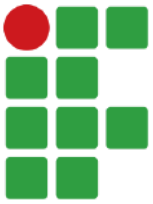


INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA

CAMPUS CAMPINA GRANDE

BACHARELADO EM ENGENHARIA DE COMPUTAÇÃO

ALFREDO RODRIGO SOUSA DA SILVA

IF ACCESS: SISTEMA DE CONTROLE DE ACESSO ELETRÔNICO UTILIZANDO TECNOLOGIA RFID E MICROCONTROLADOR

CAMPINA GRANDE

2022

ALFREDO RODRIGO SOUSA DA SILVA

IF ACCESS: SISTEMA DE CONTROLE DE ACESSO ELETRÔNICO UTILIZANDO TECNOLOGIA RFID E MICROCONTROLADOR

Trabalho de Conclusão de Curso apresentado como requisito para obtenção de título de Bacharel em Engenharia de Computação pelo Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Campus Campina Grande.

Orientador: Prof. Dr. George Sobral Silveira

CAMPINA GRANDE

2022

S586i Silva, Alfredo Rodrigo Sousa da.
IF Access: sistema de controle de acesso eletrônico utilizando tecnologia RFID e microcontrolador / Alfredo Rodrigo Sousa da Silva. - Campina Grande, 2022.
47 p.:il.

Trabalho de Conclusão de Curso - Monografia (Curso de Bacharelado em Engenharia da Computação) - Instituto Federal da Paraíba, 2022.
Orientador: Prof. Dr. George Sobral Silveira.

1.Engenharia da computação. 2. Desenvolvimento de sistemas - sistemas embarcados. 3.Controle de acesso - RFID. I. Título.

CDU 004.4

ALFREDO RODRIGO SOUSA DA SILVA

IF ACCESS: SISTEMA DE CONTROLE DE ACESSO ELETRÔNICO UTILIZANDO TECNOLOGIA RFID E MICROCONTROLADOR

Trabalho de Conclusão de Curso apresentado como requisito para obtenção de título de Bacharel em Engenharia de Computação pelo Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Campus Campina Grande.

Orientador: Prof. Dr. George Sobral Silveira

Banca examinadora:

Campina Grande, __ de _____ de ____

_____

Prof. Dr. George Sobral Silveira

_____

Prof. Dr. Alexandre Sales Vasconcelos

_____

Prof. Dr. Fagner de Araujo Pereira

CAMPINA GRANDE

2022

Aos meus pais, família, amigos e todos aqueles que sempre estiveram ao meu lado e acreditaram em mim.

AGRADECIMENTOS

A Deus, pelo dom da vida e por possibilitar que eu chegasse até aqui.

Aos meus pais, que sempre acreditaram em mim e nunca deixaram de me incentivar a continuar com os estudos.

Às minhas tias Renata e Rose, e à minha avó Francisca, que sempre foram suporte para minha jornada.

Aos meus amigos, Katiana, Luiz e Renally, que sempre estiveram comigo nos piores e nos melhores momentos.

Aos meus amigos e colegas de curso Alisson e Guilherme, que me acompanharam ao longo da minha jornada no curso.

A todos os meus professores, em especial, ao professor George, por me orientar ao longo deste trabalho, e ao professor Katyusco, que me é inspiração.

"*Que os nossos esforços desafiem as impossibilidades. Lembrai-vos de que as grandes proezas da história foram conquistadas do que parecia impossível*"

(Charles Chaplin)

RESUMO

É desejável que pessoas não consigam acessar determinados ambientes sem a devida autorização para tal. Diante dos avanços tecnológicos, restringir os acessos a ambientes ficou ainda mais fácil, especialmente com a integração de diversos sistemas de segurança. Ainda assim, muitos lugares ainda utilizam controles de acesso manuais, totalmente operacionalizados por seres humanos, e extremamente propensos a falhas de segurança. Devido ao crescente número de pessoas que circulam pelos ambientes do Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Campus Campina Grande, um maior e mais robusto controle de acesso aos ambientes da instituição passou a ser requerido. No presente projeto, foi desenvolvido, com o intuito de ser utilizado nos ambientes do IFPB campus Campina Grande, um sistema de controle de acesso eletrônico que se utiliza de tecnologia RFID e de microcontrolador para permitir ou restringir acessos a ambientes da instituição, por parte dos usuários. Nas simulações que foram executadas, o sistema se mostrou funcional na realização das tarefas a que foi proposto, tendo gerenciado corretamente os usuários cadastrados e seus respectivos ambientes e horários de acesso, garantindo, assim, a segurança, a agilidade e a praticidade no controle de acesso do instituto.

Palavras-chave: Controle de Acesso. Microcontrolador. RFID. Sistemas Embarcados.

ABSTRACT

It is desirable that people cannot access certain environments without proper authorization. In the face of technological advances, restricting access to environments has become even easier, especially with the integration of various security systems. Yet many places still use manual access controls, fully operationalized by humans, and extremely prone to security breaches. Due to the growing number of people circulating through the environments of the Federal Institute of Education, Science and Technology of Paraíba, Campus Campina Grande, greater and more robust access control to the institution's environments has become required. In the present project, an electronic access control system was developed, with the intention of being used in the environments of the IFPB campus Campina Grande, which uses RFID technology and a microcontroller to allow or restrict access to the institution's environments, by the users. In the simulations that were performed, the system proved to be functional in carrying out the tasks to which it was proposed, having correctly managed the registered users and their respective environments and access times, thus guaranteeing security, agility and practicality in controlling institute access.

Keywords: Access Control. Microcontroller. RFID. Embedded Systems.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

API	*Application Programming Interface*
CPU	*Central Processing Unit*
CSV	*Comma-Separated Values*
HTML	*HyperText Markup Language*
LED	*Light-Emitting Diode*
MER	Modelo Entidade Relacionamento
MQTT	*Message Queuing Telemetry Transport*
RFID	*Radio-Frequency Identification*
RTC	*Real Time Clock*
RX/TX	Receptor Serial/Transmissor Serial
SD	*Secure Digital*
SGBD	Sistema de Gerenciamento de Banco de Dados
SPI	*Serial Peripheral Interface*
TCP/IP	*Transmission Control Protocol/Internet Protocol*

SUMÁRIO

1 INTRODUÇÃO

A necessidade de restringir o acesso de determinados ambientes de pessoas não autorizadas existe há muito tempo. Visando principalmente a segurança, buscamos sempre utilizar mecanismos que garantam que somente pessoas com autorização consigam acessar e utilizar algum espaço. Com a evolução da tecnologia, a utilização de controles de acesso eletrônicos ficou cada vez mais frequente. No Brasil eles são utilizados há mais de 20 anos. Com eles é possível garantir que somente pessoas previamente cadastradas e autorizadas acessem e utilizem determinado ambiente. Sistemas deste tipo são diretamente responsáveis pela segurança, não só patrimonial, mas também das pessoas que fazem uso destes espaços.

A segurança, tanto patrimonial quanto individual, sempre esteve sob constantes ameaças externas e sempre foi uma preocupação em qualquer ambiente, desde as casas dos cidadãos até os grandes centros empresariais. Visando garantir uma maior segurança no acesso às áreas restritas e reduzir a ocorrência de eventos danosos a essas áreas e aos seus usuários por terceiros, os sistemas de controle de acesso vêm sendo cada vez mais empregados nas grandes e pequenas empresas, condomínios, residências e nos mais variados locais que se possa imaginar.

Sob essa perspectiva, foram desenvolvidos ao longo da história diversos tipos de controles de acesso. Desde as primeiras trancas desenvolvidas pelo ser humano, até os mais modernos sistemas de fechaduras digitais com identificação biométrica da atualidade, os controles de acesso sempre foram transformados a fim de suprir as necessidades do seu tempo. Com o advento da eletrônica e da microtecnologia, as inovações nos controles de acesso seguiram, também, por essa linha. Paralelamente a isso, surge, nos anos de 1930, a tecnologia de Identificação por Radiofrequência (RFID). Com suas raízes nos sistemas de radares utilizados na Segunda Guerra Mundial (NASCIMENTO, 2019), essa tecnologia, anos depois, também passou a ser incorporada a muitos sistemas eletrônicos para os mais diversos fins, inclusive para o controle de fluxo de pessoas.

Considerando o exposto, o presente trabalho tem como objetivo desenvolver um sistema de gerenciamento de controle de acesso de pessoas para o Instituto Federal de Educação, Ciência e Tecnologia da Paraíba - Campus Campina Grande

(IFPB-CG), utilizando as tecnologias RFID e de microcontroladores. O modelo proposto constitui-se de um ponto de acesso com um sistema embarcado microcontrolado instalado nas entradas de cada ambiente da instituição, que efetuará a revogação ou a permissão de acesso aos ambientes do IFPB-CG para os usuários, além de um sistema *web*, por onde será possível realizar todo o gerenciamento do sistema, adicionando, editando e removendo regras e usuários do mesmo. O modelo objetiva modernizar o atual controle de acesso do IFPB-CG, já que esse controle, hoje, é feito de forma manual e está sujeito a erros humanos que potencialmente podem causar falhas na segurança do campus e de seus usuários.

2 DEFINIÇÃO DO PROBLEMA

O IFPB-CG lida com um grande fluxo de pessoas todos os dias. Dentre essas pessoas, estão os alunos, professores, servidores, terceirizados, entre outros. Para garantir a segurança de todos e dos ambientes do instituto, o IFPB-CG conta com um controle de acesso totalmente manual, que é realizado por servidores da instituição mediante o registro de empréstimos e devoluções das chaves dos ambientes.

Atualmente, quando uma pessoa deseja realizar o acesso a algum dos ambientes do IFPB-CG, ela precisa se dirigir até a sala do setor de chaves, e solicitar a chave do ambiente que deseja acessar. Estando disponível, um servidor realiza o empréstimo da chave, entregando-a ao solicitante e registrando, em um livro, o nome da pessoa que solicitou, o ambiente, bem como os horários de retirada e de devolução da chave.

Todo esse processo manual torna o controle de acesso sujeito à ocorrência de erros, como o registro de datas e horários incorretos e a perda de chaves. Além disso, para que seja possível uma pessoa solicitar o acesso a um dos ambientes da instituição, ela precisa se deslocar fisicamente até o setor de chaves do campus, o que acarreta em um gasto de tempo adicional no processo.

Desta forma, o presente sistema de controle de acesso busca otimizar esse processo, com o uso de uma estrutura de hardware e software embarcado de baixo custo, aliado a um sistema de gerência *web* de código aberto, no qual será possível realizar o cadastro de usuários, de ambientes e de horários de acesso, facilitando assim todo o processo de controle dos ambientes da instituição.

