



UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE TECNOLOGIA
GRADUAÇÃO EM ENGENHARIA MECATRÔNICA

RAPHAEL GUEDES SPINELLI

**DESENVOLVIMENTO DE UM SISTEMA DE SEGURANÇA
E CONTROLE DE ACESSO**

NATAL
2018

RAPHAEL GUEDES SPINELLI

**DESENVOLVIMENTO DE UM SISTEMA DE SEGURANÇA
E CONTROLE DE ACESSO**

Trabalho de Conclusão de Curso
apresentado ao curso de Engenharia
Mecatrônica da Universidade Federal do Rio
Grande do Norte como parte dos requisitos
para a obtenção do título de Engenheiro
Mecatrônico.

Orientador: ORIVALDO VIEIRA DE SANTANA
JUNIOR

NATAL

2018



UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE TECNOLOGIA
GRADUAÇÃO EM ENGENHARIA MECATRÔNICA

**DESENVOLVIMENTO DE UM SISTEMA DE SEGURANÇA
E CONTROLE DE ACESSO**

RAPHAEL GUEDES SPINELLI

Banca Examinadora do Trabalho de Conclusão de Curso

ORIVALDO VIEIRA DE SANTANA JUNIOR
Universidade Federal do Rio Grande do Norte - Orientador

SAMAHERNI MORAIS DIAS
Universidade Federal do Rio Grande do Norte - Avaliador Interno

MARCOS OLIVEIRA DA CRUZ
Universidade Federal do Rio Grande do Norte - Avaliador externo

NATAL

2018

RESUMO

A crescente presença da Internet no dia a dia das pessoas nos últimos anos, além dos avanços tecnológicos em várias áreas como sistemas embarcados, microeletrônica, comunicação e sensoriamento, favoreceram a construção de equipamentos automatizados conectados e gerenciados pela web.

Essa monografia propõe o desenvolvimento de um sistema de segurança e controle de acesso, utilizando a tecnologia de comunicação sem fio “RFID (Radio Frequency IDentification, em português Identificação por Radiofrequência)”, a placa de prototipagem eletrônica NodeMCU da família do ESP8266 e a elaboração uma aplicação web para controle e gerenciamento remoto do sistema baseada em Python com auxílio do framework Django.

O intuito do desenvolvimento de tal sistema é a montagem de uma versão protótipo para a implantação do mesmo em diversos setores do mercado, com o objetivo de registrar as tentativas de acesso a áreas restritas, impedir o acesso de pessoas não autorizadas, facilitar e agilizar o acesso das pessoas que possuem autorização, uma vez que a tecnologia RFID não necessita de contato ou até mesmo visada direta (entre o dispositivo leitor e o identificador de cada usuário) para autenticar, autorizar, registrar e liberar ou não o acesso dos usuários. Para tal, foi desenvolvido uma versão de protótipo e com a realização dos testes foi possível comprovar a viabilidade da implantação do sistema, bem como sua facilidade de utilização.

Palavras-Chave: Automação, IoT, RFID, sistemas embarcados, NodeMCU, ESP8266, Django.

ABSTRACT

The increasing presence of the Internet in people's daily lives in recent years, besides the technological advances in several areas such as embedded systems, microelectronics, communication and sensing, favored the construction of automated equipment connected and managed by web.

This work proposes the development of a security and access control system, using the wireless communication technology "RFID" (Radio Frequency Identification), the electronics prototyping board NodeMCU model ESP8266 and the development of a Python based web application for the control and remote management of the system, using Django framework.

The goal of such system's development is to implement it in several market sectors, allowing recording attempts to access restricted areas, preventing access by unauthorized persons, facilitating and making easier the access with authorized personnel, since RFID technology does not require direct contact or even visualization between the reader device and the identifier of each user to authenticate, authorize, register and release or deny user access. For this, a prototype version was developed and with the tests, it was possible to show the feasibility of the system, as well as its ease of use.

Keywords: Automation, IoT, RFID, embedded systems, NodeMCU, ESP8266, Django.

LISTA DE FIGURAS

FIGURA 2.1.1 - Subdivisões de um sistema embarcado	11
FIGURA 2.2.1.1 - Estrutura típica de um transponder.	12
FIGURA 2.2.1.2 - Diagrama geral de um sistema de Identificação por Rádio Freqüência.	12
FIGURA 2.2.2.1 - Modelos diferentes de transponders	13
FIGURA 2.2.2.2 - Diferentes leitores RFID.	14
FIGURA 2.3.1 - Volume de pesquisas no Google sobre Wireless Sensor Networks e Internet of Things.	15
FIGURA 2.3.2 - Evolução da Internet em 5 fases.	16
FIGURA 2.3.3 - Smart idea.	16
FIGURA 2.3.4 - Tecnologias emergentes.	17
FIGURA 2.4.1 - Exemplo de URL.	18
FIGURA 2.4.2 - Solicitação e resposta para uma página web	18
FIGURA 2.5.1 - Flexibilidade da aplicação web	19
FIGURA 3.1.1 - Cartões para controle de acessos MIFARE.	20
FIGURA 3.1.2 - Leitor RFID Mfrc522 (13,56MHz)	21
FIGURA 3.2.1.1 - FAMÍLIA ARDUINO	23
FIGURA 3.2.1.2 - Diversos componentes da placa Arduino UNO.	24
FIGURA 3.2.2.1 - Família ESP8266.	25
FIGURA 3.2.2.2 - Placas de desenvolvimento ESP8266.	25
FIGURA 3.3 - IDE ARDUINO.	29
FIGURA 3.4.1.1 - Módulo Relé.	29
FIGURA 3.4.1.1 - Funcionamento de relés:	29
FIGURA 3.4.2 - Exemplos de fechaduras elétricas.	30
FIGURA 3.5.1 - Django.	31
FIGURA 4.1.1 - Fluxo do projeto.	32
FIGURA 4.2.1 - Protótipo do projeto.	33
FIGURA 4.2.2 - Esquemático do projeto.	33
FIGURA 4.2.3 - Esquema de instalação do protótipo.	34
FIGURA 4.2.4 - O controlador.	34
FIGURA 4.2.5 - O leitor.	35
FIGURA 4.3.1 - Wifi manager para NodeMCU.	36
FIGURA 4.3.2 - Funcionamento da requisição de acesso.	36
FIGURA 4.4.1 - Funcionamento do controlador de acessos da aplicação web “Unlock”.	38
FIGURA 4.4.2 - Index do sistema.	38
FIGURA 4.4.3 - Tela de Login do sistema.	39
FIGURA 4.4.4 - Tela do usuário.	39
FIGURA 4.4.5 - Tela de controle dos usufrutuários.	40
FIGURA 4.4.6 - Tela de dados do usufrutuário.	40
FIGURA 4.4.7 - Tela de controle dos dispositivos.	41

FIGURA 4.4.8 - Tela de dados do dispositivo.	41
FIGURA 4.4.9 - Tela de criação de relatório.	42
FIGURA 4.4.10 - Tela de relatório.	42
FIGURA 4.4.11 - DER da aplicação web.	43
FIGURA 5.1 - Protótipo em funcionamento.	44
FIGURA 5.2 - Confirmação de funcionamento do sistema no relatório da aplicação “Unlock”.	45
FIGURA 5.3 - Confirmação de funcionamento da função de bloqueio.	45
FIGURA 5.4 - Realização do bloqueio para teste de funcionamento da função de bloqueio.	46
FIGURA 5.5 - Relatório da confirmação de funcionamento da função de bloqueio.	46
FIGURA 5.6 - Confirmação do teste de estresse.	46

SUMÁRIO

1 INTRODUÇÃO	8
1.1 MOTIVAÇÃO, OBJETIVO E CARACTERIZAÇÃO DO PROBLEMA	8
1.2 ETAPAS	9
1.3 ORGANIZAÇÃO DO DOCUMENTO	9
2 REVISÃO BIBLIOGRÁFICA	10
2.1 SISTEMAS EMBARCADOS	10
2.2 TECNOLOGIA RFID	11
2.2.1 DEFINIÇÃO E FUNCIONAMENTO	11
2.2.2 COMPONENTES RFID	13
a) Transponder ou Tag	13
b) Transceptor ou Leitor	14
2.3 INTERNET DAS COISAS (Internet of Things - IoT)	15
2.4 COMUNICAÇÃO CLIENTE/SERVIDOR HTTP	17
2.5 APLICAÇÕES WEB	19
3 EQUIPAMENTOS E SOFTWARES UTILIZADOS	20
3.1 - TECNOLOGIA DE IDENTIFICAÇÃO - RFID	20
3.1.1 - TRANSPOUNDER E TAGS	20
3.1.2 - TRANSCECTOR E LEITOR	21
3.1.3 - COMPARAÇÃO COM OUTRAS TECNOLOGIAS DE IDENTIFICAÇÃO	21
3.2 MICROCONTROLADOR	23
3.2.1 ARDUINO	23
3.2.2 ESP8266	24
3.2.3 COMPARAÇÃO ENTRE AS FAMÍLIAS DE MICROCONTROLADORES	26
3.3 IDE ARDUINO	27
3.4 ATUADORES	28
3.4.1 - RELÉ	28
3.4.2 - FECHADURA ELÉTRICA OU FECHO ELÉTRICO	29
3.5 - SOFTWARE UTILIZADO NO DESENVOLVIMENTO DA APLICAÇÃO WEB	30
3.5.1 - DJANGO	30
4 DESENVOLVIMENTO DO PROJETO	32
4.1 FLUXO DO PROJETO	32
4.2 HARDWARE	32
4.3 PROGRAMAÇÃO DO HARDWARE	35
4.4 SOFTWARE “UNLOCK”	37
5 RESULTADOS	44
6 CONCLUSÃO	48
7 BIBLIOGRAFIA	49

1 INTRODUÇÃO

Este trabalho aborda a elaboração de um sistema de controle de acesso utilizando a tecnologia RFID (Radio Frequency Identification, em português Identificação por Radiofrequência), conceitos a respeito de IoT (Internet of Things) e sistemas embarcados, além do desenvolvimento de um aplicação web para gerenciamento e controle do sistema. Este projeto foi desenvolvido com o intuito de ser implementado em diversos setores do mercado, com a finalidade de sobrepor o uso antiquado de chaves que muitas vezes são perdidas, quebradas e copiadas gerando transtornos, além de melhorar alguns aspectos em relação à segurança, uma vez que devia facilitar a entrada de pessoas autorizadas a setores restritos e bloquear o acesso de pessoas não autorizadas.

Este capítulo apresenta a introdução deste trabalho de conclusão de curso, e está organizado em três seções. Na Seção 1.1 é apresentada a motivação para o desenvolvimento do sistema de controle de acesso, bem como a caracterização do problema em questão. Na Seção 1.2 são apresentadas as etapas do desenvolvimento do sistema e na Seção 1.3 é descrita a estrutura do restante do trabalho.

1.1 MOTIVAÇÃO, OBJETIVO E CARACTERIZAÇÃO DO PROBLEMA

A preocupação com a segurança vem crescendo mundialmente, e os investimentos relacionados a ela aumentando consideravelmente, principalmente em empresas, estabelecimentos comerciais e condomínios residenciais. Isso se deve, em grande parte, ao crescimento também dos artifícios utilizados por criminosos para ter acesso a bens privados e/ou locais aos quais não possuem permissão para entrar. Como forma de prover segurança, uma importante estratégia consiste no controle do acesso de pessoas a determinados locais, controle este que pode ser feito através de inúmeras tecnologias. Dentre as tecnologias utilizadas estão cartões magnéticos, biometria, código de barras, alarmes de detecção, softwares de monitoramento, tecnologias de automação, entre outras.

Hoje grande parte das instituições ainda possuem sistemas de controle de acesso primitivos, baseados na utilização de grandes quantidades de chaves e molhos de chaves. Tal sistema possui diversas desvantagens, como por exemplo a necessidade de se trocar fechaduras de tempos em tempos em casos de perda, cópias ilegais ou rompimento das chaves, além da dificuldade de se encontrar chaves específicas em grandes molhos pesados com diversas delas, estendendo o tempo para acesso a áreas restritas e gerando transtornos.

O projeto desenvolvido neste trabalho tem como principal motivação melhorar a segurança, facilitar e agilizar esse controle de acesso, e para tal será utilizada a RFID, ou Identificação por Radiofrequência, que é uma tecnologia sem fio destinada a coleta de dados e que se assemelha ao código de barras, conceitos a respeito de IoT (Internet of Things) e sistemas embarcados, além do desenvolvimento de um aplicação web para gerenciamento remoto e controle do sistema a ser desenvolvido, que disponibilize ao usuários adaptar o sistema às necessidades da instituição, como a seleção das pessoas que terão acesso a determinadas áreas restritas e o bloqueio de quem não faz mais parte daquele grupo que tem acesso.

1.2 ETAPAS

O desenvolvimento de um projeto de controle de acesso possui várias etapas, dentre elas, a fase de análise das tecnologias existentes no mercado para encontrar a melhor solução que atenda as necessidades, a condição financeira e a infraestrutura da instituição na qual será implantado o projeto; A seleção dos mecanismos físicos que em conjunto com o sistema tecnológico, possibilita liberar ou não o acesso de usuários como cancelas, catracas, portas, cadeados, trancas, travas, entre outros; Estudo dos possíveis meios de controle e gerenciamento do sistema proposto; E por fim, a elaboração de um protótipo funcional que atenda aos objetivos desejados.

1.3 ORGANIZAÇÃO DO DOCUMENTO

Este trabalho está organizado em 7 capítulos; No Capítulo 2 são abordados alguns conceitos importantes acerca das tecnologias utilizadas para uma melhor compreensão do sistema desenvolvido; No capítulo 3 são apresentados os equipamentos e softwares utilizados na elaboração do projeto assim como suas principais características; No capítulo 4 é abordado como o protótipo foi desenvolvido desde sua montagem ao seu funcionamento, bem como o fluxo de etapas como cada componente deve funcionar para que a tarefa proposta neste projeto seja realizada; No capítulo 5 são ressaltados os resultados do projeto e comprovado seu funcionamento através de testes; No capítulo 6 se dá a conclusão do projeto com base nas análises de testes realizados no protótipo; E por fim, no capítulo 7 são dadas as referências utilizadas na confecção deste trabalho.

2 REVISÃO BIBLIOGRÁFICA

2.1 SISTEMAS EMBARCADOS

A segunda metade do século XX foi marcada por diversos avanços tecnológicos que mudaram os hábitos e a forma como humanidade se comportava, um dos principais responsáveis por esse salto tecnológico, foi o barateamento da produção de circuitos integrados para o desenvolvimento de microcontroladores.

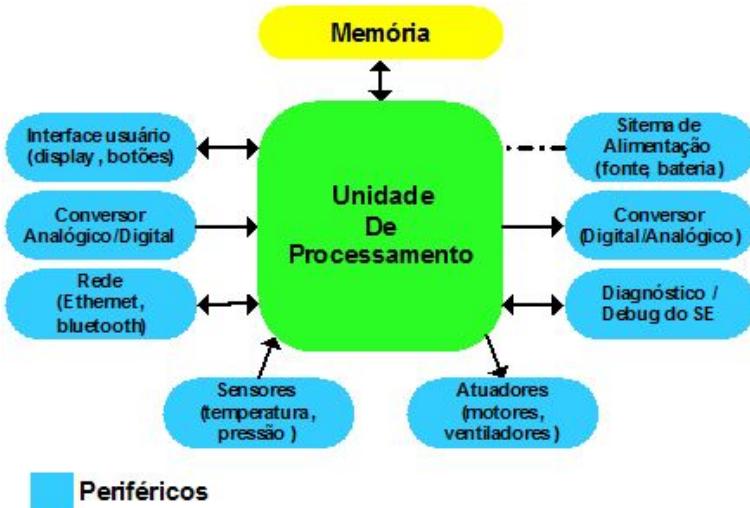
Em meados de 1980, com o custo dos microcontroladores abaixo de um dólar americano, tornou-se viável a substituição de caros componentes analógicos como capacitores e potenciômetros pela eletrônica digital controlada por pequenos microcontroladores. Nos anos seguintes, os sistemas embarcados já eram norma ao invés de exceção em dispositivos eletrônicos presentes no mercado, além de largamente utilizados na indústria e altamente estudados nas instituições de pesquisa.

