

INSTITUTO FEDERAL DE SANTA CATARINA

LUIZA ALVES DA SILVA

**Implementação de armário guarda-volumes
eletrônico com auditoria**

São José - SC

dezembro/2023

IMPLEMENTAÇÃO DE ARMÁRIO GUARDA-VOLUMES ELETRÔNICO COM AUDITORIA

Monografia apresentada ao Curso de Engenharia de Telecomunicações do campus São José do Instituto Federal de Santa Catarina para a obtenção do diploma de Engenheiro de Telecomunicações.

Orientador: Prof. Cleber Jorge Amaral, Dr.

São José - SC

dezembro/2023

RESUMO

Este projeto visa desenvolver um armário guarda-volumes integrado a uma central eletrônica que possuirá as informações dos usuários, tendo controle sobre abertura e fechamento das portas. Utilizando a avançada tecnologia RFID, a identificação dos usuários no sistema será feita de maneira eletrônica. O projeto engloba também uma adaptação mecânica para abertura eletrônica dos compartimentos. Para esse controle pretende-se efetuar a implementação de um dispositivo eletrônico, que através de uma interface de rede permitirá o acesso de usuários no sistema. Espera-se também o desenvolvimento de um serviço e aplicação de administração do sistema, que possibilitará o cadastro de usuários, verificação de compartimentos em uso e disponíveis. Resultados esperados deste projeto é que desta forma facilite tanto para os administradores do local quanto para quem faz uso desses armários guarda-volumes reduzindo os problemas com chaves mecânicas e/ou cadeados.

Palavras-chave: armário eletrônico. guarda-volume. abertura remota.

ABSTRACT

This project aims to develop a storage closet integrated with an electronic center that will have user information, having control over opening and closing doors. Using advanced RFID technology, user identification in the system will be done electronically. The project also includes a mechanical adaptation for electronic opening of the compartments. For this control, the aim is to implement an electronic device, which, through a network interface, will allow users to access the system. The development of a system administration service and application is also expected, which will enable user registration and verification of compartments in use and available. The expected results of this project are that it will make things easier for both the site administrators and those who use these storage lockers, reducing problems with mechanical keys and/or padlocks.

Keywords: electronic locker. lockers. remote opening.

LISTA DE ILUSTRAÇÕES

Figura 1 – Armário inteligente para guarda volumes	15
Figura 2 – Componentes principais para construção de armários eletrônicos	17
Figura 3 – Cilindro interno de uma fechadura mecânica	18
Figura 4 – Trava elétrica solenoide internamente	18
Figura 5 – Sensor de Proximidade Magnético	19
Figura 6 – Kit de desenvolvimento ESP32-DevKitC	20
Figura 7 – Estrutura de um quadro EPC	22
Figura 8 – Sinais PWM com diferentes <i>duty cycles</i>	24
Figura 9 – Quadro de transmissão Wi-Fi	25
Figura 10 – Arquitetura <i>Publish/Subscribe</i>	27
Figura 11 – Websocket	28
Figura 12 – Testes no protótipo inicial	30
Figura 13 – Diagrama do projeto	31
Figura 14 – Cronograma de atividades	32

LISTA DE TABELAS

Tabela 1 – Comparativo entre diversas tecnologias e padrões RFID	21
--	----

LISTA DE ABREVIATURAS E SIGLAS

AES *Advanced Encryption Standard.*

AP *Access Point.*

API *Application Programming Interface.*

BLE *Bluetooth Low Energy.*

BSS *Basic Service Set.*

DSSS *Direct Sequence Spread Spectrum.*

EPC *Electronic Product Code.*

ESP-IDF *Espressif IoT Development Framework.*

GPIO *General Purpose Input/Output.*

I2C *Inter-Integrated Circuit.*

IDE *Integrated Development Environment.*

IFSC *Instituto Federal de Santa Catarina.*

IoT *Internet das Coisas.*

JSON *JavaScript Object Notation.*

LCD *Liquid Crystal Display.*

LED *Light Emitting Diode.*

MIMO *multiple-input and multiple-output.*

MQTT *Message Queuing Telemetry Transport.*

NFC *Near Field Communication.*

PAN *Personal Area Network.*

PWM *Pulse Width Modulation.*

QR Code *Quick Response Code.*

RF *Radiofrequência.*

RFID Radio Frequency Identification.

SC-FDMA *Singe Carrier - Frequency Division Multiple Access.*

SHF *Super High Frequency.*

SMS Serviço de Mensagens Curtas.

SoC *System on a chip.*

SPI *Serial Peripheral Interface.*

TLS *Transport Layer Security.*

UART *Universal Asynchronous Receiver/Transmitter.*

UHF *Ultra High Frequency.*

UPC *Universal Product Code.*

USB *Universal Serial Bus.*

VSCoDe *VSCoDe Extension.*

WEP *Wired Equivalent Privacy.*

Wi-fi *Wireless Fidelity.*

WLAN *Wireless Local Area Network.*

WPA *Wi-Fi Protected Access.*

WPA2 *Wi-Fi Protected Access 2.*

SUMÁRIO

1	INTRODUÇÃO	10
1.1	Objetivos	11
1.1.1	Objetivo geral	11
1.1.2	Objetivos específicos	11
1.2	Organização do texto	12
2	REVISÃO BIBLIOGRÁFICA	13
2.1	Armários Guarda-volumes convencionais	13
2.2	Armários eletrônicos	13
2.2.1	Empresa Armários inteligentes	14
2.2.2	Empresa Nilko	14
2.2.3	Empresa Oppitz	14
2.2.4	Empresa Duratta	15
2.2.5	Visão geral dos armários eletrônicos disponíveis no mercado	15
2.3	Componentes para a construção de armários eletrônicos	16
2.4	Estrutura eletromecânica	17
2.4.1	Trava para abertura de compartimentos	17
2.4.2	Sensor para abertura de compartimento	18
2.4.3	Dispositivo eletrônico	19
2.4.4	Abertura eletrônica	21
2.4.5	Interface Homem-Máquina	23
2.5	Comunicação sem fio	24
2.5.1	<i>Protocolo de comunicação</i>	26
2.6	Gestão online	27
2.6.1	Banco de dados	27
2.6.2	Servidor	28
3	PROPOSTA	29
3.1	Cronograma de atividades	31
	REFERÊNCIAS	33

1 INTRODUÇÃO

Em ambientes onde há um grande fluxo de pessoas, nota-se a necessidade de armários guarda-volumes, seja para manter a organização do ambiente, como também facilitar o dia-a-dia dos usuários. Mas apesar disso, podem trazer vários problemas como, perdas de chaves, cópias indevidas e manutenção muito frequente das fechaduras mecânicas. A automatização de armários guarda-volumes pode ser uma boa solução tanto para se ter o processo administrativo simplificado e ter uma redução significativa nos problemas mencionados, fornecendo relatórios em tempo real sobre a utilização, além de otimizar o uso destes espaços.

Por exemplo, o [Instituto Federal de Santa Catarina](#) campus de São José disponibiliza uma série de serviços e auxílios para melhor atender os estudantes. O campus é frequentado por aproximadamente 1,9 mil alunos no total dos diversos cursos ofertados [IFSC \(2022b\)](#). Um desses auxílios oferecidos é a disponibilização de 75 armários guarda-volumes para os acadêmicos, sabendo que são insuficiente para todos. Os interessados realizam sua inscrição através de um Edital, podendo desfrutar deste benefício ao longo do semestre letivo. Os contemplados ficam sob posse da chave de um dos compartimentos do armário, sendo ele devolvido ao final do período vigente. Com o edital, pretende-se auxiliar a permanência do aluno na instituição e minimizando a mobilidade diária com os materiais ([IFSC, 2022a](#)).

Apesar de ser um serviço extremamente necessário aos estudantes, o edital proposto, em alguns aspectos se mostra pouco eficiente. Como mencionado anteriormente, a chave do compartimento permanece com o mesmo usuário durante todo o semestre letivo. É evidente o fato de que possui pouca quantidade de armários em relação ao número aproximado de alunos. Isso acaba resultando em muitas das reservas de chaves, mesmo que não tenha a real necessidade de fazer o uso durante o semestre. Então, caso um discente não contemplado queira fazer uso esporádico, não terá essa possibilidade, mesmo que tenha compartimentos livres.

