

**CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE FRANCA “Dr THOMAZ NOVELINO**

TECNOLOGIA EM DESENVOLVIMENTO DE SOFTWARE MULTIPLATAFORMA

**ARTHUR CESAR SOUSA MARCELINO
HUGO DE CASTRO RODRIGUES
PABLO MIGUEL SOUSA NOBREGA
VITOR SIQUEIRA SIMEÃO**

FECHADURA INTELIGENTE ELOCK

FRANCA/SP 2025

1. Introdução

O ELOCK é uma solução integrada de segurança eletrônica concebida para proporcionar controle de acesso moderno, flexível e escalável para residências, empresas e espaços compartilhados. O ELOCK combina três componentes principais, um dispositivo IoT compacto em formato de tag/NFC, um aplicativo móvel e uma interface web, permitindo que usuários autorizados realizem a abertura e fechamento de portas, portões e outros mecanismos de travamento com segurança, rastreabilidade e conveniência.

a) Descrição do problema a ser solucionado:

O aumento da urbanização, o crescimento de empreendimentos comerciais e a necessidade de maior controle sobre acessos físicos trouxeram novos desafios para a segurança cotidiana. Os métodos tradicionais, como chaves mecânicas e controles remotos convencionais, apresentam diversas limitações: perda ou cópia de chaves, ausência de histórico de uso, dificuldades na gestão de múltiplos usuários e falta de integração com sistemas digitais modernos. Além disso, o avanço da Internet das Coisas (IoT) e da conectividade móvel despertou a demanda por soluções inteligentes, seguras e acessíveis que permitam o controle remoto e a automação de acessos.

O problema central, portanto, é a carência de um sistema de controle de acesso unificado, de baixo custo e fácil implementação, que ofereça segurança, praticidade e escalabilidade para contextos como residenciais, empresariais e comunitários.

b) Objetivo do trabalho:

O principal objetivo do projeto **ELOCK** é desenvolver uma solução inteligente de controle de acesso que una hardware (tag/NFC), aplicativo móvel e plataforma web em um ecossistema totalmente integrado. O sistema deve permitir o cadastro e a gestão de usuários, o controle de múltiplas fechaduras e a execução de operações de abertura e fechamento de forma segura, rastreável e intuitiva.

Entre os objetivos específicos, destacam-se:

- Implementar uma fechadura eletrônica inteligente controlável via aplicativo e site;
- Utilizar tecnologia NFC como alternativa prática para destravação local sem dependência de rede;
- Criar uma plataforma web administrativa para o gerenciamento centralizado de dispositivos e permissões;
- Proporcionar uma interface de usuário simples e acessível, mesmo para operadores sem conhecimento técnico avançado.

c) Contribuição e importância do trabalho:

O projeto ELOCK representa uma contribuição relevante no campo da automação e segurança digital, especialmente ao propor uma solução acessível e de fácil adoção que combina hardware e software em um mesmo ecossistema. Sua importância se manifesta em diferentes dimensões:

- Tecnológica: promove a integração entre IoT, mobilidade e computação em nuvem, demonstrando como esses pilares podem ser aplicados de forma prática à segurança cotidiana.
- Econômica: oferece uma alternativa de baixo custo em comparação a sistemas de segurança complexos e caros, viabilizando o acesso à tecnologia para pequenas empresas e residências.
- Social: aumenta a segurança e o controle em ambientes coletivos, reduzindo riscos de invasões e facilitando a gestão de acessos compartilhados.
- Educacional: serve como base de estudo e desenvolvimento para projetos acadêmicos e profissionais na área de sistemas embarcados, redes e segurança da informação.

