UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIA Y TECNOLOGÍA

ESCUELA DE INGENIERÍA ELECTRÓNICA

Control de acceso de laboratorios de la Escuela de Ingeniería Electrónica utilizando identificación por radiofrecuencia

Trabajo de graduación previo a la obtención del título de:

INGENIERO ELECTRÓNICO

Autores:

JOSE GUSTAVO QUITO MARIN
MILTON RAFAEL VELE ORTIZ

Director:

ING. DANIEL ESTEBAN ITURRALDE PIEDRA Ph.D

CUENCA, ECUADOR

2024

DEDICATORIA

Dedico esta tesis a mi madre Judith Marín y a mi abuela Rosa Peñaranda, pilares inquebrantables de mi vida académica y profesional. En cada momento, tanto en los triunfos como en las adversidades, ellas estuvieron allí, ofreciéndome su apoyo incondicional y sus sabios consejos. Este proyecto no es solo un reflejo de mis esfuerzos, sino también del amor, la dedicación, y la sabiduría que ellas me brindaron. Cada logro en esta etapa lleva su sello, evidenciando su arduo trabajo y su inmensa influencia en mi vida.

En memoria de mi abuelo Enrique Marín y de mis queridos familiares, quienes, con su presencia en mi vida, encendieron e incentivaron la llama interior que alimentó mi valor para seguir adelante. Sus sabios consejos y continuas enseñanzas fueron faros de guía en mi camino.

A mis amigos y a todas las personas que colaboraron para que este logro fuera posible, les agradezco de todo corazón por su inquebrantable apoyo, su constante motivación y por estar siempre presentes. Sus manos extendidas y palabras de aliento en los momentos más desafiantes fueron la fuerza que me impulsó a no rendirme.

Con profunda gratitud, les rindo homenaje a través de estas páginas, testimonio de que su espíritu y su enseñanza perduran en mí.

José Gustavo Quito Marín

DEDICATORIA

Dedico esta tesis a mis queridos padres, Milton Vele y Gloria Ortiz, los verdaderos artífices de este logro. Su amor y apoyo incondicional han sido mi guía constante. A pesar de la distancia que la vida nos impuso, nunca dejaron de demostrarme que el amor de un padre y una madre es la fuerza más poderosa que existe. Cada página de este trabajo refleja su fortaleza y sabiduría, y es gracias a ustedes que hoy celebran este éxito. Les debo no solo cada logro alcanzado, sino también cada paso del camino que me ha llevado hasta aquí. Este proyecto resalta su influencia y amor en mi vida, y les dedico con todo mi corazón este triunfo.

A mis hermanos, Jorge y Renato, amigos y constantes fuentes de inspiración. Este logro es también gracias a su amor, sabiduría y los valiosos consejos que siempre me han brindado. Gracias por estar conmigo en las buenas y en las malas, acompañándome en cada paso de este camino.

A la inolvidable memoria de Victor Ortiz y María E. Astudillo, quienes aunque no están hoy físicamente a mi lado, me vieron crecer y sentaron las bases de la persona que soy. Cada enseñanza y cada momento compartido con ellos ha dejado una huella profunda en mi corazón y en mi espíritu. Su legado perdura en cada desafío que enfrento y en cada sueño que me atrevo a soñar.

Con todo mi amor, les dedico este proyecto que refleja su apoyo y cariño incondicional. Cada paso que doy y cada meta que alcanzo es un tributo a su amor y dedicación. Seguiré luchando y esforzándome por cumplir cada sueño, honrando siempre su inquebrantable fe en mí.

Milton Rafael Vele Ortiz

AGRADECIMIENTOS

Primero y ante todo, queremos expresar nuestra más profunda gratitud a la Universidad del Azuay, por brindarnos la oportunidad y el apoyo necesario para llevar a cabo este proyecto de tesis. Esta experiencia ha sido fundamental en nuestra formación académica y profesional.

Extendemos un sincero agradecimiento a nuestro tutor de tesis, el Ing. Daniel Iturralde, Ph.D., cuya guía, paciencia y apoyo, han sido esenciales para el desarrollo y la culminación de estos trabajos. Su sabiduría y compromiso con la excelencia han sido una fuente de inspiración.

También debemos agradecer a todos nuestros profesores que, a lo largo de nuestra carrera, han compartido su valioso conocimiento y experiencia con nosotros. Cada clase, cada conversación y cada intercambio ha enriquecido profundamente nuestro aprendizaje y nuestra perspectiva.

Por último, pero no menos importante, queremos agradecer a nuestros compañeros de carrera. Juntos hemos compartido retos, éxitos y momentos inolvidables que llevaremos siempre con nosotros. Gracias por ser parte de esta jornada y por todo el apoyo y camaradería que nos han brindado.

CONTROL DE ACCESO DE LABORATORIOS DE LA ESCUELA DE INGENIERÍA ELECTRÓNICA UTILIZANDO IDENTIFICACIÓN POR RADIOFRECUENCIA

Este artículo presenta la implementación de un sistema de control de acceso, en respuesta al creciente problema de inseguridad que afecta al país y que resulta en pérdidas significativas para diversas instituciones. Para ello, se propone desarrollar un sistema de control que permita monitorear el acceso a los laboratorios de la Escuela de Ingeniería Electrónica. El sistema propuesto emplea etiquetas RFID para registrar el acceso, enviando los datos a través de Ethernet hacia un servidor que aloja una base de datos dentro de una red local. Este servidor verifica la accesibilidad de la tarjeta y del usuario, lo que permite controlar y monitorear a los múltiples usuarios que acceden a los laboratorios. Los resultados demuestran que el sistema de acceso propuesto mejora notablemente la seguridad al proporcionar un control más limitado y efectivo sobre el acceso, lo que garantiza una mayor seguridad y eficiencia operativa en los laboratorios.

Palabras clave: RFID,Control de acceso, Ethernet, Base de Datos, Microcontrolador.

ACCESS CONTROL OF LABORATORIES AT THE SCHOOL OF ELECTRONIC ENGINEERING USING RADIO FREQUENCY IDENTIFICATION.