Além disso, o controle de acesso aos compartimentos possui alguns pontos críticos, que podem acabar trazendo sérios problemas. A segurança é uma delas, caso ocorra a perda de chaves, por exemplo, os itens armazenados ficam comprometidos até que a situação seja resolvida. Pode vir a ocorrer cópias indevidas por algum usuário malicioso e ele se sentir no direito de utilizar o benefício enquanto outra pessoa esteja fazendo uso. Além da limitação há apenas 75 acadêmicos ao longo do semestre letivo, a convivência diária neste ambiente, mostra que muitos dos alunos contemplados não fazem o devido uso dos guarda-volumes, deixando na maior parte do tempo ocioso.

Com uma gestão online dos compartimentos a segurança dos itens armazenados se torna menos vulnerável. Nos casos de arrombamento, o administrador recebe uma notificação que há uma abertura indevida, podendo agir de maneira mais rápida diante desta situação. Nos casos de esquecimento de itens, o responsável pelo estabelecimento pode entrar em contato com o usuário informando o ocorrido. Além poder ter fácil acesso da quantidade de compartimentos disponíveis. Então, os armários guarda-volumes com controle de acesso através de chaves mecânicas podem ser pouco práticos quando problemas ocorridos por eventos externos acontecerem.

No mercado existem soluções que não utilizam chaves mecânicas e é visto na prática uma grande facilidade no uso. O *Amazon Hub Locker* é um armário eletrônico desenvolvido pela empresa *Amazon* que permite que seus clientes retirem suas encomendas através de um auto-atendimento no local de instalação dos armários que acharem mais apropriado. Para o usuário pegar sua mercadoria, é preciso inserir no painel do *Locker* um código de 6 dígitos recebido por *e-mail*, então o compartimento com a respectiva mercadoria irá destravar (AMAZON, 2022). A partir disso surgiram outras empresas com ideias similares ampliando para diferentes aplicações, como condomínios, indústrias, shoppings, etc (OIHANDOVER, 2022). Em suma, abertura de compartimentos através de carteirinha de estudante, cartão de crédito, aplicativo de celular, por exemplo, se tornam soluções muito atraentes.

A ideia deste trabalho aproveita a infraestrutura atual do campus, utilizando os armários já existentes e retirando a dependência e problemas relacionados com chaves. A proposta é integrá-lo a um dispositivo eletrônico para abertura de compartimentos, para que assim alcance mais estudantes não havendo a necessidade de um edital, tornando mais seguro e diminuindo a ociosidade de compartimentos.

1.1 Objetivos

1.1.1 Objetivo geral

O objetivo deste projeto é desenvolver um protótipo de armário eletrônico com auditoria de baixo custo pra implantar no campus de São José reaproveitando os armários guarda-volumes convencionais.

1.1.2 Objetivos específicos

Para a conclusão do objetivo geral, definiu-se os objetivos específicos.

1. Desenvolver a abertura eletrônica de compartimentos;
2. Desenvolver o controle eletrônico de abertura dos compartimentos;

3. Desenvolver autenticação de usuários;
4. Desenvolver uma Interface Homem-Máquina para uso do armário;
5. Desenvolver um serviço e aplicação para cadastro e controle de usuários;
6. Desenvolver a comunicação entre estrutura eletromecânica e o servidor;
7. Desenvolver um protótipo para testar o conceito.

1.2 Organização do texto

O texto está organizado da seguinte forma: No [Capítulo 2](#) é apresentado a fundamentação teórica pra melhor compreensão do projeto como um todo. No [Capítulo 3](#) é apresentado a proposta para a execução deste projeto.

2 REVISÃO BIBLIOGRÁFICA

2.1 Armários Guarda-volumes convencionais

Em alguns locais onde há um grande fluxo de pessoas, pode ser encontrado armários guarda-volumes. Os Armário guarda-volumes é um móvel que internamente possui um conjunto de vários compartimentos, que serve para as pessoas armazenarem seus pertences pessoais durante a execução de suas tarefas diárias naquele local. Para a utilização desses compartimentos os usuários precisam estar de acordo com as regras de negócio do ambiente que se encontram.

As características dos armários convencionais variam: alguns são materiais revestidos em aço, madeira ou metal. Alguns estabelecimentos não possuem segurança física nos compartimentos, ficando a critério das pessoas que circulam naquele ambiente a confiança de não mexer em objetos pessoais de terceiros. Outros estabelecimentos possuem cadeados ou fechaduras mecânicas com chaves para trancar os compartimentos. O funcionamento é simples: caso o armário contenha chave, você solicita a chave, guarda seus pertences pessoais, tranca e carrega consigo a chave ou cadeado do respectivo compartimento.

Observa-se que as aplicações dos armários guarda-volumes são diversas, mas todas têm o mesmo objetivo: organização no ambiente e manter objetos pessoais em segurança. Em academias normalmente encontra-se armários convencionais com cadeados ou até mesmo sem nenhuma segurança. Em shoppings, supermercados e instituições normalmente possuem armários convencionais que utilizam chaves e pode ser encontrado também alguns locais que tenha um funcionário que fica responsável pelo gerenciamento e segurança dos itens guardados. Alguns incômodos como a manutenção, perda de cadeados ou de chaves, cópias indevidas e circunstâncias adversas, proporcionam uma dor de cabeça desnecessária tanto para quem faz uso quanto para os administradores do local.

Com o passar do tempo, novas tecnologias e inovações foram surgindo e hoje pode ser encontrado no mercado o uso de armários eletrônicos, diminuindo alguns problemas que podiam ser encontrados com os armários convencionais.

2.2 Armários eletrônicos

O interesse pelo uso de tecnologias novas para facilitar o dia a dia das pessoas está em constante crescimento. Os produtos a seguir oferecem soluções de armários eletrônicos para diferentes segmentos do mercado. Então, qualquer local que possua circulação de pessoas pode solicitar e fazer uso do benefício, desde que cumpra com as regras de negócio

do ambiente em questão. Os armários eletrônicos que podem ser personalizados de acordo com a solicitação do cliente, além de possuir tamanhos de compartimentos variados e ser um sistema modular, permitindo sua expansão. As soluções permitem integração com o sistema do cliente, possui também possibilidade de abertura de compartimentos através de aplicativo e também outras tecnologias de acesso.

2.2.1 Empresa Armários inteligentes

Segundo a empresa Armários Inteligentes, no *Locker* Guarda-Volumes, o usuário interage com o armário através de uma tela sensível ao toque, a abertura dos compartimentos ocorre através de senha, código de barras, *QR Code*, *RFID* ou *NFC*. O gerenciamento dos compartimentos é feito no próprio armário, sendo opcional o uso da plataforma de gestão online, que permite o controle de usuários podendo ser acessada pelo computador ou celular. Já na solução Armário autônomo o usuário possui mais de uma forma de autenticação, senha numérica + biometria, senha numérica + *RFID* ou senha numérica + código de barras. A interação com o usuário e interface administrativa ocorre através de um *LCD* e teclado numérico. Assim, possibilitando a configuração de usuários no próprio armário, não havendo a necessidade de uma plataforma *online*. No modelo Armário conectado, o usuário abre o compartimento através de um aplicativo de celular com acesso a *internet*, assim como a interface administrativa (INTELIGENTES, 2023).

2.2.2 Empresa Nilko

A empresa Nilko tem como foco armários de aço, mas também pode ser encontrado armários de plástico. A quantidade de compartimentos variam de 1 porta por coluna até 6 portas por colunas e o tamanho varia de acordo com a necessidade do cliente, pode ser visto compartimentos para objetos de pequenos volumes, compartimentos largos, carrinhos, etc. Métodos de abertura dos compartimentos podem ser através de cadeado, fechadura mecânica, teclado numérico com câmera, sem chave nenhuma ou através de aproximação. Para aberturas remotas, pode ser expandido para até 151 portas por central inteligente (NILKO, 2023).

2.2.3 Empresa Oppitz

Segundo a empresa Oppitz, seus produtos de armários inteligentes abrangem diversos casos de uso, seja para condomínios, shoppings, *e-commerce*, armazenamento de chaves, entre outros. A solução para guarda-volumes possibilita abertura dos compartimentos de diversas formas, através de senha numérica, enviada por *e-mail* ou *SMS*, *QR Code* impresso, por aplicativo ou biometria. O gerenciamento é feito através de um sistema administrativo integrado ao sistema do cliente permitindo que se tenha controle remoto dos

compartimentos. A empresa permite também a instalação de câmeras para monitoramento dos armários. Na [Figura 1](#) pode ser visto um armário guarda-volumes ([OPPITZ, 2023](#)).