2.1 OBJETIVOS

2.2.1 Objetivo geral

Desenvolver um sistema de controle de acesso microcontrolado utilizando tecnologia RFID e seu respectivo sistema de gerência via *web* para os ambientes do Instituto Federal de Educação, Ciência e Tecnologia da Paraíba - Campus Campina Grande.

2.2.2 Objetivos específicos

- Definir uma estrutura de hardware com base em material de fácil acesso no mercado e que pode ser adquirido e montado utilizando microcontrolador, sistema RFID e interface de rede.
- Implementar um sistema embarcado que vai ser carregado no hardware dos pontos de acesso para poder autenticar os usuários.
- Desenvolver um sistema de gerência *web* responsável por gerenciar todos os pontos de acesso e implementar a parte de cadastro, edição e registro de todos os usuários do sistema.

2.2 JUSTIFICATIVA

A implementação de um sistema de controle de acesso eletrônico no IFPB-CG se justifica por, dentre os principais benefícios, trazer uma maior segurança aos ambientes do instituto, restringindo o seu acesso a somente pessoas autorizadas. Além disso, o sistema também garante uma maior agilidade e facilidade nesse processo, uma vez que o sistema de controle de acesso eletrônico proposto é totalmente eletrônico e dispensa o deslocamento até o setor de chaves do IFPB-CG, impactando diretamente na otimização do tempo dos usuários, especialmente dos professores.

Atualmente no mercado existem diversos controles de acesso disponíveis para aquisição, porém, pelo IFPB-CG se tratar de uma instituição pública, o IF Access se justifica, também, por ser um sistema de *software* livre e de fácil implementação, o que facilita a sua possível futura distribuição para outras instituições públicas, e também as suas gradativas melhorias.

3 FUNDAMENTAÇÃO TEÓRICA

O IF Access foi pensado para otimizar o controle de acesso do IFPB-CG e, para tanto, necessita da utilização de diversas tecnologias em seu desenvolvimento. Essas tecnologias serão responsáveis por, juntas, disponibilizarem o sistema de gerência *web* para o sistema de controle de acesso, bem como os pontos de acesso, constituído de diferentes componentes de *hardware* conectados, e que juntos serão capazes de realizar a autenticação dos usuários e a liberação do acesso aos ambientes da instituição.

As tecnologias pensadas para o desenvolvimento do projeto foram: RFID para a fácil e cômoda autenticação dos usuários; microcontrolador para embarcar o *software* dos pontos de acesso; relógio de tempo real para o armazenamento de contagem do tempo, utilizado na autenticação; interface de rede, utilizada na conexão entre o sistema de gerência *web* e os pontos de acesso; e protocolo de troca de mensagens, responsável pelo envio de mensagens do sistema *web* para os pontos de acesso.

3.1 TECNOLOGIA RFID

A sigla RFID vem do inglês *Radio Frequency Identification*, que significa Identificação por Radiofrequência. Esta tecnologia é composta por três componentes, que são: antena, responsável por transmitir as ondas de rádio; *transceiver* (transmissor/receptor), responsável por gerar os sinais de rádio para a comunicação; e *transponder* (comumente chamada de *tag* RFID), composta também por uma antena e um microchip, onde são armazenados os seus dados. As *tags* RFID podem ser do tipo leitura ou leitura e escrita, onde a primeira possuem dados gravados de fábrica em seus microchips, e que não podem ser alterados, enquanto que a segunda pode ter seus dados alterados, através de um processo de escrita (FREITAS, 2020).

A comunicação na tecnologia RFID acontece da seguinte forma: o *transceiver* envia um sinal de rádio, que é propagado em todas as direções através da sua antena, onde esta, por sua vez, energiza e ativa a *tag* RFID, ou seja, o *transponder*, que devolve os dados contidos em seu microchip, também por sinal de rádio, para o

transceiver. Este, por último, recebe e processa esses dados (RODRIZ; RODRIGUES, 2018). Pelo fato de a comunicação se dar através de ondas de rádio, não é necessário o contato físico entre *transceiver* e *transponder*, podendo a comunicação ser estabelecida a determinadas distâncias (FREITAS, 2020).

Barsotti, Rahal e Silva (2020) veem com bons olhos o uso da tecnologia RFID em processos de monitoramento e rastreabilidade de itens. Segundo os autores, essa tecnologia é capaz de melhorar processos de gestão de estoque:

> A utilização do RFID para monitorar os estoques pode prover maior previsibilidade às empresas, trazendo inúmeros benefícios, como melhorar a previsão sobre os níveis de estoque, reabastecimento imediato nas prateleiras, redução do número da quantidade de itens em estoque, e maior transparência na informação sobre demanda, além de melhorias na confiabilidade de entrega e disponibilidade de produtos. (BARSOTTI; RAHAL; SILVA, 2020, p. 6).

Além das aplicações em empresas, a tecnologia RFID também pode ser aplicada em controles de acesso de pessoas em condomínios, escolas, repartições públicas, possibilitando o ingresso de indivíduos autorizados a esses locais, bem como o registro de horários de entrada e saída dos mesmos.

3.1.1 Tipos de etiquetas *RFID*

As etiquetas RFID, ou simplesmente *tags*, podem ser classificadas de acordo com o seu modo de funcionamento, podendo estas serem do tipo passiva, semi-passiva ou ativa. Essa classificação diz respeito ao modo como essas etiquetas são alimentadas.

3.1.1.1 Passiva

As etiquetas RFID passivas são aquelas que obtêm energia para o seu funcionamento através da indução gerada pelo campo eletromagnético resultante das ondas de rádio transmitidas pelo *transceiver*. Tal fenômeno é capaz de induzir uma pequena corrente elétrica pela etiqueta, suficiente para permitir que ela seja capaz de enviar a sua resposta para o receptor (ARAUJO, 2018).

3.1.1.2 Ativa

As etiquetas RFID ativas são aquelas que obtêm energia para o seu funcionamento através de uma bateria própria. Essas etiquetas independem da alimentação fornecida pelo leitor, e são capazes de, sozinhas, transmitirem os seus dados através de radiofrequência. Elas possuem um circuito de rádio com uma complexidade maior, e são capazes de emitir suas ondas a distâncias maiores. (CASTILHO, 2022).

3.1.1.3 Semi-passiva

Esse tipo de etiqueta RFID reúne características das etiquetas ativa e passiva. As *tags* semi-passivas são equipadas com uma fonte de energia própria, assim como a etiqueta ativa, mas neste caso, ao contrário das etiquetas ativas, a bateria não serve para iniciar uma transmissão de dados. Na semi-passiva, sua bateria serve para fornecer energia elétrica à etiqueta que auxilia na recepção da informação através das ondas de radiofrequência. Deste modo, é possível reduzir a potência do leitor, ao mesmo tempo em que se aumenta a capacidade de armazenamento de dados pela etiqueta (MAIA, 2019).

3.2 MICROCONTROLADOR

Os microcontroladores são pequenos circuitos integrados que, dentro de um único chip, possuem todos os periféricos necessários ao seu funcionamento, fazendo com que ele dependa unicamente de uma fonte de energia para operar. Um microcontrolador possui, dentre outros periféricos: uma unidade de processamento central, mais conhecida em inglês como CPU (*Central Processing Unit*), que é responsável por realizar todos os cálculos lógicos e aritméticos dos programas; uma memória, que armazena os dados em tempo de execução e o programa do usuário para o microcontrolador, este último chamado de “software embarcado”; e portas de entrada e de saída, interfaces principais do microcontrolador com o mundo externo. (SANTOS et al., 2020).

3.2.1 Arduino

O Arduino é uma plataforma de prototipagem eletrônica de *hardware* livre, que facilita o desenvolvimento de projetos de eletrônica envolvendo microcontroladores para aqueles que possuem um conhecimento básico na área (MOREIRA et al., 2018), e é uma plataforma de prototipagem que envolve praticidade e baixo custo, uma vez que, com ela, o desenvolvimento de equipamentos é simplificada e se dá de forma mais rápida, já que o projetista não precisa construir todo o seu circuito do zero para utilizar um microcontrolador. Com isso, o mesmo pode economizar tempo, mantendo a qualidade do projeto (SOUZA et al., 2021).

O Arduino conta com um microcontrolador e com pinos de entradas e saídas analógicas e digitais, pelos quais podemos instalar os periféricos, ou *shields*, que farão parte de nossos projetos. Alguns modelos da plataforma contam, ainda, com portas USB, LEDs (*Light-Emitting Diode*), interface serial RX/TX, botão de *reset*, conector de alimentação e circuito oscilador. A plataforma conta com diversos modelos, sendo o Uno um dos mais conhecidos.

A principal fabricante que desenvolve o microcontrolador para a plataforma de prototipagem Arduino é a Atmel, mas diversas empresas também fabricam seus modelos de microcontroladores, como por exemplo a Intel, a Texas Instruments, a Microchip e a Motorola.

3.2.2 Arduino Mega ADK

O Arduino Mega ADK é um dos modelos da plataforma de prototipagem Arduino. Ele conta com tudo o que foi descrito anteriormente, e o seu microcontrolador é o Atmel Atmega2560. É uma placa que opera a um nível de tensão de 5V, possui 54 pinos de entrada e saída digitais e 16 pinos de entradas analógicas, 256 KB de memória *flash*, 8 KB de memória SRAM, 4 KB de memória EEPROM, e opera a uma velocidade de *clock* de 16 MHz. Pesando 37 gramas, esse modelo de Arduino é um dos mais utilizados pelos desenvolvedores em projetos de sistemas embarcados, e por possuir uma porta USB integrada, junto com um chip controlador dedicado MAX3421E, ele é vastamente utilizados em projetos integrados

ao Android, uma vez que é possível conectar diversos dispositivos com esse sistema operacional através da sua USB (ARDUINO, 2022).

No projeto, o Arduino Mega ADK foi a plataforma de prototipagem escolhida para o sistema microcontrolado dos pontos de acesso. Essa escolha tem como base o seu custo, a sua quantidade de memória e de portas, e o seu consumo energético. Dentre as placas de prototipagem Arduino existentes no mercado, o Arduino Mega ADK é uma das que possui melhor custo benefício, pois ela é suficiente para a maioria dos projetos microcontrolados e pode ser adquirida por um preço acessível. Além disto, o Arduino Mega ADK possui uma quantidade satisfatória de memória e de portas de entrada e saída, o que possibilita a conexão de vários *shields* e periféricos, ao mesmo tempo que possui um baixo consumo energético, considerando que a mesma opera com um nível de tensão de 5V.