This article presents the implementation of an access control system in response to the growing problem of insecurity affecting the country and resulting in significant losses for several institutions. To this end, it is proposed to develop a control system to monitor access to the laboratories of the School of Electronic Engineering. The proposed system uses RFID tags to record access, sending the data via Ethernet to a server that hosts a database within a local network. This server verifies card and user accessibility, allowing control and monitoring of multiple users accessing the laboratories. The results demonstrate that the proposed access system significantly improves security by providing more limited and effective control over access, ensuring greater security and operational efficiency in the laboratories.

Keywords: RFID, Access Control, Ethernet, Data Base, Microcontroller.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Control de acceso de laboratorios de la Escuela de Ingeniería Electrónica utilizando identificación por radiofrecuencia

14

Jose Gustavo Quito Marín
Ingenieria Electrónica
Universidad del Azuay
Cuenca, Ecuador
josequito@es.uazuay.edu.ec

Milton Rafael Vele Ortiz
Ingenieria Electrónica
Universidad del Azuay
Cuenca, Ecuador
rafaelvele123@es.uazuay.edu.ec

***Resumen*—Este artículo presenta la implementación de un sistema de control de acceso, en respuesta al creciente problema de inseguridad que afecta al país y que resulta en pérdidas significativas para diversas instituciones. Para ello, se propone desarrollar un sistema de control que permita monitorear el acceso a los laboratorios de la Escuela de Ingeniería Electrónica. El sistema propuesto emplea etiquetas RFID para registrar el acceso, enviando los datos a través de Ethernet hacia un servidor que aloja una base de datos dentro de una red local. Este servidor verifica la accesibilidad de la tarjeta y del usuario, lo que permite controlar y monitorear a los múltiples usuarios que acceden a los laboratorios. Los resultados demuestran que el sistema de acceso propuesto mejora notablemente la seguridad al proporcionar un control más limitado y efectivo sobre el acceso, lo que garantiza una mayor seguridad y eficiencia operativa en los laboratorios.**

***Palabras clave*—RFID, Control de Acceso, Ethernet, Base de Datos, Microcontrolador.**

I. Introducción

Actualmente, existe una ola de inseguridad, violencia y vandalismo en el mundo, lo que plantea desafíos en el cuidado y seguridad de todos los sectores. En Latinoamerica, instituciones como empresas y universidades se han visto impactadas de manera directa, considerando que dichas instituciones albergan información valiosa y equipos de alto valor monetario. La pérdida de estos equipos e información representan un alto riesgo en la operatividad de las instituciones. Por lo tanto, es necesario el desarrollo e implementación de sistemas de seguridad que permitan el acceso controlado de las personas a lugares restringidos dentro de las instituciones antes mencionadas.

Según [1], un sistema de control de acceso es un conjunto de medidas y políticas que se utilizan para gestionar y regular quiénes están autorizados a acceder a un sistema, red, edificio, espacio físico u otros recursos específicos. Su objetivo principal es salvaguardar la seguridad de estos recursos y la privacidad al permitir el acceso exclusivamente a personas que cuenten con el permiso adecuado.

Asi también, los autores de [2], determinaron que el 60% de las empresas utilizan tarjetas de identificación con fines de control de acceso. Sin embargo, las tecnologías avanzadas están ganando terreno: el 32% utiliza identificaciones móviles, el 30% utiliza identificación biométrica y el 25% utiliza reconocimiento de patrones. Los sistemas de control de acceso físico pueden ser de gran ayuda para reducir el riesgo de violaciones de seguridad tanto internas como externas. Este informe global ha señalado que los incidentes relacionados con amenazas internas han aumentado en un 44% en los últimos dos años, con un coste promedio de 15 millones de dólares por cada incidente. En respuesta a esta creciente preocupación, el uso de tecnologías para el control de acceso físico ha experimentado un incremento significativo. En la mayoría de los casos, estos delitos son perpetrados por actores externos que realizan entradas forzadas, robos, actos de vandalismo o acceden de manera no autorizada a las instalaciones, eludiendo la lista de visitantes aprobados. Además, en ocasiones, los propios empleados pueden involucrarse en tales incidentes de forma inadvertida, como dejar puertas abiertas o ingresar accidentalmente a un edificio sin autorización.

Actualmente, la sociedad enfrenta un desafiante problema de seguridad que ha impactado significativamente a las instituciones académicas de nivel superior. Varias instituciones han sufrido pérdidas financieras considerables debido a los daños en su infraestructura. Específicamente, los laboratorios, que albergan equipos de alto valor esenciales para la investigación y el aprendizaje de la comunidad universitaria, se han convertido en un objetivo destacado para actividades delictivas [3].

Las instituciones educativas, a pesar de contar con un sistema de seguridad y el uso de llaves mecánicas, resultan un evidente problema de seguridad con limitaciones que requieren atención inmediata y efectiva. Por lo tanto, es importante abordar estas deficiencias con el fin de garantizar la integridad de los recursos y equipos de laboratorio, así

como de crear un entorno de aprendizaje seguro y propicio para los estudiantes. Esto se puede lograr mediante el desarrollo de una revisión a fondo del sistema de seguridad existente y la propuesta de su modernización, implementando tecnologías avanzadas y soluciones innovadoras que aseguren una protección más eficaz y eficiente.

Entre las soluciones que existen hoy en dia en el ámbito de este proyecto de investigación se tiene a los autores de [4], quienes presentaron un sistema de acceso inteligente basado en RFID (Radio Frequency Identification) a través del cual se puede observar de manera simplificada el rendimiento operativo, lo que resultó en una mayor eficiencia en la administración de múltiples ubicaciones y un aumento en la seguridad. Además, la implementación de sistemas multifuncionales se ha convertido en una estrategia eficaz para garantizar niveles más altos de seguridad en organizaciones públicas y privadas.

En el trabajo de [5], se propuso un sistema de control de acceso multifuncional que combina reconocimiento facial mediante PCA (Principal Component Analysis) y LDA (Linear Discriminant Analysis), tecnología RFID y un algoritmo de árbol binario dinámico para prevenir colisiones. En comparación con los sistemas tradicionales, este enfoque se destaca por su simplicidad de operación y mayor seguridad.

Por otro lado, [6] desarrollaron un sistema multifuncional que fusiona el uso de tarjetas RFID con el reconocimiento facial para el control de acceso. Su investigación concluyó que este sistema satisface los estándares de seguridad establecidos, pero con la condición de que las tarjetas RFID se ubiquen a una distancia no menor a 14 centímetros entre sí. Estos resultados respaldan y justifican la preferencia por sistemas de acceso multifuncionales para garantizar la autenticación en diversos entornos.