Ao unir conveniência, segurança e escalabilidade, o ELOCK não apenas soluciona problemas práticos do cotidiano, mas também impulsiona a transformação digital no controle de acessos, tornando-se um exemplo de inovação aplicada a contextos reais.

d) Benefícios esperados:

- Maior conveniência para usuários finais, que poderão acessar pontos controlados por múltiplos métodos (tag, app, web).
- Redução de custos operacionais comparado a sistemas tradicionais com chaves físicas ou gestão manual de acessos.
- Escalabilidade: desde uma única fechadura residencial até redes de acesso em edifícios comerciais ou condomínios com múltiplos administradores.

d) Público-alvo:

O ELOCK foi pensado para:

- Usuários residenciais que buscam modernizar o controle de acesso de suas casas.
- Condomínios e pequenas propriedades que precisam de gestão centralizada de entradas e visitantes.
- Pequenas e médias empresas que desejam administrar entradas, controlar turnos e rastrear acessos de funcionários e terceiros.

e) Visão Geral do Projeto

O ELOCK surge da necessidade crescente por controles de acesso que sejam ao mesmo tempo seguros e fáceis de gerir. A oferta tradicional de fechaduras eletrônicas frequentemente peca por soluções isoladas: um hardware com pouco suporte digital, ou um aplicativo que não integra os múltiplos pontos de acesso de um ambiente.

O ELOCK foi projetado como um ecossistema convergente: o hardware (tag/NFC) fornece a interface física e portátil para destravação; o aplicativo móvel oferece mobilidade, notificações e gerenciamento rápido de permissões; a aplicação web fornece uma camada administrativa robusta para cadastro, auditoria e configuração em larga escala.

2. Metodologia utilizada

O desenvolvimento do projeto ELOCK foi conduzido seguindo uma abordagem ágil e modular, com foco em escalabilidade, desempenho e segurança. Para garantir a integração eficiente entre os diferentes componentes — hardware IoT, aplicativo móvel e plataforma web —, foram empregadas tecnologias modernas e amplamente utilizadas no ecossistema de desenvolvimento full stack.

1. Arquitetura e Organização do Projeto

O projeto foi dividido em três principais camadas:

- Frontend Web: responsável pela interface administrativa e gestão de usuários e fechaduras.
- Aplicativo Mobile (App): voltado à interação direta com o usuário final e controle de acesso via IoT.
- Backend e Banco de Dados: responsável pelas APIs, autenticação, processamento de regras de negócio e persistência de dados.

2. Tecnologias Utilizadas

Banco de Dados

- MongoDB: escolhido por sua flexibilidade e desempenho em dados não estruturados, ideal para armazenar informações de usuários, logs de acesso e registros de fechaduras.
- O uso do Sequelize ORM facilitou a modelagem e o gerenciamento das entidades, permitindo integração entre o banco e o backend com abstração e segurança.

Backend

- NestJS: framework robusto baseado em TypeScript, adotado para estruturar a API com modularidade, injeção de dependências e suporte nativo a testes e autenticação.
- Node.js: utilizado como ambiente de execução para garantir alta performance e suporte assíncrono em requisições simultâneas.
- O backend foi desenvolvido seguindo princípios de Clean Architecture e RESTful APIs, garantindo manutenção e escalabilidade.

Frontend Web

- TypeScript e TailwindCSS foram utilizados para o desenvolvimento do painel administrativo, proporcionando uma interface limpa, responsiva e de fácil manutenção.
- O TailwindCSS permite alta produtividade no design, mantendo consistência visual e desempenho otimizado.

Aplicativo Mobile

- React Native foi adotado para o desenvolvimento do aplicativo, garantindo compatibilidade entre plataformas Android e iOS, com um único código base.
- A integração com o backend foi feita via APIs REST, possibilitando comunicação direta com o servidor para autenticação, controle de acesso e gerenciamento das fechaduras IoT.

3. Viabilidade do Projeto

a) Canvas de Negócio (Business Model Canvas - BMC)

O ELOCK foi idealizado com base em um modelo de negócio que combina inovação tecnológica e viabilidade comercial, atendendo à crescente demanda por soluções de automação e segurança conectada. O Business Model Canvas (BMC) a seguir descreve os principais elementos estratégicos do projeto.

1. Proposta de Valor

- Sistema inteligente de controle de acesso, integrando IoT, app e plataforma web.

- Eliminação do uso de chaves físicas e controle manual.
- Segurança, praticidade e conectividade em um único ecossistema.
- Acesso remoto, histórico de uso e permissões configuráveis.

