UNIVERSIDADE EDUARDO MONDLANE
FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA
CURSO DE ENGENHARIA ELECTRÓNICA

Concepção de um sistema de controle de acesso de um cofre com implementação de uma senha de alarme silencioso

Relatório do Estágio Profissional

Yuri Marcelo Tivana

Supervisor: Engº Frederico Zile (UEM)

Co-Supervisor: Engº João Júnior Massingue (Zitronica)

Maputo, Outubro 2025

UNIVERSIDADE EDUARDO MONDLANE
FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA
CURSO DE ENGENHARIA ELECTRÓNICA

Concepção de um sistema de controle de acesso de um cofre com implementação de uma senha de alarme silencioso

Relatório do Estágio Profissional

Yuri Marcelo Tivana

Supervisor: Engº Frederico Zile (UEM)

Co-Supervisor: Engº João Júnior Massingue (Zitronica)

Maputo, Outubro 2025

DECLARAÇÃO DE HONRA

Declaro sobre palavra de honra que este trabalho foi feito totalmente por minha autoria.

DEDICATÓRIA

Aos meus pais, Miguel Tivana e Neli Chomane, a minha irmã Vera Tivana , aos demais familares, amigos e colegas, e a todos que deste trabalho se vão beneficiar.

AGRADECIMENTOS

Primeiramente, agradeço à Deus, por ter me guardado até aqui e me conceder saúde, força, vontade e conhecimento para chegar até aqui.

O meu muito obrigado aos meus pais Miguel Marcelino Tivana e Neli Bernardo Chomane por terem dado tudo de si para prover condições financeiras, ambientais e emocionais para que eu conseguisse alcançar este nível académico. Agradeço também aos meus familiares e amigos por serem fontes de motivação, suporte, ideas e apoio. Quero agradecer ao meu supervisor e profissionais pelo que enriqueceram meu conhecimento com sabedoria e orientação..

E por fim, não de longe menos importante, agradeço à comunidade acadêmica da Faculdade de Engenharia da Universidade Eduardo Mondlane, especialmente o seu corpo docente que foram um pilar no seio da minha formação.

RESUMO

Concepção de um sistema de controle de acesso de um cofre com implementação de uma senha de alarme silencioso

Este trabalho descreve a concepção e implementação de um sistema de controle de acesso eletrônico para cofres, visando segurança aprimorada e funcionalidade inteligente. A solução desenvolvida combina tecnologias avançadas de autenticação, como biometria e senha, com um mecanismo inovador de senha de pânico. Esta funcionalidade permite a abertura do cofre em situações de coação, ativando simultaneamente um alarme silencioso e notificações discretas por meio do protocolo MQTT. Para a montagem do *Hardware*, foram utilizados componentes como o microcontrolador ESP32, ESP32-CAM, displays LCD, sensor biométrico de impressão digital, teclado matricial, fechadura solenoide e um relé, integrando todos na concepção do protótipo. A lógica de controle de acesso foi feita a partir da programação em linguagem baseada em C++ (Arduino Sketch). Para a comunicação, foi configurada a IoT via protocolo MQTT e HTTP, onde microcontroladores e *smartphone* atuaram como clientes, acionando alarmes no celular por meio do aplicativo MQTT Alert. Além disso, foi desenvolvido um *Painel Administrativo*, hospedado em servidor local com XAMPP, permitindo monitoramento dos acessos, alteração de senha e visualização de registros. A metodologia incluiu etapas rigorosas de pesquisa, simulação e testes práticos, garantindo a robustez do protótipo. Durante os ensaios, foram validadas tanto a capacidade de autenticação quanto a resposta eficaz em situações de emergência, incluindo a transmissão de alertas e imagens para autoridades competentes. Os resultados demonstram o potencial desta abordagem para aprimorar a segurança de ambientes críticos, proporcionando proteção discreta e eficiente contra riscos de coação ou tentativas de acesso não autorizado.

Palavras Chaves: sistema de controle de acesso, cofre eletrônico, senha de pânico, alarme silencioso, ESP32, IoT.

ABSTRACT

Concepção de um sistema de controle de acesso de um cofre com implementação de uma senha de alarme silencioso

This work describes the design and implementation of an electronic access control system for safes, aiming at enhanced security and intelligent functionality. The developed solution combines advanced authentication technologies, such as biometrics and password, with an innovative panic password mechanism. This feature allows the safe to be opened under coercion situations while simultaneously triggering a silent alarm and sending discreet notifications through the MQTT protocol. For the *hardware* assembly, components such as the ESP32 microcontroller, ESP32-CAM, LCD displays, fingerprint biometric sensor, matrix keypad, solenoid lock, and a relay were used, all integrated into the prototype design. The access control logic was implemented through programming in a C++-based language (Arduino Sketch). For communication, IoT integration was configured using both MQTT and HTTP protocols, where microcontrollers and the *smartphone* acted as clients, enabling alarm activation on mobile devices via the MQTT Alert application. In addition, an *Administrative Panel* was developed and hosted on a local server with XAMPP, allowing access monitoring, password management, and log visualization. The methodology included rigorous stages of research, simulation, and practical testing, ensuring the robustness of the prototype. During the trials, both the system's user authentication capacity and its effective response in emergency situations were validated, including the transmission of alerts and images to the relevant authorities. The results demonstrate the potential of this approach to enhance the security of critical environments, providing discreet and efficient protection against coercion risks or unauthorized access attempts.

Keywords: access control system, electronic safe, panic password, silent alarm, ESP32, IoT.

Índice de Conteúdo

Lista de Figuras

Lista de Tabelas

Lista de Acrónimos

CCTV *Closed-circuit television*. 7

HTTP *HyperText Transfer Protocol*. 20

I2C *Inter-Integrated Circuit* . 26

IDE *integrated development environment* . 24

IoT *Internet of Things*. 19

LAN *Local Area Network*. 54

LCD *Liquid Crystal Display*. 19

LED *light-emitting diode*. 19

MQTT *Message Queuing Telemetry Transport*. 20

OTPs *One Time Passwords*. 12

PCB *Printed Circuit Board*. 58

PIN - *Personal Identification Number* Número de Identificação Pessoal. 13

QoS *Quality of Service*. 54

RFID - *Radio-Frequency Identification* Identificação por rádio frequência. 14

RISC *Reduced Instruction Set Computer*. 27

UART *Universal Asynchronous Receiver-Transmitter*. 26

Capítulo 1

Introdução

1.1 Nota introdutória

A segurança patrimonial é um conjunto de medidas e sistemas implementados para proteger bens e até pessoas. Seja nas casas, empresas ou instituições públicas que frequentamos, contar com um sistema de segurança eficaz faz toda a diferença. Proteger o que é importante se tornou uma prioridade para muitos de nós.

O presente documento é um relatório de estágio para conclusão do curso de Engenharia Electrónica, sobre o assunto de segurança e a sua importância. Este trabalho tem como título: Concepção de um sistema de controle de acesso de um cofre com implementação de uma senha de alarme silencioso. É neste relatório, apresentado o processo de dimensionamento do sistema de controle de acesso, baseando- se na simplicidade e no uso sistemas micro controlados ou embarcados, tendo como uma forma de inovação e adaptabilidade a evolução da tecnologia, o uso IoT (*Internet of Things*). Este sistema será implementado como forma de um protótipo de um cofre digital, contudo, com alguns ajustes pode ser implementado para outros casos.

1.2 Formulação do problema

A segurança de bens e informações é uma preocupação tanto para indivíduos quanto para instituições. Cofres e compartimentos de acesso restrito são amplamente utilizados para proteger itens valiosos, documentos sigilosos e outros materiais sensíveis. No entanto, em situações de assalto ou coação, os proprietários podem ser forçados a fornecer acesso, o que compromete a segurança e aumenta os riscos para a vítima.

Diante desse cenário, é essencial o desenvolvimento de soluções inovadoras que permitam a solicitação de ajuda sem alertar os agressores. Sistemas de alarme silencioso já são utilizados em bancos e estabelecimentos comerciais para acionar discretamente equipes de segurança. Aplicar essa estratégia em cofres eletrônicos pode oferecer um nível adicional de proteção, garantindo que a vítima tenha um meio seguro de pedir auxílio sem agravar a situação.

O presente trabalho propõe o desenvolvimento de um sistema de controle de acesso para cofres eletrônicos que, além da autenticação convencional por senha ou biometria, incluirá um mecanismo de ”senha de pânico”. Esse recurso permitirá que, ao digitar uma senha específica ou utilizar uma impressão digital alternativa, o cofre seja aberto normalmente, mas um alarme silencioso seja acionado para notificar uma central de segurança ou autoridades competentes onde eles poderão ter acesso remoto a um vídeo vigilância para melhor estratégia de intervenção rápida.

O sistema será baseado em um microcontrolador responsável por enviar um sinal quando ele recebe inputs (teclado e/ou sensor de impressão digital), se a senha ou for igual a previamente registada, ele irá abrir cofre, caso contrário ele não abrirá.

Exposto acima, o presente trabalho propõe a resolução da seguinte pergunta de pesquisa:

Como conceber um sistema de acesso de um cofre com senha de pânico?

1.3 Relevância da pesquisa

A necessidade de proteger pertences valiosos e informações confidenciais é uma preocupação para indivíduos e instituições. Nestes casos de roubos, assaltos e invasões de propriedade, é fundamental desenvolver métodos eficazes para garantir a segurança e a proteção desses itens. O problema é agravado quando a vítima é coagida a fornecer acesso a cofres ou contas sob ameaça, situação em que a resistência pode ser perigosa. Existem situações em que alguém pode estar em perigo, seja por estar desconfiado de alguém suspeito que esteja a se aproximar ao balcão (no caso de um banco ou loja, por exemplo), ou alguém a se comportar mal ou esteja a ser agressiva, em alguns momentos é melhor pedir socorro de forma silenciosa sem que o agressor percebe, por isso foi criado o botão de pânico. Este estudo se justifica pela necessidade de aprimorar os sistemas de segurança existentes, reduzindo os riscos enfrentados por vítimas de coação e

aumentando as chances de recuperação dos bens roubados. Além disso, contribui para o avanço das tecnologias de proteção patrimonial e pode ser aplicado em diversas áreas, como residências, empresas e instituições financeiras.

Aplicando a mesma estratégia em um cofre, pode se criar um método em que durante o roubo a vítima possa usar o cofre para pedir ajuda à uma em empresa de segurança já predefinido.

1.4 Objectivos

1.4.1 Objectivo Geral

- Conceber um sistema de controle de acesso de um cofre com implementação de uma senha de alarme silencioso.

1.4.2 Objectivos Específicos

i. Descrever o princípio de funcionamento e os elementos integrados de sistema de controle de acesso de um cofre eletrônico;

ii. Dimensionar o sistema de controle de acesso, incluindo uma placa de circuito impresso optimizada;

iii. Desenvolver o script de controle para o microcontrolador, responsável pela autenticação do usuário, gerenciamento do mecanismo de desbloqueio do cofre e acionamento do alarme silencioso em situações de emergência;

iv. Implementar o recurso de vídeo vigilância remoto;

v. Testar um protótipo funcional, que demonstre na prática o princípio de funcionamento do controle de acesso, a autenticação por senha, e a ativação do alarme.

1.5 Metodologia

Para conseguir atingir o objectivo geral, a metodologia é fundamental para demostrar o caminho que a pesquisa deve trilhar para sua concepção.

1.5.1 Classificação da metodologia de investigação

a) Quanto a natureza

A natureza da pesquisa relaciona-se à contribuição de suas conclusões à ciência. Quanto à natureza, as pesquisas podem ser básicas ou aplicadas.

Básica-A pesquisa básica objetiva gerar conhecimentos novos para o avanço da ciência. Contudo, não se preocupa com a aplicação prática desses conhecimentos.

Aplicada-A pesquisa aplicada também objetiva gerar conhecimentos novos. Entretanto, tem o foco de aplicar esses conhecimentos para solucionar problemas específicos. Há, portanto, a preocupação com a aplicação prática da pesquisa.

Neste trabalho, há a necessidade de aplicar esses conhecimentos para resolver um problema específico.

b) Quanto a técnica aplicada

Este trabalho utiliza como meio de aquisiccao de dados: Pesquisa bibliográfica- que utiliza fontes constituídas por material já elaborado, constituído basicamente por livros e artigos científicos localizados em bibliotecas.

Pesquisa Documental- a que utiliza fontes primárias, isto é, dados e informações que ainda não foram tratados científica ou analiticamente.

1.5.2 Procedimentos usados no trabalho

Para a poder atingir o objectivo geral, fez-se primeiramente o levantamento dos requisitos funcionais e técnicos do sistemas, analise das tecnologias similares existentes, esboço da aquitectura do projecto, entre outros. Par este trabalho, foram seguidos os seguintes passos:

1 Pesquisa bibliográfica

2 Levantamento das necessidades e requisitos para o sistema;

3 Especificação e selecção dos componentes necessários para a construção do dispositivo;

4 Desenho do circuito electrónico e impresso;

5 Programação e simulação parcial do sistema em software;

6 Montagem de todos os componentes;

7 Testes e ajustes.

A programação dos microcontroladores é feita usando software Arduino IDE versão 2.3.4, um ambiente integrado de desenvolvimento fornecido pela empresa criadora do arduino.

Os desenho de circuitos eletrônicos e circuitos impressos são pelo EasyEDA versão standards V6.5.50.

Para a simulação de circuitos elétricos é usado o Multisim 14.1 com licensa de estudante.

Capítulo 2

Local do Estágio

2.1 Introdução

A disciplina de **Estágio Profissional** proporciona ao estudante a oportunidade de consolidar e complementar o aprendizado teórico, uma vez que permite a aplicação prática dos conteúdos estudados durante a formação acadêmica nas atividades quotidianas de uma empresa. Dessa forma, o estágio constitui um elo fundamental entre o conhecimento adquirido em sala de aula e as demandas reais do mercado de trabalho.

O presente relatório refere-se à disciplina de Estágio Profissional e descreve as atividades desenvolvidas na empresa **Zitronica LDA**, especializada em sistemas elétricos e eletrónicos, automação residencial, segurança eletrónica, robótica e Internet das Coisas (IoT). A empresa está localizada na Av. da União Africana, nº 748, Matola, N4, Maputo, Moçambique, e atua tanto em projetos próprios como na prestação de serviços para terceiros.

2.2 Objectivos do Estágio

Com a realização do estágio, pretendia-se alcançar os seguintes objetivos:

- Vivenciar o uso da segurança eletrónica no quotidiano, compreendendo sua importância em diferentes contextos residenciais, comerciais e industriais;
- Aperfeiçoar o manuseio de equipamentos, instrumentos e ferramentas eletrónicas, desenvolvendo maior destreza técnica;
- Aplicar, de forma prática, os conhecimentos teóricos adquiridos ao longo do curso, na resolução de problemas reais relacionados à área de atuação;

- Desenvolver competências em automação, robótica e IoT, acompanhando a implementação de soluções tecnológicas modernas utilizadas pela empresa;
- Estimular o pensamento crítico e a capacidade de análise por meio da observação e participação em projetos que demandam inovação e eficiência;
- Compreender a dinâmica organizacional e o ambiente profissional, incluindo práticas de trabalho em equipe, gestão de tempo e atendimento às necessidades dos clientes.

2.3 Atividades Realizadas na Empresa

Durante o período de estágio na Zitronica LDA, foram desenvolvidas diversas atividades relacionadas às áreas de atuação da empresa. Entre as principais, destacam-se:

- Acompanhamento de instalações de sistemas elétricos e eletrónicos, observando normas de segurança e boas práticas de montagem;
- Participação em projetos de automação residencial, auxiliando na integração de dispositivos inteligentes e na configuração de sistemas de controle;
- Colaboração em projetos de segurança eletrónica, incluindo instalação de câmeras de vigilância *Closed-circuit television* (CCTV), alarmes e sensores de movimento;
- Suporte técnico em sistemas de robótica e IoT, envolvendo a programação de microcontroladores e a comunicação entre dispositivos;
- Configuração e manutenção de redes locais, fundamentais para o funcionamento dos sistemas conectados;
- Análise e resolução de problemas práticos, aplicando os conhecimentos adquiridos no curso em situações reais do ambiente profissional.

Essas atividades possibilitaram não apenas o desenvolvimento de habilidades técnicas, mas também o aprimoramento de competências interpessoais, como trabalho em equipe, organização e comunicação no ambiente corporativo.

Capítulo 3

Revisão Teórica

3.1 Sistema de Controle de Acesso

O Controle de Acesso é um sistema de segurança essencial que visa monitorar e regular a entrada e saída de pessoas, veículos ou objetos em determinados locais e dispositivos. A sua importância tem se destacado cada vez mais com o avanço das tecnologias, como o reconhecimento facial, biometria e outras formas de autenticação. (Galvão 2025)

Segundo Brasiliano 2013, de uma forma resumida, controle de acesso é o sistema que permite ou não a entrada de um indivíduo ou objeto em determinados locais, em determinados horários, mediante sua identificação.

Da mesma forma que as chaves e as listas de convidados pré-aprovados protegem os espaços físicos, as políticas de controle de acesso protegem os espaços digitais. Em outras palavras, eles permitem a entrada das pessoas certas e mantêm as pessoas erradas fora. As políticas de controle de acesso dependem fortemente de técnicas como autenticação e autorização, que permitem que as organizações verifiquem explicitamente se os usuários são quem dizem ser e se esses usuários recebem o nível apropriado de acesso com base no contexto, como dispositivo, localização, função e muito mais. Estes sistemas podem ser físicos ou lógicos, onde em um sistema de controle de acesso físico limita o acesso a edifícios, salas e ativos físicos. O controle de acesso lógico limita as conexões a redes de computadores, arquivos de sistema e dados.

3.1.1 Sistema Controle de acesso eletrônico

Sistema Controle de acesso eletrônico é um sistema de segurança que utiliza tecnologias digitais para gerenciar e restringir o acesso a áreas físicas, sistemas de informação

ou recursos específicos. Ele permite que apenas pessoas autorizadas, identificadas por meios eletrônicos como senhas, cartões magnéticos, biometria, ou dispositivos de autenticação, possam entrar em locais protegidos ou acessar sistemas controlados. Alguns desses sistemas incorporam painéis de controle de acesso para restringir a entrada em salas e edifícios, bem como alarmes e recursos de bloqueio, para evitar acesso ou operações não autorizadas.

De uma forma mais simples, o funcionamento de um controle de acesso envolve identificação de um usuário com base em suas credenciais e a autorização do nível de acesso apropriado assim que ele for autenticado. Essa autenticação é feita a partir de um controlador que vai analisar a informação, e pode ser por senhas, números de identificação pessoal (PINs), tokens de segurança, varreduras biométricas ou outros fatores de autenticação. A autenticação multifator (MFA), que requer dois ou mais fatores de autenticação, costuma ser uma parte importante de uma defesa em camadas para proteger os sistemas de controle de acesso.

Depois que a identidade de um usuário for autenticada, as políticas de controle de acesso concedem permissões específicas e permitem que o usuário proceda conforme pretendido.(Microsoft 2022)

Alguns sistemas, ainda, podem ter recursos extras, como relatórios detalhados de acesso e integração com outros softwares de segurança, como câmeras de monitoramento e suporte remoto.

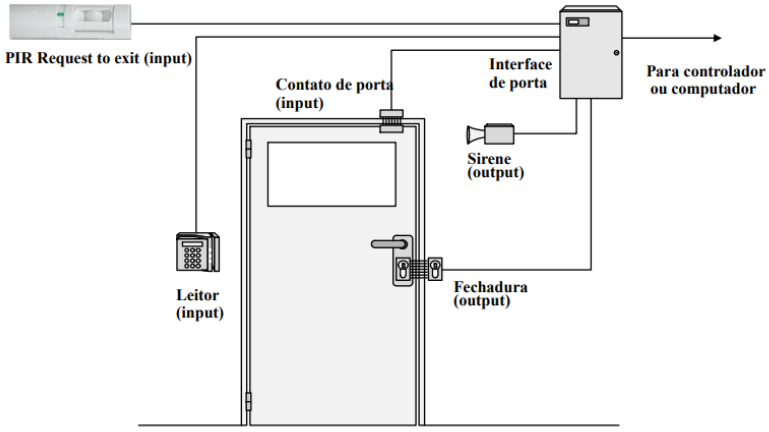


Figura 3.1: Demostração de um sistema de controle de Acesso. Fonte: Brasiliano 2013

3.1.1.1 Objectivos e Vantagens

De acordo com as definições dadas acima, podemos entender os objectivos de um sistema de controle de acesso como evitar que informações confidenciais caiam nas mãos de malfeitores, e limitar o acesso a redes, sistemas de computador, aplicativos, como informações de identificação pessoal (PIN) e propriedade intelectual. Um bom sistema de controle de acesso oferece inúmeras vantagens, como:

- **Registar a entrada e saída e ter controle total sobre o fluxo de pessoas** em determinada área, entendendo quem adentrou certo recinto, o horário em que fez o acesso, o tempo de permanência, a quantidade de pessoas em cada ambiente, etc.;
- **Reduzir os custos operacionais**, enxugando a equipe de porteiros e recepcionistas, já que o sistema consegue automatizar e centralizar processos, sem a necessidade constante de um operador;
- **Aumentar a segurança**, já que se reduz consideravelmente o acesso de pessoas não autorizadas aos ambientes. E, caso ocorra algum problema, é possível verificar rapidamente no sistema as pessoas que estiveram no local, o tempo que permaneceram e outros dados, identificando brechas na segurança.