Adicionalmente, es relevante destacar la contribución de [7], quienes presentaron un enfoque basado en fases para clasificar etiquetas RFID UHF (Ultra High Frequency) en un sistema de control de acceso de puertas. Este método se vale de una única antena lectora y múltiples lecturas de fase capturadas durante el movimiento de las etiquetas. En pruebas realizadas en un entorno real, este método demostró su capacidad para distinguir las acciones de las etiquetas (entradas, salidas y paso) a distintas velocidades, logrando una precisión global del 97% en varios escenarios de estudio.

En [8], proponen un sistema de gestión de registros basado en tecnología RFID y Arduino, ofreciendo una solución eficiente para recopilar datos relacionados con diversos tipos de productos. Este sistema permite monitorear información como la fecha de recepción, el conteo de inventario y la gestión efectiva del almacenamiento. La utilización de la comunicación RFID posibilita la administración simultánea de múltiples puntos de datos en tiempo real, lo que contribuye a una mayor eficiencia en la gestión de activos.

Además, en [9] destacan en su artículo varias vulnerabilidades que resaltan la necesidad de una autenticación segura en varios servicios, con el fin de mejorar los sistemas y reducir el riesgo de fraudes. Su investigación revela que, mediante el uso de hardware comercial económico y software de código abierto, los sistemas de seguridad basados en RFID pueden presentar diversas vulnerabilidades que deben ser mitigadas durante su implementación para lograr un nivel óptimo de seguridad.

En varios estudios recientes, se han propuesto soluciones innovadoras para el control de acceso y la seguridad en diferentes entornos. En [10], desarrollaron un sistema que utiliza un microcontrolador Arduino y tecnología RFID para automatizar la seguridad en el registro de asistencia, con el objetivo de prevenir el acceso no autorizado a las instalaciones. El sistema diseñado se distingue por su gestión automatizada mediante el uso de Oxygen.3a, lo que posibilita mantener un registro preciso de la asistencia en una base de datos. Esto resulta fundamental para que los instructores puedan mantener una lista adecuada de los estudiantes.

En su revisión literaria, [11] presentaron un sistema de control de acceso que combina el reconocimiento facial y la tecnología RFID, destacando la alta efectividad de RFID con una eficacia del 100% y un tiempo de respuesta de 0,03 segundos en comparación con el reconocimiento facial.

En [12], se enfocaron en el control de acceso mediante una tarjeta RFID y un módulo lector, especialmente en entornos corporativos y de oficina, contribuyendo al avance en la seguridad y la gestión de ingresos a áreas sensibles. El estudio realizado revela una eficacia notable en la restricción de acceso mediante el uso de una tarjeta llave con identificación única. Esto posibilita un seguimiento exhaustivo de los accesos, permitiendo la observación de datos tales como los usuarios y los eventos registrados en dicho entorno.

En [13], propusieron un sistema flexible basado en RFID para el control de acceso, con capacidad de modificar datos según las necesidades de los usuarios y alertas por SMS (Short Message Service) en caso de intrusión, aplicable en corporaciones y empresas. El rendimiento de este sistema muestra un registro de datos autenticado y eficaz para periodos de larga duracion. Con el sistema embebido mencionado, se facilita la realización de un seguimiento de múltiples datos, incluyendo la tarjeta de usuario, el nombre de usuario y la hora de llegada. Esto, a su vez, contribuye a la creación de un sistema de seguridad más eficiente.

En [14], se visualiza un sistema de control de acceso RFID para salas de examen, destacando su eficiencia y reducción de infracciones de seguridad en comparación con otros métodos. También consideraron la posibilidad de mejorar el sistema

mediante biometría, a pesar de los posibles costos adicionales. Estos estudios representan avances significativos en la gestión de seguridad y control de acceso en diversos contextos.

El estudio realizado por [15], en la provincia de Manabí, Ecuador, se enfocó en llevar a cabo un análisis de sistemas y tecnología de identificación mediante el uso del protocolo de comunicación RFID. El objetivo principal de esta investigación fue mejorar el control de acceso y salida de equipos electrónicos con el propósito de prevenir el robo de estos dispositivos. Como resultado, se logró un aumento significativo en los niveles de seguridad, junto con la provisión de un servicio de mayor calidad.

En este proyecto, se diseña e implementa un sistema de control de acceso para los laboratorios de Ingeniería Electrónica de la Universidad del Azuay. Al proporcionar una solución específica a las necesidades y realidades de una institución académica, esta investigación aporta significativamente al campo de la seguridad en entornos educativos. La integración de tecnologías innovadoras y accesibles, así como la consideración de los desafíos únicos asociados con la gestión de acceso en un entorno universitario, son lo que distingue nuestro trabajo. Además, nuestro método considera no solo la eficacia y la seguridad de la operación, sino también la facilidad de uso y la accesibilidad, lo que nos permite ofrecer una solución completa e integral a las necesidades de control de acceso en este ámbito.

En la sección II se presenta la descripción del sistema y la metodología a usar. La sección III muestra los resultados encontrados y por último en la sección IV se detallan las conclusiones obtenidas.

II. Descripción del sistema

En el presente proyecto, se diseña e implementa un sistema de control de acceso a los laboratorios de la Escuela de Ingeniería Electrónica, considerando criterios de eficiencia y seguridad. Según se muestra en la Fig. 1, el sistema se organiza en tres secciones. La sección A, denominada "RFID", se centra en el hardware que procesa la información de las tarjetas de identificación y, a través de una conexión Ethernet, transmite los datos a una base de datos la cuál determina si se otorga o se niega el acceso. La sección B, denominada "Diseño de red" explica la manera en que los dispositivos se interconectan con un servidor principal mediante un switch. Finalmente, la sección C denominada "Servidor" cuenta con una interfaz a través de la cual es posible consultar la información de los usuarios, agregar nuevos usuarios, eliminar usuarios existentes y monitorear el acceso a los distintos laboratorios.