2. Segmentos de Clientes

- Residências que buscam automação e segurança.
- Empresas e escritórios precisam controlar o acesso de funcionários e visitantes.
- Condomínios residenciais e comerciais.
- Espaços de coworking, hotéis e locações temporárias (Airbnb, por exemplo).
- Pequenos e médios negócios que necessitam de gestão de acessos em múltiplas unidades.

3. Canais de Distribuição

- Aplicativo móvel (App Store e Google Play).
- Plataforma web (acesso via navegador).
- Site oficial com área de cadastro e suporte.
- Parcerias com revendedores de equipamentos IoT e segurança.
- Marketing digital e redes sociais.

4. Relacionamento com Clientes

- Suporte técnico e atendimento remoto via chat e e-mail.
- Tutoriais e base de conhecimento online.
- Programa de fidelidade e atualização contínua do software.
- Comunicação transparente sobre privacidade e segurança dos dados.

5. Fontes de Receita

- Venda direta do dispositivo ELOCK (hardware IoT).
- Planos de assinatura para acesso premium (monitoramento, relatórios avançados, controle remoto, etc.).
- Taxas de manutenção e suporte técnico.
- Licenciamento para integradores e empresas de segurança.

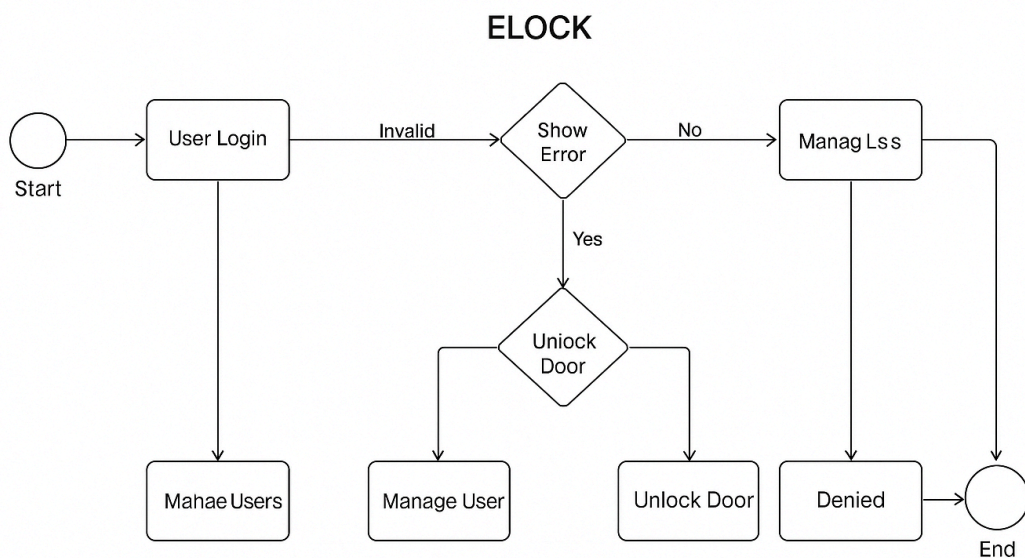
6. Recursos-Chave

- Equipe de desenvolvimento (frontend, backend, mobile e IoT).
- Infraestrutura de servidores e banco de dados na nuvem.
- Tecnologias: MongoDB, NestJS, React Native, TypeScript, TailwindCSS, Node.js.

ELOCK

PARCEIROS-CHAVE <ul style="list-style-type: none"> Fabricantes de fechaduras Provedores de hardware IoT Desenvolvedores 	ATIVIDADES-CHAVE <ul style="list-style-type: none"> Desenvolvimento de software Produção de hardware Suporte técnico 	RELAÇÕES COM CLIENTES <ul style="list-style-type: none"> Autonomia Suporte técnico
RECURSOS-CHAVE <ul style="list-style-type: none"> Equipe de desenvolvimento Infraestrutura tecnológica 	PROPOSTA DE VALOR <ul style="list-style-type: none"> Controle de acesso remoto Segurança e conveniência Integração com plataformas digitais 	CANAIS <ul style="list-style-type: none"> App móvel e plataforma web
ESTRUTURA DE CUSTOS <ul style="list-style-type: none"> Desenvolvimento Hardware e infraestrutura Suporte técnico 		SEGMENTOS DE CLIENTES <ul style="list-style-type: none"> Residências Empresas Condomínios