3.3 *REAL TIME CLOCK* (RTC)

Em muitos projetos com Arduino, se faz necessário o acompanhamento da passagem do tempo. Para isso, pode ser implementado um relógio via *software*, no próprio código do sistema embarcado. O problema é que esse tipo de implementação está sujeito a falhas que podem colocar a perder todo o tempo registrado. Um exemplo disto seria uma interrupção do fornecimento de energia elétrica para o Arduino, o que o faria desligar e interromper a contagem. Para resolver esse problema, pode-se utilizar um módulo conhecido como *Real Time Clock* (RTC), ou relógio de tempo real.

Como sugere o nome do dispositivo, o RTC é um módulo responsável por armazenar o horário atual, e contar o avanço das horas, em tempo real, como um relógio comum. A vantagem desses dispositivos é que eles possuem *hardware* dedicado, e muitas vezes dispõem de uma alimentação secundária, que os mantém energizados mesmo em faltas de energia elétrica (MOURA et al., 2020).

No projeto, o módulo RTC DS1302 é o responsável por armazenar o horário atual local do ponto de acesso, utilizado para realizar a autenticação dos usuários no sistema, para a liberação ou revogação dos acessos dos mesmos aos ambientes. Ele opera alimentado com 5V pelo próprio Arduino, mas também mantém o seu

relógio funcionando mesmo sem o fornecimento de energia elétrica externa, onde, para isto, ele utiliza a sua bateria interna de 3V.

3.4 INTERFACE DE COMUNICAÇÃO DE REDE

Para possibilitar que o Arduino se conecte com a internet, se faz necessário utilizar um *shield* que atue como interface entre a plataforma e a rede. No IF Access, o módulo *Ethernet Shield* W5100 desempenha esse papel. Ele é responsável por manter o Arduino e, consequentemente, o ponto de acesso conectados à rede, para que os mesmos possam se comunicar com o servidor *web*. Ele dispõe, ainda, de um *slot* para o uso de um cartão de memória do tipo micro SD. Tal módulo se conecta com o servidor por meio do protocolo de rede TCP/IP e recebe do servidor os pacotes com as informações de cadastro dos usuários do sistema, armazenados no banco de dados, além de enviar para o servidor *web* o histórico de utilização dos ambientes.

O *Ethernet Shield* W5100 se comunica com o Arduino através da sua interface serial de comunicação *Serial Peripheral Interface* (SPI), e opera com um nível de tensão de 5V. A velocidade de comunicação da interface de rede pode ser de 10 ou 100 megabits por segundo, ou Mbps (RUTTMANN, 2018).

3.5 PROTOCOLO DE COMUNICAÇÃO *MESSAGE QUEUING TELEMETRY TRANSPORT* (MQTT)

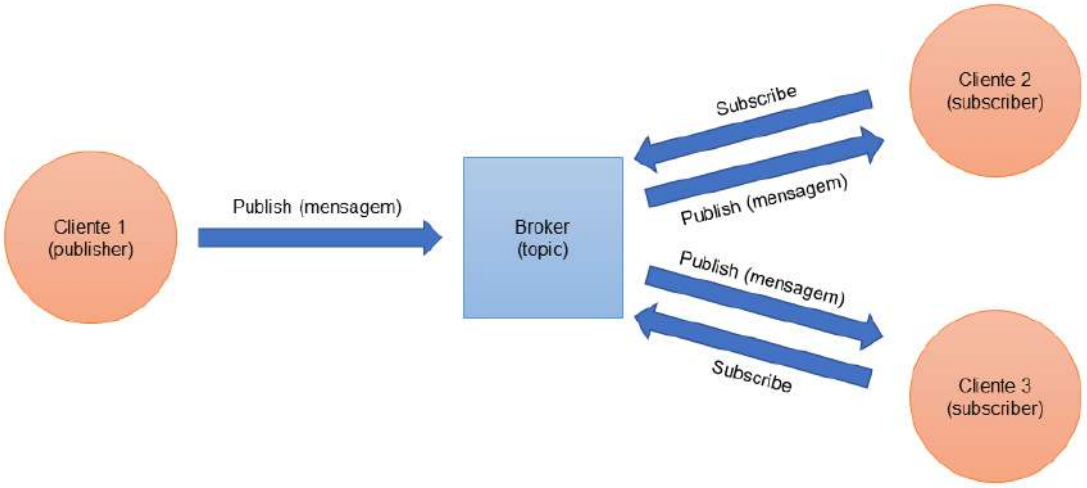
Em muitos casos, a concepção de um produto se dá com a utilização de várias plataformas diferentes. Apesar disto, é comum que essas plataformas precisem se comunicar de alguma forma. A solução para implementar essa comunicação está no uso do conceito de troca de mensagens, que consiste na comunicação entre essas diferentes plataformas através da troca de mensagens, gerenciadas por um servidor chamado de *broker*.

Para implementar um serviço de mensageria em uma aplicação, pode ser utilizado um dos protocolos de mensageria que existem. Um desses protocolos é o *Message Queuing Telemetry Transport* (MQTT), que é um protocolo de comunicação

voltado para o uso em *Internet of Things* (*IoT*) (Internet das Coisas). O protocolo MQTT funciona sobre o protocolo TCP/IP, e é baseado no modelo de comunicação cliente-servidor, onde o cliente envia e/ou recebe mensagens, e o servidor gerencia essa comunicação. Esse protocolo se tornou conhecido por ser simples, por possibilitar a comunicação bilateral, e também por oferecer um baixo consumo de dados durante a comunicação (BRITO, 2019).

O princípio de funcionamento do protocolo é simples: o cliente envia uma mensagem para um tópico específico, registrado em um servidor, ou *broker*. Em contrapartida, um outro cliente, que previamente assina esse tópico no *broker*, recebe a mensagem que foi enviada. A Figura 1 a seguir contém o fluxo comum da troca de mensagens entre sistemas utilizando o protocolo MQTT:

Figura 1. Princípio de funcionamento do protocolo MQTT



Fonte: Elaborada pelo autor.

O protocolo MQTT foi utilizado no projeto para estabelecer uma comunicação simples através de troca de mensagens via rede entre o sistema *web* e os pontos de acesso, para que o sistema possa enviar as informações de um arquivo *Comma-Separated Values* (CSV), acerca das regras de acesso dos ambientes, para os microcontroladores. Essas informações precisam chegar até eles através da rede para que os pontos de acesso possam confrontar os dados e, eventualmente, liberar ou não o acesso ao ambiente.

4 REVISÃO BIBLIOGRÁFICA

A tecnologia RFID (*Radio Frequency Identification,* ou identificação por radiofrequência) tem sido utilizada com cada vez mais frequência ao longo dos anos, para as mais variadas finalidades. Ela tem potenciais aplicações em empresas e em instituições, sendo principalmente utilizada em linhas de produção, em controle de estoque e em controles de acesso.

Vinicius Gonçalves (2019), em seu projeto, desenvolveu um aplicativo de controle de acesso, que era gerenciado por um sistema *web* hospedado em um servidor. Seu sistema era composto de leitores RFID, tags RFID, teclado numérico e microcontrolador, e o protótipo desse sistema se conectava com o servidor por meio da utilização de uma API (*Application Programming Interface*). O principal objetivo do projeto era automatizar o processo de liberação de acesso aos laboratórios da Escola de Minas.

Ribeiro et al. (2018) desenvolveram um sistema com a finalidade de controlar o acesso de pessoas a ambientes escolares utilizando tecnologia RFID e o micro-computador Raspberry Pi 3. Juntamente com leitores e tags RFID, neste projeto, os autores tinham como objetivo centralizar em seu sistema todo o gerenciamento de cadastro e permissão de acessos aos ambientes.

Seguindo a ideia de cidades inteligentes e de internet das coisas, Victor Oliveira Boppré (2018) implementou um controle e monitoramento de acesso a ambientes controlados, desenvolvido na linguagem de programação Python, utilizando o *framework* Flask. O sistema contou com o uso da plataforma NodeMCU, em comunicação com um sistema *web*, empregando o protocolo MQTT.

Alves (2019) propôs um sistema de controle de acesso distribuído com utilização de tecnologia RFID para gerenciar os acessos do Laboratório de Instrumentação Eletrônica e Controle da Universidade Federal de Campina Grande (UFCG). O projeto desenvolvido conta com uma arquitetura sem servidor, e abrange os conceitos de Computação em Nuvem e Internet das Coisas.

Na linha de tecnologia RFID, Rodriz e Rodrigues (2018) apresentam, em seu trabalho, a utilização da tecnologia para a identificação de veículos e o controle de acesso a vagas destinadas a pessoas idosas ou com deficiências. Tal projeto tinha como finalidade garantir que essas vagas somente fossem utilizadas pelas pessoas

que realmente as necessitassem, se certificando de que os direitos de mobilidade dessas pessoas fossem respeitados.

Souza et al. (2020) desenvolveram um sistema de controle de acesso veicular para o estacionamento de uma empresa utilizando a tecnologia RFID. O modelo utilizado pelos autores foi constituído por microcontrolador, onde o seu sistema embarcado foi desenvolvido utilizando a linguagem de programação C. O controle de acesso proposto envolveu o uso de uma cancela controlada por um Arduino, a qual era responsável pela liberação ou não do acesso dos veículos ao estacionamento.

Atualmente no mercado, existem diferentes modelos de controle de acesso proprietários disponíveis para aquisição. A fabricante Intelbras, empresa brasileira de produtos e soluções em Segurança, Comunicação, Redes e Energia, possui o controlador de acesso Intelbras Digiprox SA 202, que opera com três opções de acesso diferentes: através de senha numérica, da leitura de *tags* RFID e pela combinação das duas tecnologias. Esse modelo possui funções de campainha, é compatível com diferentes tipos de fechaduras do tipo eletroímã e eletromecânica e é capaz de controlar até 1.000 usuários (INTELBRAS, 2022).

A mesma fabricante dispõe, também, do modelo Smart IFR 1001, que faz parte da linha de produtos para casa inteligente da Intelbras. Esse modelo conta com a possibilidade de ser utilizado através de aplicativo de celular, e é alimentado por pilhas, prometendo uma autonomia de até 10 meses. Este modelo possibilita a gestão de até 100 senhas diferentes, e possui função não perturbe, travamento automático e ainda é compatível com os produtos Amazon Alexa e Google (INTELBRAS, 2022).