Figura 1 – *Armário inteligente para guarda volumes*



Fonte: [Oppitz \(2023\)](#)

2.2.4 Empresa Duratta

A empresa Duratta possui diversos produtos, um deles é o armário biométrico. O armário Biométrico é um equipamento para utilização interna com estrutura de aço carbono composto por 6 portas, comporta com 1 módulo + 5 portas utilizáveis com as seguintes dimensões: largura de 80 centímetros, altura de 198 centímetros e profundidade de 51 centímetros. A abertura pode ser feita através de *RFID*, código de barras ou biometria e a interface com o usuário é através de uma tela sensível ao toque, podendo ter usuário fixo ou rotativo ([DURATTA, 2023](#)).

2.2.5 Visão geral dos armários eletrônicos disponíveis no mercado

Embora os produtos mencionados anteriormente tenham se destacado, tornando a vida dos usuários mais fácil, a automação não está isenta de desafios. Um aspecto importante é a tendência predominante dessas empresas em não aproveitar os armários convencionais já existentes. Isso resulta no descarte frequente das estruturas dos produtos antigos, perdendo a oportunidade de reutilizar materiais e alcançando assim um número maior de vendas, levando em consideração que muitas empresas e locais públicos possuem armários convencionais.

Além disso, nota-se o aumento do uso de interações do usuário por meio de telas sensíveis ao toque em diversos produtos. Entretanto, essa abordagem pode resultar em uma necessidade mais frequente de manutenção, uma vez que as telas sensíveis ao toque estão

sujeitas a danos, muitas vezes fora do controle administrativo, o que pode comprometer a durabilidade do equipamento. O mesmo pode ser observado com teclados numéricos sensíveis ao toque, amplamente adotados por muitas empresas citadas anteriormente. Problemas recorrentes com a manta de contato desses teclados podem levar a uma manutenção mais frequente, impactando a eficiência e confiabilidade desses dispositivos.

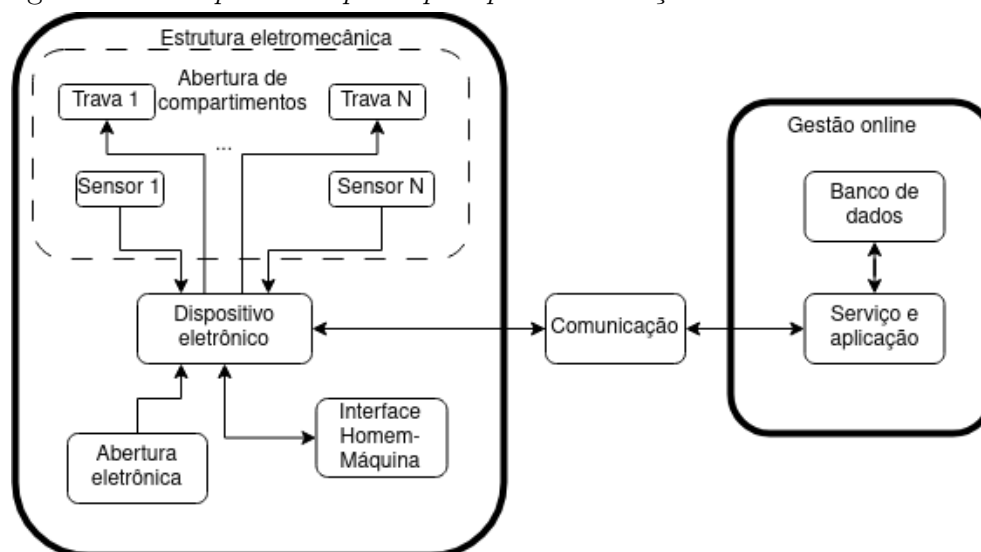
Uma análise breve de mercado revela que certos dispositivos e materiais adotados por algumas dessas empresas apresentadas possuem um custo elevado, resultando em um preço final do produto acima da média. Os leitores biométricos e armários fabricados com aço contribuem para o aumento dos custos, ambos não são materiais e dispositivos de baixo custo. Da mesma forma, a inclusão de câmeras de monitoramento não apenas encarece o produto, mas também implica em uma necessidade frequente de manutenção em caso de falhas. Outra desvantagem é a abertura dos compartimentos por aplicativo. Dessa forma, torna obrigatório o uso de um celular com acesso a *internet* na utilização do benefício limitando o uso de usuários. Assim como a necessidade de manutenção e custos de implementação frequentes, já que atualizações ocorrem para garantir a eficiência do sistema.

Para a contratação de seus serviços, a empresa Armários Inteligentes conta com uma mensalidade, nela está inclusa manutenção e atualização do sistema. O valor mais em conta dentre todos os produtos e modelos citados acima é o armário autônomo, que custa uma mensalidade de em média 8 a 10 mil reais por armário. Cada armário possui em torno de 25 compartimentos, ou seja, uma única central controla apenas um armário. Caso o cliente queira, por exemplo, 50 compartimentos, ele precisa solicitar, duas centrais, que irão se integrar e controlar todos os compartimentos.

2.3 Componentes para a construção de armários eletrônicos

A transição de armários guarda-volumes convencionais que utilizam fechadura mecânica para uma versão eletrônica não é simplesmente a remoção de chaves físicas, há uma complexidade maior nessa integração. Muitos componentes conectados entre si são necessários para que o controle desses armários ocorra de maneira eficiente. Quando o usuário se autentica e solicita a abertura de um compartimento, ao remover a fechadura mecânica e substituí-la por uma trava automática, deve-se fazer uma verificação para detectar se a porta foi aberta e fechada corretamente. Assim, o controle eletrônico avisará o usuário através uma interface o status do seu atual compartimento. Para permitir somente usuários autorizados a acessar os gabinetes, o sistema precisa ter conectividade com a *internet* e através de algum protocolo de comunicação trocar informações com um servidor, tendo assim uma gestão online. Na [Figura 13](#), é apresentado um diagrama destacando os principais componentes necessários para a construção de armários eletrônicos.

Figura 2 – Componentes principais para construção de armários eletrônicos



Fonte: Elaborada pelo autor.

2.4 Estrutura eletromecânica

Sistema eletromecânico consiste na integração de componentes elétricos e mecânicos para criar sistemas com funções específicas. Esta categoria abrange duas classificações: sistemas de energia e sistemas de controle. Nos sistemas de energia, além da ênfase na operação eficiente, são considerados fatores críticos como os custos de fabricação e as perdas energéticas. Por outro lado, nos sistemas de controle, a integridade e segurança da informação trocada desempenham papéis fundamentais, garantindo a eficácia e a confiabilidade desses sistemas (FALCONE, 1979).

2.4.1 Trava para abertura de compartimentos

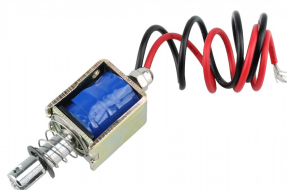
A necessidade de manter um compartimento fechado é para evitar que pessoas não autorizadas tenham acesso a esses locais guardados. Dependendo do ambiente que se encontra esse compartimento, seja ele uma porta, um armário ou um objeto, nota-se a necessidade de aumentar sua segurança, onde apenas uma trava sem nenhuma fechadura não é o suficiente.

O modelo mais comum são as fechaduras mecânicas, na Figura 3 pode ser observado o cilindro interno que a compõe com a chave no engate, ao girar permite o destravamento da fechadura. Na prática podemos encontrar algumas vulnerabilidades, para o caso de fechaduras mecânicas em armários convencionais guarda-volumes, por exemplo, indivíduos tirarem cópias dessas chaves e passar a ter acessos não autorizados ou até mesmo usuários perderem suas chaves, dificultando a retirada de seus pertences do compartimento. Dessa forma a fechadura mecânica não dá total controle de acesso ao local, já que qualquer um com a chave pode acessá-lo.