A. RFID

En esta sección, se desarrolló el diseño que se observa en la Fig.2, integrando un microcontrolador que se conecta

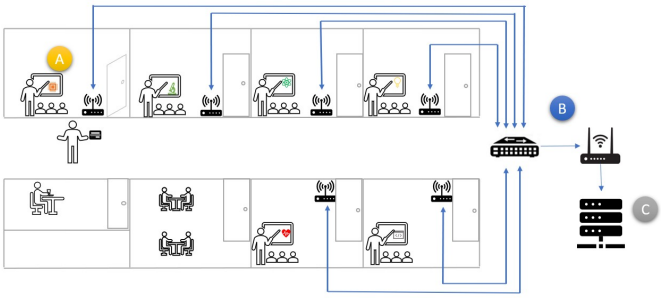


Fig. 1. Diagrama de Bloques del Sistema.

con el lector RFID. Estos lectores recogen la información de las tarjetas de cada usuario y, al capturarla, la combinan con el identificador del laboratorio en un arreglo de caracteres. Luego, esta información se envía mediante un SHIELD ETHERNET configurado con direcciones IP y MAC únicas hacia una base de datos en una Raspberry Pi. La base de datos lleva a cabo la autenticación, evaluando si se concede o no el acceso. Cuando se recibe una confirmación positiva del servidor, que verifica la correspondencia entre usuario, tarjeta RFID y laboratorio, se ilumina un LED verde indicando autorización y, al mismo tiempo, se activa un módulo MOSFET, que gestiona la apertura de una cerradura electromagnética durante un tiempo definido, facilitando el ingreso antes de volver a cerrarse. En cambio, si la respuesta es negativa, la cerradura se mantiene cerrada, impidiendo el acceso del usuario.

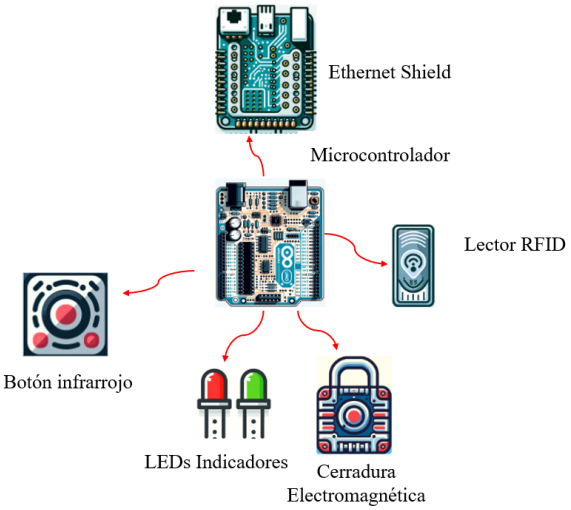


Fig. 2. Diagrama de Bloques de la Sección RFID.

En los Anexos, se presenta el esquema del circuito implementado en la sección RFID. Tanto los módulos Ethernet como RFID están conectados mediante comunicación SPI, mientras que los LEDs indicadores, el módulo MOSFET y el botón infrarrojo utilizan señales digitales para su activación.

Para programar los microcontroladores, es necesario asignarles una dirección IP (por sus siglas en ingles "Internet Protocol") y una dirección MAC únicas para identificarlos en

la red. Además, se debe configurar la dirección IP del servidor con el que se comunicarán. El siguiente paso implica obtener el código de la tarjeta RFID y enviarlo junto con el número de laboratorio asignado para ese microcontrolador. Una vez enviado, el microcontrolador espera una respuesta del servidor, la cual puede ser ”True” o ”False”. Dependiendo de esta respuesta, el microcontrolador ejecutará una acción específica. Si la respuesta es ”True”, el microcontrolador activará el LED verde y enviará una señal al módulo MOSFET para desactivar la cerradura, permitiendo así el acceso al usuario. Por otro lado, si la respuesta es ”False”, el microcontrolador activará el LED rojo y mantendrá la cerradura bloqueada, denegando el acceso al usuario. A continuación, en la Fig. 3 , presenta el diagrama de flujo utilizado para la seccion RFID detallando los pasos fundamentales para el funcionamiento del sistema descrito.

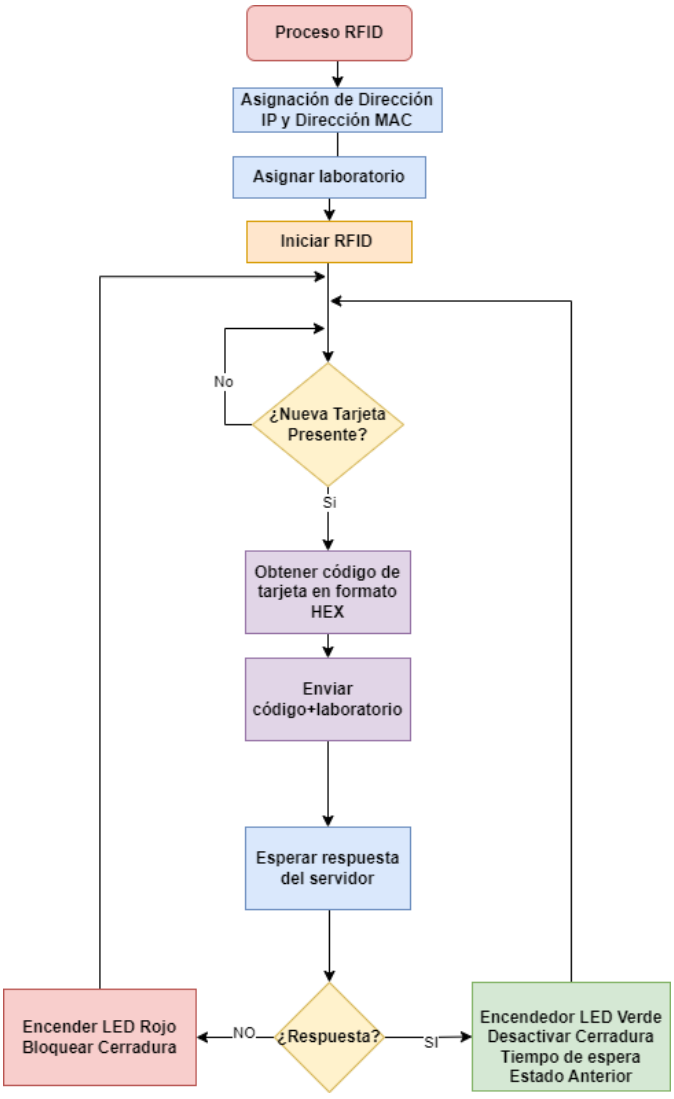


Fig. 3. Diagrama de Flujo RFID.