Já a Pado, referência no setor de segurança e reconhecida pela fabricação de cadeados e outros produtos e soluções em segurança, possui a fechadura digital biométrica FDE-101RM, que possui sensor biométrico e teclado numérico para senha. Este modelo suporta o cadastro de até 196 impressões digitais e também é alimentado por pilhas (PADO, 2022). O destaque desse modelo é a segurança promovida pelo sensor biométrico, que garante que nenhum usuário não cadastrado possa acessar um ambiente.

A fechadura *Fingerprint Electronic Touchscreen Keypad Smart Lock*, da empresa chinesa de inteligência artificial e Internet das Coisas Tuya, é um modelo de controle de acesso que possui liberação de acesso através da conexão *bluetooth*

do aparelho celular do usuário cadastrado, além de através de aplicativo, senha numérica, sensor biométrico e chave mecânica, e permite o registro de até 150 usuários. (TUYA, 2020).

A seguir, na Tabela 1, são comparadas as diversas características dos produtos proprietários anteriormente mencionados:

Tabela 1: Comparativo entre os projetos e produtos mencionados

Autor/fabricante	Produto	Limite de usuários	Interface	Método de acesso
Intelbras (2022)	Digiprox SA 202	1.000	Física	Senha, cartão RFID e multifator (senha + cartão RFID)
Intelbras (2022)	Smart IFR 1001	100	Física, aplicativo móvel e *hub* de automação proprietário da Intelbras	Senha e aplicativo de celular
Pado (2022)	FDE-101RM	196	Física	Senha e biometria
Tuya (2022)	*Fingerprint Electronic Touchscreen Keypad Smart Lock*	150	Física e aplicativo móvel	Senha, biometria, aplicativo de celular e chave mecânica

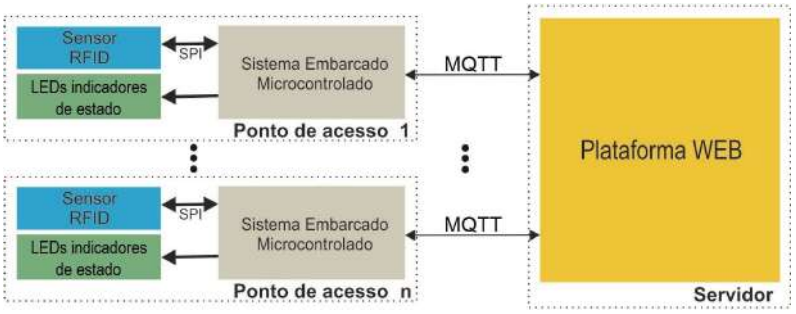
Fonte: Elaborada pelo autor.

Entre os produtos disponíveis no mercado elencados nesta seção, o IF Access tem como vantagem ser um controle de acesso de código livre, e por ser implementado pelo IFPB-CG, tem seu desenvolvimento, suas melhorias e sua manutenção a cargo da instituição, diferentemente dos produtos proprietários, que são engessados à *upgrades* e tem sua manutenção a cargo da fabricante.

5 METODOLOGIA

Para desenvolver o sistema, fez-se necessário dividir as etapas de desenvolvimento em duas: a etapa de *software* e a etapa de *hardware*. O controle de acesso eletrônico se utiliza da linguagem de programação Python e do *framework* de desenvolvimento *web* Django, além do banco de dados PostgreSQL para sua etapa de *software*, e das tecnologias RFID e de microcontrolador, através da plataforma de desenvolvimento Arduino, além de módulos de internet e de relógio de tempo real, para a sua etapa de *hardware*. Podemos ver, na Figura 2 a seguir, como é constituído o sistema de controle de acesso desenvolvido neste projeto:

Figura 2. Esquema do sistema de controle de acesso



Fonte: Elaborada pelo autor.

Cada ponto de acesso é constituído de um microcontrolador, com um sistema embarcado, além de um sensor RFID e de LEDs que representam o estado do acesso (se liberado ou não). Os pontos de acesso devem ser instalados em cada ambiente da instituição, e se comunicam via rede, utilizando o protocolo MQTT, com o servidor, que contém o *software* responsável por toda a gerência do sistema. Os pontos de acesso – o *hardware* principal do sistema – contam com um sistema de baterias, que visa suprir as necessidades energéticas do sistema em caso de interrupção do fornecimento de energia elétrica.

A utilização do sistema dá-se da seguinte forma: após o registro do usuário no servidor, é feita a correlação dele com os ambientes aos quais ele tem acesso. O servidor, por sua vez, transfere essas informações via rede, utilizando o protocolo de comunicação MQTT para todos os pontos de acesso correlacionados com o usuário. Esse envio se faz necessário para caso a rede lógica fique inoperante. Uma vez com essas informações, o ponto de acesso é capaz de realizar a autenticação de

qualquer usuário cadastrado no sistema, mediante a leitura da *tag* RFID do usuário. Ao aproximar a *tag* do leitor, o sistema efetua a leitura do código da mesma, e consulta se esse código está associado a algum usuário que se encontra cadastrado para a utilização daquele ambiente naquele horário. Em caso positivo, o acesso ao ambiente é liberado, para que o usuário possa realizar o uso do mesmo. Em caso negativo, o usuário não consegue acessar o ambiente.

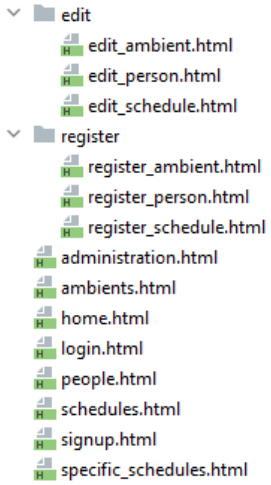
5.1 ETAPA DE *SOFTWARE*

O *software* aplicativo do servidor foi desenvolvido utilizando a linguagem de programação Python, juntamente com o *framework* para desenvolvimento para aplicações *web* Django. Também foram utilizadas as tecnologias *PostgreSQL*, *CSS3*, *JavaScript* e *HTML5*. O código de todo o sistema foi desenvolvido utilizando o sistema de controle de versão Github, e encontra-se armazenado em um repositório remoto[1]. O sistema conta com os módulos de cadastro de usuários, ambientes e pontos de acesso, e com as funcionalidades para identificar e autenticar os usuários do sistema. Além disso, o IF Access conta com a funcionalidade de gerar e enviar para os pontos de acesso, utilizando o protocolo MQTT através da rede, as informações do arquivo CSV com todas as regras de acesso configuradas no sistema.

Cada página HTML do IF Access lida diretamente com o usuário: são elas que aparecem na interface *web* do sistema para que o utilizador possa inserir os dados necessários no mesmo. As páginas HTML desenvolvidas estão divididas em dois principais grupos: edição e registro, onde as do grupo de edição são responsáveis por editar os dados do sistema (usuários cadastrados, horários preenchidos, entre outros), e também por sua remoção, enquanto que as do grupo de registro são responsáveis por alimentar o sistema com novos dados. Há ainda as páginas que estão destinadas somente à exibição de dados. Estas somente efetuam consultas ao banco de dados e exibem os resultados na tela para o usuário, como por exemplo os horários reservados para um determinado ambiente. Abaixo, na Figura 3, temos a lista com todas as páginas HTML desenvolvidas:

[1] Todo o código do sistema encontra-se armazenado em um repositório remoto do Github, e pode ser acessado através do seguinte endereço: https://github.com/AlfredoRodrigo/IFAccess.

Figura 3. Páginas HTML desenvolvidas no projeto



Fonte: Elaborada pelo autor.

Cada página HTML possui o seu modelo, seu formulário e a sua *view*. Os modelos são as tabelas que existem no banco de dados, enquanto que os formulários são os responsáveis por capturar as informações inseridas em uma página HTML pelo usuário. Já as *views* compõem a lógica da aplicação. Elas são responsáveis pela interação entre as páginas HTML e seus formulários com o banco de dados, ou seja, elas enviam informações do formulário de uma página HTML para o banco de dados, e também recuperam informações do banco de dados para serem exibidas em uma página HTML. Abaixo, na Figura 4, podemos ver a página inicial da plataforma *web* do sistema:

Figura 4. Página inicial da plataforma *web* do sistema de controle de acesso

Fonte: Elaborada pelo autor.

Através da tela inicial, o usuário pode acessar as outras três principais páginas do sistema, a saber: pessoas, ambientes e horários. Nas páginas pessoas e

ambientes, é possível cadastrar, remover e editar os dados dos usuários cadastrados e dos ambientes, respectivamente. Já na página horários é possível gerir todos os horários disponíveis para acesso aos ambientes e determinar quais usuários podem ou não acessar os ambientes em determinados horários. Essas páginas são descritas em detalhe na próxima seção.

5.1.1 Principais páginas do sistema

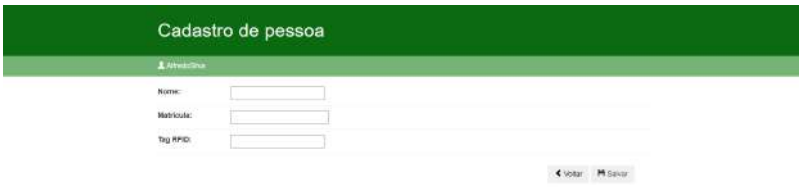
Como mencionado anteriormente, além da página inicial do sistema, possuímos outras três páginas principais: pessoas, ambientes e horários. Cada uma dessas páginas é responsável por listar e exibir na tela suas respectivas informações. Além disso, é através delas que conseguimos acessar as páginas responsáveis por adicionar, editar ou excluir os dados cadastrados. Abaixo, na Figura 5, podemos ver a página de pessoas:

Figura 5. Página de pessoas do IF Access

Fonte: Elaborada pelo autor.

Nessa página, podemos ver uma lista com todos os usuários cadastrados no sistema, onde através dela conseguimos visualizar o nome de cada usuário, sua matrícula e sua *tag* RFID. Através desta tela, é possível, ainda, escolher entre adicionar, editar ou remover uma pessoa. A adição de pessoa redireciona o usuário para um formulário (Figura 6), sendo possível preencher as informações da pessoa que se deseja cadastrar:

Figura 6: Página com formulário para inclusão de pessoa

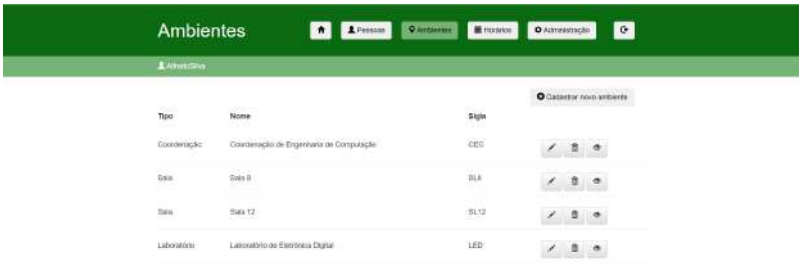


Fonte: Elaborada pelo autor.