4. Levantamento de Requisitos



a) Diagrama BPMN

b) Requisitos Funcionais

Código	Descrição	Categoria	Prioridade
RF001	Permitir o cadastro e autenticação de usuários (login/logout).	Cadastro de Entidade	Altíssima

Código	Descrição	Categoria	Prioridade
RF002	Permitir o cadastro, edição e exclusão de fechaduras inteligentes.	Cadastro de Entidade	Altíssima

Código	Descrição	Categoria	Prioridade
RF003	Permitir o emparelhamento de fechaduras via NFC/BLE com o sistema.	Cadastro de Entidade	Altíssima

Código	Descrição	Categoria	Prioridade
RF004	Realizar o destravamento de portas através do aplicativo móvel.	Funcionalidade	Altíssima

Código	Descrição	Categoria	Prioridade
RF005	Permitir destravamento por aproximação física de tag/NFC.	Funcionalidade	Altíssima

Código	Descrição	Categoria	Prioridade
---------------	------------------	------------------	-------------------

RF006	Registrar logs de eventos de abertura, fechamento e tentativas inválidas.	Funcionalidade	Altíssima
-------	---	----------------	-----------

Código	Descrição	Categoria	Prioridade
---------------	------------------	------------------	-------------------

RF007	Permitir o cadastro de novas fechaduras por meio da interface web.	Funcionalidade	Altíssima
-------	--	----------------	-----------

Código	Descrição	Categoria	Prioridade
---------------	------------------	------------------	-------------------

RF007	Permitir o cadastro de novas fechaduras por meio da interface web.	Funcionalidade	Altíssima
-------	--	----------------	-----------

Código	Descrição	Categoria	Prioridade
---------------	------------------	------------------	-------------------

RF008	Suportar múltiplas fechaduras associadas a um mesmo usuário.	Funcionalidade	Altíssima
-------	--	----------------	-----------

Código	Descrição	Categoria	Prioridade
---------------	------------------	------------------	-------------------

RF009	Permitir redefinição de senha e recuperação de conta.	Funcionalidade	Altíssima
-------	---	----------------	-----------

c) Requisitos Não Funcionais

Código	Descrição	Categoria	Prioridade
---------------	------------------	------------------	-------------------

RNF001	Todas as comunicações devem utilizar protocolos seguros (HTTPS, TLS 1.3 ou superior).	Funcionalidade	Altíssima
--------	---	----------------	-----------

Código	Descrição	Categoria	Prioridade
RNF002	O aplicativo deve ser compatível com Android (≥ 10) e iOS (≥ 14).	Funcionalidade	Altíssima

Código	Descrição	Categoria	Prioridade
RNF003	A aplicação web deve ser responsiva e compatível com navegadores modernos (Chrome, Edge, Firefox, Safari).	Funcionalidade	Altíssima

Código	Descrição	Categoria	Prioridade
RNF004	Os dados de usuários devem ser armazenados em banco de dados seguro, com criptografia em repouso (AES-256).	Funcionalidade	Altíssima

Código	Descrição	Categoria	Prioridade
RNF005	O sistema deve suportar no mínimo 100 usuários simultâneos sem perda significativa de desempenho.	Funcionalidade	Altíssima

Código	Descrição	Categoria	Prioridade
RNF006	O hardware IoT deve operar com consumo energético reduzido e autonomia mínima de 12 meses por bateria.	Funcionalidade	Altíssima

Código	Descrição	Categoria	Prioridade
RNF007	A interface deve seguir princípios de usabilidade e acessibilidade (WCAG 2.1).	Funcionalidade	Altíssima

d) Regras de Negócio

As regras de negócio do ELOCK estabelecem as condições e restrições para o funcionamento do sistema:

1. RN001 – Apenas usuários com permissão de administrador podem cadastrar novas fechaduras.
2. RN002 – Cada fechadura deve estar vinculada a uma conta principal e pode ter múltiplos usuários associados.
3. RN003 – O destravamento via aplicativo requer conexão à internet e autenticação válida.
4. RN004 – O destravamento via NFC pode operar offline, desde que o token local esteja atualizado.
5. RN006 – Logs de acesso não podem ser excluídos, apenas consultados ou exportados.
6. RN007 – O sistema deve impedir o cadastro de usuários com e-mails duplicados.
7. RN008 – Tentativas de acesso mal-sucedidas consecutivas bloqueiam o usuário.
8. RN010 – Toda operação de exclusão de usuários ou fechaduras deve ser confirmada pelo administrador responsável.

e) Casos de Uso

A seguir estão os principais casos de uso do sistema ELOCK:

1. UC01 – Cadastrar Usuário
Ator: Administrador
Descrição: Permite adicionar um novo usuário ao sistema, definindo seu nível de acesso e credenciais.
2. UC02 – Autenticar Usuário
Ator: Usuário
Descrição: Usuário realiza login no aplicativo ou site para acessar suas permissões.
3. UC03 – Registrar Fechadura
Ator: Administrador
Descrição: Cadastrar e emparelhar uma nova fechadura inteligente ao sistema.

4. UC04 – Destruar Porta via App

Ator: Usuário

Descrição: Usuário solicita abertura de uma fechadura pelo aplicativo. O sistema valida e envia o comando ao dispositivo.

5. UC05 – Destruar Porta via Tag/NFC

Ator: Usuário

Descrição: Ao aproximar a tag do leitor, a fechadura valida o token e realiza o destravamento.

6. UC06 – Consultar Logs de Acesso

Ator: Administrador/Gestor

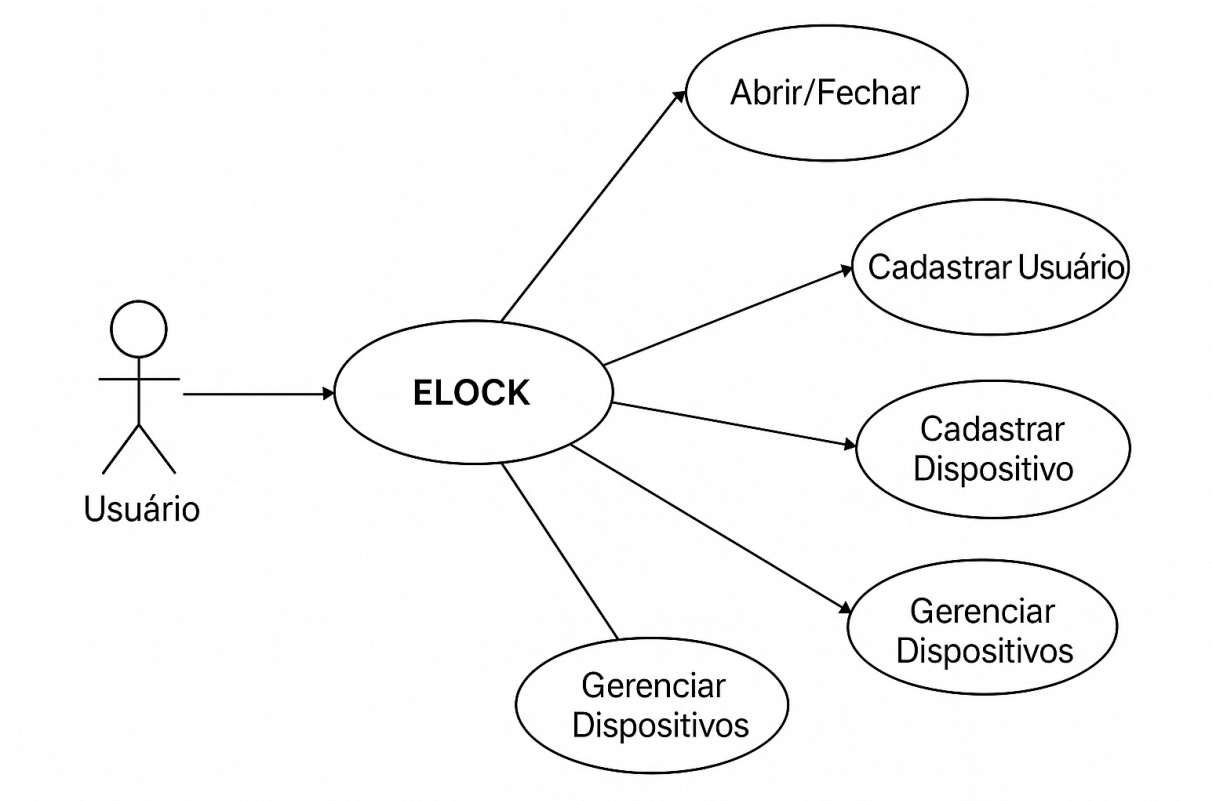
Descrição: Permite visualizar e exportar o histórico de eventos do sistema.