Os sistemas de controle de acesso ainda permitem restringir áreas de risco ou de segurança mais alta, criar listas de acesso (por exemplo para eventos internos), localizar os colaboradores dentro da empresa e integrar ao sistema de ponto eletrônico dos funcionários.

3.1.2 Tipos de Controle de Acesso

3.1.2.1 Controle de Acesso Físico

Este tipo de controle de acesso é focado em restringir o acesso a locais físicos, como edifícios, salas, instalações,cofres ou áreas específicas dentro de uma propriedade. **A3AEngenharia**, propõe como os principais métodos, os seguintes:

a) **Teclados Numéricos (PINs):**

   Usuários inserem um código numérico para obter acesso. É uma solução comum em residências e empresas.

b) **Cartões de Proximidade/RFID:**

Os usuários utilizam cartões ou tags equipados com tecnologia RFID (Radio-Frequency Identification), que ao serem aproximados de um leitor, concedem acesso. Comuns em empresas e universidadese composto de um pequeno circuito, pode ser facilmente embutida em cartões ou em chaveiros. Controles desse tipo também podem ser instalados em etiquetas, como ocorre com os controles de acesso a pedágios e a shoppings centers. A forma mais comum e usual de uso da tecnologia RFID é constituída pelos portões de garagens residenciais. Devido a seu processo de fabricação, esta tecnologia apresenta baixo índice de falsificação e falha. A leitura é feita por radiofrequência, o que dificulta o desgaste e atrito. Se destaca por ser uma das tecnologias com um bom custo benefício.

c) **Biometria**

Utiliza características físicas únicas dos indivíduos, como impressões digitais, íris, reconhecimento facial, ou reconhecimento de voz para autenticar a identidade do usuário.

As impressões digitais são formadas por linhas de elevações da pele dos dedos. Seu desenho é único para cada pessoa, constituindo, desse modo, um meio extremamente seguro de confirmação do indivíduo. Técnicas próprias de avaliação dessas linhas e suas características particulares constituem o ramo da Papiloscopia. Seus princípios são utilizados por softwares especializados capazes de fazer a leitura e a identificação individualizada.

d) **Chaves Eletrônicas (Key Fobs):**

Pequenos dispositivos eletrônicos que emitem um sinal para um leitor próximo, concedendo acesso. Comuns em garagens e entradas de edifícios.

e) **Catracas e Torniquetes:**

As catracas são equipamentos utilizados para controlar o acesso físico e fazem isso ao permitir a passagem de um único indivíduo por vez. Estes dispositivos eletromecânicos têm a função de diminuir a velocidade de acesso de pessoas ao ambientes.

Usados em locais com grande fluxo de pessoas, como estações de metrô, edifícios corporativos, e eventos onde os usuários precisam apresentar credenciais (cartão, biometria) para passar.

Figura 3.2: Exemplos de contreles de acessos fisicos. Fonte:**A3AEngenharia**

3.1.2.2 Controle de Acesso Lógico

De acordo com Microsoft 2022, esse tipo de controle de acesso é focado em restringir o acesso a sistemas digitais, redes, e informações. Ele é fundamental em ambientes de TI para proteger dados sensíveis e recursos computacionais. Os métodos principais incluem:

a) **Tokens de Autenticação:**

Dispositivos que geram códigos de uso único (one-time passwords - *One Time Passwords* (OTPs)) ou enviam esses códigos para um dispositivo móvel, que o usuário deve inserir além de sua senha, conhecido como autenticação multifator.

b) **Autenticação Multifator (MFA):**

Combinação de dois ou mais métodos de autenticação (por exemplo, senha e biometria, ou senha e token), aumentando a segurança ao exigir múltiplas formas de verificação.

c) **RBAC (controle de acesso baseado em função)**

o Nos modelos de RBAC, os direitos de acesso são concedidos com base em funções de negócios definidas e não na identidade ou tempo de serviço dos indivíduos. O objetivo é fornecer aos usuários apenas os dados de que eles precisam para realizar o trabalho, e nada mais.

d) **MAC (controle de acesso obrigatório)**

Nos modelos de MAC, os usuários recebem acesso na forma de uma autorização. Uma autoridade central regula os direitos de acesso e os organiza em camadas, que se expandem uniformemente em escopo. Esse modelo é muito comum em contextos governamentais e militares.

e) **ABAC (controle de acesso baseado em atributos)**

Nos modelos de ABAC, o acesso é concedido de forma flexível com base em uma combinação de atributos e condições ambientais, como horário e local. ABAC é o modelo de controle de acesso mais granular e ajuda a reduzir o número de atribuições de funções.

3.1.3 Cofre eletrónico

Um cofre eletrônico é um dispositivo de segurança projetado para armazenar objetos de valor, documentos importantes, ou outros itens sensíveis, protegendo-os contra acesso não autorizado. Diferente dos cofres tradicionais que utilizam chaves físicas ou combinações mecânicas, os cofres eletrônicos utilizam sistemas de bloqueio controlados por eletrônica, o que oferece maior flexibilidade e recursos adicionais de segurança.

Figura 3.3: Exemplo de um Cofre eletrónico. Fonte:[https://www.atitudemix.com.br/cofre-eletronico-digital-segredo-senha-23x17x17cm-chave-aco]

3.1.3.1 Principais Características de um Cofre Eletrônico

a) **Sistema de Bloqueio Eletrônico:**

O mecanismo de bloqueio é controlado por um painel eletrônico, onde o usuário precisa inserir uma senha, código PIN, ou usar outro método de autenticação (como biometria) para abrir o cofre.

Este sistema pode incluir recursos adicionais, como bloqueio automático após várias tentativas incorretas de abertura.

b) **Métodos de Autenticação:**

Senhas ou Códigos Número de Identificação Pessoal (PIN - *Personal Identification Number*): O método mais comum, onde o usuário deve inserir uma sequência

numérica no teclado do cofre para desbloqueá-lo.

Biometria: Alguns cofres eletrônicos avançados usam a autenticação por impressão digital ou reconhecimento facial para aumentar a segurança.

Cartões de Proximidade (RFID): Alguns modelos utilizam cartões Identificação por rádio frequência (RFID - *Radio-Frequency Identification*) para desbloquear o cofre.

c) **Alimentação:**

Cofres eletrônicos são alimentados por baterias internas. Muitos modelos têm uma indicação de nível de bateria ou alarmes para avisar quando as baterias precisam ser trocadas.

Alguns modelos possuem uma porta de alimentação externa de emergência para casos em que as baterias internas estejam descarregadas.

d) **Segurança Adicional:**

Alarme de Violação: Alguns cofres eletrônicos têm alarmes que disparam se tentativas de abertura forçada ou acesso não autorizado forem detectadas.

Código de Coação: Em alguns modelos, existe um ”código de coação”que, quando inserido, permite a abertura do cofre mas aciona silenciosamente um alarme ou notifica as autoridades, em caso de ameaça.

e) **Memória e Registros:**

Muitos cofres eletrônicos têm memória interna para registrar quem e quando o cofre foi acessado, o que é útil para auditorias de segurança.

f) **Design e Construção:** Construídos em aço ou outros materiais resistentes, os cofres eletrônicos combinam resistência física com mecanismos eletrônicos sofisticados para impedir arrombamentos.

3.1.3.2 Aplicações comuns de cofres eletrónicos

Os cofres eletrônicos têm uma ampla gama de aplicações em diversos ambientes devido à sua versatilidade, segurança e facilidade de uso. Aqui estão algumas das aplicações mais comuns como: residências,empresas e escritórios, hotéis, instituições financeiras e governamentais, comércio e varejo.

3.1.4 Alarme Silencioso

À medida que a segurança residencial e comercial se torna uma prioridade crescente, surgem inovações que buscam garantir proteção efetiva sem causar transtornos desnecessários aos vizinhos.

Diante disso, os alarmes silenciosos estão a surgir como uma solução eficaz e discreta. Estes sistemas de segurança oferecem uma maneira eficiente de detectar e relatar intrusões ou atividades suspeitas sem recorrer a sirenes estridentes que podem incomodar a comunidade local.

3.1.4.1 Funcionamento de um alarme silencioso

Um alarme silencioso, também conhecido como alarme discreto, opera de forma semelhante a um alarme de segurança tradicional, mas sem o uso de sirenes ou sons audíveis. Em vez disso, ele utiliza uma variedade de métodos para alertar os proprietários ou autoridades sobre uma intrusão, ou atividade suspeita de forma discreta.

Detecção de Intrusão

A detecção de intrusão é um elemento crucial no funcionamento dos sistemas de alarme silenciosos. Essa fase envolve a utilização de uma variedade de dispositivos e tecnologias para monitorar áreas específicas de uma propriedade, em busca de atividades suspeitas que possam indicar a presença de intrusos. Esta detecção pode ser feita através de sensores de forma automática, ou mesmo acionado pelo usuário apartir de senhas específicas ou botão de pânico.

É essencial que a detecção de intrusão em um sistema de alarme silencioso seja sensível o bastante para identificar atividades suspeitas, ao mesmo tempo, em que é configurada de forma inteligente para evitar disparos desnecessários. A integração adequada dessas tecnologias de detecção pode assegurar uma proteção eficaz da propriedade, ao mesmo tempo em que minimiza o risco de falsos alarmes.

Acionamento do Alarme

O acionamento do alarme em um sistema de alarme silencioso ocorre quando uma intrusão é detectada pelos dispositivos de segurança instalados na propriedade. Esse processo é desencadeado quando um dos sensores de intrusão detecta uma atividade suspeita, como movimento, abertura de uma porta ou janela, quebra de vidro, ou até o

acionamento dos mecanismos de pânico estabelecidos (botão).

A central de controle processa o sinal e aciona o alarme, emitindo um alerta sonoro ou enviando uma notificação para a empresa de monitoramento de segurança ou para o proprietário da propriedade, dependendo da configuração do sistema.

Notificação Silenciosa

A notificação silenciosa é uma parte essencial dos sistemas de alarme silenciosos, pois permite que os proprietários ou às autoridades sejam alertados discretamente sobre uma intrusão sem chamar a atenção dos invasores. Quando uma intrusão é detectada pelo sistema de segurança, em vez de acionar um alarme sonoro audível, o sistema envia uma notificação silenciosa para uma central de monitoramento de segurança ou para o proprietário da propriedade.

Essa notificação pode ser feita por meio de uma variedade de métodos, como mensagens de texto, notificações de aplicativos móveis, e-mails ou chamadas telefônicas automáticas. Dependendo da configuração do sistema, a notificação pode incluir informações detalhadas sobre o local da intrusão, como qual sensor foi acionado e a hora exata do evento.

3.1.4.2 Vantagens de um alarme silencioso

As principais vantagens de um alarme silencioso incluem:

- **Discrição:** Um alarme silencioso opera sem emitir alertas sonoros audíveis, o que evita chamar a atenção de intrusos e possíveis invasores, permitindo uma resposta mais discreta e eficaz às intrusões.
- **Segurança adicional:** Como o alarme não alerta intrusos sobre sua detecção, eles podem ser pegos de surpresa, aumentando a eficácia da segurança e reduzindo a chance de confrontos ou situações perigosas.
- **Comunicação discreta:** A notificação silenciosa permite que os proprietários ou às autoridades sejam alertados discretamente sobre uma intrusão, possibilitando uma resposta rápida e discreta à situação.
- **Redução de falsos alarmes:** Alarmes silenciosos são menos propensos a causar alarmes falsos, já que não emitem sons audíveis que podem ser desencadeados acidentalmente por movimentos ou eventos cotidianos na propriedade.

- **Integração com sistemas de segurança:** Alarmes silenciosos podem ser facilmente integrados a outros sistemas de segurança, como câmeras de vigilância, sensores de movimento e controle de acesso, para fornecer uma proteção abrangente e eficaz à propriedade.
- **Monitoramento remoto:**Muitos sistemas de alarme silenciosos oferecem recursos de monitoramento remoto, permitindo que os proprietários monitorem a segurança de sua propriedade em tempo real por meio de dispositivos móveis ou computadores. Essas vantagens fazem dos alarmes silenciosos uma escolha popular para aqueles que valorizam a segurança discreta e eficaz de suas propriedades.

3.2 Arquitetura de um sistema de controle de acesso eletrônico

A arquitetura de um sistema descreve a estrutura, comportamento e relações entre as entidades a ele pertencentes. Ela é uma descrição, sistematização ou formalização das interações entre as entidades e seu comportamento. A arquitetura demonstra as formas como um sistema pode trabalhar para executar tarefas.(Iugu 2024)

A arquitetura de um sistema de controle de acesso refere-se à organização e estruturação dos diferentes componentes que compõem o sistema, bem como às interações entre eles para garantir a segurança e o gerenciamento eficiente de acesso a locais ou recursos restritos.

A arquitetura de um sistema de controle de acesso abrange todos os elementos físicos e lógicos que trabalham juntos para controlar quem pode entrar ou acessar um determinado espaço, sistema ou recurso. Isso inclui dispositivos de entrada (como leitores de cartão, teclados ou scanners biométricos), o controlador central que processa as credenciais de acesso, atuadores que executam a abertura ou bloqueio de portas, e mecanismos de monitoramento ou alarmes para notificar sobre acessos não autorizados ou emergências.

definição clara da arquitetura é crucial para garantir que o sistema de controle de acesso seja:

- **Seguro:** Deve ser resistente a tentativas de violação, fraudes ou acessos não autorizados.

- **Confiável:** Deve operar corretamente e consistentemente, com redundâncias e medidas para lidar com falhas.
- **Escalável:** Capaz de expandir ou adaptar-se a novas exigências, como adicionar mais pontos de controle ou integrar novos métodos de autenticação.
- **Gerenciável:** Deve permitir fácil configuração, manutenção e monitoramento, possibilitando que administradores gerenciem permissões e monitorem atividades de forma eficiente.

A arquitetura pode variar dependendo do tipo de sistema implementado:

- **Centralizada:** Todos os dispositivos de controle e autenticação estão conectados a um único controlador central.
- **Distribuída:** Múltiplos controladores locais gerenciam suas áreas específicas, com comunicação entre si ou com um sistema central para sincronização e relatórios.
- **Baseada em Rede:** Utiliza a infraestrutura de rede para conectar todos os componentes, permitindo o controle e monitoramento remoto.

A figura 3.4 abaixo representada um diagrama de uma arquitetura básica de um sistema de controle de acesso.

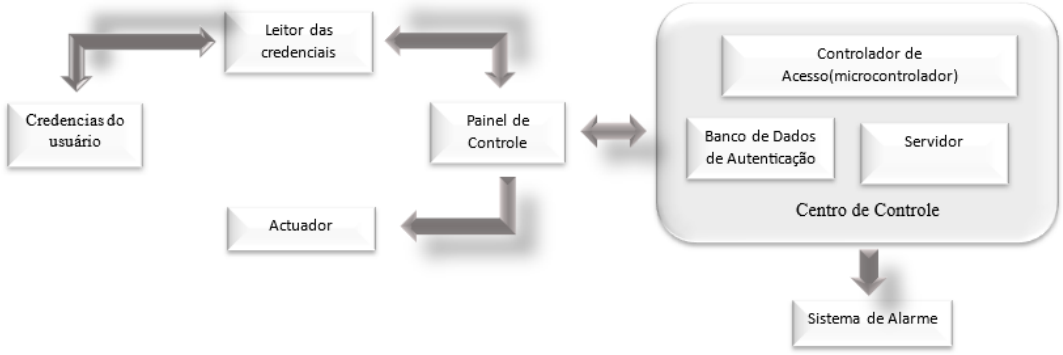


Figura 3.4: Arquitetura básica de um Sistema de Controle de Acesso. Fonte:[Autor]

Explicação do Diagrama

- **Credencias do usuário**- o bloco que representa o ponto de interação inicial, o usuário será a fonte destas credenciais (senha, Biometria, cartão RFID, etc).
- **Leitor das Credenciais**- o bloco representa o ponto de inserção das credencias, o *hardware* responsável em fazer a leitura destes valores e convertendo em sinal para

o centro de controle. Estes Dispositivos podem ser, teclados, touchpads,sensores de impressão digital, leitores de RFID e outros.

- **Actuador**- o bloco do actuador representa os mecanismos de desbloqueio, estes que vão permitir o acesso físico ao usuário. Estes mecanismos podem ser catracas, fechaduras, e outros.
- **Painel de Controle**- o bloco representa a interface do centro de controle com o usuário, permitindo com que o usuário veja o progresso, o status do sistema e possíveis alertas. Pode ser constituído por uma tela *Liquid Crystal Display* (LCD), tela touch, *light-emitting diode* (LED).
- **Centro de Controle** - é o bloco que representa o cérebro do sistema, contendo a lógica do funcionamento do programa e a base de dados das autenticações o servidor. Este bloco é o que faz a decisão de dar ou não o acesso ao usuário, comanda os outros elementos e aciona o alarme em casos de necessidade. Constituído basicamente por um microcontrolador, um servidor que faz conexão com outros computadores, por exemplo para fazer o registro de atividades para uma possível auditoria.
- **Sistema de Alarme**- o bloco que representa os componentes que vão notificar uma autenticação incorrecta ou abusiva.

3.3 IoT e Automação

O termo *Internet of Things* (IoT), ou Internet das Coisas, refere-se à rede coletiva de dispositivos conectados e à tecnologia que facilita a comunicação entre os dispositivos e a nuvem, bem como entre os próprios dispositivos. Graças ao advento de chips de computador baratos e telecomunicações de alta largura de banda, agora temos bilhões de dispositivos conectados à Internet. Isso significa que dispositivos do dia a dia, como escovas de dentes, aspiradores, carros e máquinas, podem usar sensores para coletar dados e responder de forma inteligente aos usuários.

Por outro lado, segundo o Martins 2019, a automação de processos é uma estratégia de otimização estrutural específica para determinadas atividades de uma organização. Ela pode ser utilizada em diversas frentes e garante que os métodos de trabalho se tornem mais fáceis, reduzindo a necessidade de tarefas manuais. A automação pode ser divida em 3 partes, residencial, comercial e industrial.

Quando processos automáticos são gerenciados (controlados e ou observados) através da Internet, ocorre uma relação entre a automação e IoT. O termo IoT é normalmente usado quando aplicado o uso da Internet na automação .

3.3.1 Tecnologias de comunicação

As Tecnologias de comunicação IoT desempenham um papel essencial, permitindo que os dispositivos se comuniquem entre si e com a nuvem de maneira eficiente e segura.

Essas tecnologias abrangem uma variedade de protocolos de comunicação, projetados para suportar diferentes requisitos de conectividade, como latência, consumo de energia, largura de banda e segurança. Protocolos como MQTT (Message Queuing Telemetry Transport), REST API, *HyperText Transfer Protocol* (HTTP) HTTP e LoRaWAN são amplamente utilizados para a transmissão de dados entre dispositivos e plataformas, enquanto tecnologias sem fio como Wi-Fi, oferecem soluções para conectividade em diferentes tipos de redes.

Além disso, plataformas de automação, como o IFTTT *(If This Then That)*, têm facilitado a integração de dispositivos IoT, permitindo a criação de cenários automatizados, onde ações são desencadeadas por eventos específicos. Dessa forma, a escolha adequada das tecnologias de comunicação IoT é fundamental para garantir a eficiência, segurança e escalabilidade dos sistemas IoT, especialmente em aplicações críticas.

MQTT(Message Queuing Telemetry Transport)

Segundo Cravo 2024, *Message Queuing Telemetry Transport* (MQTT) é um protocolo de transporte de mensagens que possibilita a comunicação entre máquinas e é amplamente usado para conectividade de IoT *(Internet of Things)*. É aberto, leve e tem fácil implementação, sendo executado em TCP/IP ou em outros protocolos de rede.De formato Cliente/Servidor, usa o paradigma Publish/Subscribe, em que o Cliente pode fazer “postagens/publicações” ou captar informações, enquanto o Servidor administra o envio e o recebimento desses dados.