A página de edição de usuário possui o mesmo *layout*, onde é aberto um formulário com as informações do usuário já preenchidas, estas quais podemos alterá-las e, em seguida, salvá-las. Cada entidade (pessoa, ambiente e horário) possui cadastrada uma série de informações acerca dos mesmos. Para cadastrar uma entidade “pessoa”, informa-se o nome, a matrícula e o número da tag RFID que o usuário possui.

Já a página de ambientes nos mostra na tela uma listagem de todos os ambientes da instituição que se encontram cadastrados no IF Access, sejam eles salas de aula, salas administrativas ou mesmo laboratórios. Para cada ambiente é possível, também, escolher entre editar ou removê-lo do sistema, além de visualizar todos os seus horários cadastrados. Abaixo, na Figura 7, podemos ver esta página:

Figura 7: Página de ambientes do IF Access



Fonte: Elaborada pelo autor.

Nessa página, podemos visualizar todas as informações dos ambientes, ou seja, o seu tipo, seu nome e sua sigla. Através desta tela, também é possível

adicionar um novo ambiente, onde o usuário é redirecionado para o formulário de cadastro de ambiente (Figura 8), sendo possível preencher as informações do local que se deseja cadastrar:

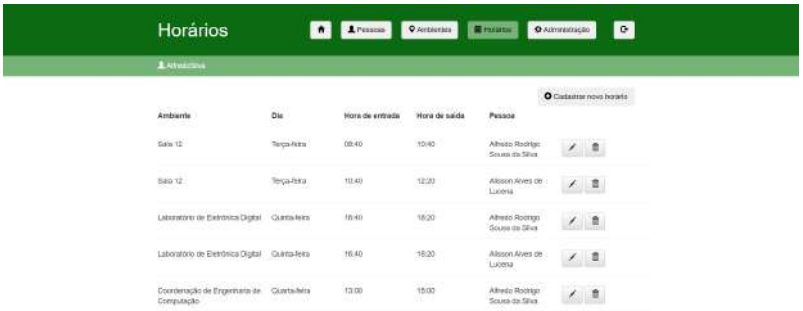
Figura 8: Página com formulário para inclusão de ambiente

Fonte: Elaborada pelo autor.

Para cadastrar uma entidade “ambiente”, informa-se o tipo de ambiente (predefinido como coordenação, sala ou laboratório), o nome, o ID (pequeno código utilizado para facilitar o reconhecimento de ambientes) e os dados que identificam aquele ponto de acesso na rede, que são o IP e a máscara de sub-rede.

Por fim, a página de horários retorna ao usuário uma lista com todos os horários que estão cadastrados no sistema, onde, para cada linha, pode-se observar o nome do ambiente, o dia em que o usuário pode acessar o ambiente, o horário de entrada e de saída e o nome do usuário que possui a permissão. Além disso, também para cada horário, é possível escolher entre adicionar, editar ou removê-lo. Abaixo, na Figura 9, é possível visualizar esta página:

Figura 9: Página de horários do IF Access



Fonte: Elaborada pelo autor.

Esta tela ainda possibilita a inclusão de um novo horário. Cada horário se resume a uma regra de permissão de acesso, e relaciona uma pessoa a um ambiente específico, onde, naquele dia e horário definido durante o cadastro, o usuário pode realizar o acesso ao ambiente. Essas informações são inseridas no sistema através do formulário exibido na Figura 10, a seguir:

Figura 10: Página com formulário para inclusão de horário

Fonte: Elaborada pelo autor.

Para a entidade “horário”, como mencionado anteriormente, é feita uma correlação entre o ambiente, o usuário e o horário de permissão de acesso. Para tal, informa-se o dia da semana, a hora de entrada e a hora de saída em que será permitido que determinado usuário use o ambiente, além do nome da pessoa e do ambiente, ambos previamente cadastrados.

Todos estes dados são armazenados em um banco de dados, responsável por armazenar todas as informações inerentes ao funcionamento do sistema e por correlacionar os ambientes com seus respectivos horários e usuários. Tais dados são armazenados de forma segura, uma vez que a permissão de alteração destes dados só é concedida a administradores, os quais só conseguem efetuar mudanças no sistema mediante autenticação, entrando com seu usuário e senha.

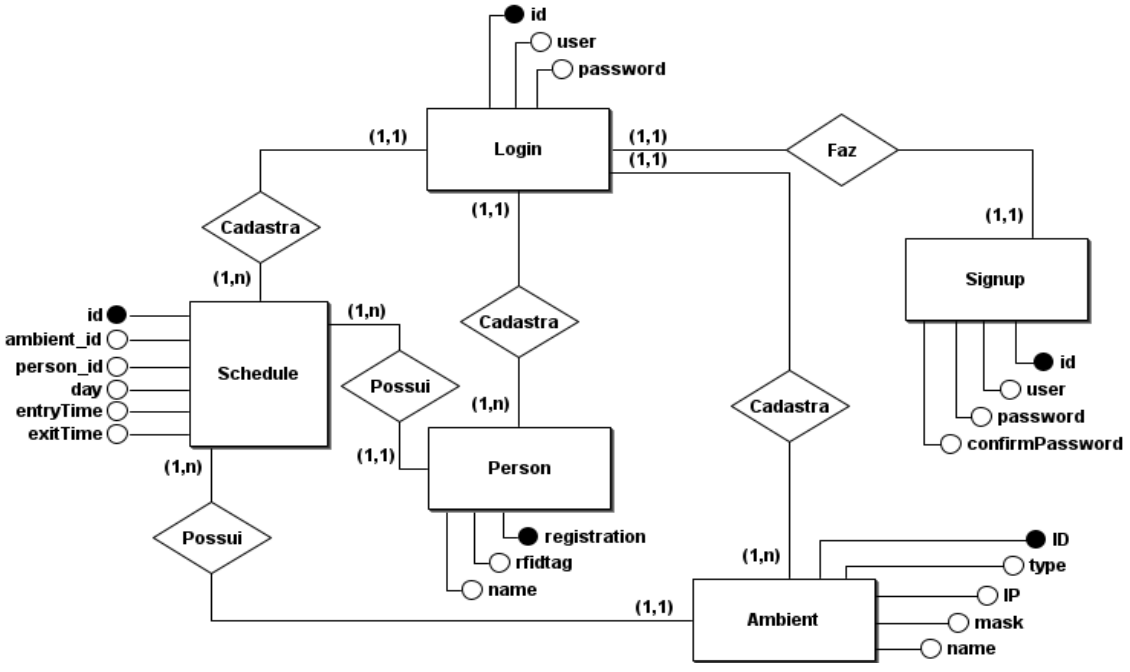
O cadastro de novos usuários no sistema, bem como o agendamento de horários para utilização dos ambientes é feito por um coordenador de curso, ou qualquer outro usuário administrador. Para deixar de ser um usuário comum e passar a ser um usuário administrador, um coordenador deve acessar o sistema e dar esse direito ao usuário em questão.

5.1.2 Banco de dados

O Sistema Gerenciador de Banco de Dados (SGBD) utilizado no sistema foi o PostgreSQL. Esse SGBD é relacional, livre, orientado a objetos e flexível em relação à linguagem de programação. Por ser relacional, o PostgreSQL se baseia em relações que existem entre as tabelas do banco de dados e seus dados, propriamente ditos.

No Django, as entidades do banco de dados são chamadas de modelos, e são descritas no arquivo “models.py”. Para o IF Access, foram desenvolvidos os modelos *Person*, *Ambient*, *Schedule*, *Signup* e *Login*. Esses modelos fazem referência às pessoas, aos ambientes, aos horários, aos usuários administradores e aos usuários logados no sistema, respectivamente. Vale salientar que existe uma diferença entre pessoa e usuário: no IF Access, pessoas possuem cadastro no sistema, e podem ou não possuir um horário reservado em algum ambiente, enquanto usuários são administradores do sistema, tendo direitos de cadastrar outros administradores, além de pessoas, ambientes e horários. Na Figura 11, podemos ver o Modelo Entidade Relacionamento (MER) do banco de dados do sistema:

Figura 11: Modelo entidade relacionamento do IF Access



Fonte: Elaborada pelo autor.

Cada entidade possui uma série de atributos que fazem referência aos objetos que representam. A entidade pessoas, por exemplo, possui os atributos *registration*, *rfidtag* e *name*, que são, respectivamente, a sua matrícula, sua *tag* RFID e o seu nome. Abaixo, na Tabela 2, encontram-se listadas todas as entidades e os seus respectivos atributos:

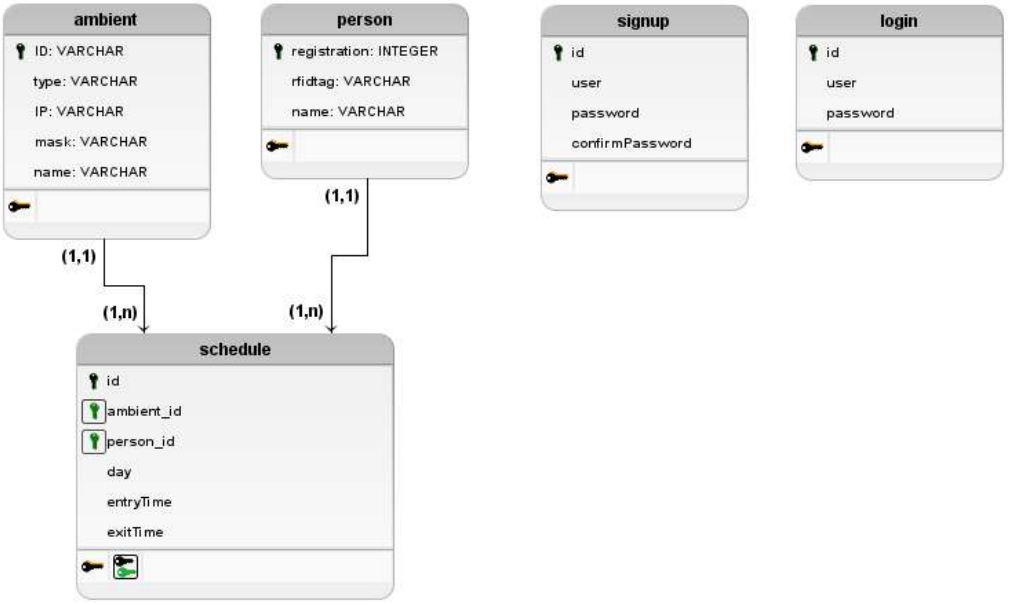
Tabela 2: entidades do banco de dados do IF Access e seus atributos

Entidade	Atributo	Descrição
Person	registration	Matrícula da pessoa
	name	Nome
	rfidtag	Tag RFID da pessoa
Ambient	ID	Pequeno código único identificador do ambiente
	type	Tipo do ambiente
	name	Nome
	IP	Endereço IP do ponto de acesso do ambiente
	mask	Máscara de sub-rede do ponto de acesso
Schedule	id	Código identificador único do horário
	day	Dia
	entryTime	Hora de entrada
	exitTime	Hora de saída
	person	Pessoa atrelada ao horário
	ambient	Ambiente atrelado ao horário
Signup	id	Código identificador único do usuário administrador
	user	Nome do usuário
	password	Senha
	confirmPassword	Confirmação de senha (exigida no cadastro)
Login	id	Código identificador único do usuário logado
	user	Nome do usuário
	password	Senha

Fonte: Elaborada pelo autor.