Existem diversas definições para designar o significado de sistemas embarcados, também nomeados sistemas embutidos, embora a maioria convirja para mesma premissa básica, segundo Marwedel (2011), sistema embarcado é um dispositivo no qual um sistema computacional é completamente encapsulado ou dedicado ao dispositivo ou equipamento que ele controla. Diferentemente de computadores de propósito geral, como o computador pessoal, um sistema embarcado realiza um conjunto de tarefas predefinidas, geralmente com requisitos específicos e restrições de memória, tamanho, energia e número limitado de funções, tendo-se assim que otimizar o projeto reduzindo seu tamanho, recursos computacionais e custo. Ou seja, o microcontrolador é um pequeno computador do tipo SoC (**S**ystem **o**n **C**hip), em que, um único circuito integrado inclui um núcleo de processador, memórias e periféricos programáveis de entrada e saída (FIGURA 2.1.1).

Em contraste aos microprocessadores utilizados em computadores pessoais, os microcontroladores são concebidos por uma demanda de aplicações embarcadas, ao se reduzir o tamanho e o custo, tornando-os econômicos e simples para automatizar e controlar digitalmente dispositivos e processos, como os sistemas de controle de automóvel, controles remotos, máquinas de escritório, dispositivos médicos, eletrodomésticos, brinquedos e outros sistemas embarcados.

Visto isso, o objetivo de um sistema embarcado é controlar processos, ou seja, atuar sobre um problema, que pode ir desde um simples acender e apagar de lâmpada automatizado ou controlar o tempo de funcionamento do microondas, até o gerenciamento autônomo de uma aeronave. Tudo isso é feito por intermédio dos periféricos, que devem ser escalados e dimensionados com base no problema alvo (FIGURA 2.1.1).

FIGURA 2.1.1 - Subdivisões de um sistema embarcado



FONTE: DELAI, (2013).

2.2 TECNOLOGIA RFID

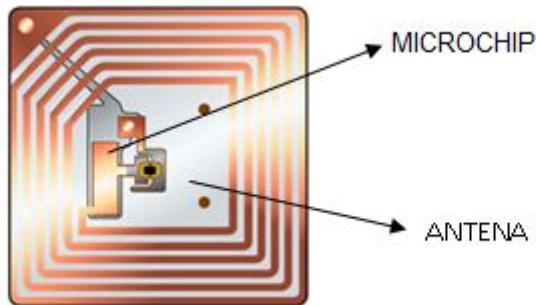
Nesta seção serão expostos conceitos inerentes à tecnologia RFID indispensáveis para um melhor entendimento do sistema desenvolvido. Na Seção 2.2.1 será apresentada a definição da tecnologia e suas características, assim como seu funcionamento, já na seção 2.2.2 serão apresentados seus principais componentes isoladamente.

2.2.1 DEFINIÇÃO E FUNCIONAMENTO

O RFID (Radio-Frequency IDentification) é um recurso de identificação automática sem fio, que utiliza a radiofrequência para receber e armazenar dados, através de instrumentos denominados etiquetas RFID.

Essa etiqueta RFID, também denominada de tag RFID, é um transponder que, constituído por chips de silício e antenas, como pode-se observar na Figura 2.2.1.1, lhe possibilita responder aos sinais de rádio enviados por uma base transmissora.

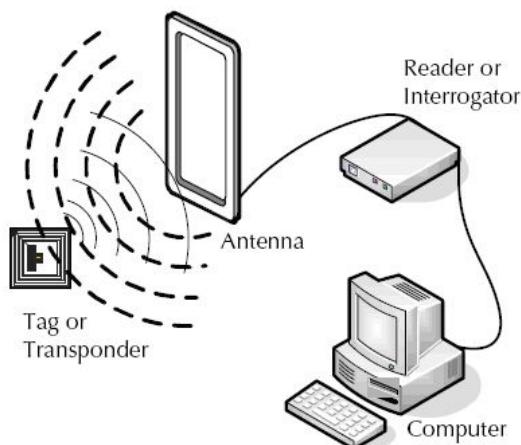
FIGURA 2.2.1.1 - Estrutura típica de um transponder.



Disponível em: <<http://www.roisoft.com.br/solucoes/roi-rfid>> Acesso em Maio. 2018.

O princípio de funcionamento dessa tecnologia, ilustrado na Figura 2.2.1.2, consiste na transmissão de ondas de radiofrequência emitidas através de um transceptor, para o transponder, a tag (etiqueta) RFID. O transponder recebe a onda de radiofrequência e responde com dados que podem ser gerenciados por um sistema computacional, ligado à base transmissora que recebeu esses dados, transformando-os em informação (Portal Teleco).

FIGURA 2.2.1.2 - Diagrama geral de um sistema de Identificação por Rádio Freqüência.



Disponível em:
<https://qperito.wordpress.com/2015/06/17/queira-o-sr-perito-comentar-como-o-rfid-tem-evoluído-e-ajudado-o-setor-jurídico/> Acesso em Maio. 2018.

Segundo Pinheiro(2006), dentre as principais características da tecnologia RFID, podemos citar a alta confiabilidade, boa segurança em operações repetitivas, alta disponibilidade no mercado, baixo custo de manutenção, boa resistência mecânica e alta vida útil dos equipamentos e tags, grande diversidade de equipamentos, portabilidade e alta proteção das etiquetas, não necessidade de contato visual para realizar leitura, leitura em movimento, leitura simultânea de várias tags, campo de leitura circular e possibilidade de operação em ambientes hostis.

2.2.2 COMPONENTES RFID

Para um melhor entendimento sobre a tecnologia RFID, é necessário compreender as funções de cada uma de suas partes constituintes. Como citado anteriormente, os sistemas RFID são compostos basicamente por três elementos: transceptor ou leitor e transponder ou tag (etiqueta).

a) Transponder ou Tag

O termo transponder, derivado da expressão TRANSmitter/resPONDER, denota a função do componente, que é de responder ao transmissor com um dado ou informação carregado na tag (etiqueta).

Esse componente apresenta-se disponível no mercado em diversos formatos (pastilhas, argolas, cartões, entre outros), tamanhos e materiais de encapsulamento (plástico, vidro, epóxi, pvc, resina, entre outros), como pode ser visto na Figura 2.2.2.1. Essas características são definidas de acordo com o ambiente de uso e a aplicação, que pode ir desde a identificação de animais, a controle de acesso de usuários em empresas e monitoramento de mercadorias por transportadoras.

FIGURA 2.2.2.1 - Modelos diferentes de transponders



Disponível em: <<https://br.pinterest.com/pin/150378075036654283>> Acesso em Maio. 2018.

Os transponders podem ser classificadas em ativos ou passivos. Os ativos são sustentados por uma bateria interna e comumente permitem processos de leitura e escrita na memória. Já as tags passivas atuam sem bateria, e sua alimentação é fornecida indutivamente através das ondas eletromagnéticas (radiofrequência), que são emitidas pelo leitor RFID, o transceptor (PINHEIRO, 2006).

Usualmente, as tags passivas possuem apenas memórias do tipo ROM (***Read Only Memory***, em português, Memória Só de Leitura), que possuem um

código pré-gravado de fábrica e não podem ser alterados. O custo dos modelos passivos é bem inferior, e tem uma vida útil bem mais elevada, quando comparados aos modelos ativos.

b) Transceptor ou Leitor

O transceptor é o equipamento que efetua a comunicação entre a etiqueta RFID e o sistema computacional que processa a informação, como pode ser visto na Figura 2.2.2.2.

Ele opera pela emissão de um sinal de radiofrequência, que através da indução eletromagnética alimenta a fonte de energia do microchip do transponder passivo. Quando a tag passa pela área de cobertura da antena do transceptor, o campo magnético é detectado pelo leitor, e então, a etiqueta responde ao leitor o conteúdo de sua memória. Assim, o transceptor recebe os dados que estão na tag, e em seguida, encaminha-os a um sistema computacional para se realizar a decodificação dos dados e o processamento da informação.

FIGURA 2.2.2.2 - Diferentes leitores RFID.



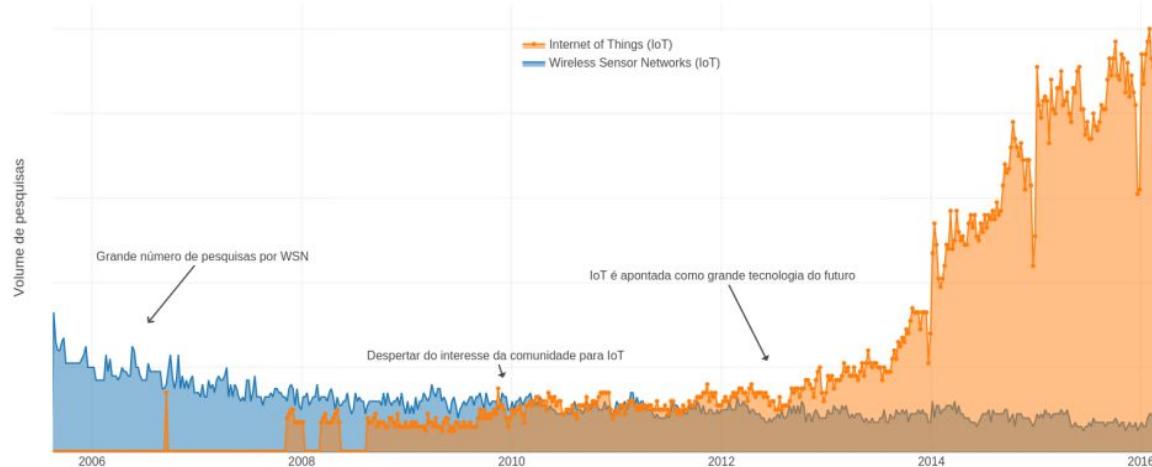
Disponível em: <<http://sparkag.com.br/produtos/rfid/>> Acesso em Maio. 2018.

Essa emissão de radiofrequência do transceptor ocorre em diversos sentidos no espaço, conforme o tipo de leitor essa distância pode variar desde alguns centímetros, até alguns metros, e depende de fatores como o tipo do transponder (ativo ou passivo), tamanho da antena, potência do leitor, frequência de rádio utilizada, entre outros. Os transceptores variam muito na sua complexidade, dependendo do tipo de tag e das funções a serem aplicadas, além disso, não necessitam de contato visual com as tags para realizar a leitura dos dados, tal leitura pode ser realizada através de vários materiais como madeira, plástico, papel, tecido, entre outros.

2.3 INTERNET DAS COISAS (Internet of Things - IoT)

De acordo com (SANTOS, et al., 2016), através dos avanços das tecnologias nos últimos anos, principalmente nas áreas de sistemas embarcados, microeletrônica, comunicação e sensoriamento, surgiu a ideia de se conectar o meio físico ao virtual, o que recebeu o nome de Internet das Coisas (Internet of Things – IoT) (FIGURA 2.3.1). Segundo Valente (2011), é uma concepção que tem como objetivo criar pontes entre acontecimentos do mundo real e as suas representações no mundo digital, através de conexões de objetos físicos com a internet.

FIGURA 2.3.1 - Volume de pesquisas no Google sobre Wireless Sensor Networks e Internet of Things.



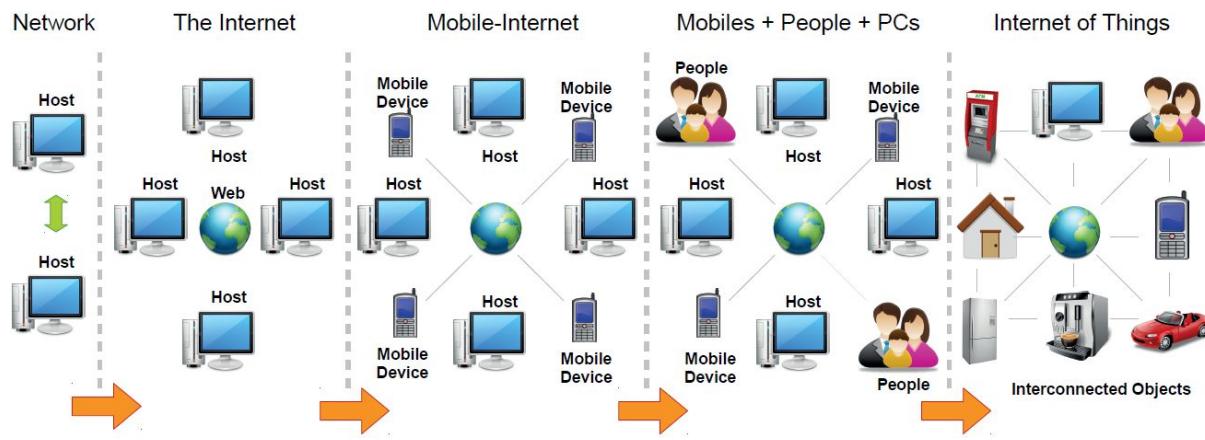
FONTE: SANTOS, et al. (2016).

Assim, podemos caracterizar a Internet das Coisas como uma rede de objetos físicos, veículos, espaços, estruturas e outras “coisas” que possuem tecnologias embarcadas, sensores e atuadores, conectados com a rede, capazes de coletar e transmitir dados.

Conforme Sérgio de Oliveira, “Internet das Coisas é muito mais que apenas ligar lâmpadas pelo smartphone. Não é somente ligar as “coisas” pela internet, mas também torná-las inteligentes, capazes de coletar e processar informações do ambiente ou das redes às quais estão conectadas.”(DE OLIVEIRA, 2017, p. 17).

Por conta disso, pode-se notar que a IoT tem alterado ainda mais o conceito de redes de computadores, segundo (KUROSE, 2012), o termo “Redes de Computadores” passou a soar um tanto envelhecido devido à grande quantidade de equipamentos e tecnologias não tradicionais que são usadas na Internet (FIGURA 2.3.2).

FIGURA 2.3.2 - Evolução da Internet em 5 fases.



FONTE: PERERA (2014).

Esses objetos inteligentes possuem papel fundamental na evolução acima mencionada, pois possuem a capacidade de comunicação e processamento aliados a sensores e atuadores, aprimorando suas utilidades. Nesse contexto, não somente mais computadores convencionais, laptops e smartphones estão conectados à grande rede, como também uma grande heterogeneidade de equipamentos tais como TVs, automóveis, consoles de jogos, câmeras, eletrodomésticos, brinquedos e a lista aumenta a cada dia. Neste novo cenário, a pluralidade é crescente e segundo a Forbes (Press, 2014), previsões indicam que mais de 40 bilhões de dispositivos estarão conectados até 2020.

Concomitantemente, uma gama de novas possibilidades de aplicações surgem como as cidades inteligentes (Smart Cities), na saúde (Healthcare) e casas inteligentes (Smart Home) (FIGURA 2.3.3), assim como desafios emergentes nas regulamentações, na segurança e padronização.

FIGURA 2.3.3 - Smart idea.



Disponível em: <<http://www.sinobusiness.dk/smart-city-smart-home/>> Acesso em Maio. 2018.

De modo geral, os desafios impostos por essas novas aplicações devem ser explorados e soluções necessitam ser propostas para que a Internet das Coisas conte com as expectativas de um futuro próximo como previsto na FIGURA 2.3.4.

FIGURA 2.3.4 - Tecnologias emergentes.



FONTE: SANTOS, et al. (2016).

Por fim, vários autores apontam que a IoT será a nova revolução da tecnologia da informação, se a poucos anos atrás embarcar inteligência em equipamentos era a tendência do presente, conectá-los será a tendência do futuro.

2.4 COMUNICAÇÃO CLIENTE/SERVIDOR HTTP

O protocolo HTTP (HyperText Transfer Protocol em português Protocolo de Transferência de Hipertexto) é o protocolo de comunicação mais utilizado na internet desde 1990 e funciona como uma sequência de transações de rede requisição-resposta no modelo computacional cliente-servidor. Por exemplo, um navegador web, cliente, e uma aplicação web hospedada em um sítio web, o servidor.

O cliente, através de uma URL FIGURA 2.4.1, remete uma mensagem de requisição HTTP para um servidor, que fornece recursos como arquivos HTML, ou realiza outras funções de interesse do cliente, e assim, retorna uma mensagem resposta para esse cliente, contendo informações de estado completas sobre a requisição e também podendo conter o conteúdo solicitado no corpo de sua mensagem (FIGURA 2.4.2).