O protocolo MQTT opera seguindo um modelo de publicação e subscrição, através de mensagens assíncronas baseadas em tópicos.

Vantagens do MQTT: Segurança, Baixa exigência, Confiabilidade, Eficiência, Baixo consumo de memória.

ZigBee

Segundo Intelbras 2023, Zigbee é um protocolo sem fio muito usado em dispositivos de casa inteligente, principalmente pela facilidade de transmitir pequenos pacotes de dados com baixo consumo de energia. Dessa forma, os dispositivos podem ser usados por meses sem a necessidade de recarregar ou trocar a bateria.

A tecnologia cria uma rede exclusiva dentro de casa para os dispositivos inteligentes, permitindo controlar inúmeros aparelhos para automação residencial por meio do celular. Para os dispositivos Zigbee funcionarem na sua casa, geralmente é necessário instalar um hub de automação. Por meio de um hub como esse, você pode gerenciar diversos dispositivos Zigbee na sua residência. Somente o hub precisa se conectar ao roteador de internet, enquanto os outros dispositivos inteligentes se conectam diretamente ao hub, não sobrecarregando o seu roteador.

Vantagens do Zigbee: custo-benefício, Baixo consumo de energia, Menos sobrecarga na rede wifi, intercomunicacao entre os dispositivos, praticidade.

Desvantagens: Necessidade de um Hub Zigbee, Equipamentos compatíveis

IFTTT *(If This Then That)*

O IFTTT é uma solução de automação simples e intuitiva. Ela possibilita que usuários com todos os níveis de conhecimento em programação criem scripts, ou applets, para gerar interações automáticas entre serviços ou dispositivos. A sigla IFTTT (*If This Then That*), do inglês “Se Isto Então Aquilo”, é uma ferramenta de automação para integrar serviços digitais, redes sociais e dispositivos inteligentes. Seu nome se baseia na função *“if-then / if-then-else”*, um dos primeiros códigos estudados em programação e presente em praticamente todas as sintaxes.

Vantagens: Simplicidade na criação de automações, suporte a vários dispositivos e serviços populares.

3.4 Microcontrolador

O microcontrolador é como se fosse um computador com somente um chip, pois possui vários componentes existentes no computador, como unidade de processamento, memórias, temporizadores, canal de comunicação todos no mesmo circuito integrado.Assim, sistemas mais compactos e tão potentes quanto um computador podem ser feitos a partir de um microcontrolador. (Menezes 2018)

O microcontrolador é um circuito único e integrado que possui, em sua composição, o

núcleo processador, suas memórias (voláteis e não voláteis) e qualquer tipo de periférico de entrada e de saída de dados. (Kassouf 2022)

Custo/benefício para soluções de aplicações que necessitam de bom desempenho de processamento, baixo custo e tamanho físico de hardware. Dentro de um microcontrolador está encapsulado o microprocessador para processamento, memória para armazenamento de programas e variáveis definidas nos programas, pinos de entrada e saída para comunicação do microcontrolador com periféricos. Essas características diferenciam o microcontrolador do microprocessador, pois esse último não possui todos esses recursos em uma única capsula (Menezes 2018).

No mercado, existem vários exemplos de microcontroladores, mas são destacados alguns deles como e o caso do Arduino, ESP32 e o PIC (*Peripherical Interface Controller*).

3.4.1 Tipos de Sinais

Os microcontroladores processam diversos tipos de sinais para controlar dispositivos e realizar tarefas específicas em sistemas embarcados. Esses sinais podem ser de natureza digital ou analógica, e o microcontrolador deve ser capaz de interpretá-los para executar as funções desejadas.

De uma forma simples podemos dividir em três tipos: analógicos, digitais e PWM.

Sinais Analógicos

Toda a grandeza Analógica é aquela que assume uma infinidade de valores ao longo do tempo de uma forma contínua e sem saltos bruscos (p.e. variação da temperatura ao longo de um dia). (Doho 2021)

Sinal analógico é qualquer sinal contínuo no tempo que pode assumir infinitos valores de amplitude dentro do seu intervalo de valores máximo e mínimo, sendo que estes podem também ser infinitos. O termo analógico refere-se a que este tipo de sinal é análogo (similar) ao da sua fonte, por exemplo quando uma pessoa fala ao telefone o sinal elétrico analógico da sua voz é análogo a onda sonora que o seu aparelho fonético gera.

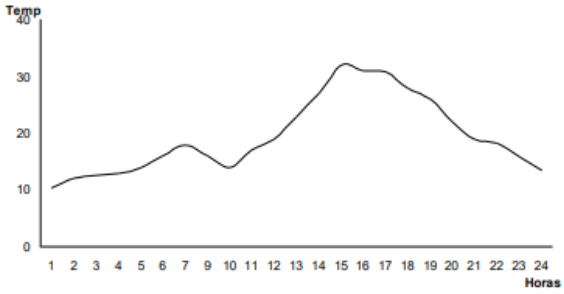


Figura 3.5: Sinais Analógico. Fonte: Doho 2021

Sinais Digitais

Toda a grandeza Digital é aquela que assume um número finito de valores e que varia de valor por saltos de uma forma descontínua (p.e. variação hora a hora da temperatura ao longo de um dia). Portanto a sua evolução no tempo consiste precisamente em saltar duns valores discretos para outros. Doho 2021

Sinal digital é qualquer sinal que assume apenas alguns valores de amplitude, sua variação de amplitude ocorre em degraus, abruptamente.

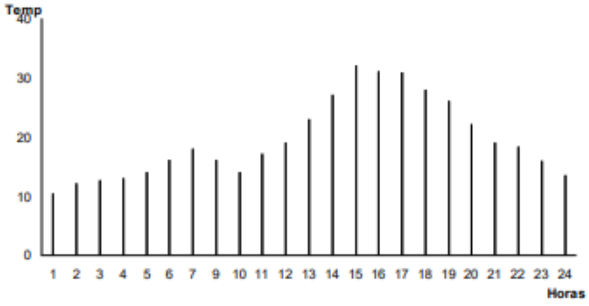


Figura 3.6: Sinais Digitais. Fonte:Doho 2021

Sinais PWM(Modulação por Largura de Pulso)

Sinal PWM é um sinal formado por uma sequência de pulsos quadrados enviados periodicamente, com a mesma frequência, porém com diferentes frações do tempo do pulso com tensão igual a zero. A fração de tempo do pulso com tensão igual a zero pode variar de 0% a 100%.

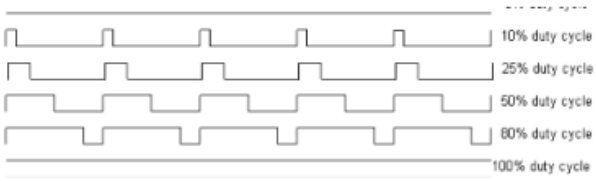


Figura 3.7: Sinal PWM Fonte:Doho 2021

3.4.2 Arduino

De acordo com Menezes 2018, o Arduino é uma plataforma eletrônica de código aberto baseada em hardware e software fáceis de usar, comumente usado para criação de dispositivos que permitam iteração com o ambiente, por isso pode ser denominado um sistema embarcado. A simplicidade dessa plataforma é uma de suas maiores vantagens, e o *bootloader* desempenha um papel essencial nesse processo.

No caso do Arduino, o bootloader permite que você carregue um novo programa no microcontrolador apenas conectando a placa ao computador via USB e usando a interface de software (IDE Arduino).

Graças ao bootloader, o processo de gravação no microcontrolador é simplificado, permitindo que o usuário evite a complexidade de usar programadores externos especializados.

A linguagem de programação contida no *software* do arduino é *open source* e é baseada na linguagem C/C^{++}. O Arduino *integrated development environment* (IDE) é o software que permite ao usuário escrever, compilar e carregar programas no Arduino. Ele oferece uma interface simples e intuitiva para o desenvolvimento de projetos. Para upload de programas para a placa Arduino é utilizada comunicação serial com o computador através de uma porta USB.

A empresa fabricante do arduino disponibiliza diferentes tipos deste produto, podendo variar de acordo com a aplicação, tamanho e preço. Dos produtos mais conhecidos encontra-se o Arduino UNO, Arduino Mega, Arduino Leonardo e Arduino nano.

3.4.2.1 Arduino Uno

O arduino uno é uma placa microcontroladora baseada no microControlador ATmega 328p. O atmega 238 usa uma arquitetura de Havard modificada, RISC, 8 bits.

O arduino uno apresenta 14 pinos digitais input/outputs (6 deles podem ser PWM), 6

pinos analógicos, um clock de 16 MHZ, um conector USB, um jack de alimentação.

O “UNO” é uma palavra italiana , essa placa é refência como a série de placas arduino com USB integrado. O Arduino uma ferramenta simples de usar e programar, mesmo para leigos em programação(o arduino usa uma linguagem de progrmação Sketch, baseada em C/C++) e eltrônico, uma vez que a plataforma já tem muitos perifféricos amigáveis (Portas e plugs de alimentação, fáceis de identificar)a um usuário comum, diferente do chip Atmega que pode não ser tão amigável para quem não tem noção de eltrónica e de programação(uma vez que este usa a linguagem C/C++ pura).

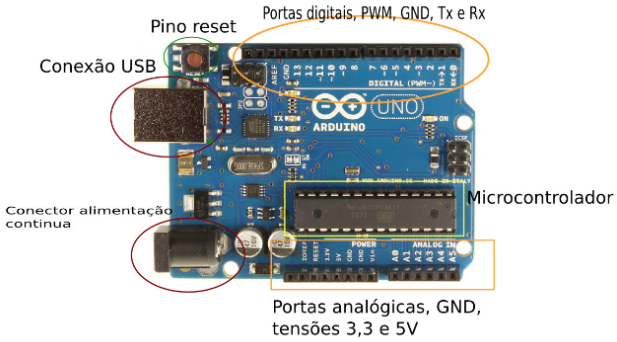


Figura 3.8: Arduino uno. Fonte: Menezes 2018

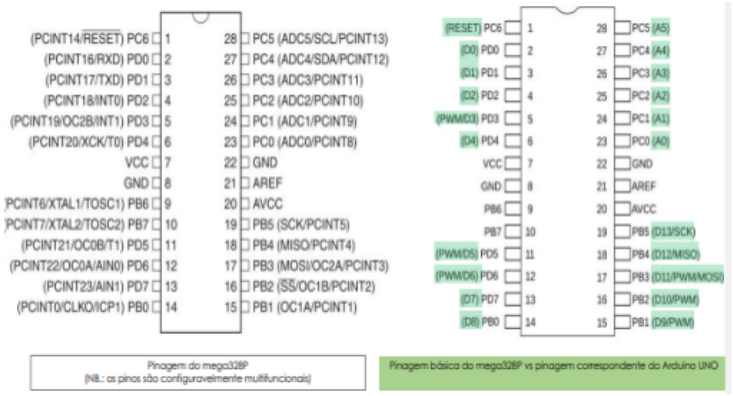


Figura 3.9: Pinos do Arduino uno vs Atmega.Fonte: Doho 2021

3.4.3 Esp32

O ESP32 é um microcontrolador de baixo custo e baixo consumo de energia desenvolvido pela empresa chinesa Espressif Systems. É considerado um dos microcontroladores mais poderosos e versáteis disponíveis no mercado.

Projetado para dispositivos móveis, eletrônicos vestíveis e aplicativos IoT, o ESP32

atinge um consumo de energia ultrabaixo com uma combinação de vários tipos de software proprietário. O ESP32 também inclui recursos de última geração, como clock refinado, vários modos de energia e escala dinâmica de energia. Expressif 2024

Este microcontrolador possui conversores CAD, portas analógicas, portas digitais e PWM. Uma das coisas que se destaca nesta placa é conectividade por Wi-Fi e Bluetooth possibilitando a conexão com os outros dispositivos com mesmas conexões. Estas placas podem ser usadas para automatização de processos com eficiência energética, automatização wireless, implementação em wearables.

Um dos principais recursos do ESP32 é o modo de baixa energia, com múltiplos estados de economia de energia, como modo de sono profundo (deep sleep) e modo de hibernação, que permitem que ele consuma apenas alguns microamperes em standby. A fabrincante disponibiliza produtos mais dedicados como é o exemplo do ESP32CAM.

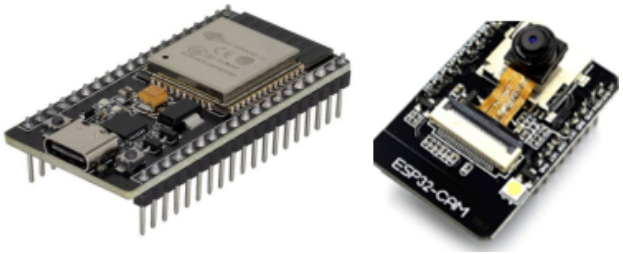


Figura 3.10: ESP32 Devkit . Fonte:Adaptado do Aliexpress.com

3.4.3.1 ESP-WROOM-32

O ESP32-WROOM-32E e o ESP32-WROOM-32UE são módulos de microcontroladores versáteis que oferecem conectividade Wi-Fi, Bluetooth e Bluetooth Low Energy (BLE), projetados para uma ampla gama de aplicações, desde redes de sensores de baixo consumo até tarefas mais exigentes, como codificação de voz, streaming de música e decodificação de MP3.

O ESP-WROOM-32 é uma placa que contém o módulo ESP32, conforme ilustra a figura 3.11, onde é possível notar suas várias funcionalidades distribuídas em sua versão com 36 pinos. Possui pinos para interface GPIO, *Universal Asynchronous Receiver-Transmitter* (UART), *Inter-Integrated Circuit* (I2C), sensores de toque, sensor de Efeito Hall, conversores AD e DA, e outros.

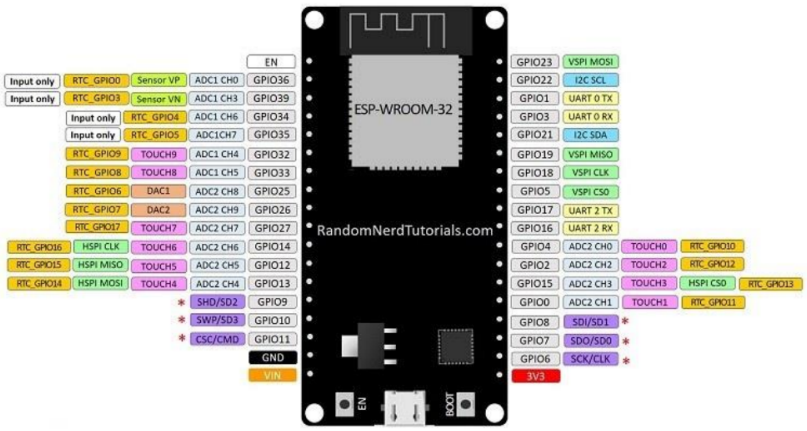


Figura 3.11: pinos e funcooes do ESP WROOM 32.Fonte: Martins 2019

3.4.4 PIC (Peripherical Interface Controller)

O Microcontrolador PIC16F628 é um poderoso e eficiente componente de fácil programação e comumente empregado no desenvolvimento de pequenos projetos eletrônicos de modo a controlar o funcionamento de sensores e componentes.

Internamente o Microcontrolador PIC16F628 possui encapsulado um microprocessador, a memória de programa e dados, a comunicação serial, o conversor analógico/digital, os geradores PWM, além de vários periféricos.

O Microcontrolador PIC16F628 foi desenvolvido pela empresa Microchip, uma das maiores empresas de tecnologia do mundo, sendo precursora na utilização da tecnologia *Reduced Instruction Set Computer* (RISC) em microcontroladores.

Através de sua arquitetura RISC, o Microcontrolador PIC16F628 traz uma nova tendência ao mercado, sendo este um equipamento com um conjunto reduzido de instruções, favorecendo conjuntos pequenos e simples de informações.

O microcontrolador PIC traz tem o papel de ser um componente de controle de projetos, apresentando diversos modelos com memoria, osciladores e quantidade de pinos diferentes. Como a maioria dos microcontroladores, ele possui uma memória programável, na qual pode-se escrever de acordo com seu parâmetro por meio da linguagem C. Seu barramento de I/O o permite receber e enviar sinais digitais e analógicos. Portanto sensores e chaves eletrônicas são as principais ferramentas usadas com o PIC. Por isso, o PIC vem sendo utilizado de modo didático e profissional, em produtos como fonte, inversores, sistemas de IOT e qualquer ocasião que é necessário o controle de sistemas lógicos, sistemas analógicos, PWM, comparadores por meio da linguagem C.(Vitor 2022

)

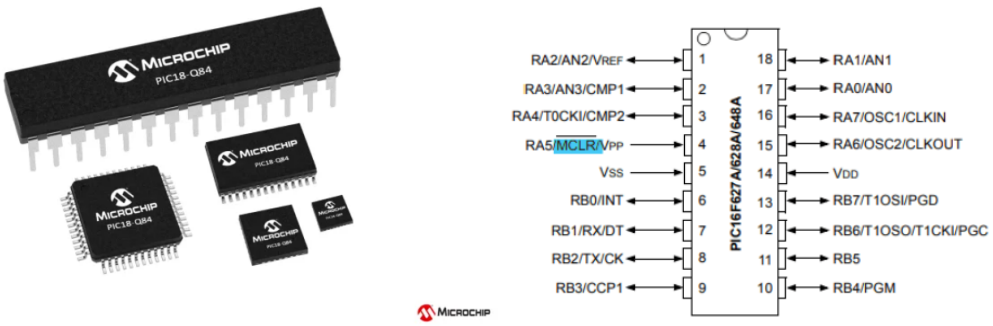


Figura 3.12: Microcontroladores PIC e Pinos do PIC16F628A. Fonte:Vitor 2022

3.4.5 Comparação entre os microcontroladores

Embora os três controladores acima descritos tenham muitas semelhanças, dentre eles existem algumas diferenças que podem constituir vantagens ou desvantagens dependendo das aplicações. Abaixo está apresentado uma tabela de algumas comparações entre estes microcontroladores:

Tabela 3.1: comparação entre os micrcontroladores.fonte[Autor]

	ARDUINO UNO R3	ESP WROOM 32	PIC16F628
Microprocessador	Atmega328p	esp32	PIC16F84A
Cores	1	2	1
Arquitetura	8 bits	32 bits	8bits
clock	16 MHz	160 MHz	20 MHz
WiFi	-	sim	-
Bluetooth	-	sim	-
RAM	2KB	512 KB	256 Kb
FLASH	32 KB	16Mb	4Mb
GPIO	14	36	16
Interfaces	SPI/ I2C/ UART	SPI/ I2C/ UART/ I2S/ CAN	USART
ADC	6	18	-
DAC	0	2	-
Tensao de operacao	3.3- 5	3.3	2-5.5

3.5 Teclados

Como forma de introduzir a senha para ser validada no sistema do cofre, pode ser usado um teclado físico. Existem diferentes tipos destes, que podem diferir quanto a forma de construção ou ate mesmo a forma de funcionamento. Alguns destes tipos podem ser:

Teclados Matriciais

Segundo Giraldo 2023, O teclado de matriz é um dispositivo bastante comum em projetos com sistemas micro-controlados como o Arduino e é basicamente composto por um conjunto de botões distribuídos em forma de matriz, que podem ser lidos usando alguns pinos do Arduino, usando o conceito de multiplexação.

Um teclado matricial é um dispositivo que agrupa vários botões e permite que eles sejam controlados usando um número menor de condutores do que precisaríamos ao usá-los individualmente. Podemos usar esses teclados como um controlador para um autômato ou um processador como o Arduino ou esp32.

Teclados Capacitivos

Os teclados capacitivos, ao contrário dos convencionais, utiliza, uma só pista para cada tecla e uma para o terra. O acionamento é detectado pela mudança da capacitância provocada pelo contato do dedo do usuário. Não há movimento do material, portanto sua vida útil será muito maior.

São utilizados especialmente entre os usuários que necessitam de um desempenho mais preciso e eficiente em suas atividades. Esses teclados são diferentes dos teclados mecânicos tradicionais, que usam interruptores físicos para registrar as teclas pressionadas. Eles detectam até mesmo a pressão mais leve, tornando a digitação mais suave e precisa.

Teclados de Membrana

São compostos de uma camada de plástico flexível com contatos elétricos impressos em sua superfície. Quando pressionado, o contato é fechado e o sinal é enviado ao microcontrolador.

Quando uma tecla de membrana é pressionada, duas camadas condutivas fazem contato, fechando o circuito e registrando o pressionamento. Estes podem ser usados em cofres portáteis e sistemas de segurança onde a durabilidade e resistência a ambientes adversos são importantes.