Figura 3 – *Cilindro interno de uma fechadura mecânica*Fonte: *AECweb (2022)*

Os modelos de fechaduras eletrônicas tem se tornado cada vez mais popular com a crescente evolução da tecnologia, muito comum em locais que necessitam de um controle maior de pessoas que o acessam. As fechaduras eletrônicas são controladas por uma tensão de alimentação, onde ao receber um pulso elétrico, a trava realiza uma ação de abertura ou fechamento. Dentro desse nicho, pode ser visto vários modelos de funcionamento, fechaduras com senha, biométricas, cartões magnéticos, solenoide, etc.

Na figura [Figura 4](#) pode ser visualizado a parte interna de uma trava elétrica solenoide. Para o seu funcionamento correto na sua composição possui uma bobina de fios com n espiras, onde ao ser aplicado uma corrente elétrica no fio condutor cria-se um campo magnético. Essa força aplicada então recolherá o pino da fechadura através de uma mola, fazendo com que seja possível abertura da trava. Com isso, pode se perceber que quando não há fonte de energia, o local guardado pela fechadura permanecerá fechado até que tudo se normalize ([CARDOSO, 2010](#)).

Figura 4 – *Trava elétrica solenoide internamente*Fonte: *Usinainfo (2023)*

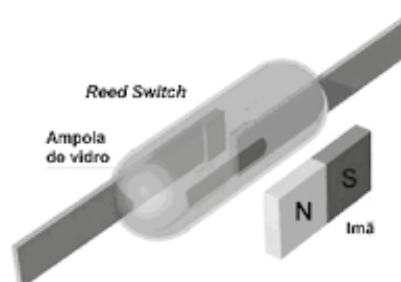
2.4.2 Sensor para abertura de compartimento

Ao utilizar uma trava eletrônica em cada compartimento, exige um monitoramento da porta para que ao trava-lo, ter a certeza que a porta esteja fechada corretamente. Por isso, nota-se a necessidade de utilização de sensores para realizar essa detecção e garantir o funcionamento correto em todos os casos de uso. Dentre todos os sensores existentes que

realizam essa tarefa, o mais adequado para essa aplicação são os sensores de proximidade magnéticos.

O princípio de funcionamento dos *Reed Switch* são baseados em converter um campo magnético em sinais digitais ou analógicos, enviando esse sinal ao sistema de controle. O componente *Reed Switch*, que pode ser visto na Figura 5, possui uma ampola de vidro e internamente possui duas laminas, que em seu estado natural não se encostam, quando detectam presença de um campo magnético, o ímã, as laminas fecham contato permitindo a passagem de corrente elétrica entre seus terminais (THOMAZINI; ALBUQUERQUE, 2020).

Figura 5 – *Sensor de Proximidade Magnético*



Fonte: Thomazini e Albuquerque (2020)

Segundo Moraes e Castrucci (2006), esses sensores de proximidade possuem vantagens e desvantagens relevantes que devem ser lavados em conta dependendo de sua aplicação. Algumas vantagens encontradas são: a vida longa do componente, o fato de possui uma fácil instalação, ser um sensor com uma resposta rápida na sua detecção e possuir baixo custo. Mas esse componente também possui algumas desvantagens, como o fato de não ser seletivo em relação ao alvo, ser sensível a interferências eletromagnéticas. Esses sensores de proximidade magnéticos são muito utilizados para detecção de abertura de portas e janelas.

2.4.3 Dispositivo eletrônico

Microcontroladores são composto por unidades de processamento, memórias e periféricos de entrada e saída em um único *chip*. Assim, possibilita o desenvolvimento de projetos complexos tornando-os mais simples. Normalmente se utiliza a linguagem de programação C para o desenvolvimento de sistemas embarcados, onde o compilador C abstrai os processadores, enquanto os periféricos de entrada e saída são configurados pelo programador que variam de cada *chip*. Por isso é importante analisar o funcionamento de cada chip, normalmente encontrado no site do fabricante (ALMEIDA, 2016).

Segundo a empresa Espressif (2023), os microcontroladores da *Serie ESP32* foram projetados para se obter robustez, versatilidade e confiabilidade em diversas aplicações *IoT* distintas como, por exemplo, *Smart home*, Agricultura inteligente, Assistência médica

robótica, etc. O *SoC* da família ESP32 é a base do *kit* de desenvolvimento *ESP32-DevKitC*, que pode ser visto na [Figura 6](#). Destaca-se alguns componentes principais nos itens a seguir:

- Processador *single/dual core*, cada um com velocidades de *clock* de até 240 MHz;
- Módulo *RF* receptor e transmissor de 2.4GHz;
- Gerador de *clock*;
- Conectividade *Wi-fi* modo Estação, modo *AP* e Estação/*AP*;
- Conectividade *Bluetooth* Clássico e *BLE*;
- *GPIO* para conexão com periféricos externos;
- Conversores analógico-digital de 12 bits e digital-analógico de 8 *bits*;
- Interfaces de comunicação como *SPI*, *I2C* e *UART*.

Figura 6 – *Kit de desenvolvimento ESP32-DevKitC*



Fonte: Elaborada pelo autor.

O ambiente de desenvolvimento para o *hardware* baseado no *chip* da Espressif ESP32 neste cenário apresentado aqui será utilizando a *IDE VSCode* e através dele, será usado a *ESP-IDF* onde possibilitará a compilação e gravação do *firmware*. É ideal que na etapa de desenvolvimento seja utilizado algum *kit* de desenvolvimento dos *SoCs* da Espressif, por exemplo, o ilustrado na [Figura 6](#). Após a instalação da *ESP-IDF* no *VSCode*, a placa do *kit* da ESP32 deve ser conectada através de um cabo *USB* - *USB A* / *micro USB B* no computador que esteja rodando algum desses sistemas operacionais: *Windows*, *Linux* ou *MacOS*.

2.4.4 Abertura eletrônica

Segundo Júnior e Farinelli (2018), sistemas de RFID é uma tecnologia para comunicações sem fio, que permite a conectividade entre periféricos. Algumas aplicações como, por exemplo, rastreamento de objetos, identificação, controle de acesso, facilitam o dia-a-dia de pessoas e empresas a níveis organizacionais. Além disso, o RFID possui uma implementação simples e de baixo custo tornando o seu uso popular e acessível.

O RFID possui três componentes principais, leitor, etiqueta e o software de gerenciamento. O leitor é um dispositivo integrado ao *software* de gerenciamento, que emite sinais permitindo a troca de informações com a etiqueta. Já a etiqueta representa o objeto a ser identificado autorizando-o a requisição ao sistema. O leitor emite um sinal RF através da sua antena, a energia transmitida é captada pela etiqueta. Dessa forma, o circuito interno da etiqueta recebe esse sinal, é alimentado e transmite de volta os dados solicitados pelo leitor. A alimentação das etiquetas acontece através do *software* de gerenciamento, é possível encontrar etiquetas ativas e passivas (JÚNIOR; FARINELLI, 2018).

Em etiquetas passivas é criada uma rede PAN, que é uma rede privada entre uma etiqueta e o leitor, normalmente tem uma distância de aproximadamente 10 a 30 centímetros, devido ao fato de que a alimentação da etiqueta passiva é recebida pelo leitor. As etiquetas com alcance de 10 centímetros para a faixa de frequência de 125 a 134 kHz são de simples implementação e baixo custo, tornando possível envio dados a uma baixa taxa de dados e o contato com água não ter influencia no seu funcionamento. Para as etiquetas com alcance de 30 centímetros para a faixa de frequência de 13.56 MHz, as aplicações mais comuns são para cartões de acesso, nessa frequência de operação, a água influencia no seu funcionamento. Por sua vez, as etiquetas ativas possuem sua própria fonte de alimentação, onde é criada uma rede pessoal PAN entre o leitor e várias etiquetas, formando uma topologia estrela, sua maior vantagem é o maior alcance de leitura de aproximadamente 30 a 100 metros, dependendo também da frequência de operação variando entre 433 MHz e 856 a 960 MHz. Além de transferir grande quantidade de dados de maneira rápida, por operar na região espectral de frequência UHF CALPOLY (2016). A Tabela 1 mostra as especificações de algumas etiquetas comerciais, com faixas de frequência de 125 a 134 KHz, 13.56 MHz, 856 a 960 MHz e 433 e 856 a 960 MHz, tipo da etiqueta e seu alcance variando de 10 cm até 100 m.