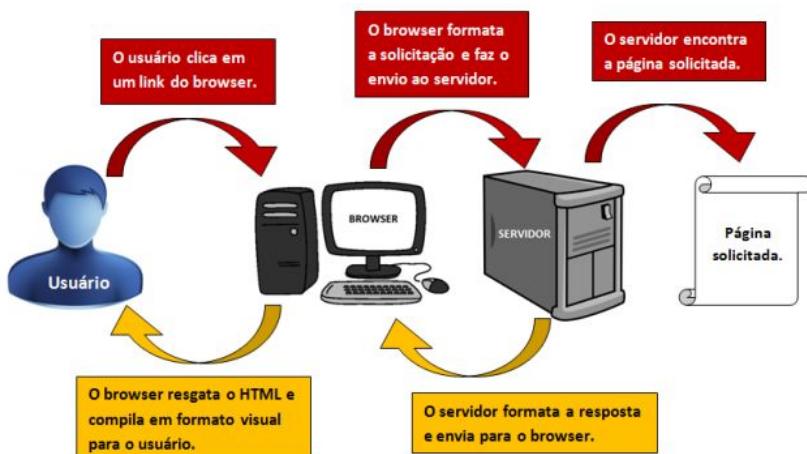
Figura 2.4.1 - Exemplo de URL.

Introdução



Disponível em: <<http://slideplayer.com.br/slide/7746940/>> Acesso em Maio. 2018.

FIGURA 2.4.2 - Solicitação e resposta para uma página web



Disponível em: <<https://www.devmedia.com.br/como-funcionam-as-aplicacoes-web/25888>> Acesso em Maio. 2018.

O protocolo HTTP define oito métodos de ação a serem realizadas no recurso especificado, ou seja, o método determina o que o servidor deve executar com o URL fornecido na requisição de um recurso.

De acordo com Thiago Vinicius (portal DEVMEDIA) e em resumo a (FIELDING, et al., 1999):

GET - O Método GET é utilizado para solicitar uma representação de um recurso específico, Requisições utilizando o Método GET devem retornar apenas dados e não devem ter qualquer outro efeito.

POST - O Método POST é utilizado para submeter uma entidade a um recurso específico, às vezes causando uma mudança no estado do recurso ou solicitando alterações do lado do servidor. O mais frequente uso desse método é na submissão de formulários.

HEAD - Similar ao método GET, o servidor apenas retoma a linha de resposta e os cabeçalhos de resposta.

PUT - O Método PUT substitui todas as atuais representações de seu recurso alvo pela carga de dados da requisição, permitindo o envio de arquivos ao servidor Web.

DELETE - O Método DELETE remove ou deleta um recurso específico.

OPTIONS - O Método OPTIONS é usado para descrever as opções de comunicação com o recurso alvo.

TRACE - Permite depurar as requisições, devolvendo o cabeçalho de um documento.

CONNECT - O Método CONNECT estabelece um túnel para conexão com o servidor a partir do recurso alvo.

2.5 APLICAÇÕES WEB

Em computação, aplicações web nomeiam, de forma geral, sistemas de informática projetados para utilização através de um navegador, da internet ou aplicativos desenvolvidos utilizando tecnologias web como HTML, JavaScript e CSS, executados a partir de um servidor HTTP (*Web Host*) ou localmente, no dispositivo do usuário (Nations, 2018).

Diferentemente de um website, segundo (blog Scriptcase, 2013), uma aplicação web funciona como uma espécie de sistema, podendo-se até dizer que esses dois termos são sinônimos. Na aplicação web, pode-se realizar muito mais ações do que em um site normal, é possível por exemplo, cadastrar informações em um banco de dados e interagir com esses dados de diversas formas através de relatórios ou processos automatizados.

Já em relação a aplicações desktop, uma aplicação web tem a vantagem de estar disponível em qualquer lugar, a qualquer hora e em qualquer tipo de dispositivo que rode um navegador web, aliviando ao desenvolvedor a responsabilidade de criar um cliente para cada tipo específico de computador ou sistema operacional (Nations, 2018) (FIGURA 2.5.1).

FIGURA 2.5.1 - Flexibilidade da aplicação web



Disponível em: <<http://www.diegomacedo.com.br/entendendo-as-aplicacoes-web/>> Acesso em Maio. 2018.

3 EQUIPAMENTOS E SOFTWARES UTILIZADOS

Neste capítulo serão apresentados os principais equipamentos e softwares utilizados na construção do projeto, assim como a função desempenhada e o motivo da escolha dos mesmos através de comparações com outras soluções encontradas no mercado.

3.1 - TECNOLOGIA DE IDENTIFICAÇÃO - RFID

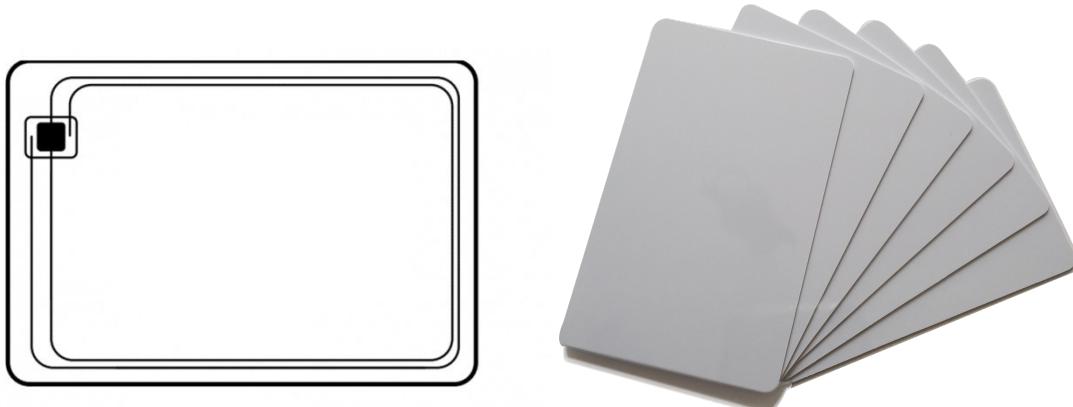
3.1.1 - TRANSPONDER E TAGS

As tags RFID utilizadas nesse projeto (FIGURA 3.1.1), de acordo com o comerciante (DMZ Connection), são passivas e do tipo MIFARE, encapsuladas em PVC, com uma memória do tipo EEPROM (*Electrically-Erasable Programmable Read-Only*) de 1 KB. Esse tipo de etiqueta utiliza-se de uma tecnologia sem contato, composta por um chip de baixa capacidade de memória e uma antena interna que detecta a aproximação do leitor RFID, em torno de 4cm de distância, através do campo magnético identificado pela frequência de operação de 13,56 MHz.

Dentre os principais benefícios deste transponder escolhido estão: a não necessidade de contato/encaixe da tag com o dispositivo de leitura, a acessibilidade do equipamento no mercado, a portabilidade, agilidade de leitura e a segurança dos dados armazenados, longa vida útil do equipamento e a possibilidade de customização em ambos os lados, com possibilidade de perfuração do cartão.

Essa tag se distingue das demais pelo preço reduzido e possibilidade de customização barata, podendo-se imprimir e perfurar ambos os lados do cartão.

FIGURA 3.1.1 - Cartões para controle de acessos MIFARE.



FONTE: (DMZ Connection).

3.1.2 - TRANSCEPTOR E LEITOR

Nesse projeto, o dispositivo transceptor RFID utilizado foi o de modelo Mfrc522, que pode ser visto na Figura 3.1.2. O dispositivo em questão é um

leitor/escritor utilizado para comunicação sem contato à uma frequência de 13,56 MHz. Tem como condições operacionais recomendadas pelo fabricante, sua tensão de entrada que deve obedecer ao intervalo de 2,5V até 3,6V e suporta uma temperatura ambiente dentro do intervalo de -25 oC até 85 oC (). Ele foi escolhido pela alta disponibilidade no mercado, preço bastante reduzido e curta distância de emissão da radiofrequência, em torno de 10 cm, necessária para maior segurança do projeto.

FIGURA 3.1.2 - Leitor RFID Mfrc522 (13,56MHz)



FONTE: Disponível em:
<https://hallroad.org/product/mfrc522-rc522-rfid-card-reader-writer-module-in-pakistan/> Acesso em Maio. 2018

3.1.3 - COMPARAÇÃO COM OUTRAS TECNOLOGIAS DE IDENTIFICAÇÃO

Atualmente, existem diversas soluções para problemas de identificação que empregam diferentes tecnologias de reconhecimento. Para este trabalho será relevante apenas compararmos a tecnologia RFID com as principais tecnologias de identificação e controle de acesso de pessoas.

Dentre as principais tecnologias desenvolvidas e presentes no mercado, com objetivo de identificação e reconhecimento para acesso de pessoas, podemos citar os módulos de acesso com teclados para senhas, os leitores de código de barra e QR code, além das tecnologias de leitura facial, biométrica e de retina.

Dentre as vantagens do RFID, quando comparado às soluções citadas anteriormente (TABELA 3.1.3), pode-se destacar: agilidade de leitura, a maior capacidade de armazenamento e leitura dos dados, a detecção sem necessidade de contato ou visada direta para a leitura dos dados e baixa necessidade de processamento para a sua utilização. Como desvantagem, a possibilidade de realização de cópia, estrago e perda do transponder não confirmam a total segurança da tecnologia, além do custo inicial elevado do RFID ser um dos principais obstáculos para o aumento de sua aplicação comercial, porém tal desvantagem só se aplica em relação aos sistemas de código de barras e teclado de senha, pois quando comparada aos demais sistemas citados, seu custo é semelhante ou até mesmo muito inferior.

TABELA 3.1.3 - Quadro comparativo das tecnologias de identificação.

	Teclado de senha	Código de barras	RFID
Custo	Muito barato	Barato	Médio
Escrita da chave de acesso	Demorada Simples	Rápida Simples	Rápida Simples
Leitura	Precisa e exata Instantânea	Precisa e exata Muito rápida	Precisa e exata Muito rápida
Contato com o dispositivo	Necessário	Aproximação sem contato	Aproximação sem contato
Armazenamento de dados	Inexistente	Inexistente	Possível
Necessidade de processamento	Muito Baixo	Baixo	Baixo
Segurança	Baixa	Baixa	Média

	Biometria	Leitor de íris	Leitura facial
Custo	Alto	Muito Alto	Muito Alto
Escrita da chave de acesso	Rápida Simples	Demorada Custosa	Demorada Custosa
Leitura	Nem precisa, nem exata Rápida	- Demorada	- Demorada
Contato com o dispositivo	Necessário	Aproximação com possível contato com o dispositivo	Aproximação com possível contato com o dispositivo
Armazenamento de dados	Inexistente	Inexistente	Inexistente
Necessidade de processamento	Alto	Muito alto	Muito alto
Segurança	Alta	Muito alto	Muito alto

Fonte: Própria

3.2 MICROCONTROLADOR

Neste capítulo serão abordados e comparados duas famílias de microcontroladores diferentes o Atmel AVR da Arduino e o ESP8266 da Espressif Systems.

3.2.1 ARDUINO

De acordo com THOMSEN(2014), o Arduino é uma plataforma de prototipagem eletrônica de código aberto, hardware livre, que possui sua própria IDE (*Integrated Development Environment* ou Ambiente de Desenvolvimento Integrado), com objetivo de criar ferramentas que são acessíveis, a baixo custo, flexíveis e fáceis de se usar por novatos e profissionais. Além disso, IDE também conta com uma interface gráfica simples e intuitiva, além de aceitar códigos em C/C++.

Uma típica placa Arduino (FIGURA 3.2.1.2) é composta por um microcontrolador Atmel, algumas linhas de entrada e saída digital e analógica, além de uma interface serial ou USB, para interligar-se ao hospedeiro, que é usado para programá-la e interagi-la em tempo real. Entretanto, em si, ela não possui qualquer recurso de rede, porém é comum combiná-la a extensões apropriadas que lhe permitem tal recurso.

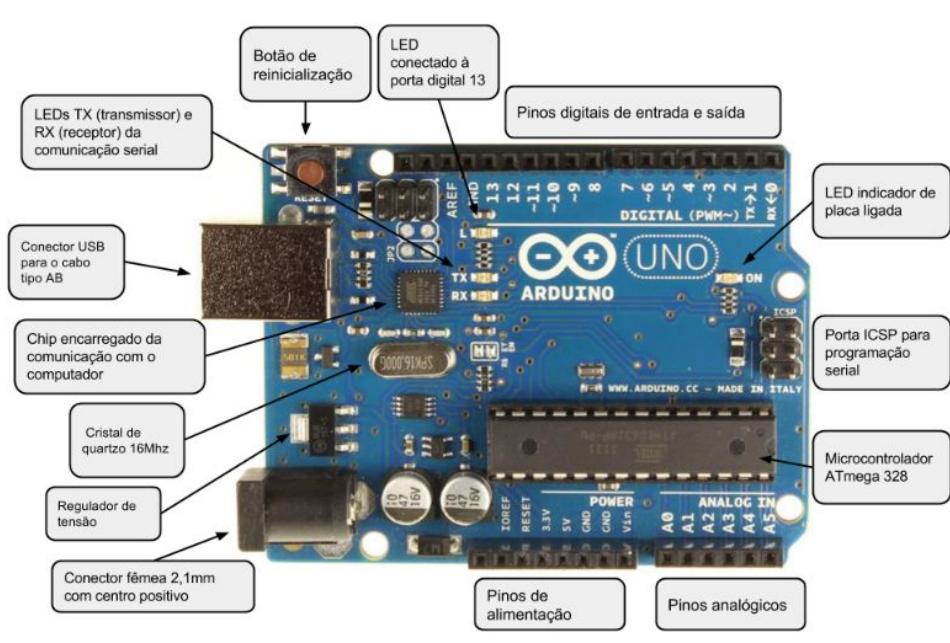
O Arduino tem uma grande comunidade de usuários, diversos trabalhos e projetos que se utilizam dessa plataforma, pela sua facilidade de uso, eficiência e sua IDE gratuita, além do grande número de ferramentas já implementadas para o mesmo.

FIGURA 3.2.1.1 - FAMÍLIA ARDUINO



FONTE: Disponível em: <<http://abraaoeletronica.com.br/arduino>> Acesso em Maio. 2018.

FIGURA 3.2.1.2 - Diversos componentes da placa Arduino UNO.



FONTE: Disponível em:

<<http://natalmakers.blogspot.com/2015/08/dispositivo-conhecendo-as-partes-do.html>> Acesso em Maio. 2018.

3.2.2 ESP8266

O ESP8266 é um microcontrolador produzido pela empresa Espressif Systems que chegou ao mercado em meados de 2014, ou seja, estudos sobre ele ainda são muito recentes, porém ele vem sendo bastante utilizado em prototipagens pelo grande diferencial de possuir um sistema de comunicação WiFi próprio a custo semelhante a um microcontrolador sem esse recurso (BENCHOFF, 2014). Também, por essa razão, ele é largamente utilizado como módulo WiFi para outros microcontroladores, barateando assim esse estilo de comunicação e possibilitando a conexão de diversos dispositivos a internet (ou rede local) como sensores, atuadores e incentivando ideias de IoT.

Essa família de microcontroladores é fornecidos numa ampla variedade de modelos (FIGURA 3.2.2.1), com diferenças perceptíveis principalmente no que tange à quantidade de portas disponíveis para acesso externo, no tamanho do módulo ou tipo de conexão com computador.

A placa de desenvolvimento da família do ESP8266 mais facilmente encontrada e difundida no mercado é o NodeMCU, uma plataforma open source, criada em 2014 para ser utilizada no desenvolvimento de projetos IoT. Suas principais diferenças em relação aos demais microcontroladores da família ESP8266 são, a presença de um conversor USB serial integrado e o preço mais acessível quando se comparado com placas de desenvolvimento mais robustas como a Wemos D1 ou o ESP32 (FIGURA 3.2.2.2).