Figura 3.13: Exemplos de teclados usados em cofres. Fonte: Adaptado de: https://www.aliexpress.com/

3.6 *Displays*

Os displays são componentes essenciais para projetos com microcontroladores, pois permitem a exibição de informações visuais como texto, números, gráficos e imagens. Eles podem variar em tamanho, tecnologia, interface de comunicação e consumo de energia, oferecendo soluções para diferentes tipos de aplicações, desde dispositivos simples até interfaces gráficas complexas. Vários tipos de displays podem ser utilizados com microcontroladores, dependendo da aplicação, da interface disponível e das necessidades de exibição. Alguns dos *displays* .

- **Displays de Segmentos (7 Segmentos e 14 Segmentos):**

  7 Segmentos: Exibe números de 0 a 9, usando sete LEDs que formam o formato numérico.

  14 Segmentos: Pode exibir números e algumas letras, com 14 LEDs formando uma matriz que permite exibir mais caracteres. Uso comum: Relógios digitais, medidores e contadores.

- **LCD Alfanumérico (Liquid Crystal Display)** Exibe texto em formato de linhas e colunas, como os populares LCD 16x2 (16 colunas, 2 linhas) ou LCD 20x4. Alguns apresentando uma luz de fundo para melhor visualização da informação. Controlado via interface paralela ou por meio de um módulo I2C para reduzir a quantidade de pinos.

  Este tipo de displyas costuma ser excelente para exibir textos simples em projectos e apesenta uma facilidade de implementação.

- **LCD gráfico 128x64**- Displays de matriz de pixels, como o LCD gráfico 128x64. Permitem a exibição de gráficos, ícones e até pequenas imagens. Pode ser conectado

ao microcontroladores usando uma interface i2c.Estes têm melhor uso em projectos que deseja-se uma apresentação um pouco mais complexa.

- **OLED (Organic Light-Emitting Diode)**- Displays com ótima qualidade de imagem e alto contraste, pois cada pixel é uma fonte de luz individual. Estes podem ter um consumo energético muito baixo quando exibindo imagens com muitos pixels apagados (preto).

Figura 3.14: Exemplo de Display usado em microcontroladores. Fonte: https://arduinoeeletronica.com.br/produto/display-lcd-168-x-64-blue-display-grafico/

3.7 Relé

Os relés são um tipo de interruptor dentro de um sistema eletrônico. O acionamento dos contatos ocorre quando a bobina é energizada, onde se cria um campo magnético que atrai o contato móvel e realiza a mudança do estado dos contatos. Os relés são revertidos por um invólucro, que funciona como uma carcaça de proteção para os componentes do relé.Esse componente pode ser utilizado para acionar mais de um circuito ao mesmo tempo com um único sinal, pode controlar sinais digitais através de uma tensão alternada e vice-versa. São muito utilizados pelo seu baixo custo e robusteza, sendo encontrados na automação predial e residencial, na indústria em geral, na distribuição de energia e para acionamentos e controle de equipamentos elétricos.

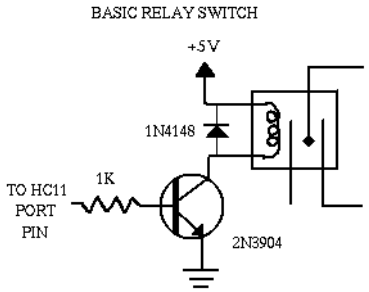


Figura 3.15: Esquema básico de um circuito com relé. Fonte:[https://web.mit.edu/rec/www/workshop/relays.html]

3.7.1 Tipos de relés

Segundo Veris 2025, existem diversos tipos de relés para uma variedade de aplicações, os três tipos mais comumente usados são relés eletromecânicos (EMR), relés de estado sólido (SSR) e relés Reed.

Relé Eletromecânicos

Os relés eletromecânicos são o tipo mais básico de relé. Eles funcionam usando a bobina eletromagnética padrão que pode manipular o contato móvel. No entanto, esse movimento físico pode demorar mais e leva a arcos internos, o que pode degradar o relé com o tempo.

Relé de estado sólido

Um relé de estado sólido opera usando um semicondutor que controla o mecanismo de comutação do relé. Isso é feito usando um sinal óptico de baixa tensão do semicondutor que, quando acionado, permite a operação da carga de alta tensão controlada. Os relés de estado sólido são conhecidos por sua operação rápida e vida útil comparativamente longa em comparação com as alternativas eletromecânicas. A principal desvantagem dos relés de estado sólido é o calor adicional que eles geram por meio da operação do semicondutor, o que pode causar problemas ou exigir soluções integradas para evitar o superaquecimento.

Relé Reed

Os relés de palheta também operam em uma base eletromecânica em seu núcleo, mas usam um design modificado para reduzir ou eliminar problemas comuns de EMR. Eles são compostos de duas lâminas de metal magnéticas suspensas dentro de um tubo de gás inerte com uma bobina. Quando a bobina é energizada, as duas lâminas são atraídas

uma pela outra, completando o circuito. Isso evita parte do desgaste que reduz a vida útil dos relés EMR típicos. Ainda assim, eles são mais lentos e não conseguem lidar com uma corrente tão alta quanto os switches SSR.

3.8 Biometria

A biometria é um termo que remete o reconhecimento de pessoas por suas características. Em sentido literal, é a ciência que estuda as medidas dos seres vivos, isto é, identifica o indivíduo por meio de suas características físicas e comportamentais.

Segundo Menezes 2018, na natureza encontra-se variados mecanismos biométricos para a identificação entre os seres vivos, através de meios sensoriais e registros de memória. Essas referências são consideradas pela ciência como habilidades de alta sofisticação e servem hoje como parâmetro para pesquisa e desenvolvimento tecnológico na área da biometria (Menezes 2018).

A capacidade de diferenciar seguramente um indivíduo é denominada como autenticidade. Os meios de autenticação que existem são diversificados e podem ser divididas em características físicas e comportamentais de cada um, visando identificá-lo de maneira única. Entre as características físicas tem-se a identificação por meio da face, geometria da mão, íris, retina, impressão digital. E as características comportamentais são identificadas pela assinatura manuscrita, voz (pode-se enquadrar também em física), maneira de caminhar

3.8.1 Características

Na analise da biometria e importante observar alguns critérios para escolha de características biométricas, estes factores podem ser:

- **Universalidade**: toda a população a ser autenticada deve possuir essa característica. A característica biométrica deve estar presente em todos os indivíduos do grupo a ser autenticado. Exemplos incluem impressões digitais, íris, rosto, entre outros;
- **Unicidade**: duas pessoas devem ser suficientemente diferentes de acordo com a característica em questão. A característica deve ser única para cada pessoa, garantindo que dois indivíduos não compartilhem a mesma medida. Isso é crucial para evitar falsos positivos;

- **Imutabilidade**: a característica deve ser suficientemente invariante durante um período de tempo;
- **Mensurabilidade**: A característica deve ser possível de ser medida de forma quantitativa ou qualitativa. Isso envolve a existência de tecnologia disponível para a captura e processamento de dados biométricos..

Ainda assim, para um sistema biométrico, isto é, um sistema que utiliza biometria para identificar pessoas, ainda há alguns fatores que devem ser considerados:

- **Desempenho**: Mede a precisão, a rapidez e a robustez do sistema. Inclui o tempo necessário para a verificação/autenticação e os recursos computacionais envolvidos. Além disso, fatores ambientais (como luz, temperatura) podem influenciar o desempenho;
- **Aceitabilidade**: os indivíduos a serem identificados devem aceitar fornecer a característica ao sistema usualmente;
- **Impostura**: refere-se ao quão fácil o sistema pode ser enganado usando métodos fraudulentos.

De acordo com os critérios de escolha das características Biométricas bem como o su sistema, pode-se fazer algumas comparações entre as diferentes características.

Característica Biométrica	Universalidade	Unicidade	Imutabilidade	Mensurabilidade	Desempenho	Aceitabilidade	Impostura
Face	Alta	Baixa	Média	Alta	Baixa	Alta	Alta
Impressão Digital	Média	Alta	Alta	Média	Alta	Média	Média
Geometria da Mão	Média	Média	Média	Alta	Média	Média	Média
Íris	Alta	Alta	Alta	Média	Alta	Baixa	Baixa
Retina	Alta	Alta	Média	Baixa	Alta	Baixa	Baixa
Assinatura Manuscrita	Baixa	Baixa	Baixa	Alta	Baixa	Alta	Alta
Voz	Média	Baixa	Baixa	Média	Baixa	Alta	Alta

Figura 3.16: Comparações entre as diferentes características Biométricas. Fonte: Menezes 2018

3.9 Base de Dados

Saxena 2025, define base de dados como uma coleção sistemática de dados armazenada eletronicamente que pode incluir palavras, números, imagens, vídeos e outros tipos de arquivos. Os bancos de dados são gerenciados usando um software especializado chamado Sistema de Gerenciamento de Banco de Dados (SGBD), que permite aos usuários armazenar, recuperar e manipular dados com eficiência.

Os bancos de dados desempenham um papel crítico no gerenciamento e organização de dados, permitindo que as empresas operem com eficiência e tomem decisões informadas. Veja por que eles são essenciais:

1. **Dimensionamento eficiente:** Os bancos de dados podem lidar com grandes quantidades de dados, dimensionando para milhões ou bilhões de registros. Sem bancos de dados, gerenciar esse nível de dados digitais seria impossível.
2. **Integridade dos dados:** regras e condições integradas nos bancos de dados garantem consistência e precisão dos dados, mesmo quando eles crescem ou mudam.
3. **Segurança de dados:** Os bancos de dados protegem informações confidenciais implementando autenticação de usuário, controle de acesso e conformidade com os regulamentos de privacidade.
4. **Análise de dados:** Os bancos de dados modernos oferecem suporte a ferramentas de análise para identificar padrões, tendências e previsões. Esse recurso ajuda as organizações a tomar decisões baseadas em dados.

3.9.1 Componentes de uma Base de Dados

Dados

Os dados são o componente central de qualquer banco de dados, representando as informações reais armazenadas. Pode incluir números, texto, imagens, vídeos ou documentos, dependendo da finalidade do banco de dados. Por exemplo, um banco de dados de clientes pode armazenar nomes, endereços e históricos de compras de clientes.

Esquema

O esquema é o blueprint ou a estrutura do banco de dados. Ele define como os dados são organizados e inclui detalhes como tabelas, colunas, tipos de dados e relacionamentos entre entidades. Por exemplo, uma tabela em um banco de dados de clientes pode ter colunas como CustomerID, Name e Email. O esquema garante consistência e ajuda

os usuários a entender como o banco de dados é projetado.

SGBD

O SGBD ou DBMS é a camada de software que permite a interação com o banco de dados. Ele gerencia o armazenamento, a recuperação e a manipulação de dados, garantindo a segurança e a integridade dos dados. Exemplos de software DBMS incluem MySQL, Oracle e MongoDB. O DBMS também lida com tarefas como backup, recuperação e otimização de consultas para manter o desempenho do banco de dados.

Consultas

Consultas são comandos usados para interagir com o banco de dados, permitindo que os usuários recuperem, manipulem ou atualizem dados. Para bancos de dados relacionais, SQL (Structured Query Language) é comumente usado. Por exemplo, uma consulta como recupera todos os clientes dos EUA. As consultas são vitais para extrair insights acionáveis e gerenciar dados com eficiência.SELECT * FROM Customers WHERE Country = 'USA';

Usuários

Os usuários são indivíduos ou aplicativos que interagem com o banco de dados. Eles podem ter diferentes níveis de acesso com base em suas funções, como administradores, desenvolvedores ou usuários finais. Por exemplo, um administrador de banco de dados pode ter controle total, incluindo a capacidade de criar ou excluir tabelas, enquanto um usuário comum pode ter permissão apenas para exibir dados específicos.

3.9.2 Tipos de Base de Dados

As bases dados podem ser classificadas com base em sua estrutura, casos de uso ou métodos de armazenamento. A melhor base de dados para uma organização específica depende de como a organização pretende usar os dados. Nos diferentes tipos de base de dados podem se destacar alguns tipos como: Bancos de dados relacionais, Bancos de dados orientados a objetos, Bancos de dados distribuídos, Bancos de dados NoSQL, Bancos de dados gráficos, Bancos de dados em nuvem e outros.

3.9.2.1 Base de dados Relacional

Uma base de dados relacional é um tipo de banco de dados que armazena e fornece acesso a pontos de dados relacionados entre si. Bancos de dados relacionais são baseados no modelo relacional, uma maneira intuitiva e direta de representar dados em tabelas. Em um banco de dados relacional, cada linha na tabela é um registro com uma ID exclusiva chamada chave. As colunas da tabela contêm atributos dos dados e cada registro geralmente tem um valor para cada atributo, facilitando o estabelecimento das relações entre os pontos de dados.O modelo relacional significa que as estruturas de dados lógicas: tabelas de dados, exibições e índices - são separadas das estruturas de armazenamento físico. Essa separação significa que os administradores de banco de dados podem gerenciar o armazenamento de dados físicos sem afetar o acesso a esses dados como uma estrutura lógica. Por exemplo, a renomeação de um arquivo de banco de dados não renomeia as tabelas armazenadas nele.

3.9.2.2 SQL (Linguagem de consulta estruturada)

SQL (Linguagem de consulta estruturada) é uma linguagem de programação utilizada para o tratamento e processamento de dados, que auxilia no armazenamento, manipulação e recuperação de dados em bancos de dados relacionais. Quando os dados precisam ser recuperados de um banco de dados, o SQL é usado para fazer a solicitação. O SQL é usado por administradores de banco de dados, desenvolvedores e analistas de dados para tarefas como definição de dados, controle de acesso, compartilhamento de dados, escrita de scripts de integração de dados e execução de consultas analíticas.

O SQL é usado para armazenar, recuperar, gerenciar e manipular dados em sistemas de gerenciamento de bancos de dados (DBMS). Ela é compatível com aplicações de processamento de transações e análise de dados e se integra sem dificuldades a várias linguagens de programação, como Java, permitindo que os desenvolvedores criem aplicações de processamento de dados de alto desempenho para diferentes necessidades de business intelligence.

Capítulo 4

Desenho e Implementação do Protótipo

4.1 Desenvolvimento da Solução

O desenvolvimento do trabalho foi dividido em 2 etapas. A primeira etapa consistiu na identificação e seleção dos componentes que pudessem atender os requisitos do funcionamento do sistema, levando em consideração o custo benefício de cada um e sua facilidade de aquisição no mercado. Na segunda, o *hardware* e *software* do sistema foram desenvolvidos, tendo em vista atender todos os objetivos propostos pelo trabalho.

4.1.1 Descrição Funcional do Sistema

O presente projeto propõe o desenvolvimento de um sistema de controle de acesso eletrônico voltado para cofres ou salas de acesso restrito, utilizando como base um microcontrolador programável. O sistema é responsável por realizar a autenticação do usuário por meio de senha numérica e/ou biometria (impressão digital), controlando assim uma fechadura elétrica que permite ou bloqueia o acesso à porta do compartimento protegido.

De forma geral, o funcionamento do sistema consiste na verificação dos dados inseridos pelo usuário: se a senha ou a biometria coincidir com os dados previamente cadastrados, a fechadura será acionada, permitindo a abertura do cofre. Caso contrário, o acesso é negado, reforçando a segurança contra tentativas de intrusão.

Como diferencial de segurança, foi implementada uma senha de pânico, especialmente pensada para situações de coação. Ao ser inserida, essa senha é tratada de forma distinta: embora permita a abertura da fechadura a fim de não levantar suspeitas por parte de um possível agressor , ela aciona um alarme silencioso que envia automaticamente um sinal de alerta para uma central de segurança, além de ativar uma câmera

de vigilância posicionada no local, que transmite imagens em tempo real. Esse recurso visa possibilitar uma resposta rápida por parte de autoridades ou agentes responsáveis, aumentando a proteção da vítima e a eficácia na prevenção de roubos ou invasões.

Todos os registros de acesso, incluindo tentativas bem-sucedidas e malsucedidas de autenticação, são armazenados em uma base de dados hospedada em um servidor. Essas informações são organizadas de forma cronológica e incluem dados como o tipo de autenticação utilizada, data, hora e status da tentativa (sucesso, falha ou senha de pânico). O sistema conta com um painel administrativo acessível via computador, por meio do qual é possível visualizar, filtrar e analisar esses registros. Essa funcionalidade torna-se essencial em processos de auditoria, controle interno ou análise forense, permitindo identificar padrões de uso, tentativas de violação de segurança ou comportamentos suspeitos relacionados ao acesso ao cofre.

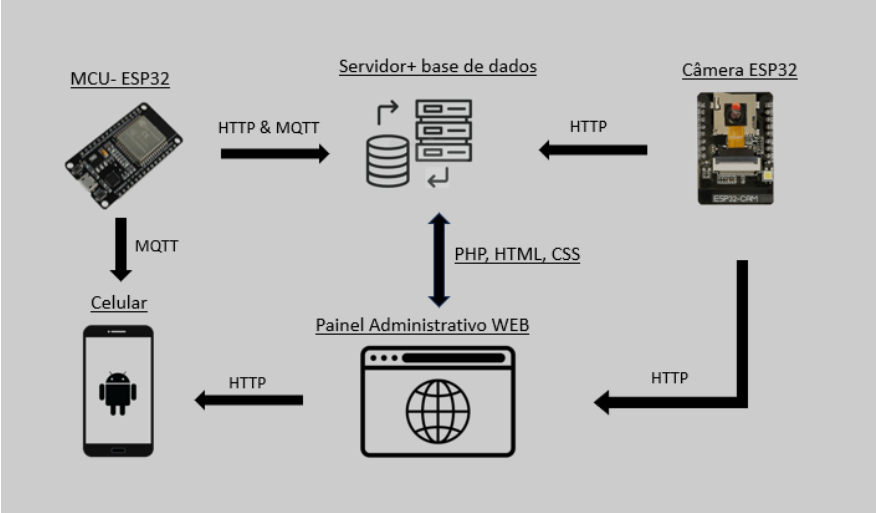


Figura 4.1: Arquitectura da solução proposta. Fonte: [Autor]

4.1.2 Requisitos Funcionais

Hardware:

- Microcontrolador de baixo consumo energético;
- Interface (Display);
- Sensor biométrico
- Teclados
- Módulo de comunicação
- Fonte de alimentação

- Fechadura eléctrica;

Software:

- Firmware embarcado para autenticação;
- Aplicação para a notificação do alarme;
- Banco de Dados para armazenar os registros;
- Servidor Backend para fazer a intercomunicação dos dispositivos;
- Painel administrativo.

4.2 Dimensionamento do *Hardware*

4.2.1 Escolha do Microcontrolador

O microcontrolador ou MCU, é o cérebro do hardware do cofre, pois ele é responsável na interligação física dos componentes do sistema, este será responsável pelo processo de autenticação do usuário, acionamento do alarme e conexão remota com o servidor. A escolha deste, é baseado em alguns critérios.
Actualmente existem no mercado diversos microcontroladores de fabricantes diferentes, alguns mencionados no capitulo 3.4, destacam os seguintes:

- Microcontroladores da família AVR - Os mais comuns e amplamente usados em protótipos;
- Microcontroladores da família ESP32 - fabricados pela Espressif;
- Microcontroladores da família PIC, fabricados pela Microchip;
- Microcontroladores da família Raspberry pico.

4.2.1.1 Critérios para Escolha

Para evitar decisões aleatórias que possam comprometer o projeto, é fundamental adotpar critérios que garantam eficiência, reduzam gastos desnecessários e evitem a inviabilidade técnica e financeira da solução proposta. A seguir, apresentam-se os principais fatores considerados na escolha do microcontrolador ESP32 WROOM usados em placas de desenvolvimento ESP32 devKit.

Facilidade de Aquisição

Entre as famílias de microcontroladores analisadas, destaca-se a ampla disponibilidade dos dispositivos das famílias ESP e Arduino no mercado moçambicano. Essa facilidade de aquisição local elimina a necessidade de importações, que podem ser morosas e onerosas, além de permitir reposição e manutenção mais ágil durante o desenvolvimento e testes.

Características do Projeto

Considerando que o sistema em desenvolvimento exige comunicação remota, a conectividade é um dos principais requisitos técnicos. Embora existam módulos que podem ser acoplados a placas como o Arduino para prover acesso à rede, os microcontroladores da família ESP apresentam conectividade Wi-Fi integrada, o que os torna mais vantajosos em termos de custo, simplicidade e espaço. Além disso, possuem capacidade de processamento e memória interna suficientes para armazenar e executar todo o código necessário ao projeto, dispensando a divisão de tarefas entre múltiplos controladores.