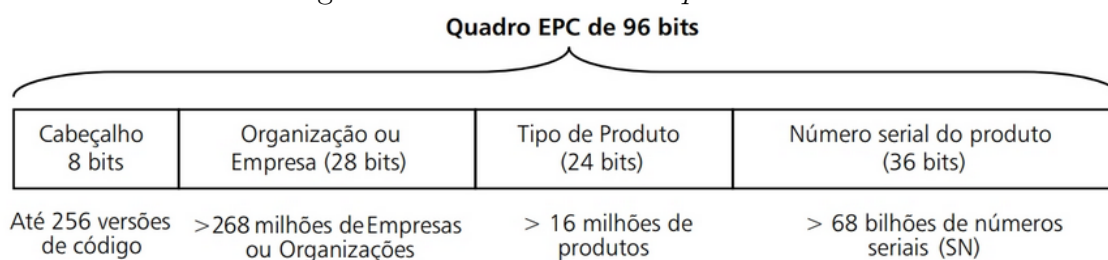
Tabela 1 – Comparativo entre diversas tecnologias e padrões RFID

Tipo de etiqueta	Faixa de frequência	Alcance
Passiva	125 a 134 kHz	10 cm
Passiva	13.56 MHz	30 cm
Ativa	433 MHz e 856 a 960 MHz	30 a 100 m

Fonte: Elaborada pelo autor.

Após isso, é importante ressaltar uma característica importante nas etiquetas **RFID**, os quadros **EPC**. As etiquetas podem permitir leitura e escrita de dados, dependendo de sua memória interna. Essas informações são codificadas através de um identificador único conhecido como **EPC**, sucessor do identificador único **UPC** que é proveniente do código de barras. O **EPC** tem a função de identificar exclusivamente um objeto por conter informações suficientes para que o objeto seja direcionado corretamente **CALPOLY (2016)**. A **Figura 7** a seguir pode ser visto a estrutura de um quadro **EPC**, possui 96 bits e é dividido em cinco campos. O primeiro campo é o cabeçalho de 8 *bits*, possuindo até 256 versões de código diferentes, o segundo campo é organização ou empresa de 28 *bits*, possuindo mais de 268 milhões de tipos diferentes, o terceiro campo é o tipo de produto de 24 *bits*, possuindo 16 milhões de tipos diferentes e o quarto campo é o número de série de 36 *bits*, possuindo mais de 68 bilhões de números seriais.

Figura 7 – *Estrutura de um quadro EPC*



Fonte: *Rochol (2018)*

Em relação a segurança da troca de dados realizada a partir da aproximação entre leitor e etiqueta, podemos observar que o sistema é vulnerável, porque normalmente não possuem um grande poder computacional para permitir a criptografia. Por isso é necessário uma proteção nas etiquetas para impedir um acesso não autorizado, essa proteção pode ocorrer através da segurança física ou de protocolo. Segurança física é basicamente impedir a leitura, já que no caso das etiquetas passivas, que atuam no espectro de baixa frequência e alta frequência precisam de curto alcance, esse tipo de segurança é fácil de ser aplicado, mantendo essas etiquetas em um local seguro. No caso de segurança de protocolo, é exigido algum tipo de autenticação, senha e/ou criptografia entre a troca de dados antes de exibir as informações da etiqueta. A adição de uma segurança de protocolo aumenta o custo da etiqueta. No caso de uma etiqueta de alta frequência que já possui curto alcance, é mais recomendado e usual ter uma implementação mais sofisticada, como por exemplo, criptografia **AES (CALPOLY, 2016)**.

Atualmente, a utilização de cartões equipados com tecnologia de aproximação, como os cartões de transporte público e cartões de crédito, tornou-se uma prática bastante difundida. Nesse contexto, a autenticação de usuários por meio de objetos já presentes e rotineiramente utilizados simplifica a automatização dos armários de maneira mais econômica, eliminando a necessidade de custos adicionais associados a *tags RFID*, por

exemplo. Nesse caso, o sistema utilizaria apenas a identificação do cartão não debitando nenhum valor do saldo.

2.4.5 Interface Homem-Máquina

A Interface Homem-Máquina (IHM) desempenha um papel crucial na interação entre os usuários e o sistema, tornando-se um dos componentes principais do sistema. A interface com o usuário não deve ser apenas intuitiva, mas também agradável, visando minimizar ao máximo possíveis erros durante o uso. Conforme evidenciado na [subseção 2.2.5](#), é comum empregar uma interface gráfica, muitas vezes exibida em uma tela sensível ao toque. A programação dessa interface contribui significativamente para a melhoria da experiência do usuário.

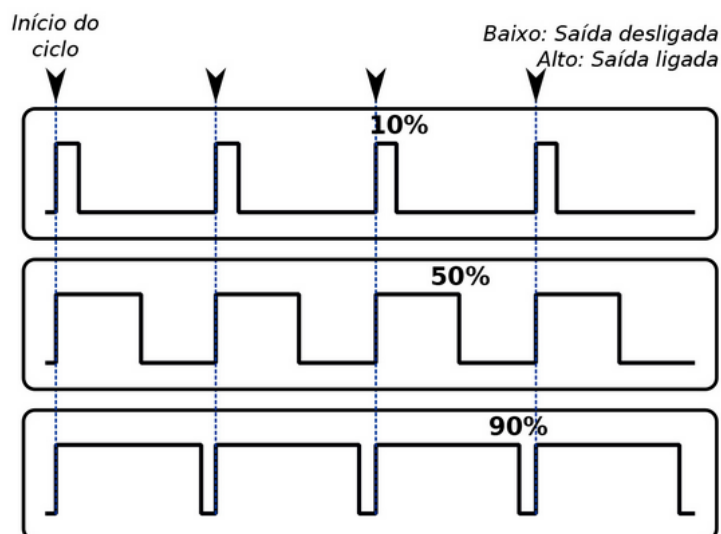
Sob o ponto de vista econômico, a interface gráfica nem sempre é a escolha mais apropriada. A interação com o usuário pode se manifestar por meio de diversos elementos visuais e sonoros intuitivos, direcionados a evitar equívocos. A inclusão de um *buzzer* para alertar sobre a abertura ou travamento de portas apresenta-se como uma opção interessante. Da mesma forma, LEDs com diferentes cores podem ser empregados para indicar o status dos armários, tais como a disponibilidade de compartimentos, o estado das portas, a ocupação total dos compartimentos, entre outras informações relevantes. Essas abordagens visam não apenas a eficácia operacional, mas também aprimoram a comunicação efetiva entre o usuário e o sistema.

O PWM é um sinal digital que modifica a largura do pulso de um sinal elétrico de maneira controlada. Esse método mantém constante a frequência do sinal, mas alterando a proporção entre o tempo em que o sinal está em nível alto e o tempo em que está em nível baixo, resultando em uma forma de onda quadrada. A proporção de tempo em que o sinal está em nível alto em relação ao ciclo completo do sinal é conhecido como *duty cycle*. A [Figura 8](#) mostra três sinais PWM com diferentes *duty cycles*. No primeiro sinal é visto um *duty cycle* de 10% do tempo em nível alto, no segundo sinal é visto um *duty cycle* de 50% do tempo em nível alto e por último o sinal é visto um *duty cycle* de 90% do tempo em nível alto ([ALMEIDA, 2016](#)).

Segundo [ALMEIDA \(2016\)](#), ao vincular a saída PWM a um gerador de som, como um *buzzer*, é possível controlar a frequência do sinal inserindo uma tensão variável ao longo do tempo. O *buzzer* desempenha o papel crucial de converter esses sinais elétricos em ondas sonoras, proporcionando alertas auditivos aos usuários do sistema durante a realização de operações específicas. Essa interação sonora serve como um meio eficaz de comunicação, fornecendo alertas sobre as ações executadas.

Os LEDs são dispositivos semicondutores que emitem luz quando estão diretamente polarizados. Possui dois terminais, positivo e negativo, também conhecidos como ânodo e

Figura 8 – Sinais PWM com diferentes duty cycles



Fonte: ALMEIDA (2016)

cátodo. Normalmente o componente possui uma lente de plástico colorido, entre as cores mais comuns encontradas nesses componentes estão o vermelho, amarelo e verde. Além disso, a intensidade da luz emitida varia proporcionalmente à corrente que percorre o circuito, proporcionando controle preciso sobre a luminosidade do LED (ALCIATORE; HISTAND, 2014).