B. Diseño de red

Se ha seleccionado una topología de red en estrella para el sistema de control de acceso, como se ilustra en la Fig. 4. La red desplegada incluye 6 microcontroladores que están interconectados con el servidor a través de un switch. Esta configuración facilita la comunicación entre los distintos microcontroladores y el servidor dentro de la red local con la dirección 192.168.1.0/24.

La red implementada facilita la comunicación punto a multipunto cuando los microcontroladores envían su información al servidor. Esto es esencial para permitir consultas en tiempo real a la base de datos alojada en el servidor, lo que garantiza la verificación de las credenciales de acceso de manera eficiente y oportuna.

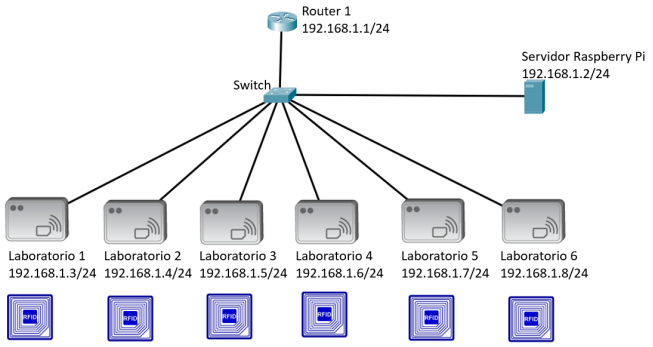


Fig. 4. Topología de la red

En la Tabla I se presenta un ejemplo de la asignación de direcciones de la red, donde se detalla las direcciones IP asignadas a cada dispositivo dentro del sistema de control de acceso. Esta tabla es fundamental para garantizar la correcta configuración y funcionamiento de la red, permitiendo así una comunicación efectiva entre los microcontroladores y el servidor.

TABLA I
TABLA DE ASIGNACIÓN DE DIRECCIONES

Dispositivo	Interfaz	Dirección Ip/Máscara de Subred	Gateway
R1	eth1	192.168.1.1/24	— —-
Servidor	NIC	192.168.1.2/24	192.168.1.1
Lab 1	NIC	192.168.1.3/24	192.168.1.1
Lab 2	NIC	192.168.1.4/24	192.168.1.1
Lab 3	NIC	192.168.1.5/24	192.168.1.1
Lab 4	NIC	192.168.1.6/24	192.168.1.1
Lab 5	NIC	192.168.1.7/24	192.168.1.1
Lab 6	NIC	192.168.1.8/24	192.168.1.1

C. Servidor

En la última sección del sistema, se centra en la comunicación entre el servidor y los diferentes microcontroladores. Para este propósito, el microcontrolador envía un arreglo

que contiene el identificador de la tarjeta y el número del laboratorio. Esta información es recibida por el servidor, el cual procede a verificarla contra una tabla específicamente designada para tal comparación. Si la información enviada por el microcontrolador coincide con la almacenada en dicha tabla, el servidor entonces registra los datos en otra tabla. Esta última incluye la información del usuario, su identificador, el laboratorio al que accedió, la fecha y hora exacta del acceso. Tras el registro exitoso de los datos, el servidor envía una respuesta específica siendo esta "True" o "False". En la Fig.5 se ilustra el diagrama de flujo utilizado para el proceso del servidor.

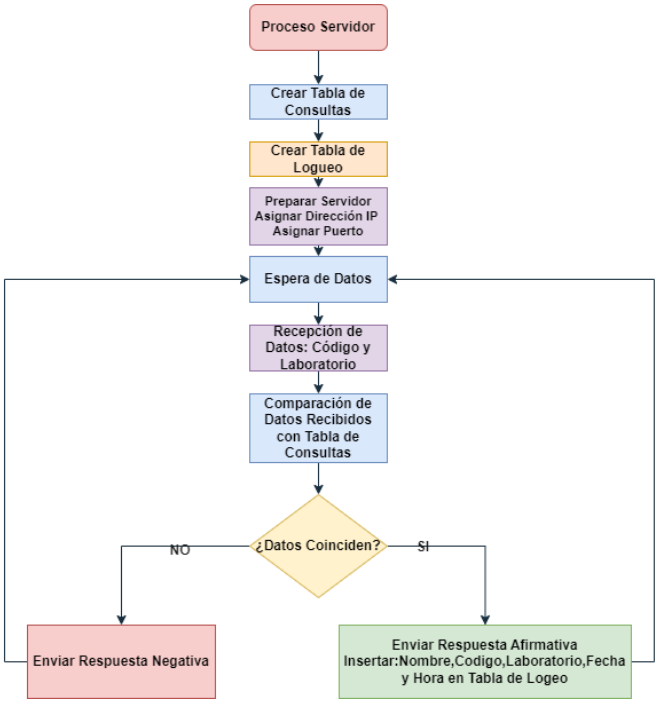


Fig. 5. Diagrama de Flujo Servidor.

Para el monitoreo del servidor, se diseñó una interfaz de usuario gráfica que facilita el control en tiempo real de los distintos laboratorios. Esta interfaz incluye varias pestañas, cada una con funciones específicas destinadas a la gestión del control de acceso.