Suporte da Comunidade

Optar por plataformas com ampla comunidade de desenvolvedores é uma estratégia que facilita o desenvolvimento e acelera a resolução de problemas. A vasta documentação e a disponibilidade de bibliotecas prontas para sensores e módulos tornam o trabalho mais eficiente, permitindo que o foco seja voltado à customização e integração, em vez da implementação do zero. Os MCUs ESP apresentam uma grande comunidade de usuários, o que torna ideal para este projecto.

4.2.2 Modulo LCD 16x2-i2c

Para a interface visual do sistema, foi escolhido o modulo lcd 16x2-i2c, pois este apresenta facilidade de aquisição no mercado, baixo curso e apresenta as características técnicas suficientes implementação do projecto. LCD 16x2 I2C é uma versão de um display de cristal líquido de 16 colunas e 2 linhas, que utiliza uma interface I2C (Inter-Integrated Circuit), facilitando a comunicação com microcontroladores, como o ESP32 ou Arduino, usando apenas dois pinos para comunicação de dados.Este modulo pode ser programado mediante o uso de uma biblioteca que será responsável pela configuração do circuito.

Características Principais:

- Resolução: 16 colunas e 2 linhas, o que significa que pode exibir até 32 caracteres simultaneamente.

- Interface I2C: A interface I2C utiliza apenas dois pinos de dados (SDA - Serial Data Line e SCL - Serial Clock Line), permitindo a conexão simplificada com microcontroladores. Isso reduz o número de pinos necessários, se comparado ao LCD sem I2C, que utiliza até 7 pinos.
- Backlight: A maioria dos LCDs I2C 16x2 vem com um controle de retroiluminação (backlight), que pode ser ligado ou desligado programaticamente.
- Contraste: O contraste da tela pode ser ajustado por um potenciômetro no módulo I2C, permitindo melhorar a visibilidade dos caracteres dependendo do ambiente.

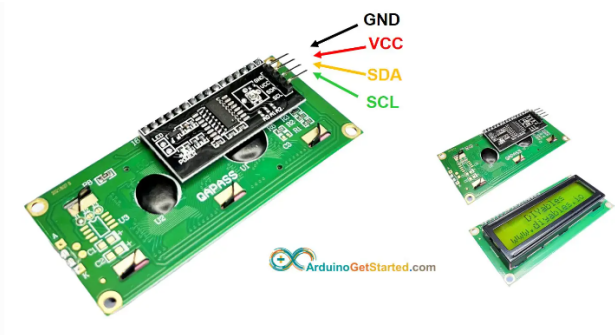


Figura 4.2: Modulo LCD+i2c. Fonte: https://arduinogetstarted.com/tutorials/arduino-lcd-i2c

4.2.3 Fechadura Solenóide

A Fechadura Solenoide trata-se de um pequeno tipo de actuador eletromagnético, constituído por uma bobina e um núcleo ferromagnético móvel, conectado às paredes do dispositivo através de uma mola.

Esta fechadura é do tipo NF (Normal Fechada) e quando aplicado 12V nos terminais da solenóide uma corrente elétrica é conduzida pelos fios da bobina a energizando, ou seja, atravessada por uma corrente elétrica, é gerado um campo magnético, que, por sua vez, permite a atração do núcleo, de modo a comprimir a mola. E conforme é desenergizado a mola expande liberando o êmbolo.

Essas fechaduras solenóides são uma ótima maneira para controle de acesso como abertura de portas, fechaduras, gavetas, armários, etc., sendo projetado para trabalhar diretamente com 12V, o que o torna uma óptima combinação para projetos incorporados.

Especificações:

- Tensão de Operação: 12V

- Corrente de Operação: 0.42A
- Lingueta: 7mm
- Medidas: 27 x 15,4 x 17 mm
- Tempo máximo de acionamento: 10s

Figura 4.3: Fechadura Solenóide. Fonte:https://www.aliexpress.com

4.2.4 Teclado Matricial

Dos diversos teclados abordados na secção 3.5, os critérios usados para a escolha do teclado foram: o uso de menor cabos, menor custo e facilidade de aquisição. Estes dispositivos agrupam os botões em linhas e colunas formando uma matriz, um arranjo que dá origem ao seu nome. Um arranjo retangular puro de colunas NxM é frequente, embora outros arranjos sejam igualmente possíveis.

Os teclados matriciais são predominantes em eletrônica e computação. Na verdade, teclados de computador normais são teclados matriciais, sendo um bom exemplo de um teclado matricial com um arranjo não retangular.

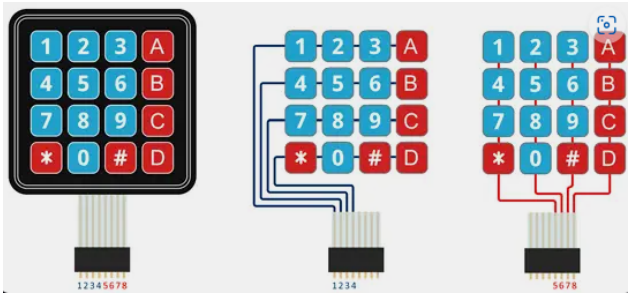


Figura 4.4: Teclado MAtricial 4x4 para Arrduino. Fonte: Giraldo 2023

Para programar o Teclado ou Teclado no Arduino ou qualquer outro microcontrolador, basta seguir a seguinte sequência na ordem:

- Inicialmente, conectamos o teclado matricial aos pinos do MCU. Para isso, será importante ser capaz de identificar quais são as colunas e linhas do teclado.
- As linhas do teclado serão conectadas em pinos digitais configurados como saídas.
- As Colunas do Teclado serão conectadas em pinos digitais configurados como entradas e com o PULLUP habilitado (portanto, essas entradas estarão sempre recebendo um 1 lógico, caso nenhum botão seja pressionado).
- Definimos todas as saídas (Linhas) para 1 lógica ou 5v, ou seja, vamos deixá-las ligadas.
- Aplicamos o conceito de multiplexação: Aqui vamos enviar um 0 lógico para cada linha e vamos ler todas as colunas, se for detectado que alguma coluna recebeu o zero lógico, indica que o botão que compartilha a linha e a coluna foi pressionado, caso contrário, coloco a linha novamente no lógico 1 e verifico a próxima linha.

Esta programação pode ser feita mediante o uso de uma biblioteca que fará toda essa configuração.

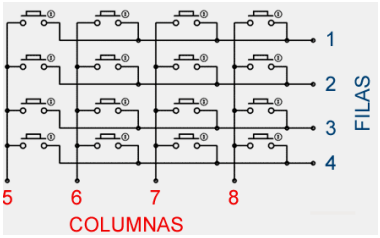


Figura 4.5: Esquema do teclado Matricial. Fonte: Giraldo 2023

4.2.5 Sensor óptico de impressão digital- AS608

O sensor óptico de impressão digital AS608 pode ser usado para digitalizar impressões digitais e também pode enviar os dados processados para um microcontrolador via comunicação serial. Todas as impressões digitais registradas são armazenadas neste módulo. O AS608 é capaz de armazenar até 127 impressões digitais individuais.

Funcionamento

- **Captura da impressão digital**: O usuário coloca o dedo sobre a superfície do sensor óptico, que ilumina a impressão digital e captura sua imagem.
- **Processamento**: A imagem capturada é convertida em dados digitais e comparada com os registros no banco de dados.

- **Verificação**: Se a impressão digital for reconhecida, o sistema confirma a autenticidade do usuário.

Características mais importantes

- backlight azul;
- Tensão de alimentação: 3,3 V;
- Fornecimento máximo de corrente: 60mA;
- Resolução: 500dpi;
- Tempo máximo de imagem de impressão digital: 1s;

Pinagem do Modulo

- V+: Fonte de alimentação do módulo – 3.3V;
- GND: Terra;
- TX: Transmissor Serial;
- RX: Receptor serial ;

Figura 4.6: Modulo AS608. Fonte: Aliexpress.com

4.2.6 Dimensionamento do regulador de Tensão

Um regulador de tensão é um dispositivo, geralmente formado por semicondutores, tais como diodos e circuitos integrados, que tem por finalidade a manutenção da tensão de saída de um circuito elétrico. Sua função principal é manter a tensão produzida pelo gerador dentro dos limites exigidos pela bateria ou sistema elétrico que está alimentando. Um regulador de tensão é incapaz de gerar energia. A tensão de entrada deve ser sempre superior à sua tensão de regulagem nominal. Dependendo do projeto, ele pode ser usado para regular uma ou mais tensões AC ou DC.

A tabela 4.1 apresenta um consumo estimado dos principais componentes do circuito, salientando os valores de corrente são máximos e podem não ser atingidos em simultâneo, podendo também serem atingidos em pequenos intervalos de tempo.

Tabela 4.1: Consumo máximo estimado dos componentes do sistema. Fonte:[Autor]

Ordem	Carga	I_{max}	$V_{Nominal}$
1	ESP 32 devKit	260mA	5V
2	lcd 16x2 + i2C	30mA	5v
3	Sensor Biométrico AS608	60mA	3v3
4	Relé 1 canal 5V	90mA	5v
5	buzer	50mA	5v
6	Fechadura Solenóide	420 mA	12v
	LED(2)	20mA	1.2V

O consumo total estimado da fonte de alimentação é de 930mA, então fixa-se que a fonte de alimentação deve ter 12v e pelo menos 1A.

4.2.6.1 Modulo Módulo Regulador 7805

O 7805 é um regulador de tensão de saída fixa IC da família 78XX. Outras variedades são 7809 e 7812, dando saídas de 9 V e 12 V, respectivamente. É fácil de ser empregado porque possui apenas três pinos e alguns componentes externos são necessários. A folha de dados com as especifica coes usadas como base para o dimensionamento, pode ser encontrada no Anexo A1.1.

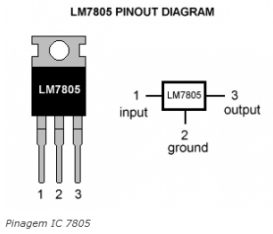


Figura 4.7: Pinagem do lm7805. Fonte: https://www.electronicsforu.com/technology-trends/learn-electronics/7805-ic-voltage-regulator

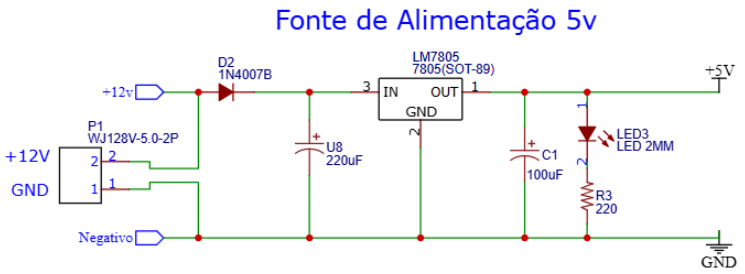


Figura 4.8: Circuito regulador 5v. Fonte: Autor

O circuito da figura 4.8 representa o regulador que sera a fonte de alimentação do sistema alimentada por uma fonte de 12v, onde esta tensão é a mesma usada para fechadura, segue-se com diodo retificador 1N4007 com uma queda de 0,7v, usado para proteção contra polaridade inversa ao circuito. Depois, é ligado o regulador Lm7805, onde são colocados 2 capacitores de desvio (1 na entrada e outa na saída do 7805), estes protegem contra picos de tensão, ruido e estabilizam a tensão, a escolha dos valores são baseados nas recomendações do fabricante do LM7805. Na saída do regulador encontramos um LED acompanhado de um resistor para limitar a sua corrente, para indicação do funcionamento da fonte.

Para a protecção do LED é necessário um resistor, este permitirá que o LED não sofra de sobrecorrente. Abaixo temos o cálculo dos resistores usados para limitar a corrente sem diminuir demais o seu brilho no projecto.

$$R_{min} = \frac{V_{in} - V_d}{I_{dmax}} = \frac{5 - 1.2}{20} 1000 = 190\Omega$$

O valor acima calculado não é um valor típico comercial, então surge uma necessidade de aproximar a um valor padronizado e de fácil aquisição que é o resistor de 220 (ohm). Com base nesse resultado determinamos a potência do resistor:

$$P = I^2 \times R = (20 \times 10^{-3})^2 \times 220 = 0.088\,\mathrm{W}$$

Com esse valor da potência e tendo em conta os valores comerciais, o valor do resistor será:

$$R = 220\,\Omega,\ \frac{1}{8}\,\mathrm{W},\ \pm 10\%.$$

4.3 Arquitetura do *Software*

A arquitetura do software foi planejada para garantir a segurança, confiabilidade e eficiência no controle de acesso ao cofre, permitindo a autenticação de usuários, o acionamento de alarmes em situações de coação, o registro de eventos em banco de dados, o envio de alertas em tempo real e a configuração do sistema por meio de uma interface web.

A estrutura do sistema foi modularizada para facilitar o desenvolvimento, a manutenção e a escalabilidade. Os principais módulos estão descritos a seguir:

Módulo de Autenticação de Usuário – Responsável por verificar se o usuário possui autorização para acessar o cofre, este módulo opera com autenticação em duas camadas:

- **Autenticação Biométrica**: Primeira etapa da verificação, na qual o sistema compara a digital fornecida com os dados cadastrados na base local do microcontrolador.
- **Autenticação por Senha**: Segunda etapa da autenticação, em que a senha digitada pelo teclado matricial é comparada com a senha armazenada no sistema.
- **Verificação de Senha de Pânico**: Caso o usuário insira uma senha previamente cadastrada como “senha de pânico”, o sistema libera o acesso normalmente, mas aciona o módulo de alarme silencioso, ativando protocolos de segurança sem alertar um possível agressor.

Módulo de Controle de Acesso – Após a autenticação bem-sucedida, este módulo é responsável por enviar um sinal elétrico ao relé, que ativa a fechadura e permite a abertura do cofre. Ele também impede a abertura caso a autenticação falhe, garantindo a integridade do sistema.

Módulo de Alarme Silencioso – Este módulo é ativado exclusivamente quando a senha de pânico é detectada. Sua função é permitir uma resposta discreta e remota a uma possível situação de coação. Suas funções principais incluem:

- **Envio de Notificação Silenciosa**: Utiliza o protocolo MQTT para enviar uma mensagem de alerta para um servidor ou dispositivo remoto, notificando discretamente uma central de segurança ou contato de confiança.
- **Ativação de Câmera de Vigilância**: Inicia a captura e transmissão de imagens por meio de uma câmera integrada (ex.: ESP32-CAM), permitindo o monitoramento remoto em tempo real do ambiente.

Módulo de Registro de Eventos – Todos os acessos, tentativas válidas ou inválidas, bem como eventos de alarme, são registrados em uma base de dados hospedada em um servidor. Esses dados podem ser utilizados para auditorias, análises forenses e controle de uso do sistema.

Módulo de Interface Web Administrativa – A configuração do sistema, bem como a visualização dos registros de acesso, é realizada por meio de uma plataforma web acessível em rede local ou remotamente. O painel permite ações como: alteração de senha, cadastro de usuários, visualização de logs e definição de contatos para notificação de emergência.

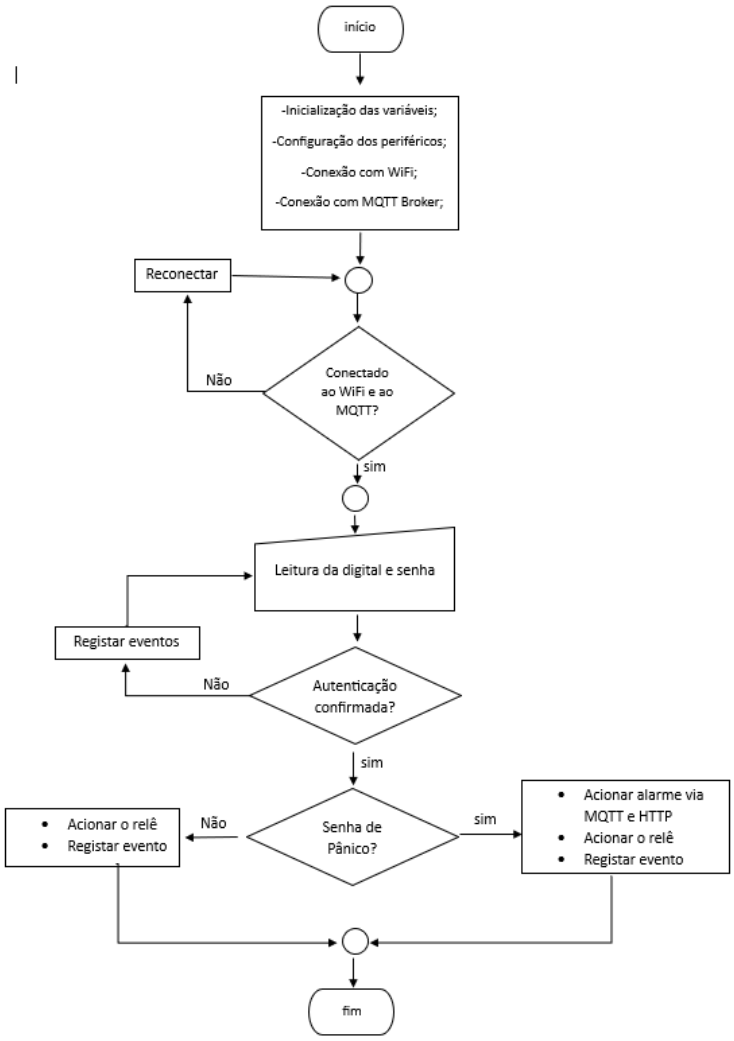


Figura 4.9: Fluxograma de funcionamento de controle de acesso.Fonte:[Autor]

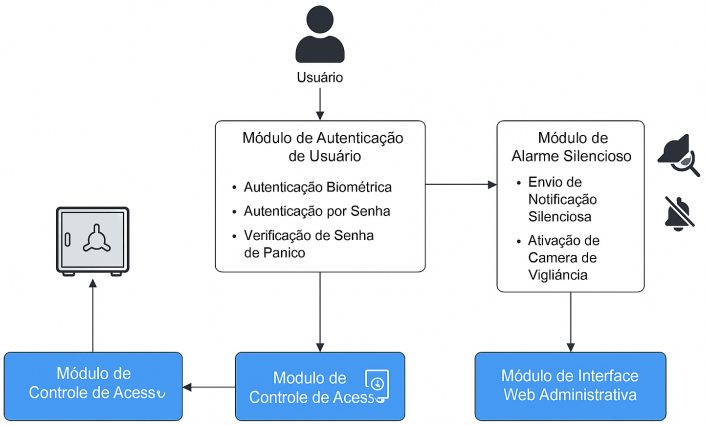


Figura 4.10: Arquitectura do Software. Fonte: [Autor]

4.3.1 Base de Dados- MySQL

O sistema dispõe de um banco de dados para o registros de acessos e a informação dos usuários cadastrados no sistema de controle de acesso. Para este projecto foi usado o MySQL.

O MySQL- um sistema de base de dados relacional rápido, fiável, escalável e fácil de usar- foi concebido para lidar com aplicações de produção pesados e de missão crítica. É uma base de dados comum e fácil de iniciar com baixa utilização de memória, disco e CPU, gerida por um Sistema de Gestão de Bases de Dados Relacional- Relational Data base Management System (RDMS).

4.3.1.1 Relacionamento entre as tabelas

No modelo de banco de dados relacional proposto para o sistema de controle de acesso ao cofre, a tabela *usuarios* é responsável por armazenar as informações essenciais de cada pessoa autorizada a interagir com o sistema. Já a tabela *logs acesso* tem como função registrar todas as tentativas de autenticação, sejam elas bem-sucedidas, malsucedidas ou relacionadas a eventos críticos como o uso de senha de pânico.

O relacionamento entre essas duas tabelas é do tipo um-para-muitos (1:N), ou seja, um único usuário pode estar associado a vários registros de acesso ao longo do tempo, mas cada registro de acesso está obrigatoriamente vinculado a apenas um usuário.

Essa estrutura permite:

- Rastrear com precisão quem realizou cada tentativa de acesso;

- Analisar o histórico completo de ações de um determinado usuário;
- Realizar auditorias de segurança com base nos dados individuais;
- Identificar padrões suspeitos de comportamento (ex: múltiplas falhas em sequência).

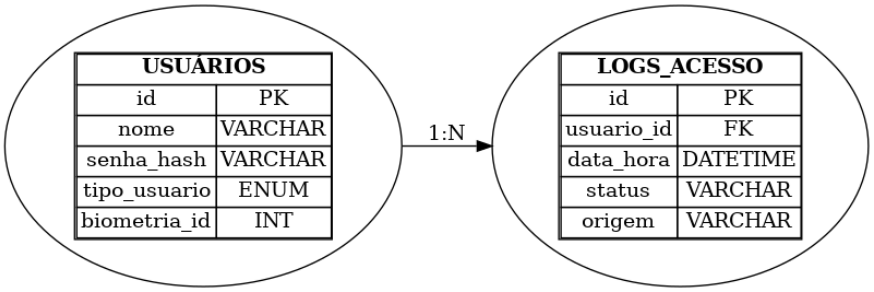


Figura 4.11: Relação entre tabelas. Fonte:[Autor]

4.3.2 Painel Administrativo

O painel administrativo do sistema foi concebido como uma interface web acessível por navegadores em computadores ou dispositivos móveis conectados à rede. Sua principal finalidade é permitir que o responsável pelo sistema possa monitorar, gerenciar e configurar funcionalidades críticas do controle de acesso ao cofre de forma remota, segura e eficiente.