2.5 Comunicação sem fio

O *Wi-fi*, é uma tecnologia de comunicação sem fio que segue as especificações de normas determinadas pelo padrão IEEE 802.11. Os componentes básicos para a criação de uma rede *wireless* são conhecidos como *BSS* formado por várias estações (STAs) e pode ter ou não um ponto de acesso. No caso de uma rede com um AP, é conhecida como rede de infra-estrutura, nesse caso, as estações se conectam no ponto de acesso, se autenticam e trocam informações criptografadas (FOROUZAN, 2010).

As faixas de frequência principais do *Wi-fi* são de 2,4GHz e 5GHz. A faixa de frequência utilizada pela *WLAN* de 2,400 GHz até 2,4835 GHz, está no canal de radiofrequências na faixa *UHF*, possuindo uma largura de 83,5 MHz. O padrão utilizado nessa faixa é IEEE 802.11b e g e utiliza a modulação *DSSS*. Já a faixa de frequência de 5,725 GHz até 5,850 GHz, está no canal de radiofrequências na faixa *SHF*, possuindo uma largura de 125 MHz. O padrão utilizado nessa faixa é IEEE 802.11a/ac e utiliza as modulações *SC-FDMA* e *MIMO 8* (ROCHOL, 2018).

Segundo Júnior e Farinelli (2018), a arquitetura básica do *Wi-fi* possui três camadas:

- **LLC (*Logical link control*)**: Responsável por carregar um protocolo de alto nível

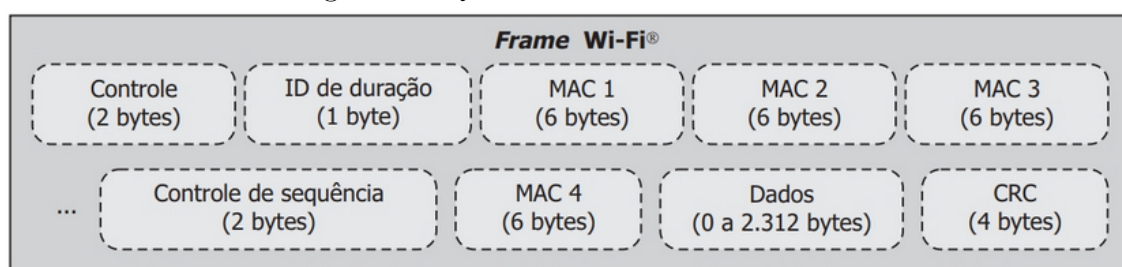
(TCP, UDP e IP).

- **MAC (*Media Access Control*)**: Responsável por montar o quadro de transmissão.
- **Física**: Responsável por controlar o envio das informações.

O pacote(*frame*) de transmissão Wi-Fi pode ser visto na [Figura 9](#), possui nove campos, descritos a seguir.

- **Controle**: contém a versão do protocolo, total de 2 *bytes*. O segundo campo é de ID *Identity* de duração, que contém um valor configurado automaticamente pelo *hardware*, total de 1 *byte*.
- **ID de duração**: contém um valor configurado automaticamente pelo *hardware*, total de 1 *byte*.
- **MAC 1 a 4**: contém respectivamente endereço do destinatário, de origem, do transmissor, do receptor e alcance máximo, total de 6 *bytes*.
- **Controle de sequência**: contém o número do pacote caso tenha sido dividido em vários pacotes, para saber a ordem dos pacotes, total de 2 *bytes*.
- **Dados**: contém a informação a ser transmitida, total de 0 a 2.132 *bytes*.
- **CRC(*Cyclic Redundancy Check*)**: contém um calculo para detecção de erros do pacote, para verificar sua integridade, total de 4 *bytes*.

Figura 9 – Quadro de transmissão Wi-Fi



Fonte: Júnior e Farinelli (2018)

O pacote de transmissão pode ser enviado com criptografias diferentes, depende da configuração da rede *Wi-fi* adotada pelo usuário. Ao utilizar a segurança **WEP**, é um protocolo que possui uma chave de acesso de 128 *bits*. Ao utilizar a segurança **WPA**, é um protocolo que possui uma chave de acesso de 256 *bits*. E por último o **WPA2** é uma evolução do **WPA** e considerado o mais seguro entre os três. Vale mencionar que o **WEP** e **WPA** já foram quebrados por força bruta (JÚNIOR; FARINELLI, 2018).

2.5.1 *Protocolo de comunicação*

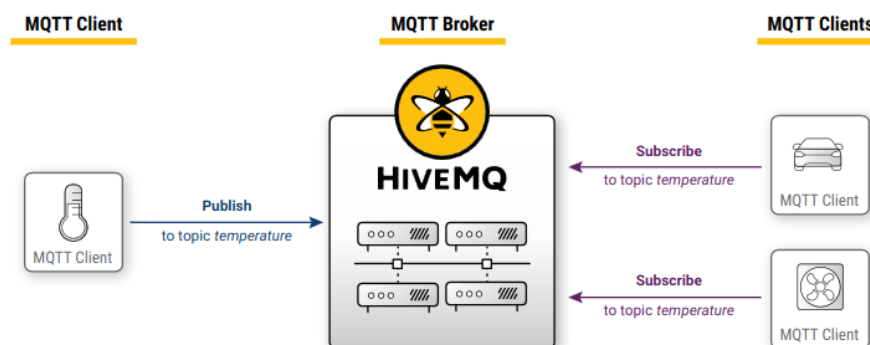
Protocolo de comunicação é um conjunto de regras e formatos a fim de padronizar a comunicação entre dois dispositivos, mesmo que tenham linguagens diferentes. É importante especificar o formato dos dados nas mensagens e sequência das mensagens trocadas (COULORIS et al., 2013).

Segundo IBM (2023), os *message brokers* são protocolos de comunicação orientado a mensagens. São responsáveis por garantir que a mensagem chegue corretamente ao seu destino sem se importar onde estão e quem são esses destinatários. Eles utilizam fila de mensagens para garantia de entrega e confiabilidade, por isso a mensagem é retirada da fila apenas após sua confirmação. Como mencionado acima, eles não se importam se o destinatário está disponível, isso ocorre devido ao fato de utilizarem o sistema de mensagens assíncronas. Dessa forma, garantindo a eficiência mesmo em ambiente hostis. É possível encontrar dois modelos de *message broker*:

- **Sistema de mensagens ponto a ponto:** Cada mensagem na fila é enviada uma por vez apenas para um destinatário. Transações financeiras, por exemplo, é um dos cenários de uso, onde precisa-se garantir que a transação ocorreu corretamente e apenas entregue ao destino certo.
- **Sistemas de mensagens de publicação/assinatura:** um produtor publica em um tópico e os consumidores inscritos naquele tópico receberão a mensagem. Uma plataforma de *streaming*, por exemplo, onde um criador de conteúdos publica seus vídeos e apenas inscritos receberão a notificação.

O MQTT é um protocolo de mensagens do modelo *publish/subscribe* orientado a eventos voltado para aplicações IoT por possuir uma implementação simples e de baixo consumo, adequado para troca de mensagens entre dispositivos com a mínima largura de banda. O mecanismo de autenticação deste protocolo é através de usuário/senha, por isso faz-se necessário o uso de TLS (criptografia da conexão TCP/IP) (MORAES; HAYASHI, 2021).

Como pode ser visto na Figura 10, na arquitetura *publish/subscribe* os clientes não trocam mensagens diretamente entre si, como no Sistema de mensagens ponto a ponto. Através do *Broker MQTT*, clientes publicam em determinados tópicos e outros clientes se inscrevem nesses tópicos para serem notificados quando ocorrer um evento. No caso da Figura 10, um cliente responsável pela temperatura, publica no tópico temperatura e outros dois clientes se inscrevem nesse tópico para recebem mensagens quando ocorrer um evento. Os cliente não precisam se conhecer, tudo ocorre através do MQTT *broker*.

Figura 10 – *Arquitetura Publish/Subscribe*

Fonte: *HiveMQ* (2020)

2.6 Gestão online

A administração e controle eficazes de um benefício disponibilizado para os usuários são de extrema importância para assegurar o seu uso otimizado. Nesse contexto, a gestão online se torna uma ferramenta essencial, possibilitando o acompanhamento em tempo real de compartimentos livres, a análise de uso e a ciência pela parte administrativa em casos de esquecimento de objetos, podendo assim, avisar o usuário. A capacidade de gerenciamento online não apenas aprimora a eficiência operacional, mas também oferece uma abordagem proativa para atender às necessidades dinâmicas dos usuários, resultando em uma experiência mais ágil, transparente e adaptável.