III. Resultados

Después de concluir la sección II, se llevaron a cabo pruebas específicas para cada componente del sistema con el fin de verificar su correcto funcionamiento en las etapas previamente descritas. Estas pruebas incluyeron la evaluación del funcionamiento de los microcontroladores encargados de adquirir los códigos de las tarjetas RFID, así como su comportamiento en respuesta a las señales recibidas del servidor. En la Figura 6.a se ilustra el comportamiento del microcontrolador al leer el código de la tarjeta y recibir una respuesta positiva. Por otro lado, en la Figura 6.b se muestra el comportamiento del microcontrolador al leer el código de la tarjeta y recibir una respuesta negativa.

```
09:45:35.540 -> Cliente Ethernet y RFID iniciado
09:45:35.577 -> 10.10.234.12
09:45:45.720 -> Datos enviados:  ,2347E305,3
09:45:46.198 -> Respuesta recibida: 'True'    a)
09:45:46.198 -> Acceso Permitido
09:45:46.230 -> Led verde Encendida
09:45:46.270 -> Cerradura Abierta
```

```
09:47:03.597 -> Datos enviados:  ,DC671349,3
09:47:04.112 -> Respuesta recibida: 'False'
09:47:04.112 -> Acceso Denegado
09:47:04.112 -> Led rojo Encendida          b)
09:47:04.149 -> Cerradura Bloqueada
```

Fig. 6. a) Proceso de envío de datos y respuesta positiva procesada por el microcontrolador. b) Proceso de envío de datos y respuesta negativa procesada por el microcontrolador

Después de completar las pruebas relacionadas con la topología de la red, se llevaron a cabo evaluaciones de conectividad entre el servidor y los módulos Ethernet destinados a operar en los diversos laboratorios. La Fig. 7 permite visualizar la conectividad entre los múltiples microcontroladores y el servidor, los cuales se encuentran en la red local.

```
pi@raspberrypi:~ $ arp -a
? (10.10.234.7) at ac:ae:ab:ef:da:dd [ether] on eth0
? (10.10.234.3) at ce:de:fe:ef:fe:ef [ether] on eth0
? (10.10.234.6) at aa:bb:fe:ef:fe:ef [ether] on eth0
? (10.10.234.5) at bc:de:fe:ef:fe:ef [ether] on eth0
? (10.10.234.2) at dc:2c:6e:88:b1:5b [ether] on eth0
? (10.10.234.1) at 00:1b:17:00:01:10 [ether] on eth0
? (10.10.234.4) at da:ab:be:ef:fa:ef [ether] on eth0
```

Fig. 7. Dispositivos Conectados en la red local.

Finalmente, en cuanto a la parte del servidor, se efectuaron pruebas enfocadas en la integración de una Interfaz de Usuario Gráfica, organizada en dos pestañas que buscan optimizar el monitoreo del sistema como se observa en la Fig.8.

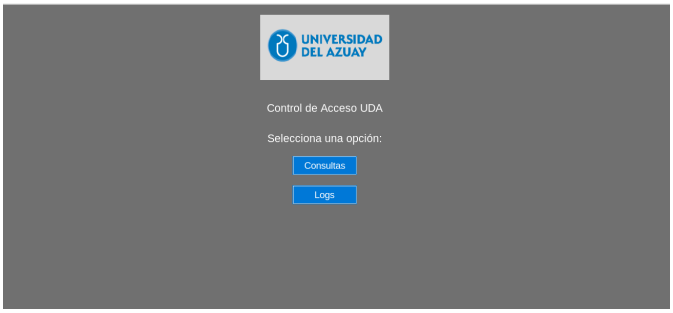


Fig. 8. Interfaz Gráfica de Usuario.

La primera pestaña incluye una tabla de consultas diseñada en SQLite3. Esta tabla facilita a los usuarios la identificación de su nombre, el código de su tarjeta RFID y los laboratorios a los que tienen acceso. Además, esta sección incorpora herramientas que permiten la edición de los datos previamente asignados, así como una función para eliminar

registros. También se dispone de una opción de búsqueda para localizar los datos de los usuarios de manera eficiente. En la Fig.9 se puede observar el contenido de la primera pestaña correspondiente a la interfaz gráfica.

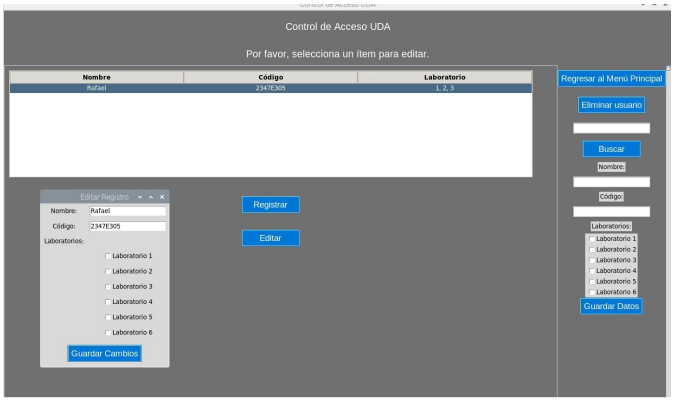


Fig. 9. Página de Consultas de Usuarios.

En cuanto a la segunda pestaña, ésta presenta una tabla que registra los accesos a los distintos laboratorios. Dicha tabla incluye el nombre del usuario, el código de la tarjeta RFID, el laboratorio al que se ingresó, así como la fecha y hora del acceso, facilitando así el seguimiento de las entradas. Adicionalmente, esta pestaña ofrece una funcionalidad para filtrar por fechas, lo que mejora significativamente la visualización y el análisis de los registros en base a un intervalo de tiempo específico. La Fig. 10 muestra un vistazo a esta segunda pestaña de la interfaz gráfica.

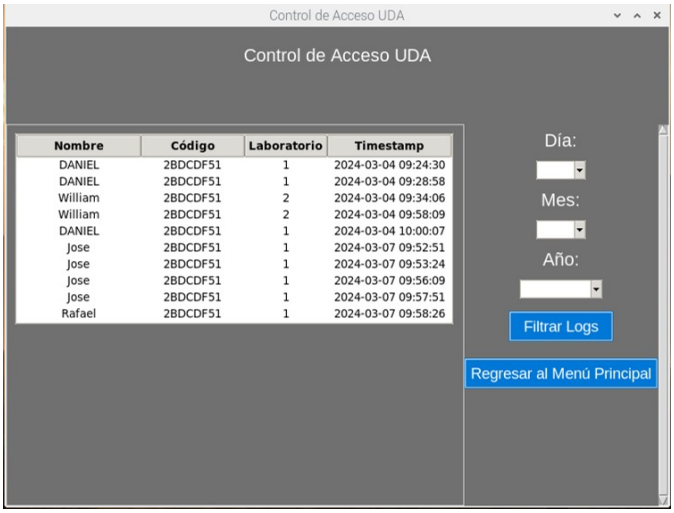


Fig. 10. Página de Ingreso de Usuarios.