O painel foi desenvolvido utilizando tecnologias como HTML, CSS, PHP, javaScript e MySQL, oferecendo uma interface amigável e responsiva. As informações exibidas na interface são obtidas diretamente da base de dados do sistema, que armazena todos os eventos de autenticação, alertas e configurações.

4.3.2.1 Funcionalidades principais

O painel administrativo é composto por diversos módulos com funcionalidades específicas:

- **Visualização de registros de acesso**: Exibe, em tempo real, os eventos registrados no sistema, incluindo acessos autorizados, tentativas inválidas e ativações da senha de pânico. O administrador pode aplicar filtros por data, horário, status (sucesso, falha, pânico) e nome do usuário, facilitando auditorias e análises forenses.
- **Alteração de senha de acesso**: O sistema permite a alteração da senha principal do cofre de forma remota. Essa funcionalidade é útil em casos em que a senha

tenha sido comprometida, garantindo maior agilidade na resposta a incidentes de segurança.

- **Cadastro e gerenciamento de usuários**: É possível cadastrar novos usuários autorizados, definir o tipo de acesso (usuário comum ou administrador), associar identificadores biométricos e remover usuários inativos. Todas essas ações são registradas no sistema para rastreabilidade.
- **Monitoramento por vídeo**: O painel pode exibir, quando configurado, imagens ou transmissões ao vivo provenientes de uma câmera integrada (ex.: ESP32-CAM). Essa funcionalidade é especialmente útil durante a ativação da senha de pânico, possibilitando o acompanhamento em tempo real da situação no local do cofre.
- **Configurações gerais do sistema**: Permite ajustes de parâmetros operacionais, como tempo de abertura da fechadura, tempo limite de autenticação, configuração de contatos de emergência para notificação silenciosa, entre outros.
- **Exportação de relatórios**: Os registros podem ser exportados em formatos como CSV ou PDF, permitindo a geração de relatórios para fins de controle interno ou apresentação institucional.

4.3.2.2 Segurança da interface

A segurança do painel administrativo é um aspecto fundamental. Por isso, foram adotadas as seguintes medidas:

- Autenticação por senha para acesso ao painel;
- Validação de sessões e proteção contra acesso não autorizado;
- Possibilidade de uso de HTTPS para comunicação segura, caso o sistema seja publicado externamente;
- Controle de permissões baseado no tipo de usuário (admin ou comum).

4.3.2.3 Tecnologias usadas

HTML

O HTML é uma linguagem de marcação usada em páginas da web para estruturar todo o conteúdo que deve ser exibido aos usuários.HTML significa HyperText Markup Language, ou Linguagem de Marcação de Hipertexto, em tradução para o português. O funcionamento do HTML se dá por meio do uso de tags, que marcam cada parte do conteúdo,

facilitando a interpretação pelos softwares.Um código HTML pode conter códigos de linguagens como PHP e JavaScript.(Toledo 2025)

CSS

O CSS é uma linguagem de folhas de estilo que define a disposição e o layout dos elementos de uma página. A linguagem é responsável pela formatação do que será exibido pelo navegador. Ou seja, o design, as cores, links e as fontes, permitindo modificar o visual de vários elementos ao mesmo tempo.

PHP

OPré-processo de hipertexto- Hypertext Preprocessor (PHP) é uma linguagem de pro gramação server-side (lado servidor), muito utilizado em páginas Web por oferecer inte ractividade entre o usuário e a aplicação, tornando às páginas dinâmicas. Seu código fica embutido junto a linguagem de marcação do HTML.

As requisições são submetidas através da Uniform Resource Locator (URL) onde, vão para o servidor que se encarrega de interpretar o código em PHP que faz a montagem da página em HTML devolvendo para o navegador. Através destas requisições também é possível fazer consultas em base de dados.

JavaScript

É uma linguagem de programação de comportamento que permite a criação de conteúdos dinâmicos, controle de mídias e animações para deixar seu site mais interativo e interessante.

4.3.3 Protocolo MQTT- (Message Queuing Telemetry Transport)

Foi descrito na secção 3.3.1, que o MQTT (Message Queuing Telemetry Transport) é um protocolo de transporte de mensagens que possibilita a comunicação entre máquinas e é amplamente usado para conectividade de IoT (Internet of Things). É aberto, leve e tem fácil implementação, sendo executado em TCP/IP ou em outros protocolos de rede.

Este protocolo foi escolhido dentre os outros apresentados, por ser de código aberto, apresentar ferramentas gratuitas para sua configuração, é um protocolo leve e capaz de rodar em dispositivos de baixa potencia e consumo energético, apresenta praticidade na integração de mais dispositivos no sistema.

Funcionamento fo protocolo MQTT

O protocolo MQTT opera seguindo um modelo de publicação e subscrição, através de mensagens assíncronas baseadas em tópicos. Estes são os principais pontos do seu

funcionamento:

- **Publicação e Subscrição**: Neste protocolo, existem dois participantes principais: o publicador (cliente que publica mensagens) e o assinante (cliente que recebe mensagens). Os tópicos são adotados para categorizar as mensagens. Neste caso os clientes será o esp32, esp32cam e o terminal que vai receber a notificação do alarme (ex: Android, windows, etc)
- ***Broker* MQTT**: É o servidor central que recebe os dados dos publicadores e os encaminha para os assinantes de interesse. É responsável pelo gerenciamento dos participantes. O broker de um servidor MQTT pode ser baseado em nuvem (rodando dentro de toda rede *internet*) ou pode ser um servidor local(rodando dentro da mesma rede *Local Area Network* (LAN)).Alguns dos serviços de Broker podem ser: Mosquitto Broker, Maqiatto, HiveMQ, entre outros.
- **Tópicos**: Funcionam como canais ou categorias de mensagens. Os assinantes se inscrevem nos tópicos específicos de seu interesse para receber as mensagens.
- **QoS (Quality of Service)**: O MQTT suporta diferentes níveis de *Quality of Service* (QoS) para assegurar a entrega dos dados.
- **Conexão Persistente**: Clientes deste protocolo podem estabelecer uma conexão persistente com o broker, diminuindo a sobrecarga de restabelecimento de conexões e possibilitando uma comunicação contínua.
- **Payload** – será o conteúdo da mensagem que será enviada.

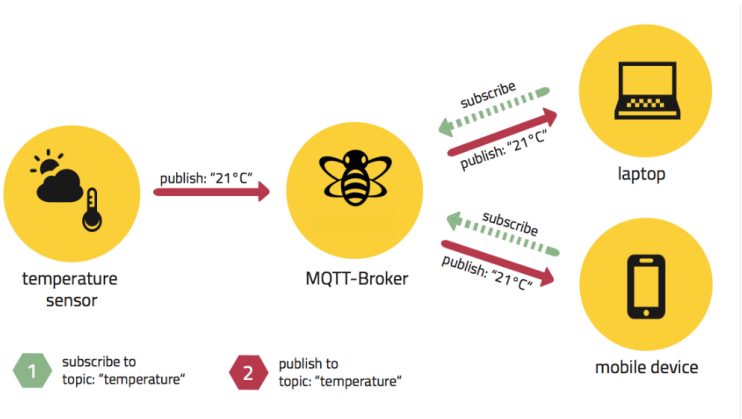


Figura 4.12: exemplo de uma rede MQTT. Fonte: https://blog.elo7.dev/mqtt

4.3.3.1 Configuração do Broker

Para que seja estabelecida uma conexão entre todos os clientes da rede, mesmo que não estejam ligados à mesma rede, surge a necessidade de usar um serviço de broker com acesso à nuvem. Para este projecto foi escolhido o Maqiatto Broker. Como primeiro passo é necessário fazer o cadastro na plataforma para obter as credenciais.

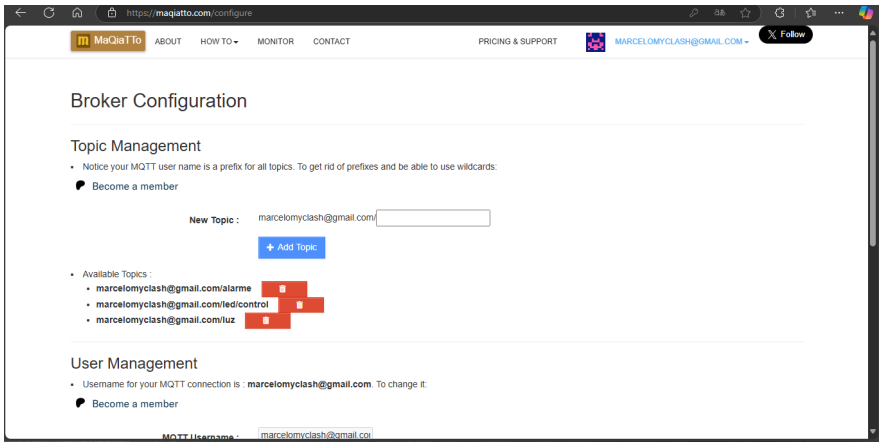


Figura 4.13: Configuração da conta do broker. Fonte:[Autor]

Para a configuração do Broker são necessários dados como: webserver -"www.maqiatto.com". porta- "1883". username- "macelomyclash@gmail.com ". senha: "marcelo".

O microcontrolador do cofre é responsável por estabelecer conexão com a internet e o broker para acionar o alarme em um outro dispositivo, havendo necessidade de configurar neste também.

```
#ifndef WiFiMqttConfig_h
#define WiFiMqttConfig_h

#include <WiFi.h>
#include <PubSubClient.h>

// Configurações da rede Wi-Fi
const char* ssid = "Galaxy Martiva";
const char* password = "12345678";

// Configurações do broker MQTT
const char* mqttServer = "15.236.203.194"; // www.maqiatto.com
const int mqttPort = 1883;
// Credenciais de autenticação MQTT
const char* mqttUser = "marcelomyclash@gmail.com";
const char* mqttPassword = "marcelo";
```

Figura 4.14: configuração do WiFi e MQTT no Esp32. Fonte: [Autor]

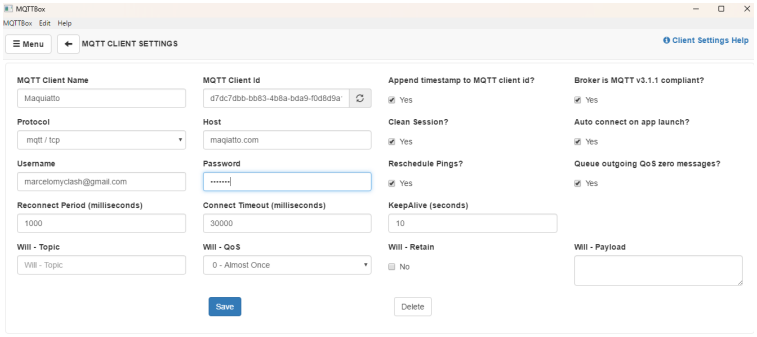


Figura 4.15: configuração do broker no MQTTbox Fonte: [Autor]

4.3.3.2 Configuração do do Alarme

Quando o usuário digitar a senha de pânico o microcontrolador publica uma mensagem no tópico do broker ”marcelomyclash@gmail.com/alarme”, daí um celular com um aplicativo pré-configurado fica a espera dessa mensagem para acionar um alarme sonoro. Neste caso foi usado o aplicativo”MQTT Alert ”na figura 4.16.

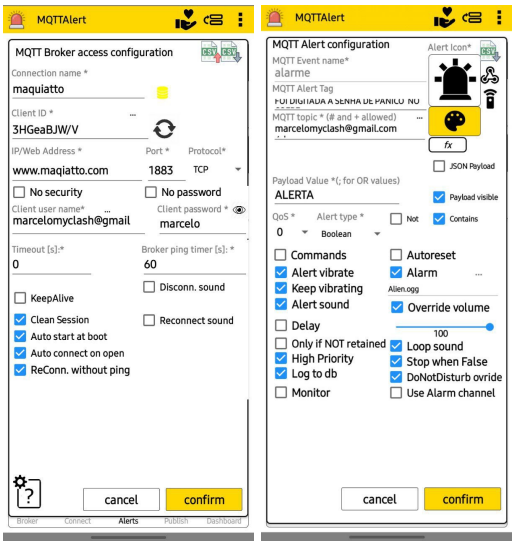


Figura 4.16: Configuracao do MQTT Alert. Fonte:[Autor]

4.4 Custos e Mão de Obra

Para o desenvolvimento do protótipo, há necessidade de aquisição dos componentes que compõem o sistemas, os componentes e escolhidos para implementação da solução experimental, os custos são apresentados na tabela 4.4, considerando que para uma implementação final, os custos podem sofrer uma alteração, uma vez que foram usados

servidores locais ao invés de servidores na nuvem (pagos) . E a mão de obra para produção deste projecto é estimado em dezoito mil(18.000,00) meticais. Totalizado cera de Trinta mil (30.000,00) meticais.

Tabela 4.2: Custos dos componentes. Fonte: Autor

Componente	Descrição	Qde	Preço (MZN)
ESP32-WROOM-32U	ESP32-D0WD-V3, 64Mbit PSRAM, 4MB SPI flash	1	1500,00
ESP32 CAM +ADAPTADOR	4 MB PSRAM, câmera OV2640, Wifi 2.4Ghz	1	1750,00
LCD +I2C	Display LCD 16x02+ módulo i2c	1	700,00
Sensor de Biometria	Módulo AS608	1	1500,00
Relê	1 canal 5V	1	250,00
Teclado Matricial	4x4	1	400,00
Fechadura Solenoide	12v VDC	1	1200,00
Buzzer	Buzzer passivo 5v	1	130,00
LM7805	Regulador de Tensão para 5v	1	50,00
Terminal Blocks	Terminal blocks 2 pinos	12	300,00
Diodos	1N4007	2	50,00
Transistor	BC547	1	50,00
Capacitores	220uF e 22uF	1	50,00
Fonte de alimentação	Fonte de 9v , 1 A	1	400,00
Portinhola de eletricidade	Metálica de 300x250x150mm	1	1200,00
Manufacturação da PCB	PCB de duas camadas	5	1700,00
	Total		11230.00

Capítulo 5

Ensaios e Resultados

Neste capítulo serão apresentados os ensaios do que resultou da concepção no capítulo anterior, possível melhoramento na interação entre os dispositivos hardware e no funcionamento da lógica do sistema . Estes ensaios foram feitos de forma a validar alguns aspectos como: a autenticação de dois passos (biometria e senha), o acionamento do circuito de controle da fechadura, a interface do usuário (display) e a comunicação do sistema com o painel administrativo e o dispositivo movel que recebe o alarme no caso de pânico.

5.1 Resultado dos circuitos Impresso

Para facilitar a homologação dos diferentes circuitos do projeto, optou-se pelo desenvolvimento de uma *Printed Circuit Board* (PCB). Essa placa foi projetada para integrar o microprocessador, o regulador da fonte de alimentação, os diferentes módulos utilizados, o relé e os terminais de conexão, de forma mais organizada. Dessa maneira, obteve-se maior centralização dos componentes e melhor arranjo do sistema, garantindo praticidade na montagem e manutenção do projeto.

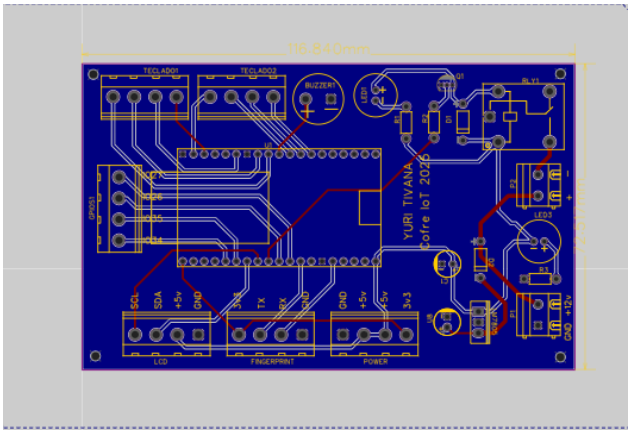


Figura 5.1: Desenho da PCB. Fonte:[Autor]

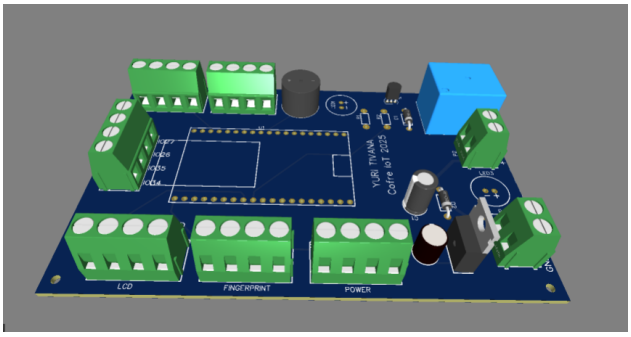


Figura 5.2: Renderização da PCB. FOnte:[Autor]

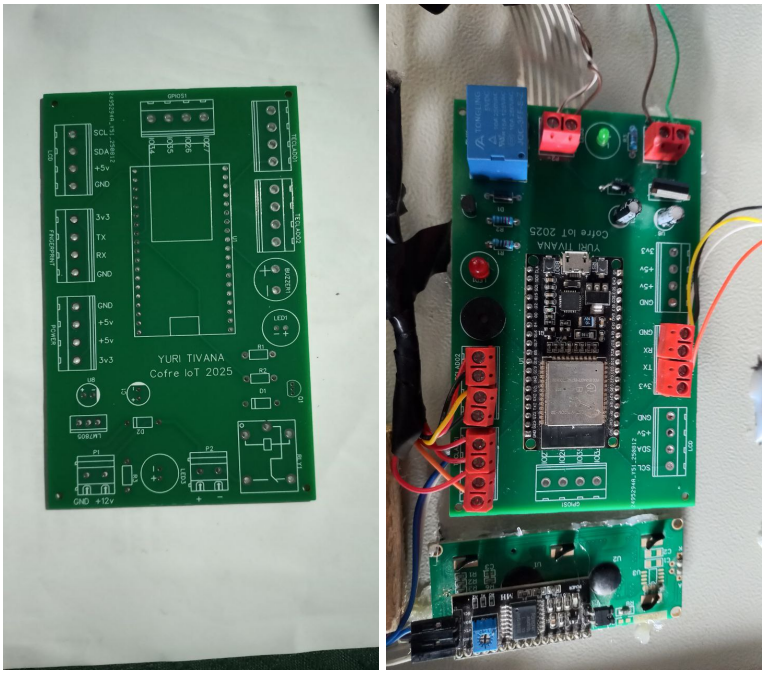


Figura 5.3: Placa de circuito Impresso. Fonte:[Autor]

5.2 Ensaio do sistema

Para simular o acesso à página web como se estivesse em um ambiente real de internet, utilizou-se o software XAMPP. Essa ferramenta permite transformar o computador em um servidor local, integrando três componentes principais: Apache Server (responsável pelo serviço de hospedagem), MySQL (o sistema de gerenciamento de banco de dados adotado neste projeto) e PHP (linguagem de programação utilizada para a lógica do sistema).

O uso do XAMPP mostrou-se vantajoso por ser uma solução gratuita e de fácil configuração, além de simular com fidelidade as funcionalidades oferecidas por serviços de hospedagem comerciais pagos. Dessa forma, tornou-se possível desenvolver, testar e validar o sistema em ambiente local antes de uma possível implantação em um servidor remoto.

A comunicação entre o microcontrolador (ESP32) e o painel administrativo (hospedado no XAMPP) ocorre na mesma rede local. Para isso, o servidor (computador) recebe um endereço IPv4, que é utilizado como referência em todas as requisições realizadas pelo microcontrolador, garantindo a troca de informações com o banco de dados e o processamento das respostas do sistema.