2.6.1 Banco de dados

Banco de dados é uma coleção de dados que são gerenciados por de um Sistema de Gerenciamento de Banco de Dados (SGBDs). Os SGBDs armazena e recupera esses dados que são valiosos, grandes volumes de dados e normalmente acessado por várias aplicações ao mesmo tempo. Dentre os diferentes modelos de dados existentes neste projeto será utilizado um tipo de banco de dados NoSQL (*Not Only SQL*), que é baseado no modelo de dados não relacional, não utiliza tabelas para representação de seus dados. Ao invés disso, armazena seus dados através de chave/valor. Sistema de armazenamento chave/valor apesar de ser um sistema de armazenamento simples, atende a alta demanda de dados e sendo escalável. Esses sistemas são muito utilizados em aplicações web. O banco de dados utilizado neste projeto é o MongoDB que armazena dados através de valores no formato JSON (SILBERSCHATZ, 2020).

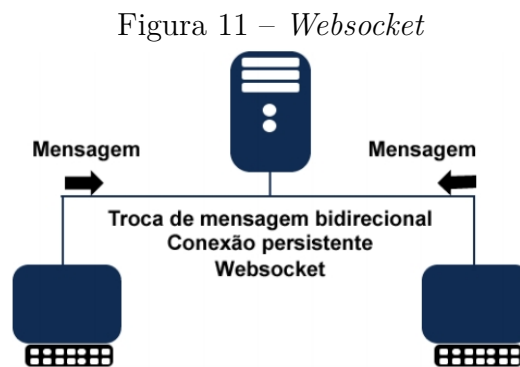
Para utiliza o banco de dados MongoDB, é preciso instalar e configurar o MongoDB corretamente no sistema. Na API do MongoDB, inicialmente é preciso criar uma coleção para armazenar objetos no formato JSON. Quando objetos são criados dentro dessa coleção, automaticamente é incluído identificadores para cada um deles. É possível também consultar esses objetos armazenados no banco com funções específicas para inserir,

consultar, alterar e excluir (SILBERSCHATZ, 2020).

2.6.2 Servidor

Ao desenvolver armário guarda-volumes com uma central inteligente, é necessário fazer uma *interface* administrativa para gerenciar os usuários e monitorar os compartimentos. Por isso, é importante desenvolver um servidor na nuvem para que remotamente, o administrador dos armários possa fazer esse gerenciamento e monitoramento do sistema geral.

Segundo Ferreira (2021), os protocolos *Websockets* são muito utilizados em servidores *web* para transferir dados entre cliente e servidor. Como mostra a Figura 11, o *WebSocket* realiza uma comunicação bidirecional em tempo real. Neste projeto, o *WebSocket* tem o objetivo de encapsular o protocolo *MQTT*.



Fonte: Ferreira (2021)

3 PROPOSTA

Houve início deste projeto no Ideias Inovadoras de 2021. No primeiro momento, foram feitos estudos e pesquisas na internet e utilizados conhecimentos anteriores para compreender se a trava escolhida geraria algum problema posterior, se possui fácil integração com outros sistemas e sua montagem. No final desta pesquisa pôde ser observado que a trava elétrica solenoide é a mais adequada, um dos fatores importantes é caso falte energia, a trava não abrirá, mantendo os objetos em segurança.

Após isso, foram feitas pesquisas sobre o funcionamento de um sensor que seria colocado dentro de cada compartimento. Este sensor tem o objetivo de verificar se o armário está vazio, para liberar o uso aos outros usuários, evitando assim seu desuso. Após essas pesquisas validar com profissionais se é um sensor adequado e de baixo custo, para então efetuar a compra dos materiais necessários e realizar os testes. No final desta etapa pôde ser observado que desta forma tornaria o projeto com um custo muito elevado e esta ideia foi descartada.

A próxima etapa foi uma análise dos tipos de sensores para a detecção de fechamento da trava em cada compartimento. Nessa pesquisa concluiu-se que para um protótipo inicial seria usado um sensor de presença de luminosidade LDR acoplado a trava de cada compartimento por ser mais simples e barato. No final do projeto em si, através de testes foi observado que não é o sensor adequado, pois dependendo da iluminação do ambiente, não detecta. Por isso será utilizado o sensor de contato.

Inicialmente definiu-se desenvolver um módulo capaz de gerenciar 6 compartimentos existentes em um armário. Após isso, foi desenvolvido o layout da placa de circuito impresso, e então solicitada sua fabricação. Foram desenvolvidas também 6 placas do sensor de luminosidade (LDR) para o monitoramento dos estados das portas dos compartimentos, sendo eles aberto e fechado.

Apenas a parte modular do sistema foi apresentada e validada, o microcontrolador da ESP32 foi implementado através de dois botões simulando usuários distintos em cenários de uso dos compartimentos. Os cenários respeitaram os casos de uso e especificações do protocolo definidas previamente. Na [Figura 12](#), pode ser visto a montagem desta etapa. A conclusão deste projeto foi que o sensor de luminosidade é inadequado. O projeto não teve continuidade por falta de tempo.

A ideia deste projeto é aproveitar os conhecimentos adquiridos no Ideias Inovadoras e aprimorar o produto tornando-o mais adequado. Para tornar este produto minimamente viável, no seu desenvolvimento estará associado às entregas parciais, para então concluir o protótipo dos armários inteligentes. Nesta etapa de construção, o projeto conta com

Figura 12 – Testes no protótipo inicial

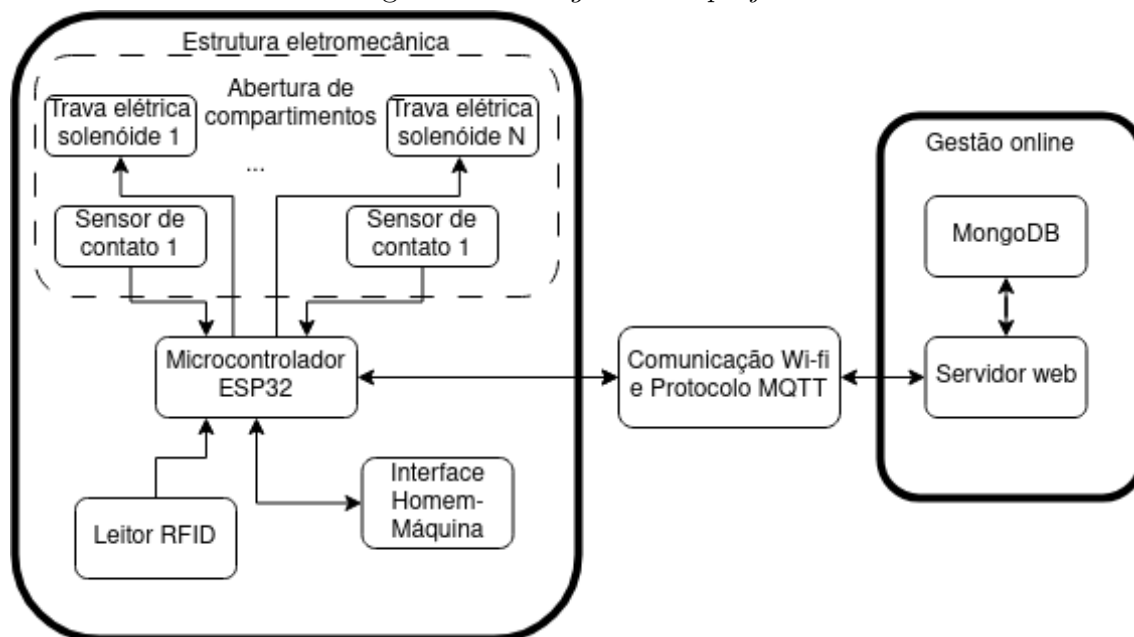


Fonte: *Autoria própria*

o desenvolvimento da parte mecânica, eletrônica, administrativa e integração entre os sistemas. Inicialmente foi desenvolvido um diagrama do produto ilustrado na [Figura 13](#) e a partir dele, serão realizadas divisões em etapas para entregas parciais baseadas em MVP.