Uma das grandes vantagens em utilizar plataformas baseadas no ESP8266, é a possibilidade de se programar utilizando a IDE do Arduino. E, assim como em

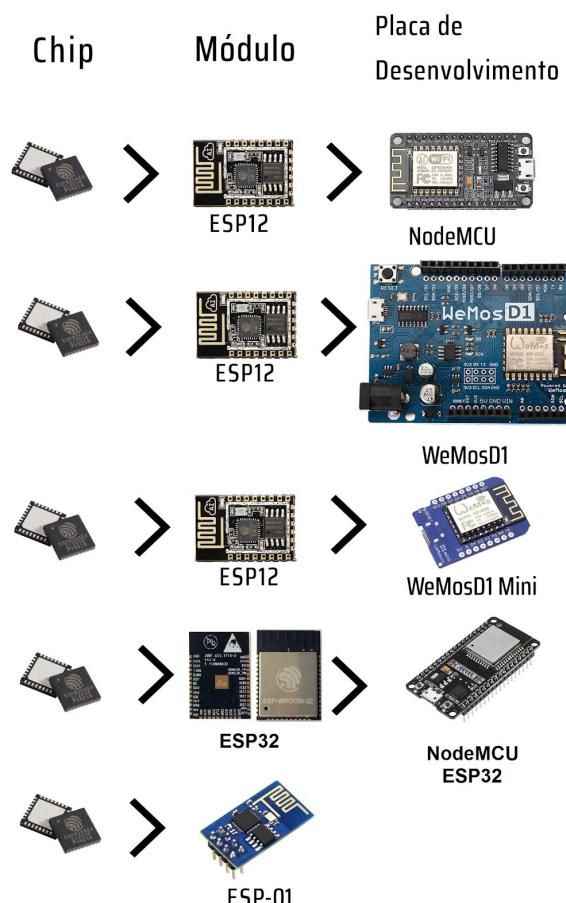
outras placas dessa família, o NodeMCU além de ser compatível com o ambiente de desenvolvimento do Arduino, a placa também pode ser programada na linguagem LUA e MicroPython.

FIGURA 3.2.2.1 - Família ESP8266.



FONTE: Disponível em: <<http://edukatikateaching.blogspot.com/2015/07/esp8266-iot.html>> Acesso em Maio. 2018.

FIGURA 3.2.2.2 - Placas de desenvolvimento ESP8266.



FONTE: Edição própria.

3.2.3 COMPARAÇÃO ENTRE AS FAMÍLIAS DE MICROCONTROLADORES

Com a finalidade de se obter um protótipo de fácil instalação, optou-se pela conexão wifi ao em vez da conexão cabeadas, por esse motivo, a primeira grande diferença que devemos observar entre a família do Arduino e do ESP8266 é a comunicação via Wifi. Nenhuma placa regular do Arduino possui um protocolo de comunicação sem fio próprio, precisando assim de algum módulo extra instalado para realizar esse tipo de operação.

Outros grandes diferenciais que tendem a favor da escolha pelo ESP8266 são o desempenho e o custo, como mostrado na Tabela 1, o ESP12 do NodeMCU supera em praticamente todas as especificações quando se comparado ao microcontrolador do Arduino, o ATmega328. Além disso, mesmo que a placa de prototipagem NodeMCU saia às vezes no mercado por um preço pouco mais elevado que uma placa regular do Arduino, o montante do Arduino com o módulo extra de comunicação ultrapassa significativamente o custo de uma placa de prototipagem NodeMCU que já conta com essa função embutida.

Como consta na Tabela 1 e de acordo com (HU INFINITO), o Arduino UNO possui um microcontrolador ATMega 328P, 16MHz de velocidade de processamento, uma memória RAM de 2 KB e uma memória flash de 32 KB, enquanto o NodeMCU consta com um microcontrolador ESP 12 de 160 MHz de velocidade de operação (10 vezes mais rápido que o Arduino), uma memória RAM de 20KB e uma memória flash de 4MB.

Dessa forma, por já contar com uma plataforma de comunicação embutida, uma melhor performance e um preço acessível, foi decidido pelo uso da plataforma de prototipagem NodeMCU com ESP12.

TABELA 1 - NodeMCU x Arduino UNO

	NodeMCU v1.0	Arduino UNO
Microcontrolador	ESP-12E module, with Espressif ESP8266 32bits	ATmega328
Voltagem Operacional	3.3V	5V e 3.3V
Tensão de entrada	4,5 ~ 9V	4,5 ~ 20V
Pinos E/S digitais	10 (dos quais 10 podemos ser saídas PWM)	14 (dos quais 6 podemos ser saídas PWM)
Pinos analógicos	1	6
Flash Memory	4MB	32 KB
RAM	20KB	2 KB
Velocidade de Processamento	160MHz	16 MHz
Conectividade	Inclusa	Separada
Custo	Por volta de	Por volta de

	R\$22,00	R\$ 25,00
Documentação	Mediana	Excelente
Maturidade	Recente	Maduro

Fonte: Tabela Própria

3.3 IDE ARDUINO

IDE, do inglês *Integrated Development Environment* ou Ambiente de Desenvolvimento Integrado, é um programa de computador que reúne características e ferramentas de apoio ao desenvolvimento de software com o objetivo de agilizar, simplificar e melhorar a produtividade deste processo.

O arduino possui uma IDE própria (FIGURA 3.3), que pode ser utilizada por diversos outros microcontroladores, e precisa ser baixada e instalada como o ambiente de programação composto de um editor, um compilador, um carregador e um monitor serial.

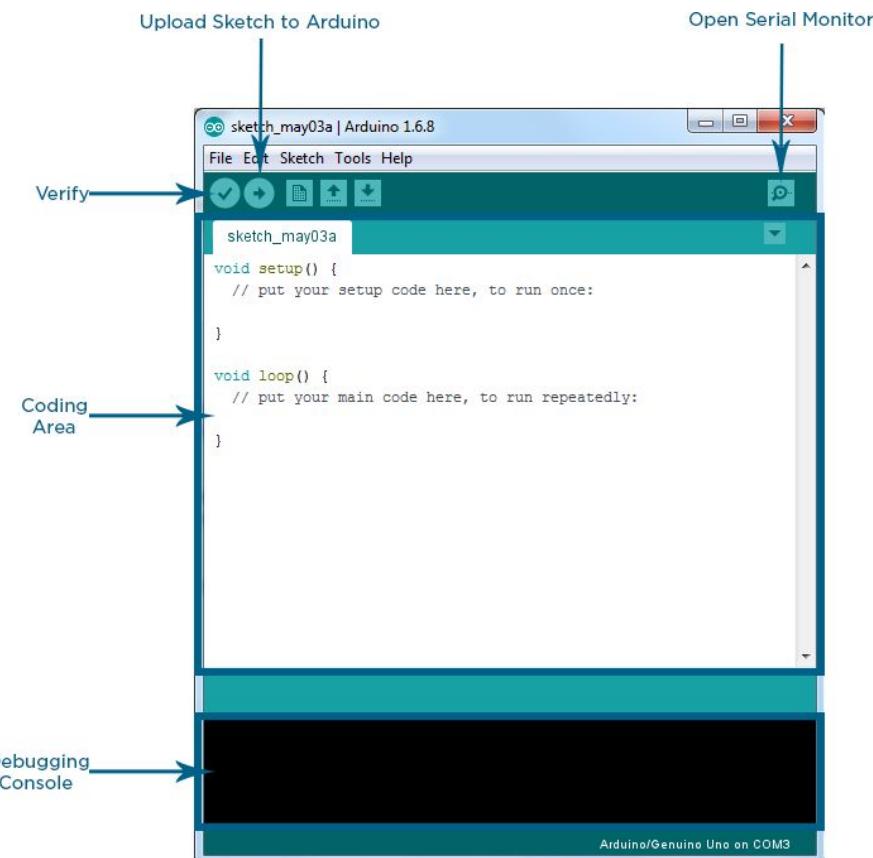
A IDE já possui algumas bibliotecas e funções próprias, mas também permite que o usuário adicione outras.

De acordo com Ricardo Rodrigues (OLIVEIRA, 2017), os programas na IDE do Arduino são denominados “sketchs” e se utilizam da linguagem C/C++, nesse ambiente existem duas funções obrigatórias, a função `setup()` e a função `loop()`. A função `setup()` é chamada toda vez que o dispositivo é ligado, sendo a primeira função a ser chamada, nela se realizam todas as chamadas de inicialização do programa.

Já a função `loop()`, que é chamada necessariamente após a função `setup()`, funciona como um laço, sempre ao seu final, a função é chamada novamente, até que um comando seja dado para a função parar ou o dispositivo seja desligado. Nessa função são realizadas todas as chamadas que são pertinentes ao funcionamento normal da placa, ou seja, o serviço que programa deve realizar ao longo do seu funcionamento.

Uma das grandes vantagens em utilizar plataformas baseadas no ESP8266, é a possibilidade de se programar utilizando a IDE do Arduino. Assim como em outras placas da família ESP8266, o NodeMCU também é compatível com o ambiente de desenvolvimento do Arduino. Ao ser utilizado a IDE do Arduino para programar o NodeMCU, será possível fazer o uso de diversas bibliotecas que já fazem grande parte da programação.

FIGURA 3.3 - IDE ARDUINO.



FONTE: Disponível em: <<https://core-electronics.com.au/tutorials/arduino-ide-tutorial.html>> Acesso em Junho. 2018.

3.4 ATUADORES

3.4.1 - RELÉ

O relé (FIGURA 3.4.1.1) é uma espécie de interruptor eletrônico, de acordo com o portal (MUNDO DA ELETRÔNICA), sua movimentação física ocorre quando a corrente elétrica percorre as espiras de sua bobina, criando assim um campo magnético que atrai a alavancas responsáveis pela mudança do estado do contato (FIGURA 3.4.1.2).

A principal vantagem do relé é que os contatos que acionam o circuito de carga estão completamente isolados do circuito de comando, possibilitando-se trabalhar com diferentes tensões entre os circuitos.

Entretanto, é importante salientar as limitações dos relés em relação a corrente e tensão máxima suportadas entre os terminais, caso esse fator não seja levado em consideração a vida útil do dispositivo poderá ficar comprometida devido ao desgaste, podendo comprometer também o circuito.

Existem no mercado diversos tipos de relés, cada qual com suas devidas características de funcionamento e aplicações, para a prototipagem deste projeto foi utilizado o Módulo Relé 5V, SRD-05VDC-SL-C, de acordo com portal (THOMSEN,

2013), com tempo de resposta entre 5 e 10 ms, corrente de operação de 15 a 20 mA, tensão de operação 5V e controle de carga de até 220V AC.

FIGURA 3.4.1.1 - Módulo Relé.



FONTE: Disponível em:

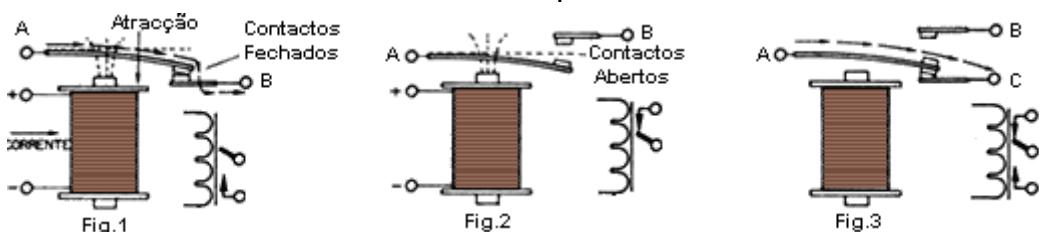
<<https://pt.aliexpress.com/item/1-Channel-12V-relay-module-with-optical-coupling-isolation-relay-MCU-expansion-board-high-level-trigger/32765328522.html>> Acesso em Junho. 2018.

FIGURA 3.4.1.1 - Funcionamento de relés:

Fig.1- O relé fecha o circuito entre os terminais A e B.

Fig.2- O relé abre o circuito entre os terminais A e B.

Fig.3- O relé comuta a tensão que entra no terminal A comutando entre o terminal B e C.



FONTE: Disponível em: <<https://www.electronica-pt.com/rele>> Acesso em Junho. 2018.

3.4.2 - FECHADURA ELÉTRICA OU FECHO ELÉTRICO

O principal componente que deve ser analisado para o entendimento do protótipo desenvolvido é o objeto a ser controlado, que nesse projeto é uma fechadura elétrica através do acionamento de um Relé, que a depender das características da fechadura deve ser dimensionado a ser implantado entre a saída do sistema de controle e a entrada da fechadura elétrica.

De acordo com o portal (PIRES), o acionamento de uma fechadura elétrica, ou fecho elétrico, se dá através de uma bobina elétrica (solenóide), que ao ser percorrida por uma corrente elétrica, transforma-se em um eletro imã, que atrai uma lingueta de ferro abrindo a fechadura e liberando o acesso. Através de uma mola que empurra a lingueta de volta, ocorre o travamento da fechadura. Ou seja, a eletrificação do componente aciona seu destravamento até que ele seja utilizado, após a utilização ele é travado novamente de forma mecânica.

Por utilizar-se de um relé para seu acionamento, a tensão utilizada pela fechadura elétrica pode variar, possibilitando a utilização de diversos tipos diferentes de fechaduras elétricas neste projeto.

Para o exemplo apresentado neste projeto, foi mensurado um relé que aguenta uma carga de 12V na saída do sistema de controle de acesso, pois a

fechadura em questão (FIGURA 3.4.2) possui como característica uma tensão de alimentação de 12V, como a maioria das fechaduras encontradas no mercado.

FIGURA 3.4.2 - Exemplos de fechaduras elétricas.



FONTE: Disponível em: <<http://www.hdl.com.br/produtos/fechaduras/fecho-eletrico>> Acesso em Junho. 2018.

3.5 - SOFTWARE UTILIZADO NO DESENVOLVIMENTO DA APLICAÇÃO WEB

3.5.1 - DJANGO

Segundo o portal (GSTI), Django é um framework gratuito e de código aberto, escrito em Python, mantido pela **Django Software Foundation (DSF)**, uma organização independente e sem fins lucrativos, com objetivo de facilitar a criação de sites complexos com banco de dados orientados (FIGURA 3.5.1). Ou seja, é um conjunto de componentes que ajuda no desenvolvimento rápido e fácil para aplicações web utilizando o padrão **Model-Template-View (MTV)** e o princípio DRY (**Don't Repeat Yourself**), onde faz com que o desenvolvedor aproveite ao máximo o código já feito, evitando repetições.

Dentre suas principais características, é possível listar:

“Mapeamento Objeto-Relacional (ORM) - Com o ORM do Django você define a modelagem de dados através de classes em Python. Com isso é possível gerar suas tabelas no banco de dados e manipulá-las sem necessidade de utilizar SQL.

Interface Administrativa - No Django é possível gerar automaticamente uma interface para administração dos modelos criados através do ORM.

Formulários - É possível gerar formulários automaticamente através dos modelos de dados.

URLs Amigáveis - No Django não há limitações para criação de URLs amigáveis e de maneira simples.

Sistema de Templates - O Django tem uma linguagem de templates poderosa, extensível e amigável. Com ela você pode separar design, conteúdo e código em Python.

Sistema de Cache - O Django possui um sistema de cache que se integra ao memcached ou em outros frameworks de cache.” (GSTI).

Através dessa ferramenta e do banco de dados SQLite, que por padrão já vem instalado na ferramenta, foi desenvolvida a aplicação web chamada “Unlock” que faz parte deste projeto.

FIGURA 3.5.1 - Django.



FONTE: Disponível em:

<<https://www.slideshare.net/guilegarcia/minicurso-de-django-desenvolvimento-gil-web-com-django-e-python>> Acesso em Junho. 2018.