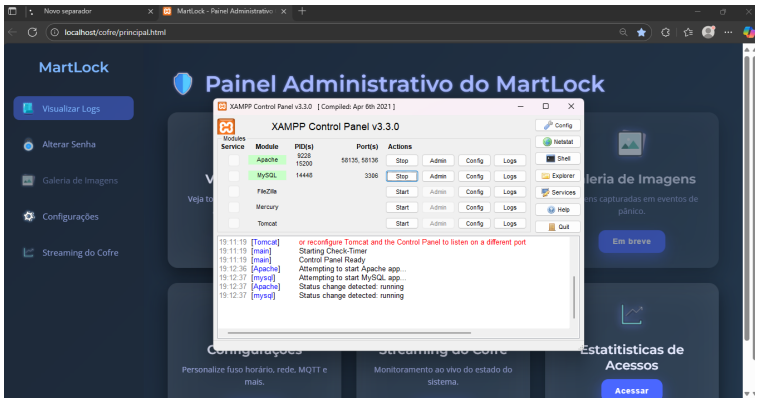


Figura 5.4: XAMPP Control painel. Fonte [Autor]

5.3 Teste do Dispositivo

Para validar as funcionalidades do sistema, foram introduzidas as senhas para testar os diversos estados de funcionamento. A seguir são mostrados os resultados obtidos nos testes em situações como:

Sistema em lobby(a espera das credenciais)- quando iniciado o sistema, essa será

a tela inicial apresentada, aguardando que o usuário coloque o seu dedo para validação de primeiro passo. Depois do dedo ser validado o sistema pede uma senha.

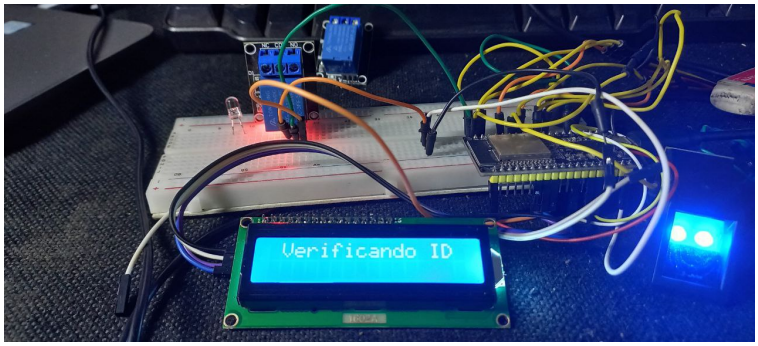


Figura 5.5: Pagina Inicial do sistema. Fonte:[Autor]

Senha incorrecta introduzida- quando o usuário introduz a senha incorrecta, o relê não é acionado e o sistema é bloqueado após 4 tentativas erradas consecutivas.

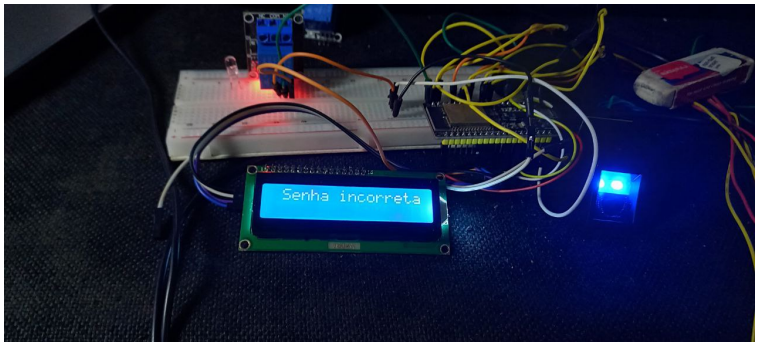


Figura 5.6: Resposta à senha incorrecta. Fonte:[Autor]

Senha correcta introduzida- quando o usuário introduz a senha correcta, o relê é acionado abrindo a fechadura e o sistema retorna página inicial.

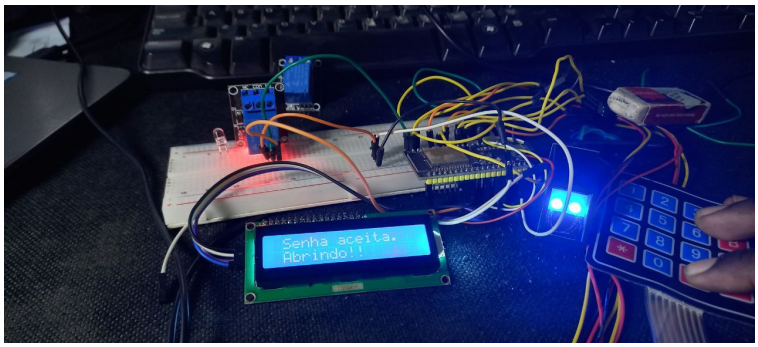


Figura 5.7: Resposta à senha correcta. Fonte:[Autor]

Senha de pânico introduzida- Neste caso, o relê é acionado abrindo o cofre e também é publicada a mensagem de alerta no tópico do Broker para acionar o alarme em

um outro dispositivo.

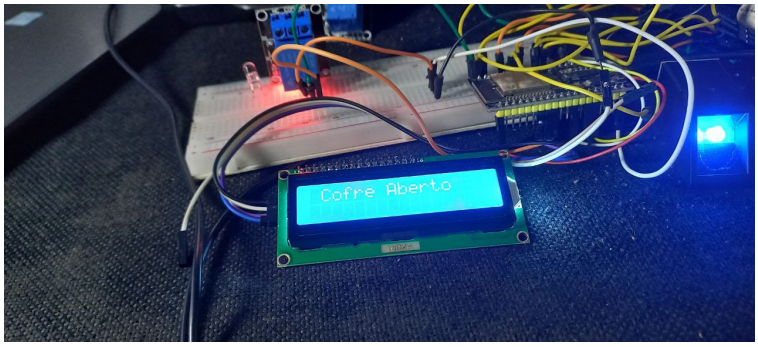


Figura 5.8: Resposta quando estiver em Pânico Fonte:[Autor]

Notificação em um outro dispositivo- quando o dispositivo que está inscrito no tópico onde foi publicada a mensagem de alerta recebe esta mensagem, este gera um alarme e depois retorna para pagina inicial.

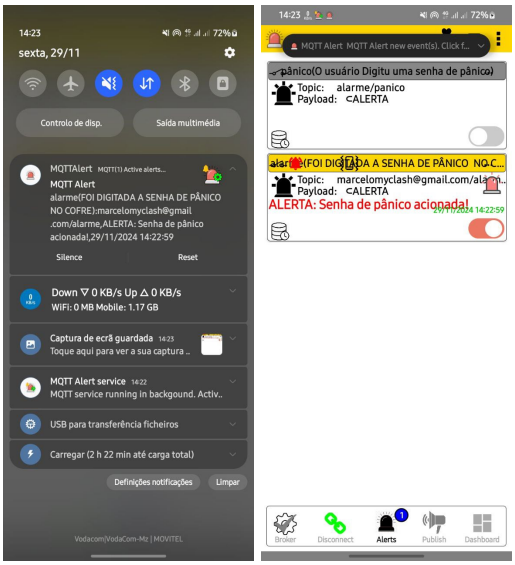


Figura 5.9: Notificação no MQTT Alert. Fonte:[Autor]

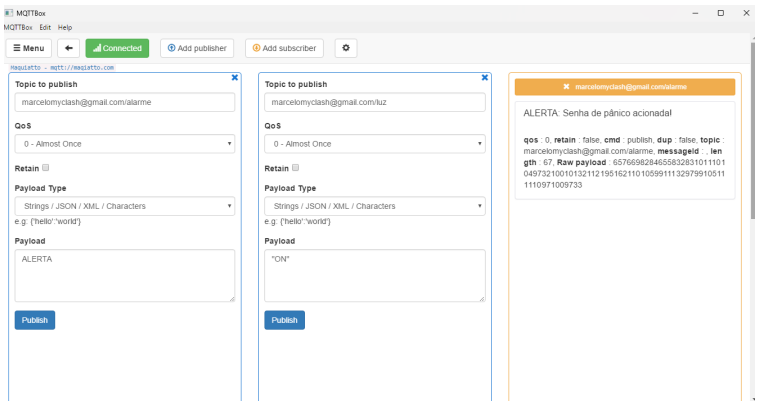


Figura 5.10: Leitura da mensagem publicada no Broker. Fonte:[Autor]

Figura 5.11: Protótipo de um cofre com todo sistema integrado. Fonte: [Autor]

5.4 Painel Administrativo

O teste do website consistiu em, ver os registos de acesso, alterar senha do cofre, assistir a transmissão, entre outras funcionalidades.

Figura 5.12: Paginal Principal do Website. Fonte:[Autor]

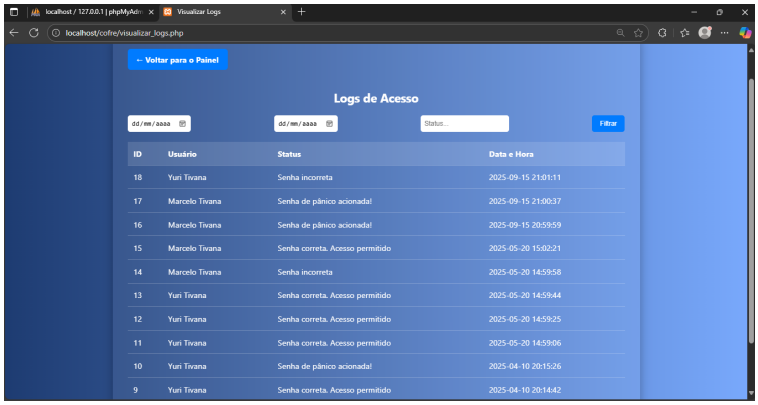


Figura 5.13: Logs de Acessos registados pelo sistema. Fonte:[Autor]

5.5 Avaliação dos resultados

Os resultados obtidos após os testes práticos demonstraram que o sistema de controle de acesso desenvolvido apresenta vantagens significativas em relação aos convencionais e a outros sistemas de controle de acesso baseados apenas em senha.

Em comparação com sistemas tradicionais que utilizam apenas senhas numéricas, o uso do sensor biométrico AS608 aumentou consideravelmente o nível de segurança. Enquanto uma senha pode ser descoberta ou compartilhada, a autenticação biométrica garante identificação única e intransferível, reduzindo o risco de acesso indevido.

A integração do ESP32 com o servidor web via protocolo MQTT proporcionou uma comunicação rápida e estável. Em comparação com o uso de requisições HTTP convencionais, observou-se que o MQTT apresentou menor latência e maior eficiência na troca de dados, especialmente em eventos críticos como o modo de pânico.

Comparando com sistemas de cofres convencionais, que normalmente não possuem histórico digital, este projeto oferece rastreabilidade completa dos eventos, permitindo auditorias e análises futuras. A implementação de filtros por data e status na interface web também facilitou a visualização e o controle dos registros, superando a limitação de sistemas que apenas armazenam logs localmente no microcontrolador.

Tabela 5.1: Comparação entre o sistema convencional e o sistema proposto (Cofre IoT).

Critério	**Sistema Convencional**	**Sistema Proposto (Cofre IoT)**
Autenticação	Apenas senha	Senha + Biometria
Registro de eventos	Inexistente ou manual	Automático (MySQL + Web)
Comunicação	Local	Wi-Fi + MQTT (tempo real)
Monitoramento remoto	Não disponível	Interface web integrada
Nível de segurança	Médio	Alto
Notificação de pânico	inexistente	remoto

Capítulo 6

Conclusão e Recomendações

6.1 Conclusão

O desenvolvimento do sistema de controle de acesso para cofres, com implementação de senha de alarme silencioso, demonstrou ser um avanço significativo na integração de tecnologias de segurança com soluções inteligentes baseadas em IoT. O trabalho possibilitou a construção de uma solução que equilibra eficiência, inovação e acessibilidade, destacando-se pela abordagem orientada à proteção de usuários em situações de risco. O desenvolvimento deste trabalho permitiu alcançar os objetivos propostos de maneira satisfatória, abordando todas as etapas necessárias para a concepção de um sistema de controle de acesso de um cofre com alarme silencioso.

Inicialmente, foi detalhado o princípio de funcionamento de sistemas de controle de acesso de acordo com algumas literaturas, apresentando os componentes principais e suas interações. Essa abordagem foi essencial para compreender como cada elemento contribui para o controle de acesso seguro e eficiente obedecendo os requisitos que estes sistemas apresentam, desde a autenticação até a notificação em situações de emergência.

O dimensionamento do sistema foi realizado com base nos requisitos e funcionalidades propostas pela solução . Componentes como o microcontrolador ESP32, o sensor biométrico de impressão digital e a fechadura elétrica foram selecionados e integrados ao protótipo. Esse dimensionamento assegurou que o sistema atendesse às expectativas de desempenho, confiabilidade e baixo custo. Tendo sido desenhado uma PCB que pudesse englobar e centralizar os diferentes módulos do projecto, garantindo uma alimentação estável e um optimo arranjo .

A programação do microcontrolador desempenhou um papel crucial no sucesso do projeto. A lógica de controle foi desenvolvida para garantir uma autenticação precisa dos usuários e o gerenciamento eficaz do mecanismo de desbloqueio do cofre. Além disso, a implementação da funcionalidade de senha de pânico e o acionamento do alarme silencioso em situações de coação, e os sistema de vigilância demonstraram a aplicabilidade prática da solução desenvolvida.

Como o último objectivo, os testes realizados validaram o protótipo funcional, evidenciando sua capacidade de atender aos requisitos estabelecidos. O sistema mostrou-se capaz de autenticar usuários de maneira confiável, ativar o alarme silencioso discretamente e notificar as autoridades competentes em casos de emergência.

Por fim, a conclusão do projeto demonstra o potencial das soluções tecnológicas no fortalecimento de medidas de segurança pessoal e institucional. Os resultados obtidos, aliados à flexibilidade do sistema, abrem caminhos promissores para novas aplicações, tanto no aprimoramento do protótipo quanto na sua adaptação para outros contextos, consolidando a relevância do trabalho na criação de soluções práticas, eficientes e orientadas à segurança.

6.2 Recomendações

Com base nos resultados obtidos e na análise do desempenho do sistema desenvolvido, são apresentadas a seguir algumas recomendações que visam aprimorar a segurança, confiabilidade e usabilidade do cofre inteligente:

1) **Melhorar o sistema de vigilância interna:** Recomenda-se a utilização de câmeras com maior resolução e integração completa com o sistema web, permitindo o acesso remoto às imagens em tempo real e o armazenamento automático de capturas em caso de alerta de pânico ou tentativa de intrusão.
2) **Implementar um sistema de alimentação ininterrupta (UPS):** Sugere-se adicionar baterias internas recarregáveis ou um módulo de energia de emergência, garantindo o funcionamento do cofre mesmo durante falhas de energia elétrica.
3) **Elaborar um manual de utilizador e manutenção:** A criação de um documento técnico e operacional que descreva as etapas de instalação, utilização e procedimentos de manutenção preventiva facilitará o uso e a expansão do sistema.

4) **Aprimorar a interface web e o painel administrativo:** Recomenda-se a inclusão de novos recursos, como gráficos de estatísticas, filtros de logs mais avançados, exportação em diferentes formatos (PDF, Excel) e autenticação de múltiplos níveis de acesso.

5) **Implementar notificações inteligentes:** Sugere-se integrar funcionalidades de gestão e integração de usuários e biometrias usando o website.

6) **Otimizar o consumo energético do ESP32:** Configurar modos de economia de energia e desligamento automático de periféricos quando o sistema estiver em estado ocioso.

7) **Gestão de usuários e biometria através do website** Registar automaticamente todas as alterações de senha, atualizações de firmware e comandos recebidos via MQTT, para manter a rastreabilidade completa das ações no sistema.

8) **Implementar backups automáticos da base de dados:** Configurar cópias de segurança periódicas do banco MySQL para evitar a perda de dados em caso de falhas no servidor.

Referências Bibliográficas

Brasiliano, Antonio Celso (2013). “Gestão de Riscos Corporativos 2013”. Em: URL: https://www.brasiliano.com.br/revista-gestao-de-riscos.

Cravo, Edilson (out. de 2024). “Protocolo MQTT: como funciona, dicas e informações importantes”. Em: Acessado em 22/10/2024. URL: https://blog.kalatec.com.br/protocolo-mqtt/.

Damirchir, Mohammad (set. de 2022). “Introdução aos Microcontroladores PIC – Parte 1”. Em: Acessado em 23/09/2024. URL: https://electropeak.com/learn/interfacing-fpm10a-as608-optical-fingerprint-reader-sensor-module-with-arduino/.

Doho, Gonçalves Justino (mar. de 2021). “Breve Introdução à Arquitectura e Programação Básica de Microcontroladores- AVR ATmega328”. Em.

Expressif (2024). “ESP32”. Em: Acessado em 23/09/2024. URL: https://www.espressif.com/en/products/socs/esp32.

Galvão, Luis Eduardo Ferreira (jan. de 2025). “Sistemas de Controle de Acesso”. Em: Acessado em 29/03/2025. URL: https://a3aengenharia.com.br/conteudo/artigos-tecnicos/sistema-de-controle-de-acesso/#elementor-toc__heading-anchor-0.

Giraldo, Sergio Andres Castaño (set. de 2023). “Teclado Matricial”. Em: Acessado em 10/10/2024. URL: https://controlautomaticoeducacion.com/sistemas-embebidos/arduino/teclado-matricial-keypad/.

Intelbras (jan. de 2023). “O que é Zigbee? Conheça um dos padrões mais utilizados para funcionamento das casas inteligentes”. Em: Acessado em 22/10/2024. URL: https://blog.intelbras.com.br/o-que-e-zigbee/.

Iugu, Redação (jun. de 2024). “Arquiteto de Sistemas: o que é, o que faz e como se tornar um”. Em: Acessado em 23/08/2024. URL: https://www.iugu.com/blog/arquiteto-de-sistemas.

Kassouf, Samir (ago. de 2022). “Microcontrolador: descubra o que é, como funciona e para que serve”. Em: Acessado em 23/09/2024. URL: https://blog.kalatec.com.br/microcontrolador/.

Kustro, Guilherme (mar. de 2023). “Protocolo MQTT: O Que é, Como Funciona e Vantagens”. Em: Acessado em 23/10/2024. URL: https://www.automacaoindustrial.info/mqtt/.

Lakatos, Eva e Marina de Andrade Marconi (2003). *Fundamentos de Metodologia Científica*. 5ª ed. São Paulo: Atlas.

Martins, Victor Ferreira (ago. de 2019). “AUTOMAÇÃO RESIDENCIAL USANDO PROTOCOLO MQTT, NODERED E MOSQUITTO BROKER COM ESP32 E ESP82”. Em.

Menezes, Árly Assis Martins Cordeiro (fev. de 2018). “Implementação de um sistema para acesso pessoal ao Laboratório de Automação Predial do DECAT”. Em.

Microsoft (ago. de 2022). “O que é controle de acesso?” Em: Acessado em 23/08/2024. URL: https://www.microsoft.com/pt-br/security/business/security-101/what-is-access-control.

Ogata, Katsuhiko (2020). *Engenharia de controle moderno*. Trad. por Heloísa Coimbra de Souza. 5ª ed. São Paulo: Pearson Education. ISBN: 978-85-4301-375-6.

Saxena, Tanya (jan. de 2025). “What is Database?” Em: Acessado em 22/04/2025. URL: https://www.geeksforgeeks.org/what-is-database/.

Toledo, Victor (jun. de 2025). “O que é HTML? Entenda para que serve e como funciona a linguagem de marcação”. Em: Acessado em 20/07/2025. URL: https://tecnoblog.net/responde/o-que-e-html-entenda-para-que-serve-e-como-funciona-a-linguagem-de-marcacao/.

Veris (dez. de 2025). “What is a Relay? Relay Types, How They Work, Applications”. Em: Acessado em 22/04/2025. URL: https://www.veris.com/blog/relay-types-how-they-work-applications.

Vitor, João (set. de 2022). “Introdução aos Microcontroladores PIC – Parte 1”. Em: Acessado em 23/09/2024. URL: https://blog.eletrogate.com/introducao-aos-microcontroladores-pic-parte-1/.

Anexos

Anexo 1

Folhas de dados

1.1 Folha de dados LM7805

7805• THREE-TERMINAL POSITIVE VOLTAGE REGULATOR IC

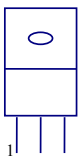
FEATURES:
- OUTPUT CURRENT IN EXCESS OF 1A;
- NO EXTERNAL COMPONENTS REQUIRED;
- INTERNAL SHORT CIRCUIT CURRENT LIMITING;
- INTERNAL THERMAL OVERLOAD PROTECTION;
- OUTPUT TRANSISTOR SAFE-AREA COMPENSATION;
- OUTPUT VOLTAGE OFFERED IN 4% TOLERANCE.