Después de implementar el servidor, se llevaron a cabo pruebas de funcionalidad del sistema para verificar la recepción de la información enviada por los microcontroladores. En el primer caso, al recibir la información y verificarla en la sección de consultas, como se observa en la Fig. 6a, se procede a comprobar al usuario con su ID y laboratorio en la página de ”Logueo”, registrando la fecha correspondiente para su monitoreo. Caso contrario, si el usuario no está registrado en el sistema o en el laboratorio específico, el servidor no encontrará ninguna coincidencia, ignorando al usuario y denegando el acceso como se mencionó en la Fig.6b. A continuación, en la Fig.11 se puede observar los resultados impresos por el monitor serial del servidor.

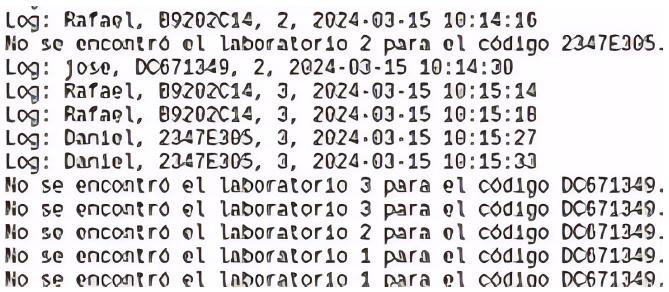


Fig. 11. Respuestas impartidas por el Servidor.

IV. Conclusiones

El presente proyecto se orientó hacia la implementación de un sistema de control de acceso con el propósito primordial de mejorar la seguridad en los laboratorios de la Escuela de Ingeniería Electrónica de la Universidad del Azuay. Tras concluir las pruebas del sistema de control, se obtuvieron las siguientes conclusiones.

La adquisición de datos del módulo RFID se llevó a cabo con éxito, al igual que la transmisión de datos a través de Ethernet, sin experimentar pérdida alguna de información. Este resultado satisfactorio se atribuye al uso del protocolo TCP, conocido por su capacidad para asegurar una transmisión fiable de datos y prevenir contratiempos en las etapas posteriores del sistema. Como consecuencia, el procesamiento de las respuestas por parte del servidor se realizó de manera apropiada, lo que contribuye significativamente a la mejora de la seguridad en los laboratorios.

La infraestructura de red implementada en el sistema proporciona un alto nivel de seguridad gracias al empleo de dispositivos Ethernet Shield. Estos dispositivos se adhieren al modelo OSI para garantizar una comunicación segura y confiable, tanto en términos de transmisión como de recepción de información. Además, la arquitectura de la topología de red ha sido diseñada para permitir una escalabilidad óptima, facilitando la adición de más microcontroladores en caso de ser necesario para la expansión del sistema.

El servidor desempeña sus funciones con eficiencia, ejecutando de manera efectiva la interfaz de usuario y estableciendo comunicación con los distintos microcontroladores. La interfaz de usuario ha sido desarrollada con un enfoque en la facilidad de uso, permitiendo que los administradores la utilicen sin enfrentar dificultades significativas. Tanto la funcionalidad de la ventana de consulta como la de inicio de sesión cumplen con sus respectivas funciones, contribuyendo así a fortalecer la seguridad en los múltiples laboratorios.

La interfaz de usuario ofrece una experiencia intuitiva en términos de su manejo, con una disposición clara de los elementos que facilitan la interacción del administrador con el sistema y reduce la probabilidad de errores durante su operación.

La comunicación establecida entre el servidor y los microcontroladores se caracteriza por su robustez, lo que garantiza una transmisión confiable de datos. Esta robustez es esencial para asegurar que los comandos enviados desde la interfaz de usuario lleguen de manera correcta a los dispositivos de control en los laboratorios, y viceversa, lo que permite un control efectivo sobre el acceso a los mismos.

Durante la implementación del proyecto de control de acceso a los laboratorios, se identificó como uno de los principales desafíos la gestión de la alimentación para los microcontroladores. Aunque las especificaciones del microcontrolador indicaban su capacidad para soportar los 12V suministrados a la cerradura, se determinó que el regulador de voltaje del microcontrolador no cumplía con las especificaciones del datasheet. Como solución, se implementó una segunda fuente de alimentación de 5V exclusiva para el microcontrolador y sus componentes, mientras que la alimentación de 12V se destinó a la sección de potencia. Esta estrategia permitió separar eficazmente las necesidades de alimentación y garantizar un suministro estable para cada componente del sistema.

El proyecto presentado se posiciona como un prototipo inicial con miras a servir como base para futuras mejoras del sistema o para una expansión de la red a nivel de facultad o incluso a nivel institucional. Esta fase inicial de desarrollo proporciona una estructura sólida sobre la cual se pueden implementar nuevas características, optimizaciones y escalabilidad, permitiendo así adaptar el sistema a las cambiantes y futuras necesidades de la institución.

REFERENCIAS

[1] TIC Portal, "Control de acceso: ¿cómo actúa dependiendo del tipo de software?" S.f. [Online]. Available: https://www.ticportal.es/glosario-tic/control-acceso

[2] Avigilon; creator, "Physical access control system (pacs): Components + examples," May 2023. [Online]. Available: https://www.avigilon.com/blog/physical-access-control

[3] J. Guambaña, "Utilizando explosivos, antisociales roban cajero automático en la universidad del azuay," *El Universo*, Mar. 2022. [Online]. Available: https://www.eluniverso.com/noticias/ecuador/utilizando-explosivos-antisociales-roban-cajero-automatico-en-la-universidad-del-azuay-nota/

[4] X. Wang and Y. Wang, "An office intelligent access control system based on rfid," in *2018 Chinese Control And Decision Conference (CCDC)*, 2018, pp. 623–626.

[5] H.-W. Lee, "Design of multi-functional access control system," *IEEE Access*, vol. 9, pp. 85 255–85 264, 2021.

[6] J. I. V. Luna, F. J. S. Rangel, G. S. Guzmán, and M. A. L. Acosta, "Sistema de acceso usando una tarjeta rfid y verificación de rostro," *Ingenius: Revista de Ciencia y Tecnología*, vol. 20, pp. 108–118, 2018. [Online]. Available: https://doi.org/10.17163/ings.n20.2018.10

[7] A. Buffi, B. Tellini, A. Motroni, and P. Nepa, "A phase-based method for uhf rfid gate access control," in *2019 IEEE International Conference on RFID Technology and Applications (RFID-TA)*, 2019, pp. 131–135.