Todas as entidades do banco de dados possuem uma chave primária única, representadas pelos atributos destacados como identificadores (círculos pretos) no modelo entidade relacionamento (Figura 11). A entidade *Schedule*, além disso, possui duas chaves estrangeiras, que relacionam o horário com o ambiente e a pessoa. Dessa forma, o sistema consegue entender em qual horário cada pessoa pode acessar cada ambiente através do relacionamento da entidade de horários com as entidades *Person* e *Ambient*. Abaixo (Figura 12), no modelo lógico do banco de dados, podemos visualizar esse relacionamento:

Figura 12: Modelo lógico do banco de dados do IF Access



Fonte: Elaborada pelo autor.

Neste modelo, as chaves estão representadas pelo ícone preto em formato de chave, e as chaves estrangeiras estão representadas pelo ícone verde, no mesmo formato.

5.1.3 *Deploy* da aplicação

Para que a aplicação pudesse ficar acessível através da internet, se fez necessário a implantação do sistema em um servidor *web*. Para tal, foram analisados os servidores gratuitos existentes, e o PythonAnywhere e o Heroku foram os candidatos a serem utilizados no IF Access.

O PythonAnywhere é um servidor gratuito voltado para a hospedagem na nuvem de sites desenvolvidos em Python. Servidores do tipo também são conhecidos como Platform as a Service (PaaS), por fornecerem a plataforma necessária para o desenvolvimento e entrega de aplicações *web*. Com total suporte ao Django, o PythonAnywhere é um servidor simples de hospedar, já que todo o ambiente Python já está configurado e pronto para utilização. Apesar disto, o servidor não fornece suporte ao protocolo de comunicação MQTT, indispensável para a comunicação da plataforma *web* do IF Access com os pontos de acesso através da rede. Por esta razão, o seu uso foi descartado, e o servidor *web* escolhido foi o Heroku[2].

O Heroku é um servidor *web* que faz parte da Salesforce Platform, e que assim como o PythonAnywhere, é também considerado uma PaaS. Esse servidor possui foco em desenvolvimento rápido para qualquer tipo de aplicação, possibilitando a implantação rápida através do seu deploy automático. O Heroku oferece suporte a diversas linguagens de programação, é escalável e trabalha com o banco de dados PostgreSQL, que pode ser totalmente integrado ao Salesforce Data. Um ponto importante é que esse servidor fornece suporte ao protocolo de comunicação MQTT, e por isso foi utilizado no IF Access.

Por se tratar de um trabalho inicial, e de uma proposta que pode ser melhorada no futuro, em novas versões, o IF Access utiliza um broker MQTT externo, no qual a aplicação hospedada no Heroku se conecta para realizar a troca de mensagens com os pontos de acesso. Porém, é possível instalar um servidor MQTT junto com o servidor *web*, na mesma plataforma, a fim de se aumentar a segurança do sistema.

5.2 ETAPA DE *HARDWARE*

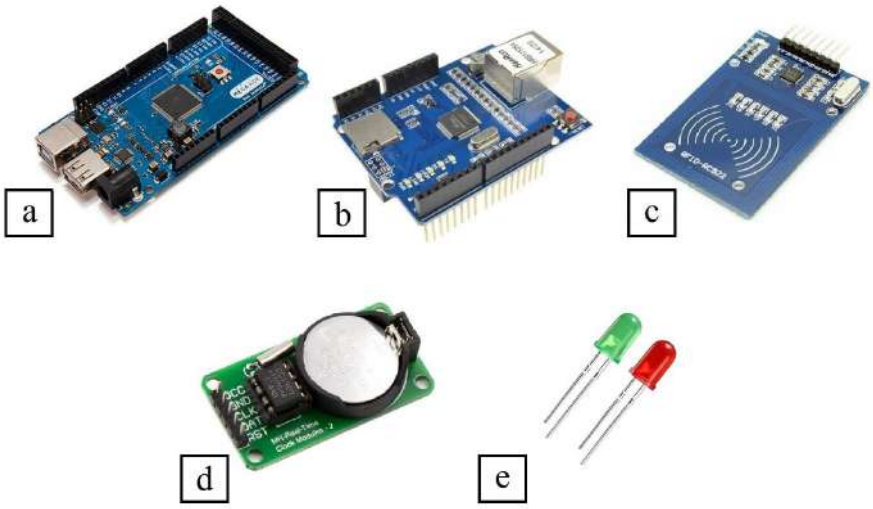
O sistema conta com a instalação de um ou mais pontos de acesso, integrados pelo *software* hospedado em um servidor *web*. Essa integração só é possível, dentre outros fatores, por causa do *hardware* empregado nos pontos de

[2] O sistema está disponível no seguinte endereço: https://ifaccess.herokuapp.com/. Para o primeiro acesso, é necessário realizar o cadastro em: https://ifaccess.herokuapp.com/signup.html.

acesso do projeto. Para se permitir ou não a entrada de pessoas nos ambientes mediante autenticação, se faz necessário o uso de um *hardware* que faça a abertura e o fechamento dos ambientes, bem como o reconhecimento do pessoal autorizado e a conexão dos pontos de acesso com o servidor.

O *hardware* pensado para o projeto envolve as tecnologias anteriormente citadas na seção 2 deste documento, que são as tecnologias RFID, microcontrolador e sistema embarcado, além de LEDs para representar o estado do acesso. Abaixo, na Figura 13, podemos ver o hardware utilizado no projeto para efetuar a autenticação dos usuários:

Figura 13. Hardware utilizado no IF Access. (a) Arduino Mega ADK. (b) Ethernet Shield W5100. (c) Leitor RFID MFRC522. (d) Relógio de Tempo Real RTC DS1302. (e) LEDs verde e vermelho.



Fonte: Elaborada pelo autor.

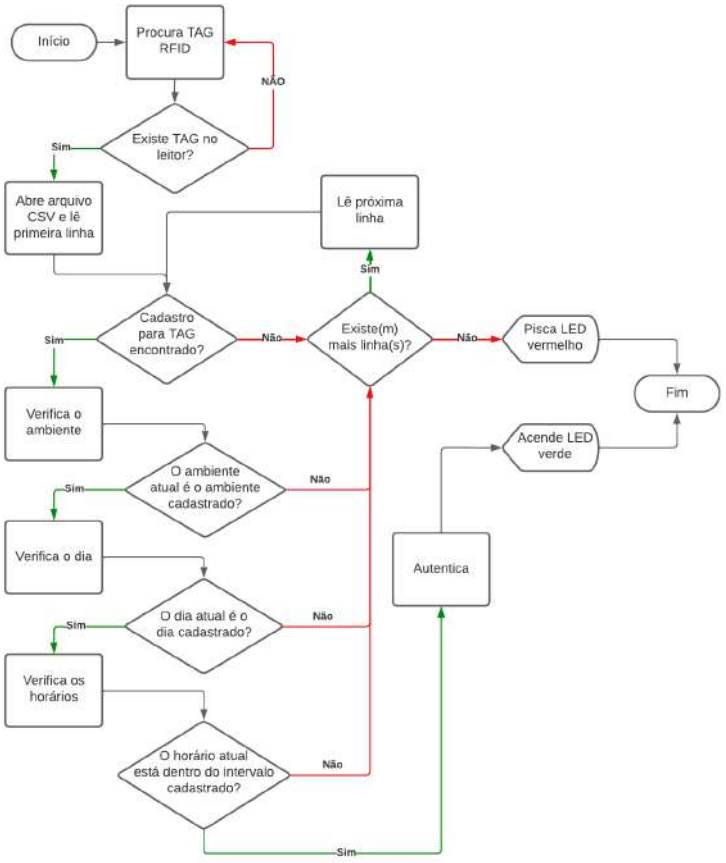
Cada usuário do sistema é equipado com uma *tag* RFID, de uso individual, que pode ser um cartão ou um chaveiro, conforme mostrados na Figura 14:

Figura 14. *Tags* RFID. (a) Cartão RFID. (b) Chaveiro RFID

Fonte: Elaborada pelo autor.

Essas tags são previamente configuradas no software hospedado no servidor web, com informações acerca do usuário proprietário da tag, como nome, CPF, matrícula e informações dos ambientes e horários em que o usuário pode acessar tais ambientes. Essas tags, uma vez configuradas, quando aproximadas do leitor RFID, são lidas pelo ponto de acesso, que verifica se determinado usuário tem permissão para acessar aquele ambiente naquele horário. Essas informações são enviadas pelo servidor web ao ponto de acesso durante a configuração, e ficam no mesmo permanentemente, até que uma nova configuração seja realizada. Tanto o hardware quanto o software foram pensados de forma a atender o especificado no diagrama de fluxo de autenticação apresentado na Figura 15 a seguir:

Figura 15: Diagrama de fluxo do processo de autenticação do IF Access



Fonte: Elaborada pelo autor.