Para a composição de armários inteligentes, é essencial que possua um sistema inteligente para interação entre usuário e o armário. É necessário um microcontrolador integrado no armário para acrescentar um sistema inteligente nele. O usuário interage com o armário através da aproximação de uma tag no leitor RFID, caso esse usuário/tag esteja cadastrado e autorizado, conseguirá acesso a um dos compartimentos. O leitor RFID será controlado pelo microcontrolador, assim como as fechaduras eletrônicas, permitindo ou não a abertura dos compartimentos. Caso o usuário seja autorizado, o sistema inteligente envia um comando para abertura de uma das travas elétricas solenoide. Após o usuário finalizar sua interação com o compartimento, é necessário um sensor de contato para verificar se a porta está devidamente fechada antes de trava-la. O sistema inteligente precisa de acesso a internet para acessar o banco de usuário cadastrados no servidor e permitir essas interações. A troca de mensagens entre o sistema e o servidor será através do protocolo MQTT e o padrão utilizado nessa troca de mensagens será no formato JSON.

Figura 13 – Diagrama do projeto



Fonte: Autoria própria

3.1 Cronograma de atividades

Na primeira etapa é necessário realizar a integração entre usuário e o armário, através da tecnologia RFID. O usuário interage com o armário através da aproximação de uma tag no leitor RFID, caso esse usuário/tag esteja cadastrado e autorizado, conseguirá acesso a um dos compartimentos. Nesta etapa será feita a integração do leitor RFID com o microcontrolador da ESP32.

Na segunda etapa, caso o usuário seja autorizado, o sistema inteligente envia um comando para abertura de uma das travas elétricas solenoide. Nesta etapa será feita a integração das travas elétricas solenoide com o microcontrolador da ESP32. A quantidade de travas associadas ao microcontrolador poderá ser expandida com o expensor de portas GPIO, nesta etapa isso será analisado, assim como a distancia máxima entre os fios que ligam a trava ao microcontrolador. Após isso será feito a associação de usuário autorizado, ocorre a abertura de uma das travas.

Na terceira etapa, após o usuário finalizar sua interação com o compartimento, é necessário um sensor de contato para verificar se a porta está devidamente fechada antes de trava-la. Nesta etapa será feito a integração da trava com o sensor.

Na quarta etapa é necessário desenvolver a interface administrativa, onde o servidor é acessado pelo administrador através de um login, para então interagir com o banco de dados para cadastro de usuários. Nesta etapa será feito um servidor local interagindo com o banco de dados do MongoDB.

Na quinta etapa é necessário realizar a interação do servidor com o armário. O

microcontrolador precisa de acesso a internet para acessar o banco de usuário cadastrados no servidor e permitir as interações. A troca de mensagens entre o sistema e o servidor será através do protocolo MQTT e o padrão utilizado nessa troca de mensagens será no formato JSON. Nesta etapa será desenvolvido a integração do Microcontrolador com o módulo Wi-fi para ter acesso ao servidor através do protocolo MQTT.

Figura 14 – *Cronograma de atividades*

Atividades	Semanas																
	Dez.				Janeiro					Fevereiro				Março			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
A1	✓	✓	✓	✓	✓												
A2						✓	✓										
A3								✓	✓								
A4										✓	✓	✓	✓				
A5														✓	✓	✓	✓

Fonte: *Autoria própria*

REFERÊNCIAS

- AECWEB. *Fechaduras mecânicas Para portas vai-e-vem*. [S.l.], 2022. Disponível em: <<https://api.aecweb.com.br/cls/catalogos/hafele/fechaduras.pdf>>. Acesso em: 12 set. 2023. 18
- ALCIATORE, D. G.; HISTAND, M. B. *Introdução à mecatrônica e aos sistemas de medições*. [S.l.]: Grupo A, 2014. ISBN 9788580553413. 24
- ALMEIDA, R. D. *Programação de Sistemas Embarcados - Desenvolvendo Software para Microcontroladores em Linguagem C*. [S.l.]: Grupo GEN, 2016. 23, 24
- ALMEIDA, R. de. *Programação de Sistemas Embarcados - Desenvolvendo Software para Microcontroladores em Linguagem C*. [S.l.]: Grupo GEN, 2016. ISBN 9788595156371. 19
- AMAZON. ULP. 2022. <<https://www.amazon.com/ulp/view>>. Acesso em: 14 nov. 2022. 11
- CALPOLY. *Center for Global Automatic Identification Technologies*. Poly Gait, 2016. (Acesso em: 11 set. 2023). Disponível em: <<https://polygait.calpoly.edu/>>. 21, 22
- CARDOSO, J. *Engenharia Eletromagnética*. [S.l.]: Grupo GEN, 2010. ISBN 9788595156975. 18
- COULORIS, G. et al. *Sistemas distribuídos*. [S.l.]: Grupo A, 2013. ISBN 9788582600542. 26
- DURATTA. *Armário Biométrico*. 2023. <<https://www.duratta.com.br/produto/armario-biometrico/>>. Acesso em: 03 dez. 2023. 15
- ESPRESSIF. *ESP32 Series Datasheet*. [S.l.], 2023. Disponível em: <https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf>. Acesso em: 10 out. 2023. 19
- FALCONE, A. G. *Eletromecânica, vol. 1*. [S.l.]: Blucher, 1979. ISBN 9788521216599. 17
- FERREIRA, A. G. *Interface de programação de aplicações (API) e web services*. [S.l.]: Editora Saraiva, 2021. ISBN 9786553560338. 28
- FOROUZAN, B. A. *Comunicação de dados e redes de computadores*. [S.l.]: Grupo A, 2010. ISBN 9788563308474. 24
- HIVEMQ. *MQTT MQTT 5 Essentials*. [S.l.]: HiveMQ GmbH, 2020. 27
- IBM. *O que são message brokers?* 2023. (Acesso em: 13 out. 2023). Disponível em: <<https://www.ibm.com/br-pt/topics/message-brokers>>. 26
- IFSC. *Edital 005/2019: Chave dos armários em 2019.2*. 2022. <<https://www.ifsc.edu.br/documents/35941/1078237/EDITAL+005-2019+chave+dos+arm%C3%A1rios+em+2019.2.pdf>>. Acesso em: 14 nov. 2022. 10

IFSC. *Estudantes*. 2022. <<https://www.ifsc.edu.br/web/campus-sao-jose/estudantes>>. Acesso em: 14 nov. 2022. 10

INTELIGENTES, A. *Soluções para guarda de volumes*. 2023. <<https://www.armariosinteligentes.com.br/solucoes/guarda-volumes-inteligente/>>. Acesso em: 07 abril 2023. 14

JÚNIOR, S. L. S.; FARINELLI, F. A. *DOMÓTICA - AUTOMAÇÃO RESIDENCIAL E CASAS INTELIGENTES COM ARDUINO E ESP826*. [S.l.]: Editora Saraiva, 2018. ISBN 9788536530055. 21, 24, 25

MORAES, A. de; HAYASHI, V. T. *Segurança em IoT*. [S.l.]: Alta Books, 2021. ISBN 9788550816548. 26

MORAES, C. C. de; CASTRUCCI, P. de L. *Engenharia de Automação Industrial*. [S.l.]: Grupo GEN, 2006. ISBN 9788521619765. 19

NILKO. *Armários*. 2023. <<https://www.nilko.com.br/armarios/>>. Acesso em: 03 dez. 2023. 14

OIHANDOVER. *Oihandover - Soluções*. 2022. <<https://oihandover.com/#solucoes>>. Acesso em: 14 nov. 2022. 11

OPPITZ. *Armário inteligente para guarda volumes / capacetes em shoppings*. 2023. <<https://oppitz.com.br/produtos/armarios-inteligentes/>>. Acesso em: 7 nov. 2023. 15

ROCHOL, J. *Sistemas de comunicação sem fio*. [S.l.]: Grupo A, 2018. ISBN 9788582604564. 22, 24

SILBERSCHATZ, A. *Sistema de Banco de Dados*. [S.l.]: Grupo GEN, 2020. ISBN 9788595157552. 27, 28

THOMAZINI, D.; ALBUQUERQUE, P. U. B. D. *Sensores industriais*. [S.l.]: Saraiva, 2020. 19

USINAINFO. *Mini Solenóide 12V NF Tipo Tranca JF-0520B*. 2023. (Acesso em: 15 set. 2023). Disponível em: <<https://www.usinainfo.com.br/mini-fechadura-eletrica-solenóide/mini-solenóide-12v-nf-tipo-tranca-jf-0520b-5246.html>>. 18