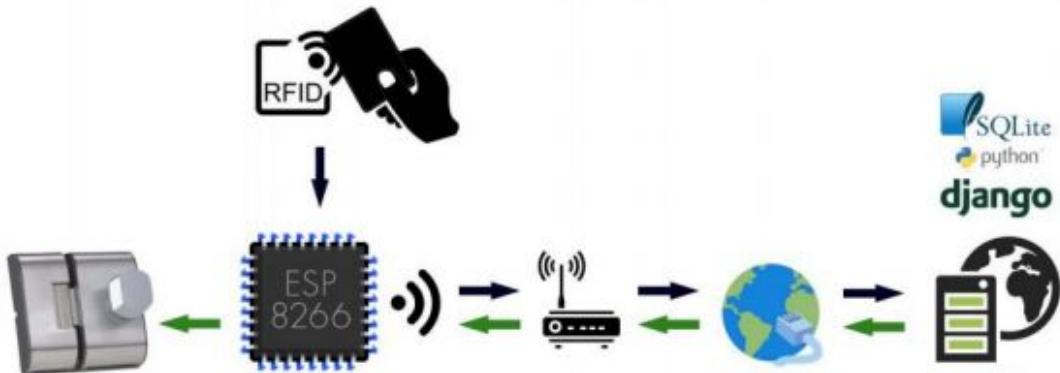
4 DESENVOLVIMENTO DO PROJETO

Neste capítulo será apresentado com detalhes o desenvolvimento do projeto.

4.1 FLUXO DO PROJETO

Como é demonstrado na Figura 4.1.1, o sistema consiste em uma tag RFID, única e pessoal, sendo lida por um Leitor RFID, modelo Mfrc522, controlado pelo Esp8266, que através de uma rede de internet wifi se comunica com a aplicação Web e solicita assim um acesso. O servidor da aplicação, responsável por autenticar, autorizar e registrar os acessos, responde ao controlador a possível liberação do acesso, caso liberado, o controlador Esp 8266 NodeMcu aciona o relé que por fim possibilita a passagem na porta através do destravamento da tranca elétrica.

FIGURA 4.1.1 - Fluxo do projeto.



FONTE: Edição própria.

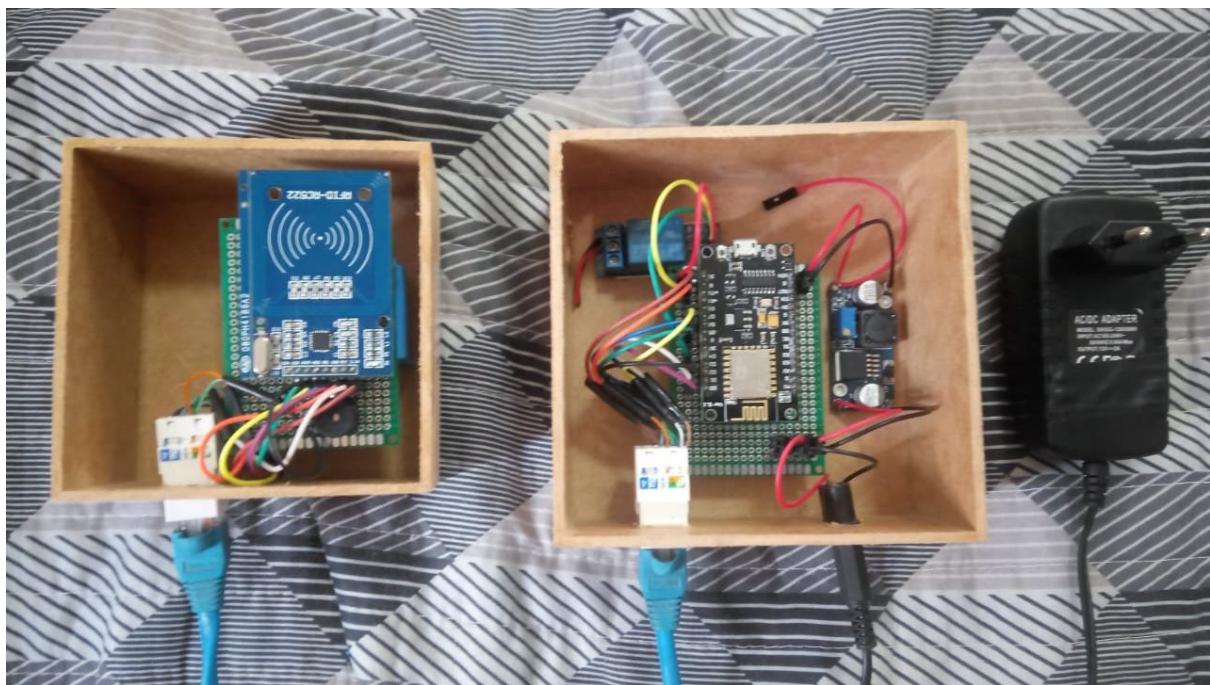
4.2 HARDWARE

Como mostrado na figura 4.2.1 e evidenciado na figura 4.2.3, o hardware é dividido em dois dispositivos distintos, denominados controlador e sensor, ligados através de um cabo de rede par trançado com conectores RJ45.

O primeiro dispositivo, o controlador (FIGURA 4.2.4), conta com o microcontrolador NodeMCU, um relé de 5V, os conectores de energia e fêmea do RJ45, e por fim um módulo regulador de tensão ajustável XL6009 STEP UP DC-DC para se poder ter acesso a tensões de 5V e 12V, além da 3,3V obtida do microcontrolador.

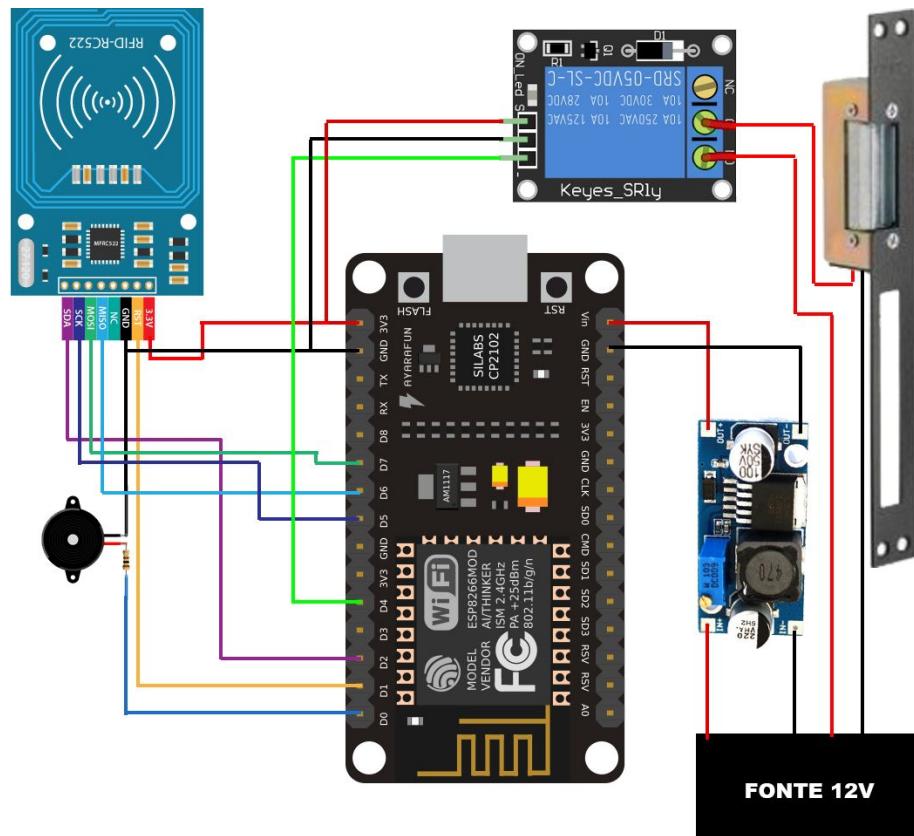
Já no segundo dispositivo, o sensor (FIGURA 4.2.5), encontram-se o transponder RFID Mfrc522, o outro conector fêmea do RJ45 e um buzzer utilizado para apitar no momento que se aproxima uma tag do leitor, visto que o transponder utilizado não conta com um por padrão.

FIGURA 4.2.1 - Protótipo do projeto.



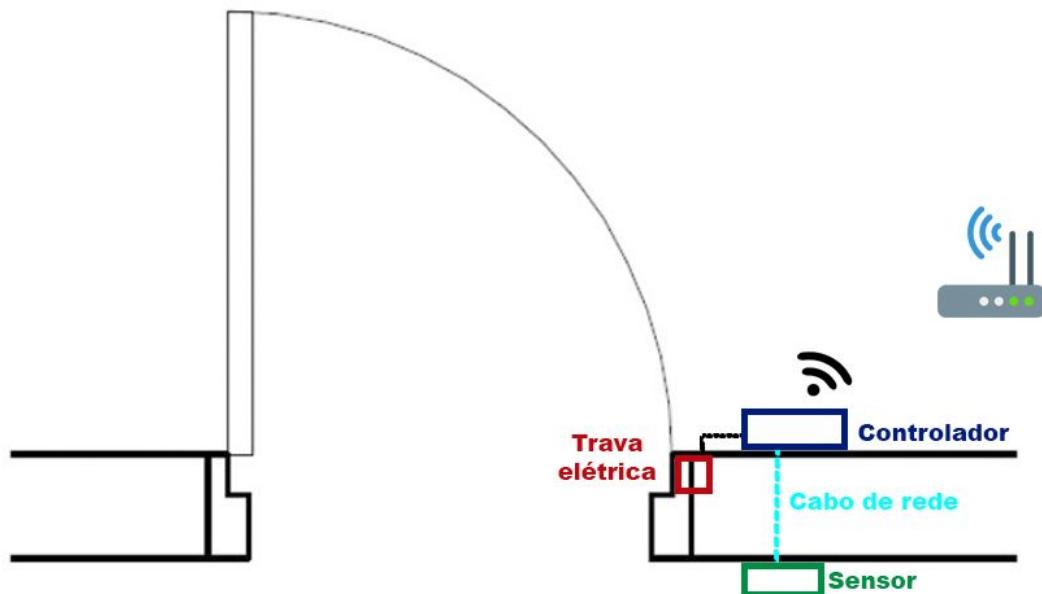
FONTE: Imagem própria.

FIGURA 4.2.2 - Esquemático do projeto.



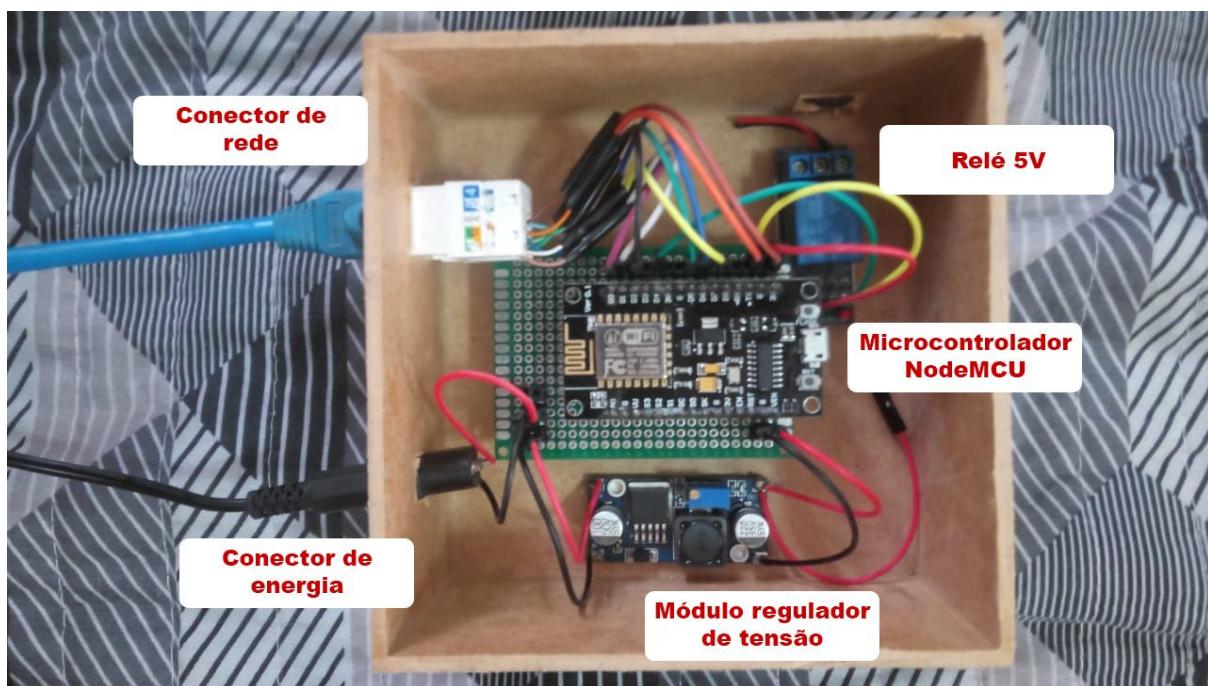
FONTE: Imagem própria.

FIGURA 4.2.3 - Esquema de instalação do protótipo.



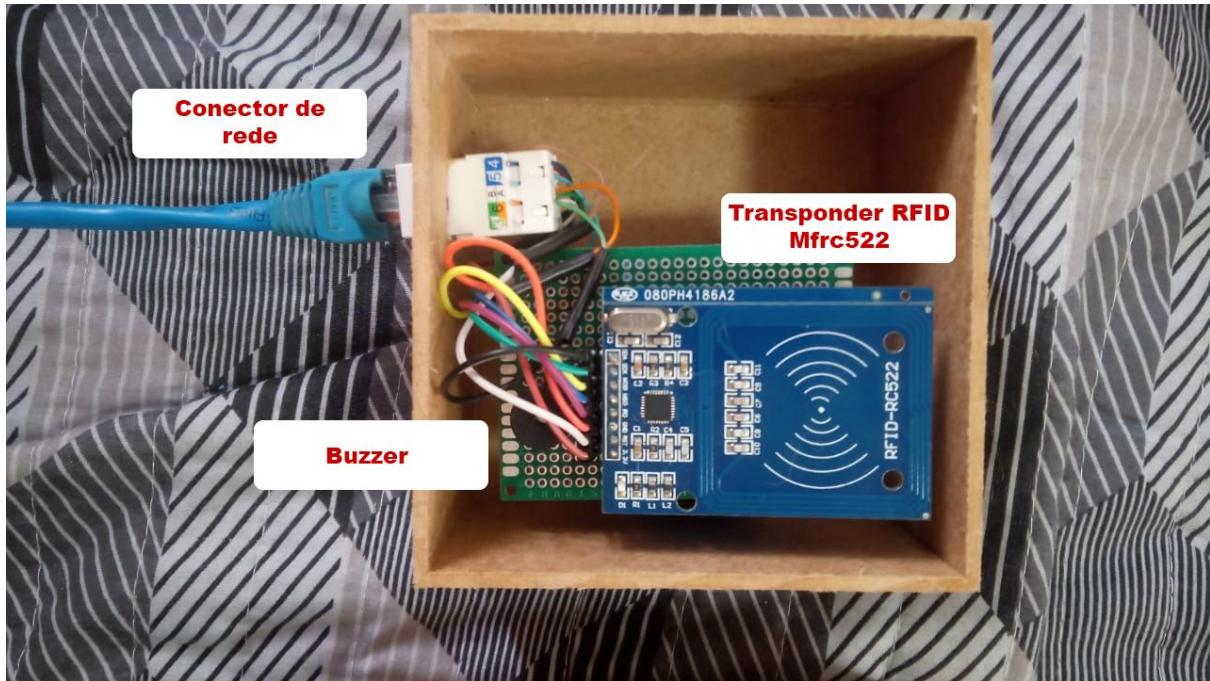
FONTE: Imagem própria.

FIGURA 4.2.4 - O controlador.



FONTE: Imagem própria.

.FIGURA 4.2.5 - O leitor.



FONTE: Imagem própria.