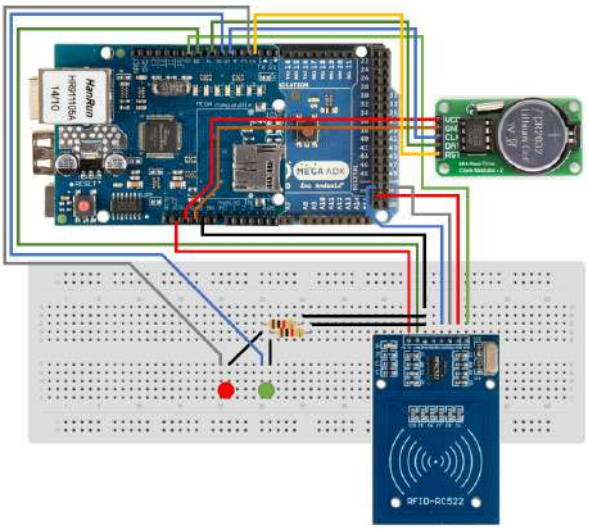
O Arduino, no projeto, opera com um sistema embarcado que é responsável por toda a lógica que tem como finalidade liberar ou não o acesso aos ambientes. No Arduino, um algoritmo efetua o confrontamento dos dados lidos pelo leitor RFID com as informações contidas em sua memória e checa se o usuário que tentou

efetuar a autenticação naquele momento está autorizado a entrar no ambiente. Uma vez autenticado, o Arduino sinaliza para o usuário se o acesso ao ambiente foi ou não liberado, através dos LEDs indicadores verde e vermelho.

5.2.1 Montagem do *hardware* do ponto de acesso

A montagem do ponto de acesso consistiu na junção de todos os elementos de hardware anteriormente descritos, utilizando a *protoboard* e fios, além de uma sólida base de madeira para fixar todas as peças. Para tal, foi utilizado o esquema de ligação dos fios descrito na Tabela 3. O esquemático de todo o circuito, evidenciando a ligação de todos os componentes e dos fios, pode ser visto na Figura 16 a seguir:

Figura 16. Esquemático do circuito do ponto de acesso



Fonte: Elaborada pelo autor.

Tabela 3. Ligação dos pinos dos componentes com os pinos do arduino

Componente	Pino do componente	Pino do Arduino
RFID	SDA	9
	SCK	52 (SCK)
	MOSI	51 (MOSI)
	MISO	50 (MISO)

	IRQ	Não utilizado
	GND	GND
	RST	8
	3.3V	3.3V
RTC	VCC	5V
	GND	GND
	CLK	5
	DAT	7
	RST	2
LEDs	+Vermelho	3
	-Vermelho	Resistor
	+Verde	6
	-Verde	Resistor
	Resistor	GND

Fonte: Elaborada pelo autor.

5.2.2 Software embarcado do projeto

O sistema embarcado utiliza a linguagem de programação Arduino, que é muito similar à linguagem de programação C++. O código fonte é responsável por especificar o comportamento e a interação do microcontrolador com seus respectivos periféricos. É neste código fonte que se encontram especificadas as instruções de funcionamento para o microcontrolador, para o módulo *Ethernet Shield*, para o leitor RFID e para os LEDs que indicam o estado da autenticação do usuário. O código embarcado do Arduino também encontra-se armazenado no repositório do sistema, no Github[3].

O código se utiliza de quatro bibliotecas: *MFRC522*, que disponibiliza, dentre outras, as funções de leitura e escrita de tags RFID; SPI, que especifica a

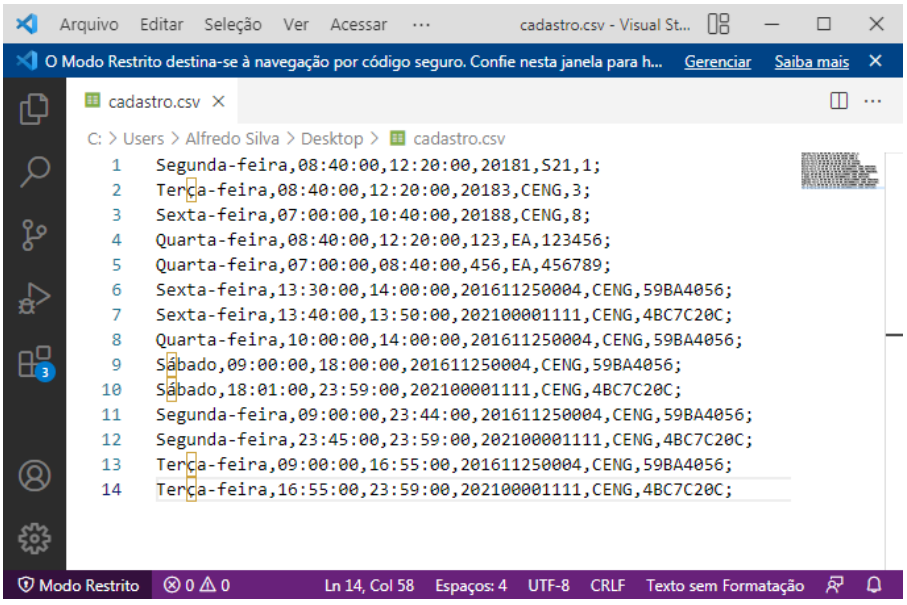
[3] O código utilizado pelo Arduino encontra-se no repositório do IF Access no Github, e pode ser acessado diretamente através do seguinte endereço: https://github.com/AlfredoRodrigo/IFAccess/tree/master/firmware/IF_ACCESS.

comunicação entre o microcontrolador e o leitor RFID, utilizando a interface SPI e o protocolo de comunicação SPI; *Ethernet*, que provê a comunicação entre o Arduino e a *Ethernet Shield*, bem como a comunicação de todo o ponto de acesso com a rede; SD, que provê as funções necessárias para a leitura e escrita em cartão de memória (utilizado para o armazenamento do arquivo CSV no Arduino); MQTT, que provê a comunicação do Arduino com o broker MQTT através da internet; e as bibliotecas ThreeWire, virtualbotixRTC e RtcDS1302, que provêm os métodos necessários para a utilização do módulo de relógio.

O código embarcado foi escrito de forma gradual, tendo sido desenvolvido primeiramente, o código de leitura da etiqueta RFID. O mesmo é responsável por integrar o leitor RFID ao Arduino, e permitir a comunicação entre os dois. Além disso, ele realiza a leitura da tag RFID, capturando o código enviado pela mesma, para posterior utilização na autenticação do usuário.

Em seguida, o módulo de cartão SD, contido no módulo Ethernet, foi integrado ao software. O mesmo acessa o cartão SD em busca do arquivo "cadastro.csv", que contém todas as informações necessárias para autenticação do usuário. Na Figura 17 abaixo, é possível observar um exemplo deste arquivo CSV gerado, onde constam os dados dos horários de acesso, com os nomes dos dias, os horários de entrada e de saída, a matrícula do usuário cadastrado, o código do ambiente e a tag RFID do usuário registrado, separados por vírgula:

Figura 17. Arquivo CSV gerado pelo sistema *web* do IF Access



Fonte: Elaborada pelo autor.

Após isto, o módulo RTC foi integrado ao sistema. O código inicializa o horário no relógio, atualizando o mesmo com a hora atual, sempre que o código é compilado no Arduino. A hora e a data ficam armazenadas no relógio mesmo quando não há aporte energético para o Arduino, pois o mesmo possui uma autonomia fornecida pela bateria de 3V, presente no módulo de relógio.

O módulo *Ethernet* foi o penúltimo a ser integrado ao ponto de acesso. O módulo *Ethernet* foi configurado na mesma faixa de IP da rede local, e submetido a um teste de conexão, utilizando o comando "ping" no prompt de comando do Windows. Esse comando envia pequenos pacotes para o endereço informado, e atesta o seu recebimento. Abaixo, na Figura 18, podemos ver um dos testes de ping realizados no Arduino:

Figura 18. Teste de ping, para testar a conexão do Arduino

Fonte: Elaborada pelo autor.

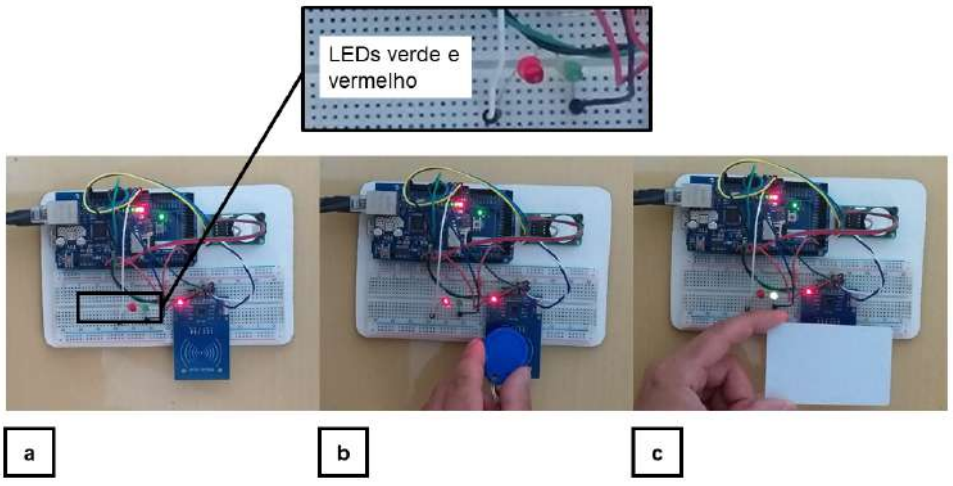
Como visto, o Arduino conseguiu se conectar à rede através do IP 192.168.0.200, tendo respondido positivamente aos testes de conexão realizados. Ao enviar quatro pacotes através da rede, o Arduino conseguiu recepcionar todos os quatro pacotes, tendo 0% de perda.

6 RESULTADOS

O IF Access se propôs como uma alternativa para modernizar o controle de acesso aos ambientes do campus, se valendo de um processo automático de autenticação, totalmente eletrônico, que oferece uma maior agilidade, praticidade e segurança às pessoas que utilizam esses ambientes. O IF Access mostra sua funcionalidade no controle de acesso quando consegue realizar com sucesso uma autenticação, utilizando a tag RFID e a leitura das regras de acesso dentro do arquivo CSV, em seu cartão SD. Além disso, se mostra funcional, também, quando consegue se conectar à rede e capturar as mensagens com as informações do acessos que a ele são endereçadas.