[8] R. Challa, B. Reddaiah, and K. G. Srinivasa, "Efficient record management using rfid - arduino technology," *International journal of computer applications*, 2018.

[9] H. Pereira, R. Carreira, P. Pinto, and S. I. Lopes, "Hacking the rfid-based authentication system of a university campus on a budget," in *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 2020, pp. 1–5.

[10] K. Bakht, A. U. Din, A. Shehzadi, and M. Aftab, "Design of an efficient authentication and access control system using rfid," in *2019 3rd International Conference on Energy Conservation and Efficiency (ICECE)*, 2019, pp. 1–4.

[11] B. Wahyudono and D. Ogi, "Implementation of two factor authentication based on rfid and face recognition using lbp algorithm on access control system," in *2020 International Conference on ICT for Smart Society (ICISS)*, 2020, pp. 1–6.

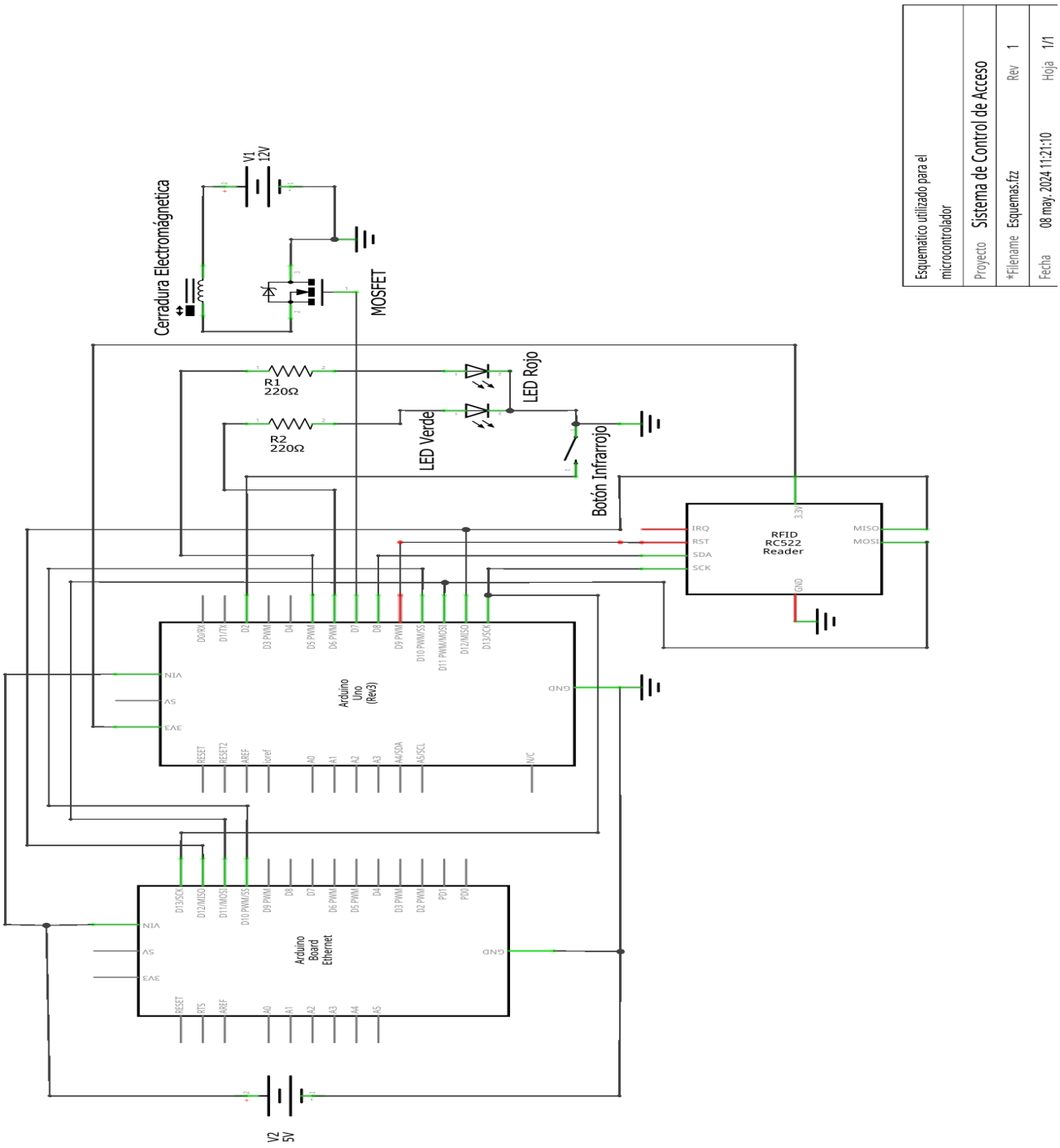
[12] N. Boyko, V. Solohub, and A. Stasiuk, "System of restriction access with the help of nodemcu and rfid module," in *2019 IEEE 14th International Conference on Computer Sciences and Information Technologies (CSIT)*, vol. 1, 2019, pp. 50–55.

[13] O. A. Allah, S. Abdalla, M. Mekki, and A. Awadallah, "Rfid based access control and registration system," in *2018 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*, 2018, pp. 1–4.

[14] D. J. Morerwa, P. Owolawi, and G. Aiyetoro, "Examination hall access control system using radio frequency identification," in *2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)*, 2020, pp. 1–6.

[15] J. M. Pinargote-Ortega, M. d. R. Cruz-Felipe, G. P. Demera Ureta, R. D. Escobar-Moreira, and G. I. Medranda-Cobeña, "Rfid en el servicio bibliotecario de la utm," *Revista científica*, vol. 3, no. 36, p. 341–355, 2019.

V. ANEXOS


Esquematico utilizado para el microcontrolador
Proyecto Sistema de Control de Acceso
*Filename Esquemas.fzz Rev 1
Fecha 08 may. 2024 11:21:10 Hoja 1/1
V1
12V
Cerradura Electromágnetica
MOSFET
R1
220Ω
R2
220Ω
LED Rojo
LED Verde
Botón Infrarrojo
RFID
RC522
Reader
IRQ
RST
SDA
SCK
MISO
MOSI
3.3V
GND
Arduino
Uno
(Rev3)
Arduino
Board
Ethernet
V2
5V