4.3 PROGRAMAÇÃO DO HARDWARE

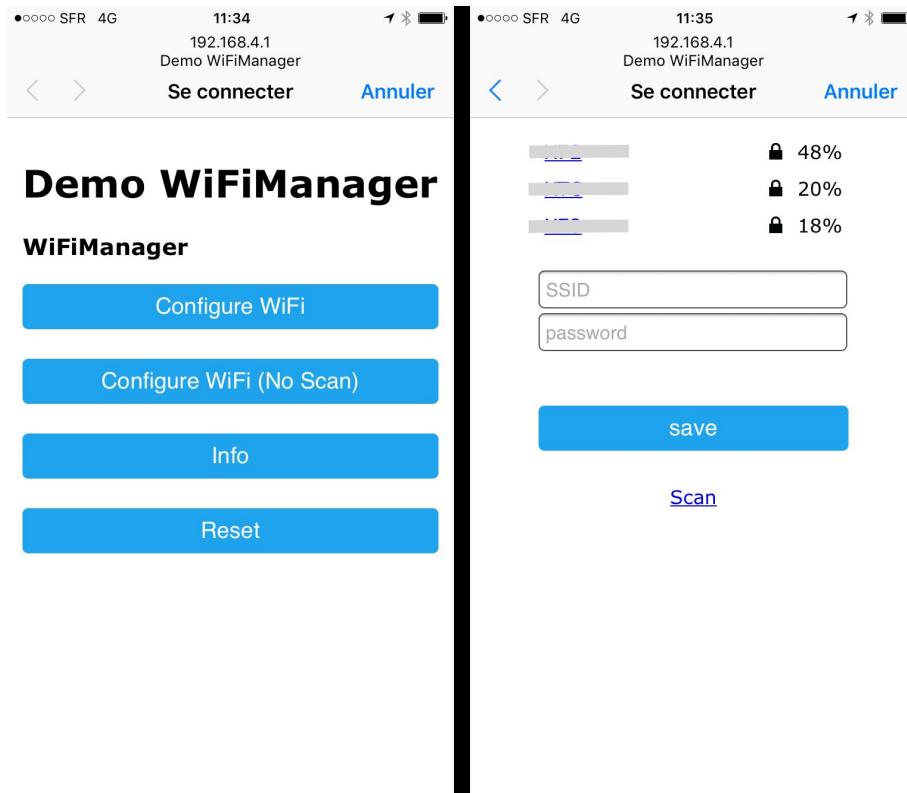
Para programar a placa de prototipagem NodeMCU, seguiu-se o tutorial da Filipeflop (THOMSEN, 2016) para se programar na IDE do Arduino que conta com bibliotecas, um design amigável e muita informação disponível na web, o que facilitou a programação desse hardware.

Foram utilizadas bibliotecas tanto para facilitar a programação com o leitor RFID como a biblioteca “MFRC522.h”, quanto para se fazer uso de rede wifi pela placa NodeMCU como as bibliotecas “ESP8266HTTPClient.h”, “ESP8266WiFi.h”, “DNSServer.h”, “ESP8266WebServer.h” e “WiFiManager.h” que configura o NodeMCU para tentar se conectar ao último ponto de acesso salvo e em caso de falha, move o ESP para o modo “Access Point” e ativa o DNS e o WebServer (ip padrão 192.168.4.1) (FIGURA 4.3.1), onde é possível configurar uma nova rede de internet para placa sem precisar reprogramá-la.

Como é explicado na figura 4.3.2, o microcontrolador recebe o código da tag através do transponder RFID, o salva em uma variável e concatena a uma URL que já conta com o código único do dispositivo.

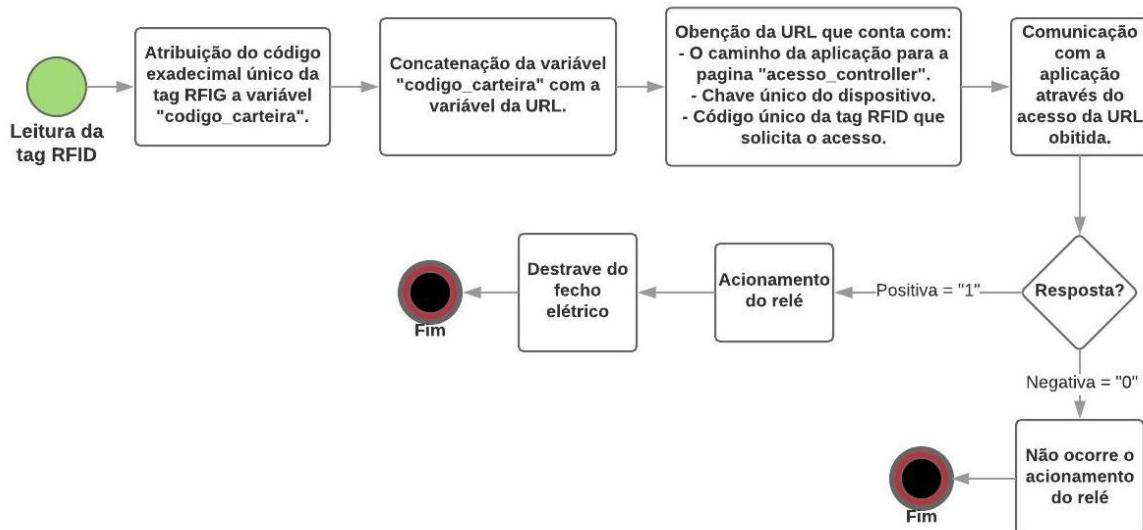
Essa URL acessada, dará entrada na aplicação web que responderá ao conjunto de dados enviados com “0” ou “1”, respectivamente para bloquear e liberar o acesso, ligando ou não o relé que ativa a tranca eletrica.

FIGURA 4.3.1 - Wifi manager para NodeMCU.



FONTE: Disponível em:
https://diyprojects.io/wifimanager-library-easily-manage-wi-fi-connection-projects-esp8266/#.Wy_cF1VKjIU Acesso em Junho. 2018

FIGURA 4.3.2 - Funcionamento da requisição de acesso.



FONTE: Imagem própria.

4.4 SOFTWARE “UNLOCK”

Elaborado para esse projeto em python através do framework Django, com mais de 20 funcionalidades para gerenciamento do sistema, o software denominado “Unlock” é talvez o componente mais complexo desse sistema e tem a função de receber do hardware, via o método GET da requisição HTTP, os dados referentes a tentativa de acesso, código RFID do cartão do usufrutuário e chave do dispositivo acessado, registrar essa tentativa, autenticar sua validade e autorizar ou não esse acesso, como mostrado no fluxograma da figura 4.4.1. Além disso é também uma plataforma central e amigável de gerenciamento (FIGURA 4.4.2), onde o usuário através de um perfil pessoal pode controlar seus vários dispositivos, administrando e monitorando seus acessos, diferentemente de vários dispositivos presentes no mercado que possuem gerenciamento descentralizados e normalmente dispostos nos próprios aparelhos.

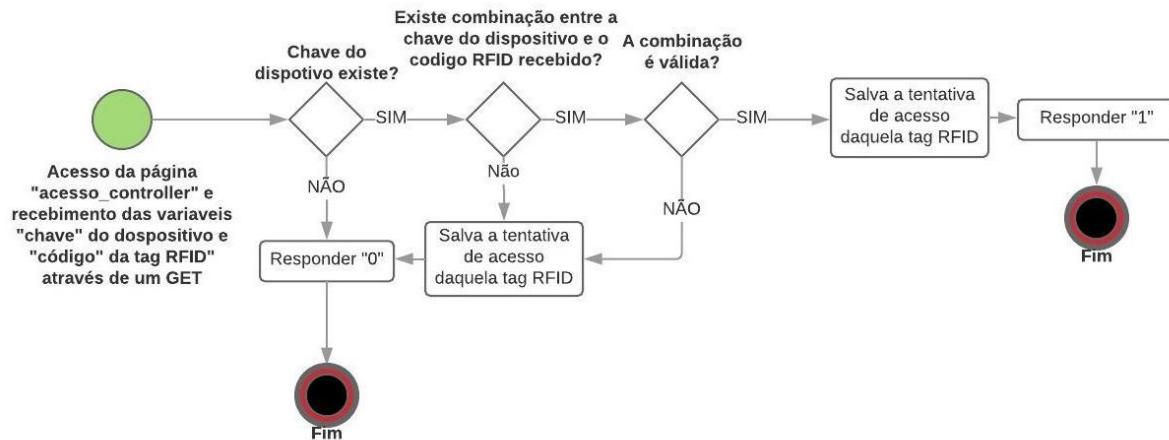
Funções automatizadas e restritas à aplicação:

- Receber dados referentes a tentativas de acesso.
- Registrar tentativa de acesso.
- Autenticar a validação do acesso.
- Enviar autorização/bloqueio do acesso.

Funções disponíveis ao usuário da aplicação:

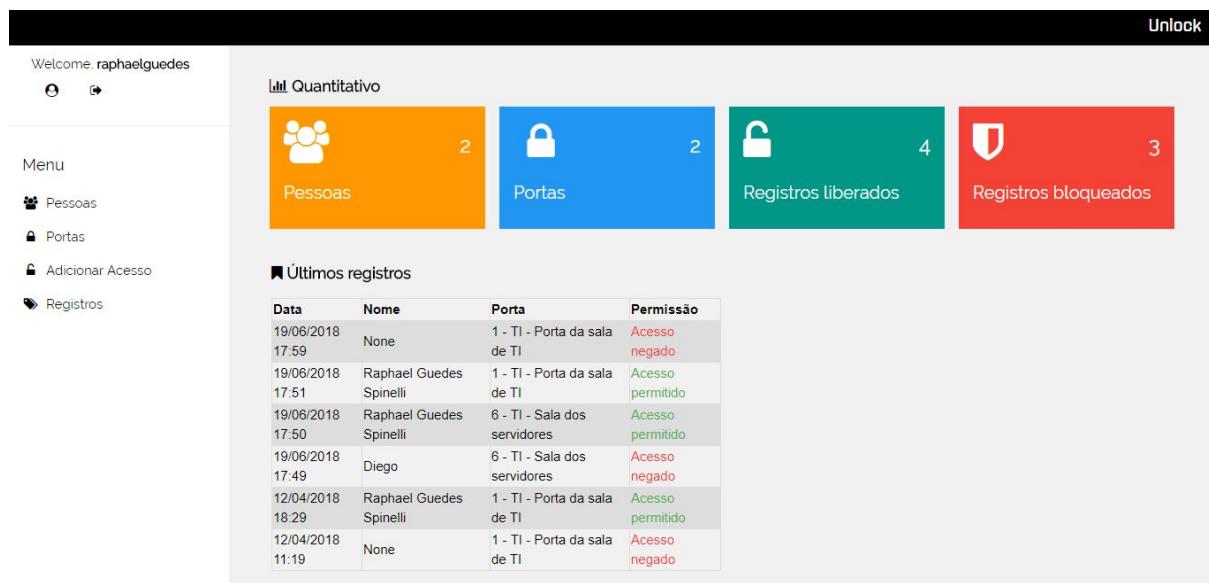
- Realizar login / logout / novo cadastro / recuperar senha e visualizar / modificar dados do usuário (FIGURA 4.4.3 e FIGURA 4.4.4).
- Adicionar / modificar / visualizar / excluir usufrutuário do serviço (FIGURA 4.4.5 e FIGURA 4.4.6).
- Adicionar / modificar / visualizar / excluir dispositivos (portas) (FIGURA 4.4.7 e FIGURA 4.4.8).
- Adicionar / excluir setores.
- Adicionar / bloquear / desbloquear / visualizar acessos. (FIGURA 4.4.6)
- Gerar / visualizar relatórios personalizados de tentativas de acessos. (FIGURA 4.4.9 e FIGURA 4.4.10).

FIGURA 4.4.1 - Funcionamento do controlador de acessos da aplicação web “Unlock”.



FONTE: Imagem própria.

FIGURA 4.4.2 - Index do sistema.



FONTE: Imagem própria.

FIGURA 4.4.3 - Tela de Login do sistema.



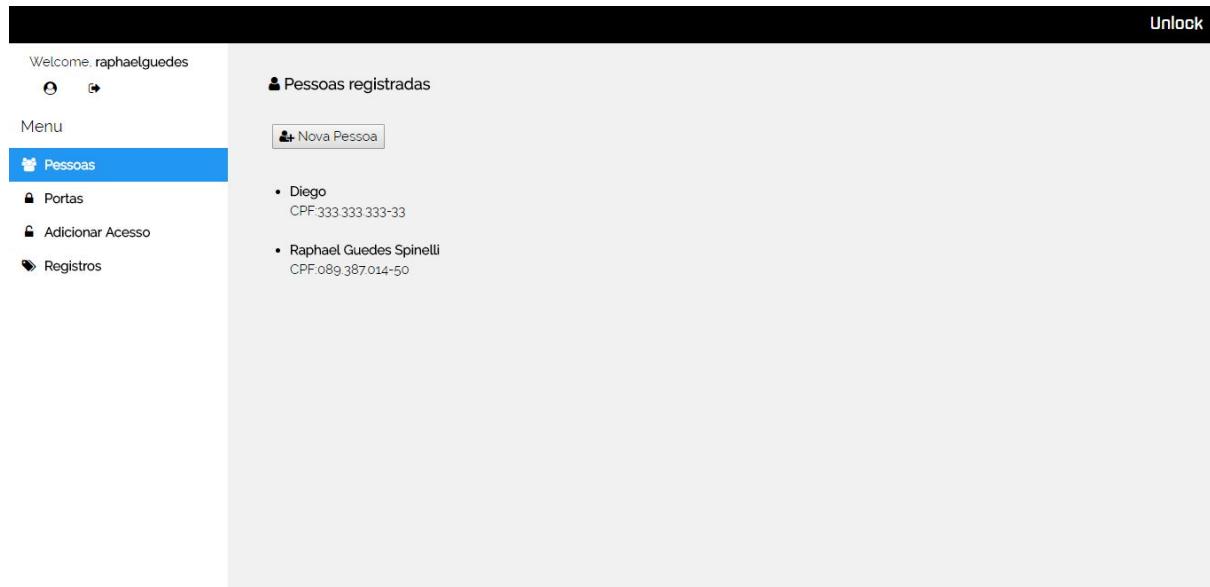
FONTE: Imagem própria.

FIGURA 4.4.4 - Tela do usuário.

A screenshot of a user profile page titled "Meu Usuário". The header includes the "Unlock" logo and a "Welcome raphaelguedes" message with a sign-out link. On the left, a sidebar menu lists "Menu", "Pessoas", "Portas", "Adicionar Acesso", and "Registros". The main content area displays the user's details: "Username: raphaelguedes", "Nome: Raphael Guedes Spinelli", and "E-mail: suporte@abcfc.com.br". Below these details are two links: "Alterar dados" and "Mudar senha".

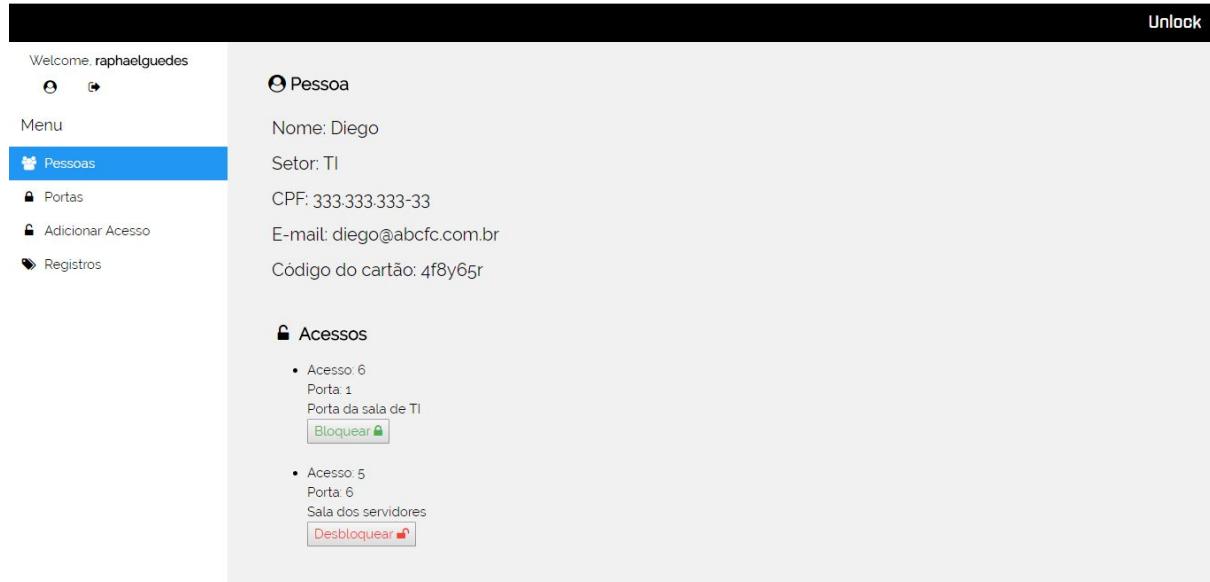
FONTE: Imagem própria.