O sistema web do IF Access realiza com êxito o cadastro de seus usuários, bem como o cadastro de ambientes e de horários. Além disso, ele consegue os correlacionar, gerando de forma correta o arquivo CSV a ser enviado ao Arduino de cada ponto de acesso, com as informações necessárias para garantir a autenticação de cada usuário. Na Figura 19 a seguir, é possível observar o circuito do ponto de acesso totalmente montado, com o Arduino e todos os módulos necessários ao funcionamento do IF Access, e o comportamento de um dos testes realizados:

Figura 19. Circuito e testes realizados. (a) Demonstração do circuito pronto. (b) Teste com o chaveiro RFID não cadastrado. (c) Teste com o cartão RFID cadastrado



Fonte: Elaborada pelo autor.

Na realização dos testes com o hardware, de forma a simular uma situação real do comportamento do sistema, foi possível notar que o IF Access se comportou

da forma esperada, acendendo os LEDs correspondentes para representar as situações em que o usuário era ou não autenticado, com base nas regras contidas no arquivo CSV. Posteriormente, uma fechadura eletromecânica juntamente com um relé poderão ser integrados ao projeto, substituindo os LEDs que atualmente representam o funcionamento da mesma.

7 CONCLUSÃO

Como consequência do crescente número de pessoas que frequentam o IFPB Campus Campina Grande, surgiu uma maior circulação de pessoas no setor de distribuição de chaves a fim de conseguir acesso a algum ambiente da instituição, o que, no atual modelo de controle de acesso do campus, é uma situação suscetível a inúmeros problemas e falhas, além de não ser ágil e prático. Diante do exposto, se faz necessário a adoção de um sistema eletrônico de controle de acesso capaz de operacionalizar a logística de acessos aos ambientes do instituto. Neste trabalho, pudemos observar como se deu o desenvolvimento do projeto IF Access, transcorrendo por todas as etapas de desenvolvimento do sistema, abrangendo a fase do desenvolvimento do *software web*, bem como a etapa de montagem do *hardware* do ponto de acesso, com a utilização de todas as tecnologias anteriormente descritas, e da escrita do código do *software* embarcado no Arduino.

De acordo com os resultados obtidos, o sistema proposto atinge o objetivo almejado no desenvolvimento do projeto, resultando em um sistema de controle de acesso microcontrolado capaz de gerir as permissões de acesso dos usuários aos ambientes do Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Campus Campina Grande.

O projeto IF Access, além de fácil implementação e manutenção, fornece a garantia da segurança e agilidade que um controle de acesso deve ter, além de possuir um baixo custo e ser construído com a utilização de equipamentos de *hardware* que são de fácil aquisição no mercado, embarcado com um *software* de código aberto e totalmente escrito com ferramentas gratuitas, tornando o IF Access uma alternativa aos controles de acesso convencionais.

REFERÊNCIAS

ALVES, B. M. V. **Desenvolvimento de um sistema distribuído de controle de acesso por RFID com arquitetura sem servidor baseada em computação em nuvem**. 2019. 75p. Monografia (Trabalho de Conclusão de Curso)–Curso de Engenharia Elétrica, Universidade Federal de Campina Grande, Campina Grande, 2019.

ARAUJO, J. I. L. **Etiqueta RFID Passiva para Monitoramento da Frequência Respiratória**. 2018. 53p. Monografia (Trabalho de Conclusão de Curso)–Curso de Engenharia Elétrica, Universidade Federal de Campina Grande, Campina Grande, 2018.

ARDUINO. **Arduino Mega ADK Rev3**. [*S. l.*]: Arduino, 2022. Disponível em: <https://docs.arduino.cc/retired/boards/arduino-mega-adk-rev3>. Acesso em: 13 jul. 2022.

BARSOTTI, C. F.; RAHAL, E. J.; SILVA, M. C. **Análise dos Benefícios da Gestão de Estoque por Meio de Sensores RFID em um Contexto de Indústria**. 2020. 20p. Monografia (Trabalho de Conclusão de Curso)–Curso de Engenharia Civil, Universidade Presbiteriana Mackenzie, São Paulo, 2020.

BOPPRÉ, V. O. **Modelo para controle de acesso utilizando Internet das Coisas**. 2018. 72p. Monografia (Trabalho de Conclusão de Curso)–Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2018.

BRITO, T. **Mensageria**. [*S. l.*]: Medium, 2019. Disponível em: <https://medium.com/@devbrito91/mensageria-1330c6032049#:~:text=%E2%80%9C%20Mensageria%20%C3%A9%20um%20conceito%20que,%2Fm%C3%B3dulo%20de%20mensagens).%E2%80%9D>. Acesso em: 25 fev. 2022.

CASTILHO, L. H. dos S. **Estudo de Uma Solução para Monitoramento Remoto da Umidade de Solo por Meio da Tecnologia RFID e Sensores Capacitivos**. 2022. 106p. Dissertação (Pós-Graduação em Engenharia Elétrica e Informática Industrial)–Engenharia Elétrica, Universidade Tecnológica Federal do Paraná, Curitiba, 2022.

FREITAS, R. B. de. **Controle e Segurança Patrimonial por RFID no Departamento Acadêmico de Eletrônica da UTFPR Campo Mourão**. 2020. 75p. Dissertação (Pós-Graduação em Inovações Tecnológicas)–Inovações Tecnológicas, Universidade Tecnológica Federal do Paraná, Campo Mourão, 2020.

GONÇALVES, V. R. **Sistema de controle de acesso utilizando autenticação por RFID e gerenciamento por meio de software WEB**. 2019. 68p. Monografia (Trabalho de Conclusão de Curso)–Escola de Minas, Universidade Federal de Ouro Preto, Ouro Preto, 2019.

INTELBRAS. **Controlador de acesso 125kHz**. c2022. Disponível em: <https://www.intelbras.com/pt-br/controlador-de-acesso-125khz-digiprox-sa-202>. Acesso em: 11 ago. 2022.

_____. **Fechadura Smart de Sobrepor IFR 1001**. c2022. Disponível em: <https://loja.intelbras.com.br/fechadura-smart-de-sobrepor-ifr-1001/p>. Acesso em: 11 ago. 2022.

MAIA, G. Q. **Protótipo de Controle de Acesso Utilizando RFID para Automatização da Segurança Interna da UFERSA - Campus Mossoró**. 2019. 54p. Monografia (Trabalho de Conclusão de Curso)─Curso de Engenharia Elétrica, Universidade Federal Rural do Semi-Árido, Mossoró, 2019.

MOREIRA, M. M. P. C. *et al*. Contribuições do Arduino no Ensino de Física: Uma Revisão Sistemática de Publicações na Área do Ensino. **Caderno Brasileiro de Ensino de Física**, [*S. l.*], v. 35, n. 3, p. 721-745, 2018. Disponível em: <https://periodicos.ufsc.br/index.php/fisica/article/view/2175-7941.2018v35n3p721>. Acesso em: 16 jul. 2022.

MOURA, M. B. *et al*. Protótipo de um Dinamômetro de Baixo Custo para Medição de Força Muscular Utilizando Arduino. *In*: I Encontro de Computação do Oeste Potiguar - Pocket, 4., 2020, Mossoró. **Anais** [...]. Mossoró: UFERSA, 2020.

NASCIMENTO, M. G. **Eficiência da Tecnologia RFID na Área Comercial:** Interferências Eletromagnéticas. 2019. 22p. Monografia (Trabalho de Conclusão de Curso)─Curso de Engenharia Elétrica, Universidade Presbiteriana Mackenzie, São Paulo, 2019.

PADO. **Fechadura Digital Biométrica de Embutir FDE-101 Rolete Magnético**. c2022. Disponível em: <https://www.lojapado.com.br/fechadura-digital-biometrica-de-embutir-fde-101-rolete-magnetico/p>. Acesso em: 11 ago. 2022.

RIBEIRO, D. G. *et al*. Sistema de Controle de Acesso de Ambientes Integrando Tecnologia RFID e Raspberry. *In*: **IV Congresso de Educação Profissional e Tecnológica do IFSP**. 2018.

RODRIZ, L. D.; RODRIGUES, T. S. **Sistema de Controle de Acesso Veicular à Vaga Especial Utilizando Tecnologia RFID**. 2018. 89p. Monografia (Trabalho de Conclusão de Curso)─Curso de Engenharia Elétrica, Instituto Federal de Educação, Ciência e Tecnologia de Goiás, Jataí, 2018.

RUTTMANN, M. E. **Protótipo de um Dispositivo Gerenciador de Equipamentos Via Ethernet para Economia de Energia**. 2018. 63p. Monografia (Trabalho de Conclusão de Curso)─Curso de Ciência da Computação, Universidade Regional de Blumenau, Blumenau, 2018.

SANTOS, B. S. *et al*. Automação de Casas e Estabelecimentos Comerciais Através de Microcontroladores: Uma Revisão da Aplicabilidade do Arduino. **Revista Tecnológica da Fatec Americana**, Americana, v. 8, n. 2, p. 70-80, 2020.

SOUZA, L. G. *et al*. O Uso do Arduino para o Estudo de Circuitos do Tipo RC. **Conexões - Ciência e Tecnologia**, [*S. l.*], v. 15, p. 1-10, 2021. Disponível em: <http://www.conexoes.ifce.edu.br/index.php/conexoes/article/view/1914/1551>. Acesso em: 13 jul. 2022.

SOUZA, L. I. *et al*. Automatização do Controle de Acesso a Portaria na Entrada e Saída de Veículos nas Dependências da Empresa. **Tekhne e Logos**, v. 11, n. 1, p. 60-68, 2020.

TUYA. **Fingerprint Electronic Touchscreen Keypad Smart Lock**. c2022. Disponível em: <https://expo.tuya.com/product/866103>. Acesso em: 11 ago. 2022.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
Campus Campina Grande
R. Tranqüilino Coelho Lemos, 671, Dinamérica, CEP 58432-300, Campina Grande (PB)
CNPJ: 10.783.898/0003-37 - Telefone: (83) 2102.6200

Documento Digitalizado Ostensivo (Público)

Trabalho de Conclusão de Curso

Assunto: Trabalho de Conclusão de Curso
Assinado por: Alfredo Silva
Tipo do Documento: Anexo
Situação: Finalizado
Nível de Acesso: Ostensivo (Público)
Tipo do Conferência: Cópia Simples

Documento assinado eletronicamente por:

- **Alfredo Rodrigo Sousa da Silva**, **ALUNO (201611250004) DE BACHARELADO EM ENGENHARIA DE COMPUTAÇÃO - CAMPINA GRANDE**, em 23/09/2022 13:51:07.

Este documento foi armazenado no SUAP em 23/09/2022. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 633583
Código de Autenticação: f5381c859a