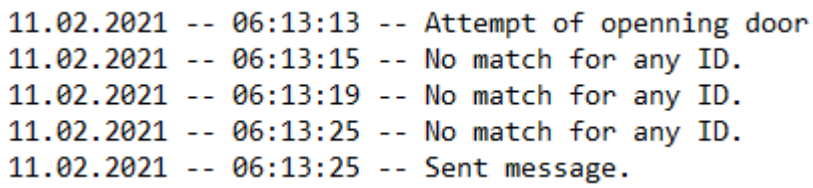
Gráfico de resultados

Nota: El número de accesos en general son 75.

Se realizó pruebas con el sistema funcionando 24 horas diarias durante dos semanas, al iniciar las pruebas se tenía registrados dos usuarios, por lo que al agregar dos más, se tuvieron cuatro usuarios autorizados en total. El reporte generado por el sistema en este lapso de tiempo contiene; el intento de ingreso de usuarios registrados, así como no registrados. Al analizar el listado de novedades del reporte se contabilizó: un total de 45 accesos correctos, 30 intentos inválidos, dando como resultado 7 alertas de mensajes de texto como se muestra en la Figura 26. Nueve de los accesos incorrectos no generaron alerta de mensaje de texto, se asume que es por mala ubicación de la huella o por utilizar un dedo incorrecto; ya que seguido del intento fallido se registra un acceso exitoso. Como muestra en la Figura 27. En caso de requerir el documento completo de eventos, generado por el sistema referirse al Anexo H.

Figura 27

Ingreso del usuario principal



Nota. El mensaje es en enviado pasado los 3 intentos fallidos.

4. Conclusiones y Recomendaciones

4.1. Conclusiones

- Bajo la búsqueda de información relevante y disponibilidad en el mercado nacional se seleccionó los siguientes módulos para el sistema de seguridad residencial: Sensor de huella digital R305, módulo D3231, módulo lector de tarjeta MicroSD, módulo GA6.
- El código fuente que está cargado el sistema embebido utiliza la función FINGER.GETIMAGE() que permite realizar una lectura de la huella dactilar, y mediante el comando FINGER.IMAGE2TZ la extracción de características y comparación de la huella dactilar para autenticar el usuario, es decir permitir o prohibir el ingreso al domicilio a través de la cerradura eléctrica.
- En el domicilio habitan tres usuarios por lo que el uso del módulo R305 es apto, ya que permite el registro de hasta 16 usuarios, de esta forma la necesidad de registro es cubierta completamente. El sistema fue implementado en la puerta de acceso interna por lo que no se encuentra expuesta a condiciones extremas de intemperie.
- Al ser puesto el sistema en pruebas durante dos semanas seguidas se encontró como resultado 45 accesos correcto, se registra 30 accesos incorrectos de los cuales 21 resultaron en 7 alertas de mensajes y los 9 restantes se asume que son por mala ubicación de la huella dactilar, ya que seguido se registra el acceso exitoso.

4.2. Recomendaciones

- Es necesario mantener como opción el uso de llave en la cerradura eléctrica ya que por el corte de suministro eléctrico el sistema de acceso biométrico queda inhabilitado.
- Para un mejor funcionamiento del sistema se debe registrar mínimo dos huellas dactilares por usuario, de modo que pueda acceder, aún si sufrió una laceración o cicatriz en uno de los dos dedos registrados.
- Es de vital importancia verificar la información técnica de los elementos que se utilizan en el desarrollo del proyecto con la finalidad de evitar causar daños en los mismos.