FIGURA 4.4.5 - Tela de controle dos usufrutuários.



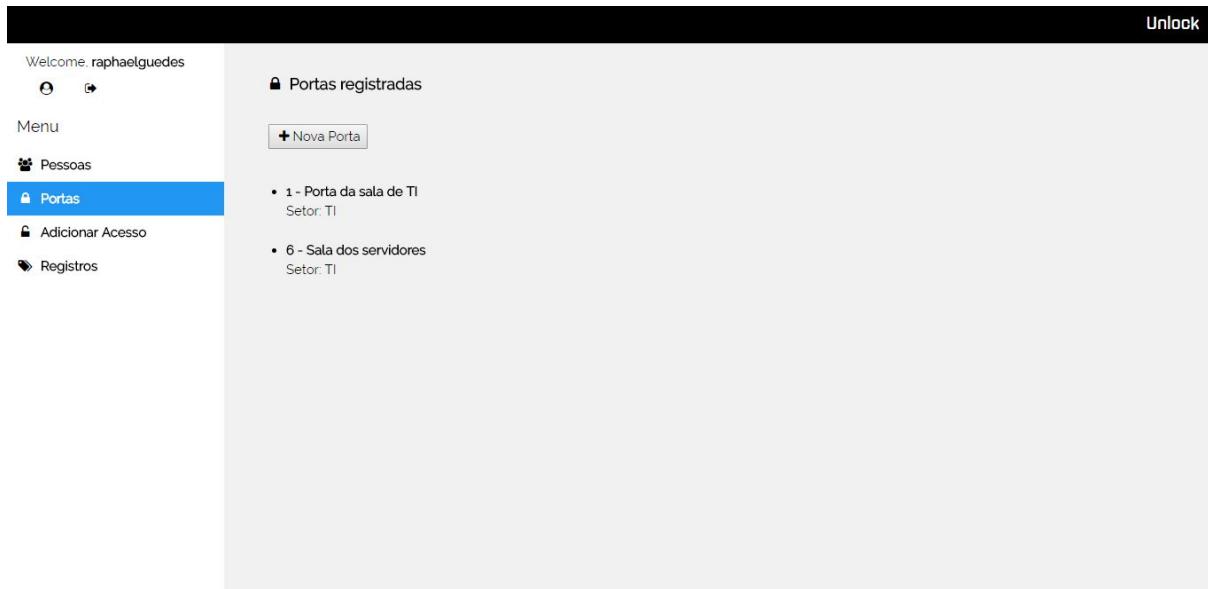
FONTE: Imagem própria.

FIGURA 4.4.6 - Tela de dados do usufrutuário.



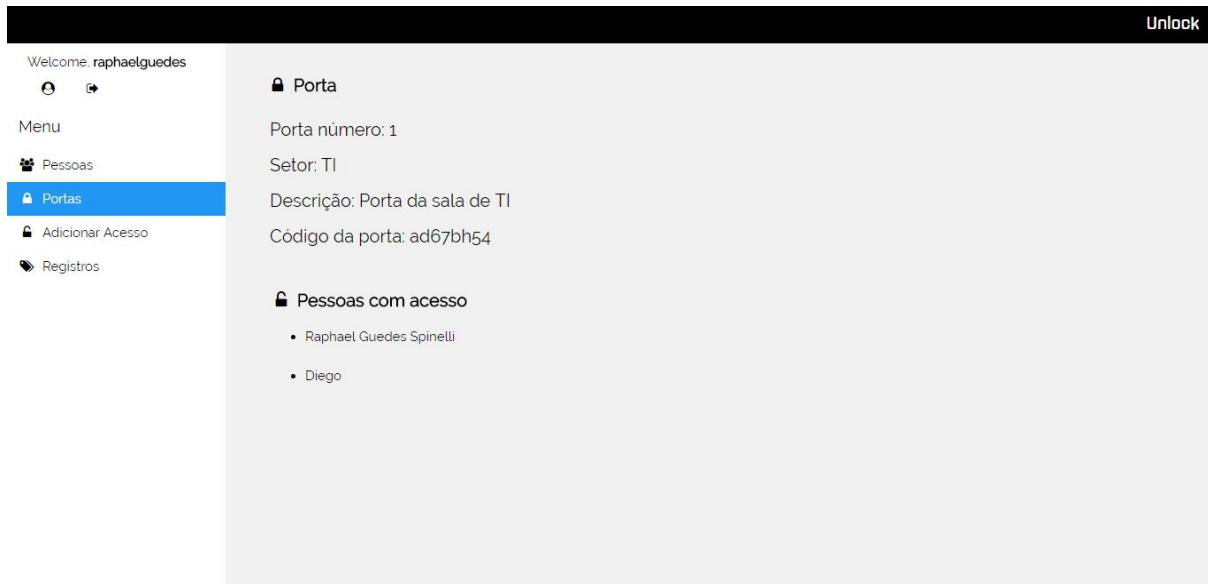
FONTE: Imagem própria.

FIGURA 4.4.7 - Tela de controle dos dispositivos.



FONTE: Imagem própria.

FIGURA 4.4.8 - Tela de dados do dispositivo.



FONTE: Imagem própria.

FIGURA 4.4.9 - Tela de criação de relatório.

FONTE: Imagem própria.

FIGURA 4.4.10 - Tela de relatório.

Data	Nome	Código do cartão	Porta	Setor	Permissão
19/06/2018 17:59	None	fg5rd	1	TI - Porta da sala de TI	Acesso negado
19/06/2018 17:51	Raphael Guedes Spinelli	tv45hb	1	TI - Porta da sala de TI	Acesso permitido
19/06/2018 17:50	Raphael Guedes Spinelli	tv45hb	6	TI - Sala dos servidores	Acesso permitido
19/06/2018 17:49	Diego	4f8y65r	6	TI - Sala dos servidores	Acesso negado
12/04/2018 18:29	Raphael Guedes Spinelli	tv45hb	1	TI - Porta da sala de TI	Acesso permitido
12/04/2018 11:19	None	AV56F3	1	TI - Porta da sala de TI	Acesso negado
11/04/2018 23:57	Raphael Guedes Spinelli	tv45hb	1	TI - Porta da sala de TI	Acesso permitido

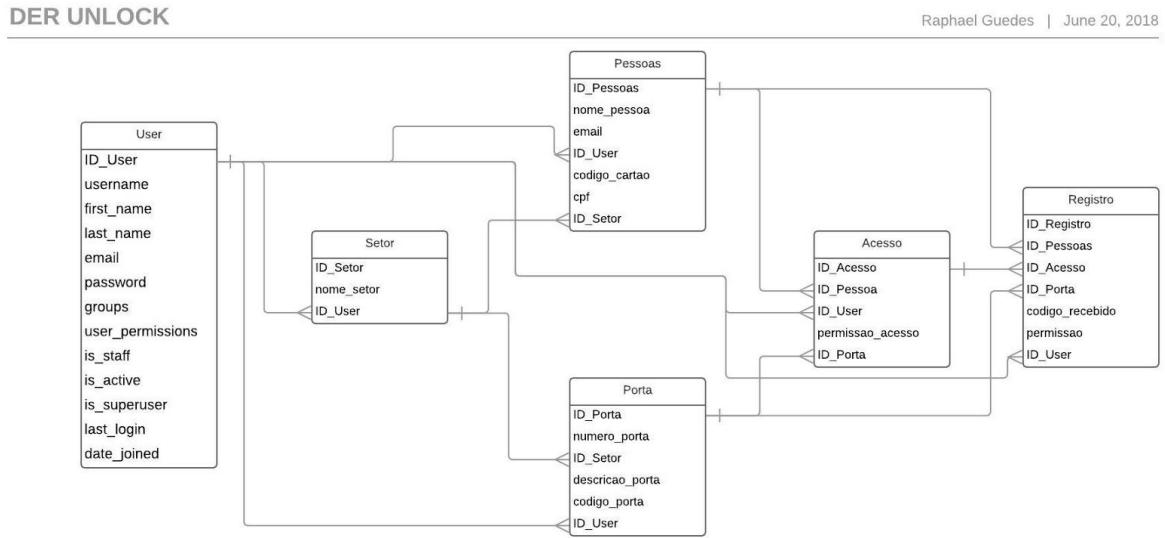
FONTE: Imagem própria.

Essas funções de gerenciamento só são possíveis graças a um banco de dados bem estruturado. Como mostra a figura 4.4.11, o banco de dados foi modelado com 6 tabelas, “User” para dados dos usuários da aplicação, “Setor” para poder setorizar as seguintes duas tabelas, “Porta” para dados dos dispositivos do sistema, “Pessoas” para dados dos usufrutuários do sistema, ou seja, as pessoas que terão acessos, “Acessos” que é uma tabela de relação entre os dispositivos e as pessoas e por fim “Registros” para gravar os dados das tentativas de acessos.

É através da tabela “Acessos” que se faz a análise de liberação ou não dos acessos. E a partir das chaves estrangeiras “ID_User” da tabela “User” nas demais tabelas, diferentes usuários administradores (User) do sistema de controle de

acesso “Unlock”, tem acesso restrito a seus próprios dispositivos (porta), usufrutuários (pessoas), setores, acessos e registros, ou seja, cada usuário da aplicação terá sua própria interface de gerenciamento isolada de outros usuários, possibilitando a utilização de um mesmo servidor central único para todos os administradores de dispositivos, porém não inviabilizando também a utilização de diferentes servidores pontuais, localizados divididos por instituições por exemplo.

FIGURA 4.4.11 - DER da aplicação web.



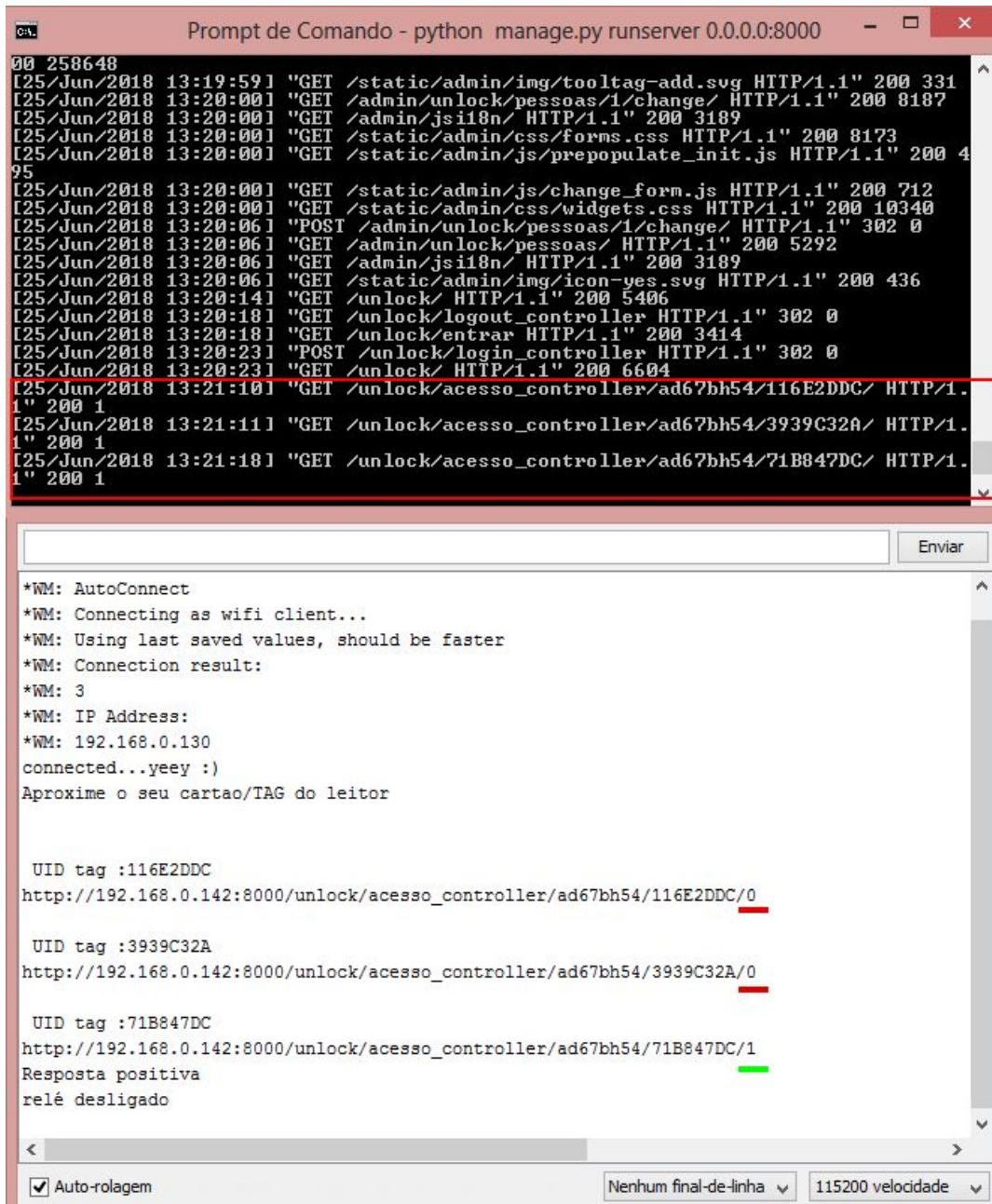
FONTE: Imagem própria.

5 RESULTADOS

Com a conclusão deste projeto, foram obtidos os protótipos iniciais do hardware e do software do sistema de segurança e controle de acesso, assim como a comprovação de seu funcionamento.

Conforme demonstrado na figura 5.1, a realização do teste inicial de funcionamento nos revela que o hardware se conecta com uma rede wifi de acesso a internet já salva na memória, realiza 3 tentativas de acessos com tags diferentes e libera o acesso exclusivamente da tag cadastrada e habilitada no sistema (FIGURA 5.2).

FIGURA 5.1 - Protótipo em funcionamento.



The figure consists of two screenshots of computer interfaces. The top window is titled 'Prompt de Comando - python manage.py runserver 0.0.0.0:8000' and shows a command-line log of HTTP requests from June 25, 2018, at 13:19:59. The bottom window is a terminal or log viewer showing the output of a tag reader application. It displays connection logs, IP address information, and three successful access attempts corresponding to the log entries above. The third attempt is highlighted with a green bar.

```

[00 258648
[25/Jun/2018 13:19:59] "GET /static/admin/img/tooltag-add.svg HTTP/1.1" 200 331
[25/Jun/2018 13:20:00] "GET /admin/unlock/pessoas/1/change/ HTTP/1.1" 200 8187
[25/Jun/2018 13:20:00] "GET /admin/jsi18n/ HTTP/1.1" 200 3189
[25/Jun/2018 13:20:00] "GET /static/admin/css/forms.css HTTP/1.1" 200 8173
[25/Jun/2018 13:20:00] "GET /static/admin/js/prepopulate_init.js HTTP/1.1" 200 4
95
[25/Jun/2018 13:20:00] "GET /static/admin/js/change_form.js HTTP/1.1" 200 712
[25/Jun/2018 13:20:00] "GET /static/admin/css/widgets.css HTTP/1.1" 200 10340
[25/Jun/2018 13:20:06] "POST /admin/unlock/pessoas/1/change/ HTTP/1.1" 302 0
[25/Jun/2018 13:20:06] "GET /admin/unlock/pessoas/ HTTP/1.1" 200 5292
[25/Jun/2018 13:20:06] "GET /admin/jsi18n/ HTTP/1.1" 200 3189
[25/Jun/2018 13:20:06] "GET /static/admin/img/icon-yes.svg HTTP/1.1" 200 436
[25/Jun/2018 13:20:14] "GET /unlock/ HTTP/1.1" 200 5406
[25/Jun/2018 13:20:18] "GET /unlock/logout_controller HTTP/1.1" 302 0
[25/Jun/2018 13:20:18] "GET /unlock/entrar HTTP/1.1" 200 3414
[25/Jun/2018 13:20:23] "POST /unlock/login_controller HTTP/1.1" 302 0
[25/Jun/2018 13:20:23] "GET /unlock/ HTTP/1.1" 200 6604
[25/Jun/2018 13:21:01] "GET /unlock/acesso_controller/ad67bh54/116E2DDC/ HTTP/1.
1" 200 1
[25/Jun/2018 13:21:11] "GET /unlock/acesso_controller/ad67bh54/3939C32A/ HTTP/1.
1" 200 1
[25/Jun/2018 13:21:18] "GET /unlock/acesso_controller/ad67bh54/71B847DC/ HTTP/1.
1" 200 1

*WM: AutoConnect
*WM: Connecting as wifi client...
*WM: Using last saved values, should be faster
*WM: Connection result:
*WM: 3
*WM: IP Address:
*WM: 192.168.0.130
connected...yeey :)
Aproxime o seu cartao/TAG do leitor

UID tag :116E2DDC
http://192.168.0.142:8000/unlock/acesso_controller/ad67bh54/116E2DDC/0

UID tag :3939C32A
http://192.168.0.142:8000/unlock/acesso_controller/ad67bh54/3939C32A/0

UID tag :71B847DC
http://192.168.0.142:8000/unlock/acesso_controller/ad67bh54/71B847DC/1
Resposta positiva
relé desligado

```

FONTE: Imagem própria.