ABSOLUTE MAXIMUM RATINGS (Ta= 25° C)

Characteristic	Symbol	Norm	Unit
Input Voltage	Vin	V	35
Maximum Dissipated Power(with heat sink)	Ptot(max)	W	15
Maximum Dissipated Power(without heat sink)	Ptot(max)	W	1.5
Thermal Resistance Junction to Case	OjC	°C/W	5.0
Thermal Resistance, Junction to Air	OjA	°C/W	65
Junction Temperature	T_j	150	°C

Tc=-45÷+70°C

TO-220



1. Input
2. GND
3. Output

ELECTRICAL CHARACTERISTICS
(Vin=10V,Io=0.5A,Ci=0.33mkF,Co=0.1mkF,Tj=0+125°C, unless otherwise noted.)

Characteristic	Symbol	Norm			Unit
		Min	TYP	Max	
Output Voltage(Tj=25°C)	Vo	4.8		5.2	V
Output Voltage (5.0mA≤Io≤1.0A,Po≤15W) 7.0V≤Vin≤20V	Vo	4.75		5.25	V
Line Regulation(Tj=+25°C) 7.0V≤Vin≤25 V 8.0 V≤Vin≤12 V	ΔVv			100 50	mV
Load Regulation(Tj=+25°C) 5.0mA≤Io≤1.5A 0.25A≤Io≤0.75A	ΔVi			100 50	mV
Quiescent Current(Tj=+25°C)	Ib			8.0	mA
Quiescent Current Change7.0 V≤Vin≤25 V 5.0mA≤Io≤1.0 A	ΔIb			1.3 0.5	mA
Dropout Voltage(Io=1.0A,Tj=+25°C)	Vi-Vo		2.0		V
Short Circuit Current Limit(Ta=+25°C),Vin=35V	Isc		0.4		A
Peak Output Current(Tj=+25°C)	Imax		2.2		A
Average Temperature Coefficient of Output Voltage	TCVo		0.3		mV/°C

1.2 Folha de dados 1N4007

TYPES 1N4001 THRU 1N4007
SILICON RECTIFIERS

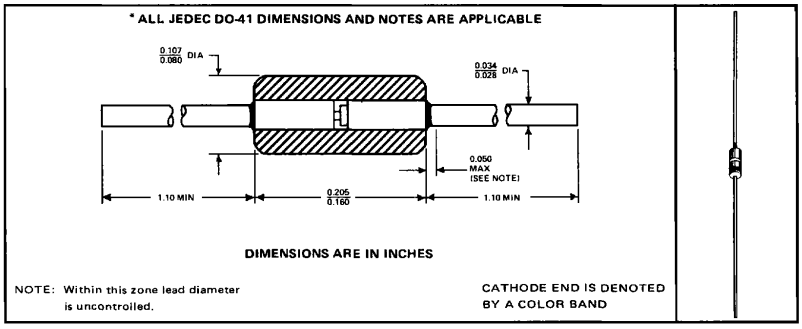
BULLETIN NO. DL-S 7211698, NOVEMBER 1972

50-1000 VOLTS • 1 AMP AVERAGE

- Rugged Double-plug Construction
- Hermetic Case
- 30-Amp Surge Rating

description and mechanical data

These one-amp rectifier diodes are the product of combining the best of both silicon material processing and packaging technologies. The silicon die is a mesa oxide-passivated structure which has additional nitride passivation and glass passivation over the junction. Years of volume production have shown the double-plug package to have the highest inherent mechanical integrity of all hermetic-case diodes.



***absolute maximum ratings at specified ambient† temperature (unless otherwise noted)**

		1N4001	1N4002	1N4003	1N4004	1N4005	1N4006	1N4007	UNIT
V_{RM}	Peak Reverse Voltage from −65°C to 175°C (See Note 1)	50	100	200	400	600	800	1000	V
V_R	Steady State Reverse Voltage from 25°C to 75°C	50	100	200	400	600	800	1000	V
I_O	Average Rectified Forward Current from 25°C to 75°C (See Notes 1 and 2)	1							A
I_{FRM}	Repetitive Peak Forward Current, 10 Cycles, at (or below) 75°C (See Note 3)	10							A
I_{FSM}	Peak Surge Current, One Cycle, at (or below) 75°C (See Note 3)	30							A
$T_{A(opr)}$	Operating Ambient Temperature Range	−65 to 175							°C
T_{stg}	Storage Temperature Range	−65 to 200							°C
	Lead Temperature 3/8 Inch from Case for 10 Seconds	350							°C

10

NOTES: 1. These values may be applied continuously under single-phase, 60-Hz, half-sine-wave operation with resistive load. Above 75°C derate I_O according to Figure 1.
2. This rectifier is a lead-conduction-cooled device. At (or above) ambient temperatures of 75°C, the lead temperature 3/8 inch from case must be no higher than 5°C above the ambient temperature for these ratings to apply.
3. These values apply for 60-Hz half sine waves when the device is operating at (or below) rated values of peak reverse voltage and average rectified forward current. Surge may be repeated after the device has returned to original thermal equilibrium.

*JEDEC registered data. This data sheet contains all applicable registered data in effect at the time of publication.

†The ambient temperature is measured at a point 2 inches below the device. Natural air cooling is used.

TEXAS INSTRUMENTS
INCORPORATED
POST OFFICE BOX 5012 • DALLAS, TEXAS 75222

1.3 Folha de dados 2N3904

2N3904

SMALL SIGNAL NPN TRANSISTOR

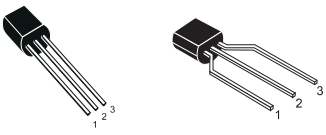
PRELIMINARY DATA

Ordering Code	Marking	Package / Shipment
2N3904	2N3904	TO-92 / Bulk
2N3904-AP	2N3904	TO-92 / Ammopack

- SILICON EPITAXIAL PLANAR NPN TRANSISTOR
- TO-92 PACKAGE SUITABLE FOR THROUGH-HOLE PCB ASSEMBLY
- THE PNP COMPLEMENTARY TYPE IS 2N3906

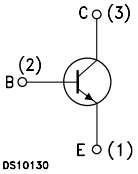
APPLICATIONS

- WELL SUITABLE FOR TV AND HOME APPLIANCE EQUIPMENT
- SMALL LOAD SWITCH TRANSISTOR WITH HIGH GAIN AND LOW SATURATION VOLTAGE



TO-92 Bulk **TO-92 Ammopack**

INTERNAL SCHEMATIC DIAGRAM



ABSOLUTE MAXIMUM RATINGS

Symbol	Parameter	Value	Unit
V_{CBO}	Collector-Base Voltage (I_E = 0)	60	V
V_{CEO}	Collector-Emitter Voltage (I_B = 0)	40	V
V_{EBO}	Emitter-Base Voltage (I_C = 0)	6	V
I_C	Collector Current	200	mA
P_{tot}	Total Dissipation at T_C = 25 °C	625	mW
T_{stg}	Storage Temperature	-65 to 150	°C
T_j	Max. Operating Junction Temperature	150	°C

Anexo 2

Código do microcontrolador

2.1 Arduino Sketch

O Arduino Sketch refere-se ao código de programação baseado na linguagem C++, com uso de algumas bibliotecas este pode ser compilado para um microcontroladoresda familia ESP.

main.ino | fingerprint.cpp | fingerprint.h | lcd.ino | WiFiMqttConfig.h

```
#include <Keypad.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <Adafruit_Fingerprint.h>
#include <HardwareSerial.h>
#include "WiFiMqttConfig.h" // Incluir o arquivo de configuração

#define buzzer 5
#define relay 25
#define FINGERPRINT_RX 13
#define FINGERPRINT_TX 14

LiquidCrystal_I2C lcd(0x27, 16, 2);  // Endereço 0x27 para LCD 16x2

const byte ROWS = 4;
const byte COLS = 4;

char keys[ROWS][COLS] = {
  {'1', '2', '3', 'A'},
  {'4', '5', '6', 'B'},
  {'7', '8', '9', 'C'},
  {'*', '0', '#', 'D'}
};

byte rowPins[ROWS] = {18, 19, 21, 22};
byte colPins[COLS] = {23, 17, 16, 4};

Keypad teclado = Keypad(makeKeymap(keys), rowPins, colPins, ROWS, COLS);

char senha[] = "8413";
char senhaPanico[] = "9999";
char digitada[5];
int indice = 0;
int estado = 0;
int id;
bool digitalReconhecida = false;

HardwareSerial mySerial(1);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

```

Figura 2.1: Configuração das variáveis e dos IOs. Fonte:[Autor]

main.ino | fingerprint.cpp | fingerprint.h | lcd.ino | WiFiMqttConfig.h

```
#ifndef WiFiMqttConfig_h
#define WiFiMqttConfig_h

#include <WiFi.h>
#include <PubSubClient.h>
#include <HTTPClient.h>

// ==================== CONFIGURAÇÕES DE REDE ====================
const char* ssid = "Galaxy Martiva";
const char* password = "12345678";

// ==================== CONFIGURAÇÃO DO BROKER MQTT ====================
const char* mqttServer = "10.41.138.227";  // IP doPC com Mosquitto
const int mqttPort = 1883;                  // Porta padrão MQTT

WiFiClient espClient;
PubSubClient client(espClient);

// Variável para armazenar a senha atual vinda do servidor
String senhaAtualServidor = "";

// ==================== CONEXÃO WI-FI ====================
void setup_wifi() {
    Serial.println();
    Serial.print("Conectando-se a ");
    Serial.println(ssid);
    WiFi.begin(ssid, password);
    while (WiFi.status() != WL_CONNECTED) {
        delay(500);
        Serial.print(".");
    }
    Serial.println("\nWiFi conectado!");
    Serial.print("Endereço IP: ");
    Serial.println(WiFi.localIP());
}
```

Figura 2.2: Configuração das conectividades. Fonte:[Autor]

main.ino fingerprint.cpp fingerprint.h lcd.ino WiFiMqttConfig.h

```
70  void loop() {
71    if (!digitalReconhecida) {
72      id = identificarImpressao();
73      if (id == 3 || id ==2) {
74        digitalReconhecida = true;
75        lcd.clear();
76        lcd.setCursor(1, 0);
77        lcd.print("ID Confirmada!");
78        delay(2000);
79        lcd.clear();
80        lcd.setCursor(1, 0);
81        lcd.print("Digite a senha:");
82      } else if (id != -1) {
83        lcd.clear();
84        lcd.setCursor(1, 0);
85        lcd.print("Verificando ID");
86        return;
87      } else {
88        lcd.clear();
89        lcd.setCursor(1, 0);
90        lcd.print("Aguardando digital");
91        delay(2000);
92        lcd.clear();
93        lcd.setCursor(1, 0);
94        lcd.print("Verificando ID");
95        return;
96      }
97    } else {
98      char tecla = teclado.getKey();
99      if (tecla != NO_KEY) {
100       if (tecla == '*') {
101         indice = 0;
102         memset(digitada, 0, sizeof(digitada));
103         lcd.clear();
104         lcd.setCursor(1, 0);
105         lcd.print("Digite a senha:");
106         return;
107       }
```

main.ino fingerprint.cpp fingerprint.h lcd.ino WiFiMqttConfig.h

```
96      }
97    } else {
98      char tecla = teclado.getKey();
99      if (tecla != NO_KEY) {
100       if (tecla == '*') {
101         indice = 0;
102         memset(digitada, 0, sizeof(digitada));
103         lcd.clear();
104         lcd.setCursor(1, 0);
105         lcd.print("Digite a senha:");
106         return;
107       }
108
109       if (tecla == '#' && indice == 4) {
110         digitada[indice] = '\0';
111         if (strcmp(senha, digitada) == 0) {
112           estado = 3;
113           lcdDisplay(estado);
114           digitalReconhecida = false;
115           registrarLog(id, "Senha correta. Acesso permitido");
116         } else if (strcmp(senhaPanico, digitada) == 0) {
117           estado = 4;
118           lcdDisplay(estado);
119           digitalReconhecida = false;
120           client.publish("alarme/panico", "ALERTA: Senha de pânico acionada!");
121           registrarLog(id, "Senha de pânico acionada!");
122         }else if(strcmp(senhaAtualServidor.c_str(), digitada) == 0) {
123           estado = 3;
124           lcdDisplay(estado);
125           digitalReconhecida = false;
126           registrarLog(id, "Senha correta. Acesso permitido");
127         }
128          else {
129           estado = 2;
130           lcdDisplay(estado);
131           registrarLog(id, "Senha incorreta");
132         }
133         indice = 0;
134         estado = 0;
135       } else if (indice < 4 && tecla != '#') {
136         digitada[indice] = tecla;
137         indice++;
138         estado = 1;
139       }
```

Figura 2.3: Decisões da Autenticação. Fonte:[Autor]

Anexo 3

Painel Administrativo

3.1 Codigos do desenvolvimento do *website*

O painel administrativo é um website baseado em linguagens HTML, CSS, PHP, JavaScript.

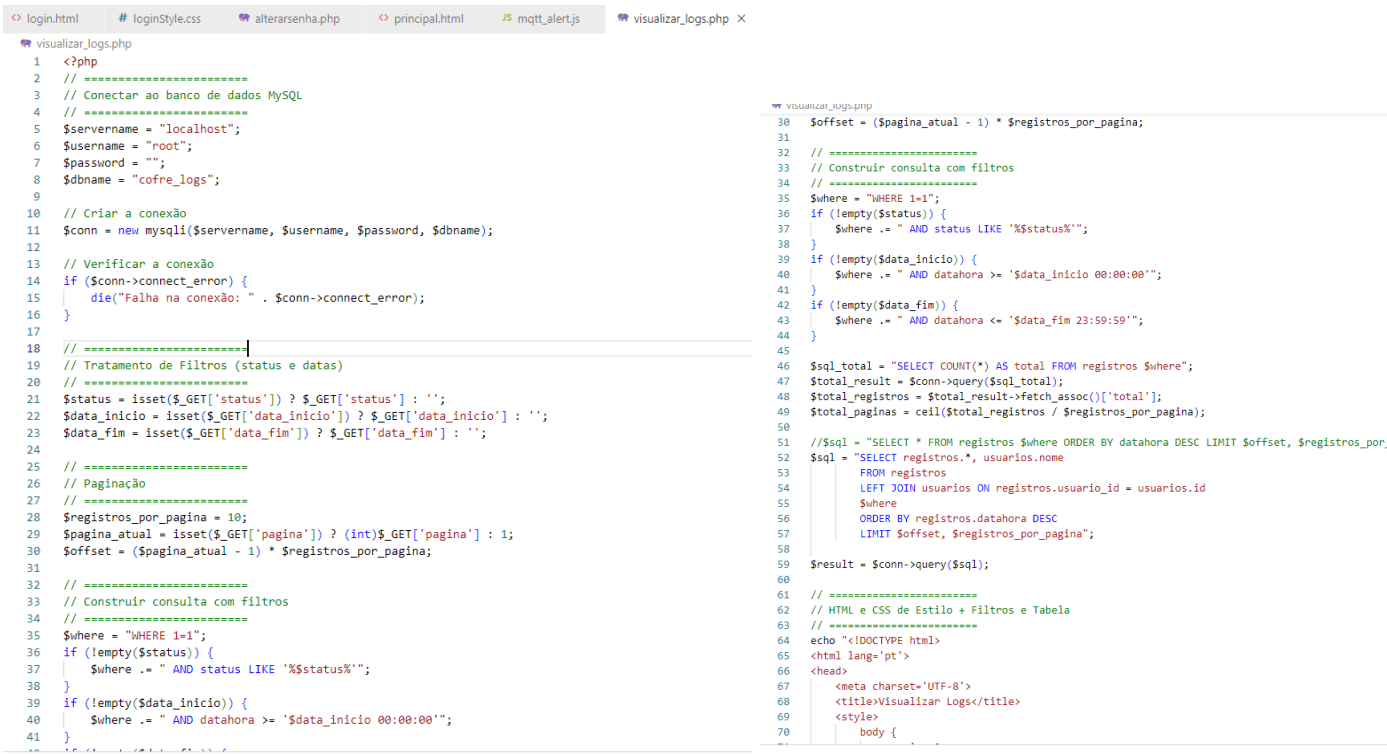


Figura 3.1: Código fonte da pagina de registros. Fonte:[Autor]

alterarsenha.php

```php
<!DOCTYPE html>
<html lang="pt-br">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Alteração de Senha</title>
    <link rel="stylesheet" href="style.css">
</head>
<body>
    <div class="container">
        <h1>Alterar Senha</h1>
        <form action="alterar_senha.php" method="POST">
            <div class="form-group">
                <label for="senha-atual">Senha Atual:</label>
                <input type="password" id="senha-atual" name="senha_atual" required>
            </div>
            <div class="form-group">
                <label for="nova-senha">Nova Senha:</label>
                <input type="password" id="nova-senha" name="nova_senha" required>
            </div>
            <div class="form-group">
                <label for="confirmar-senha">Confirmar Nova Senha:</label>
                <input type="password" id="confirmar-senha" name="confirmar_senha" required>
            </div>
            <button type="submit" class="btn">Alterar Senha</button>
        </form>
    </div>
    <script src="Script.js"></script>
</body>
</html>

```

Figura 3.2: HTML para pagina da alteração da senha. Fonte: [Autor]

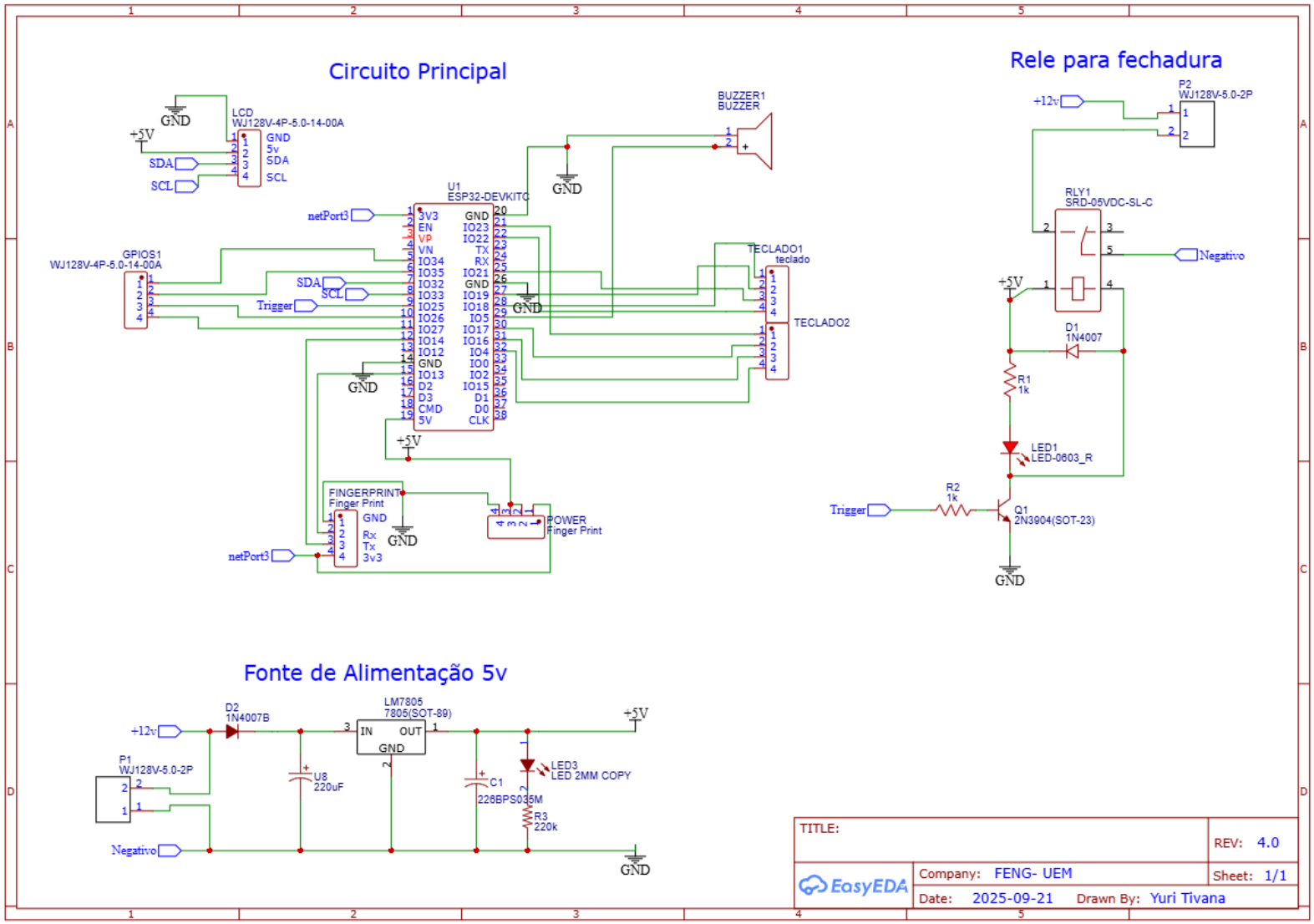


Figura 3.3: Esquema Eletrico do projecto.Fonte:[Autor]