5. Bibliografía

Acebo, M. M. (2018). *Implementacion de acceso inteligente a las oficinas de coordinacion y sala de docentes en la carrera de ingenierias en sistemas computacionales.* Manabí: Facultad de ciencias técnicas. Recuperado el 06 de Enero de 2021

Alvarado, B. E. (2010). *Análisis, diseño e implementación de un sistema de inmótica para el edificio administrativo de la facultad técnica para el desarrollo de la Universidad Católica de Santiago de Guayaquil.* Guayaquil: Facultad de Educación Técnica para el Desarrollo. Recuperado el 06 de Enero de 2021

BORJA, C. T. (8 de Enero de 2008). *dsi.uclm.* Recuperado el 6 de ENERO de 2021, de https://www.google.com/search?sxsrf=ALeKk01NdLh4q_Iv-6pIerQL0oo1h4eDDg%3A1609984234494&ei=6mj2X5nTHdCg5wL_yLqQBA&q=Tipos+de+reconocimiento+biom%C3%A9trico+pdf&oq=Tipos+de+reconocimiento+biom%C3%A9trico+pdf&gs_lcp=CgZwc3ktYWIQAzoECAAQRzoGCAAQFhAeOggIIRAWEB

Cadillo, J. L. (2018). *Modelo de sistema biométrico de interfaz híbrida para cerraduras de seguridad electrónicas.* Arequipa: Facultad de ingeniería de producción y servicios. Recuperado el 06 de Enero de 2021

Castillo, D. (18 de Septiembre de 2019). *Mundo Eléctrico Residencial*. Recuperado el 22 de Enero de 2020, de https://denicastillo2002.blogspot.com/2019/09/pulsadores.html

Cisneros, A. (11 de Noviembre de 2012). *DIARIVM*. Recuperado el 28 de julio de 2020, de Universidad de Salamanca: https://diarium.usal.es/andres_cisneros/author/andres_cisneros/

COSETINO, I. L. (2016). *www.rnds.com.ar.* Recuperado el 6 de ENERO de 2021, de http://www.rnds.com.ar/articulos/045/rnds_152w.pdf

Electrostore. (2019). *Electrostore*. Recuperado el 22 de Enero de 2021, de https://grupoelectrostore.com/shop/placas-para-programacion/raspberry/accesorios-para-raspberry/lector-de-huella-dactilar-biometrico-digital-fingerprint-r305/

Herrador, R. E. (2009). *Guía de Usuario de Arduino.* San Francisco: Creative Commons.

Madrid, H. E. (2018). *Implementación de un sistema de seguridad para el control de acceso mediante una cerradura electrónica – biométrica en la capilla cristo del consuelo del cantón jipijapa.* Manabí: Facultad de ciencias técnicas. Recuperado el 06 de Enero de 2021

Marquez, I. J., Niño, M. J., & Luengas, L. A. (2017). Sistema de control de acceso por biometría. *Visión electrónica*, 25. Recuperado el 28 de NOVIEMBRE de 2020

Página Oficial de Arduino. (30 de Julio de 2020). *Arduino*. Recuperado el 4 de agosto de 2020, de Arduino Nano: https://store.arduino.cc/usa/arduino-nano

Reyes, C. (2008). *Microcontroladores PIC.*

Reyes, C. A. (2008). *Microcontroladores PIC.* Quito: Rispergraf.

Rugarcía, J. R. (2 de Mayo de 2019). Diseño de un prototipo de una cerradura inteligente para las viviendas bajo circunstancias determinadas. *Diseño de un*

prototipo de una cerradura inteligente para las viviendas bajo circunstancias determinadas, 6. Puebla, México: Ingenieria de Macatrónica. Recuperado el 28 de Noviembre de 2020

S.A.C, C. N. (2020). *Travex*. Recuperado el 22 de Enero de 2020

Seguridad, n. (2017). *Ncs seguridad*. Recuperado el 18 de Enero de 2021, de http://ncseguridad.es/hogar/

Serrano, J. F. (2006). Sistema de monitoreo integral para casa habitacion. *Revista digital universitaria*, 19. Recuperado el 28 de NOVIEMBRE de 2020

Valle, L. d. (2020). *Programar Fácil*. Recuperado el 22 de Enero de 2021, de https://programarfacil.com/

ANEXOS