FIGURA 5.2 - Confirmação de funcionamento do sistema no relatório da aplicação “Unlock”.



The screenshot shows a table titled "Relatório geral de registros" (General Access Log Report) from the "Unlock" application. The columns are: Data (Data), Nome (Name), Código do cartão (Card Code), Porta (Door), Setor (Sector), and Permissão (Permission). The data rows are:

Data	Nome	Código do cartão	Porta	Setor	Permissão
25/06/2018 13:21	Raphael Guedes Spinelli	71B847DC	1	TI - Porta da sala de TI	Acesso permitido
25/06/2018 13:21	None	3939C32A	1	TI - Porta da sala de TI	Acesso negado
25/06/2018 13:21	None	116E2DDC	1	TI - Porta da sala de TI	Acesso negado

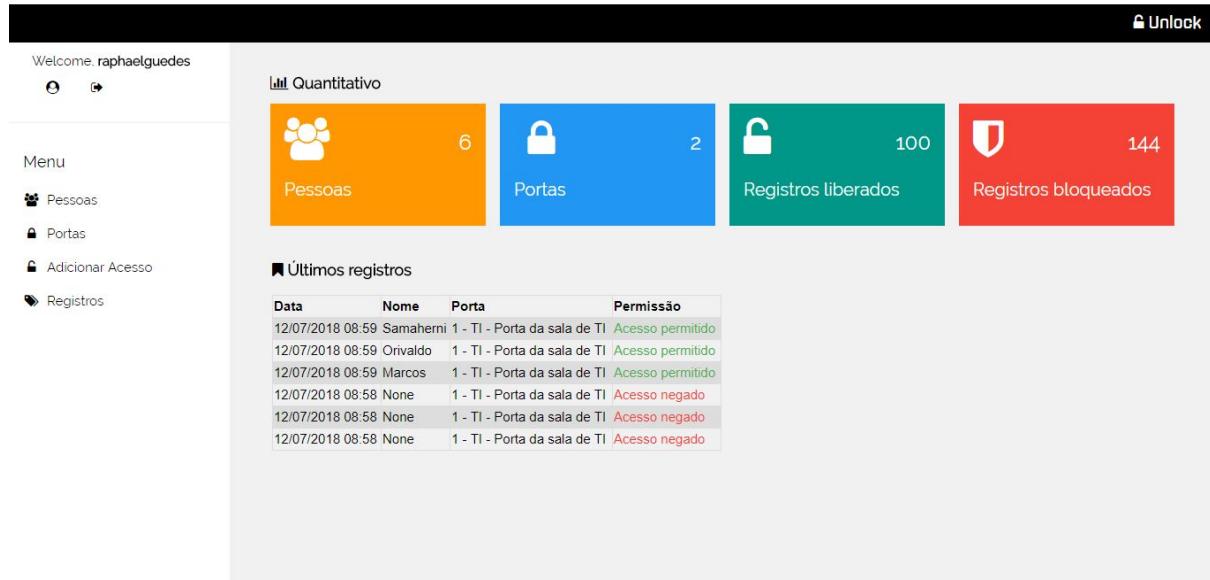
FONTE: Imagem própria.

Em seguida para comprovar o funcionamento da função de bloqueios, cadastrou-se 3 novos usufrutuários dando-lhes as mesmas permissões acessos e foram realizados um acesso para cada um deles (FIGURA 5.3).

Como mostrado na figura Figura 5.3, todos os acessos foram realizados com sucesso, como esperado. Em seguida, bloqueou-se o acesso de um dos usufrutuários (FIGURA 5.4) e foram refeitas as solicitações de acesso.

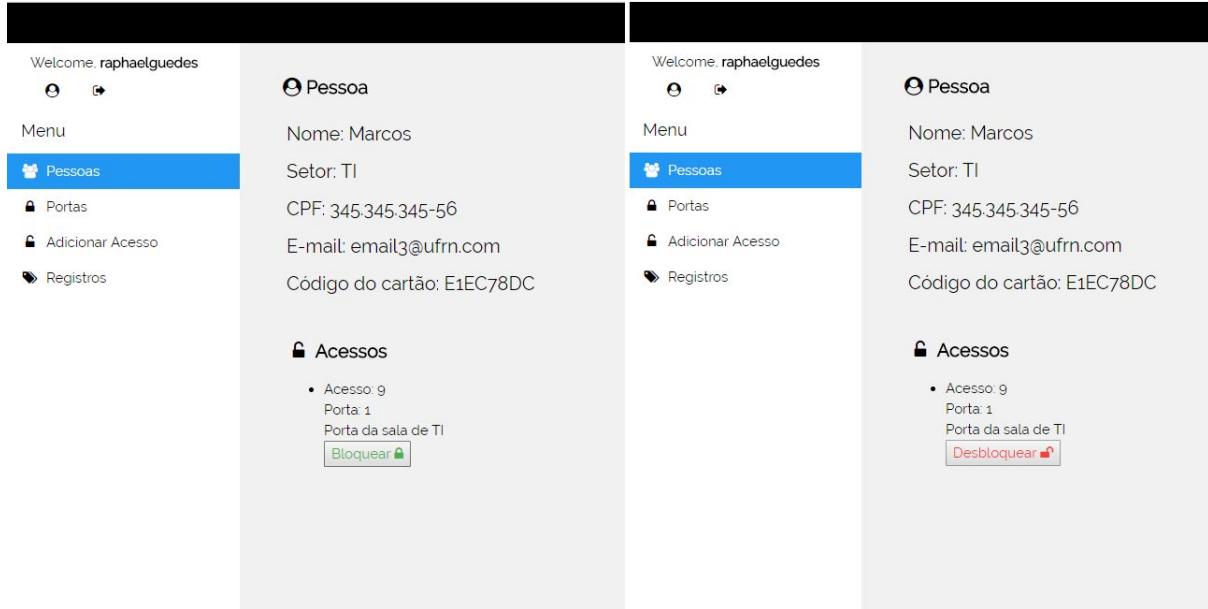
Conforme pode ser visto no relatório de acessos da Figura 5.5, é possível notar que o usufrutuário em questão não obteve acesso permitido após a realização de seu bloqueio, confirmando o funcionamento da função.

FIGURA 5.3 - Confirmação de funcionamento da função de bloqueio parte1.



FONTE: Imagem própria.

FIGURA 5.4 - Realização do bloqueio para teste de funcionamento da função de bloqueio.



FONTE: Imagem própria.

FIGURA 5.5 - Confirmação de funcionamento da função de bloqueio parte2.

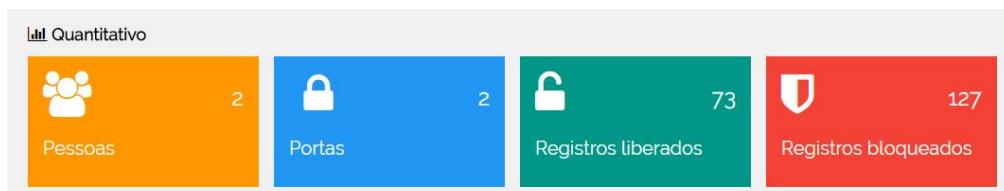
Relatório geral de registros						Unlock
Data	Nome	Código do cartão	Porta	Setor	Permissão	
12/07/2018 09:13	Marcos	E1EC78DC	1	TI - Porta da sala de TI	Acesso negado	
12/07/2018 09:12	Samaherni	813578DC	1	TI - Porta da sala de TI	Acesso permitido	
12/07/2018 09:12	Orivaldo	61EC78DC	1	TI - Porta da sala de TI	Acesso permitido	
12/07/2018 08:59	Samaherni	813578DC	1	TI - Porta da sala de TI	Acesso permitido	
12/07/2018 08:59	Orivaldo	61EC78DC	1	TI - Porta da sala de TI	Acesso permitido	
12/07/2018 08:59	Marcos	E1EC78DC	1	TI - Porta da sala de TI	Acesso permitido	

FONTE: Imagem própria.

Comprovado o funcionamento do protótipo, realizou-se ao sistema uma série de exames de estresse para saber como ele se comportava quando forçado a trabalhar no seu limite de operações. Para isso foram realizados 200 tentativas de acessos no menor tempo possível de execução com diferentes tags RFID.

O resultado deste exame (FIGURA 5.3) nos mostrou que o sistema funcionou corretamente em todas tentativas de acesso, contabilizando 73 registros liberados e 127 bloqueados.

FIGURA 5.6 - Confirmação do teste de estresse.



FONTE: Imagem própria.

Além disso, o hardware passou também por um ciclo de mais de 20 reinicializações sem apresentar erros ao ligar, conectando ou gerando uma requisição para se conectar a uma rede todas as vezes.

Com base nesses testes realizados é possível confirmar o funcionamento do protótipo, contudo comprehende-se a necessidades de mais testes, como testes em campo, outros testes de estresse e testes com mais dispositivos funcionando ao mesmo tempo.

6 CONCLUSÃO

Após a montagem do protótipo, o sistema passou por testes para a verificação de possíveis erros e confirmação de funcionamento. Finalizados os reparos nos códigos e no hardware, foi realizado ao sistema exames de estresse para testar seus limites, avaliar seu comportamento e medir seu desempenho.

Com base na boa execução dos testes realizados com o protótipo, é possível concluir a viabilidade da implantação do sistema em diversas áreas de atuação, bem como sua facilidade de utilização e instalação, contudo comprehende-se a necessidades de mais testes, como testes em campo e outros testes de estresse.

Na realização dos testes foi possível comprovar também as facilidades provenientes da tecnologia RFID, como a praticidade no momento da verificação e liberação do acesso, uma vez que os usufrutuários do sistema não necessitam digitar senhas ou entrar em contato com o equipamento, além da confiabilidade, tendo em vista que na fase de testes não ocorreu nenhum erro de validação proveniente da tecnologia.

Entretanto, foi possível notar possíveis melhorias no sistema que precisam ser melhor estudadas, analisadas e desenvolvidas para se começar a pensar na transformação do protótipo em produto, como a dependência de energia e rede com internet para o sistema funcionar, questões de segurança em relação a utilização de conexão wifi, elaboração de uma placa circuito impresso, mais opções de gerenciamento para a aplicação, além de uma possível melhor comunicação do hardware com a aplicação web através do protocolo MQTT (**Message Queuing Telemetry Transport**).

7 BIBLIOGRAFIA

THOMSEN, Adilson. **Como programar o NodeMCU com IDE Arduino.** 2016. Disponível em: <<https://www.filipeflop.com/blog/programar-nodemcu-com-ide-arduino/>> Acesso em: Abril de 2018.

GSTI, Portal. **O que é Django?** Disponível em: <<https://www.portalgsti.com.br/django/sobre/>> Acesso em: Abril de 2018.

OLIVEIRA, Ricardo Rodrigues. **USO DO MICROCONTROLADOR ESP8266 PARA AUTOMAÇÃO RESIDENCIAL.** (2017). Disponível em: <<http://monografias.poli.ufrj.br/monografias/monopoli10019583.pdf>> Acesso em: Junho de 2018.

PIRES, Cosme. **Fechaduras Eletrônicas ou Elétricas – Como Escolher?** Disponível em: <<https://www.fazfacil.com.br/reforma-construcao/fechaduras-eletronicas/>> Acesso em: Junho de 2018.

THOMSEN, Adilson. **Controlando lâmpadas com Módulo Relé Arduino.** (2013). Disponível em: <<https://www.filipeflop.com/blog/controle-modulo-rele-arduino/>> Acesso em: Junho de 2018.

MUNDO DA ELETRÔNICA. **Como funciona um relé? O que é um relé?** Disponível em: <<https://www.mundodaeletrica.com.br/como-funciona-um-rele-o-que-e-um-rele/>> Acesso em: Junho de 2018.

HU Infinito. **Módulo WiFi ESP8266 NodeMcu ESP-12E.** Disponível em: <<http://www.huinfinito.com.br/home/1145-modulo-wifi-esp8266-nodemcu-esp-12e.html>> Acesso em: Maio de 2018.

BENCHOFF, Brian. **THE ESP8266 WIFI MODULE (IT'S \$5).** (2014). Disponível em: <<https://hackaday.com/2014/08/26/new-chip-alert-the-esp8266-wifi-module-its-5/>> Acesso em: Maio de 2018.

THOMSEN, Adilson. **O que é Arduino?.** (2014). Disponível em: <<https://www.filipeflop.com/blog/o-que-e-arduino/>> Acesso em: Maio de 2018.

DMZ Connection. **Cartão Mifare ISO.** Disponível em: <<http://www.dmzconnection.com/cartao-mifare-iso/>> Acesso em: Maio de 2018.

Blog Scriptcase. **A diferença entre um Site e uma Aplicação WEB.** (2013). Disponível em: <<http://www.scriptcaseblog.com.br/diferenca-site-aplicacao-web/>> Acesso em: Maio de 2018.

Nations, Daniel. **What Exactly Is a Web Application?**. (2018). Disponível em: <<https://www.lifewire.com/what-is-a-web-application-3486637>> Acesso em: Maio de 2018.

FIELDING, Hypertext Transfer Protocol -- HTTP/1.1. (1999). Disponível em: <<https://www.w3.org/Protocols/rfc2616/rfc2616.html>> Acesso em: Maio de 2018.

Portal DEVMEDIA, **Como funcionam as aplicações web.** Disponível em: <<https://www.devmedia.com.br/como-funcionam-as-aplicacoes-web/25888>> Acesso em: Maio de 2018.

PINHEIRO, José Maurício dos Santos. **RFID: O fim das filas está próximo?**. (2006). Disponível em: <<http://www.teleco.com.br/pdfs/tutorialrfid2.pdf>> Acesso em: Maio de 2018.

Portal Teleco. **RFID: O que é?**. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialrfid/pagina_1.asp> Acesso em: Maio de 2018.

DELAI, André Luiz. **Sistemas embarcados: a computação invisível.** (2013). Disponível em: <<https://www.hardware.com.br/artigos/sistemas-embarcados-computacao-invisivel/conceito.html>> Acesso em: Maio de 2018.

MARWEDEL, Peter. **Embedded System Design: Embedded Systems Foundations of Cyber-Physical Systems.** 2nd ed. Springer, 2011.

VALENTE, Bruno Alexandre Loureiro. **Um middleware para a Internet das coisas.** 2011.

DE OLIVEIRA, Sergio. **Internet das Coisas com ESP8266, Arduino e Raspberry Pi.** Primeira Edição. São Paulo: Novatec Editora Ltda, 2017.

SANTOS, B. P., Silva, L. A., Celes, C. S., Borges, J. B., Peres, B. S., Vieira, M. M., . . Loureiro, A. A. (maio de 2016). **Internet das Coisas: da Teoria à Prática.** Livro Texto Minicursos - SBRC, 2016.

KUROSE, J. F. and Ross, K. W.. **Computer Networking: A TopDown Approach.** 6th edition. Pearson,(2012).

PERERA, Charith, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. **Context aware computing for the internet of things: A survey.** VOL. 16, NO. 1. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 2014.

Press, Gil.**Internet of Things By The Numbers: Market Estimates And Forecasts.** Forbes, 2014.