7. UC08 – Revogar Permissão de Acesso

Ator: Administrador

Descrição: Permite ao administrador bloquear ou remover permissões de usuários.

f) Diagrama de Caso de Uso



5. Manual do Usuário (ou Guia de Uso)

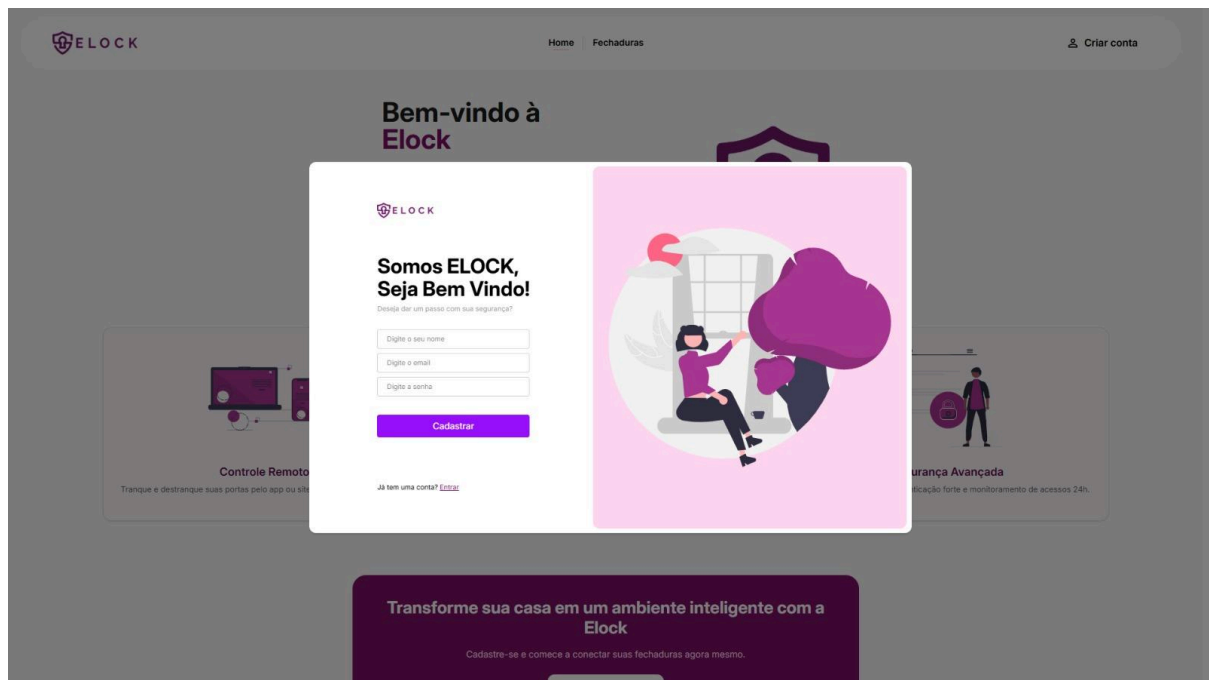
a) Instalação e configuração

6. Telas do Projeto

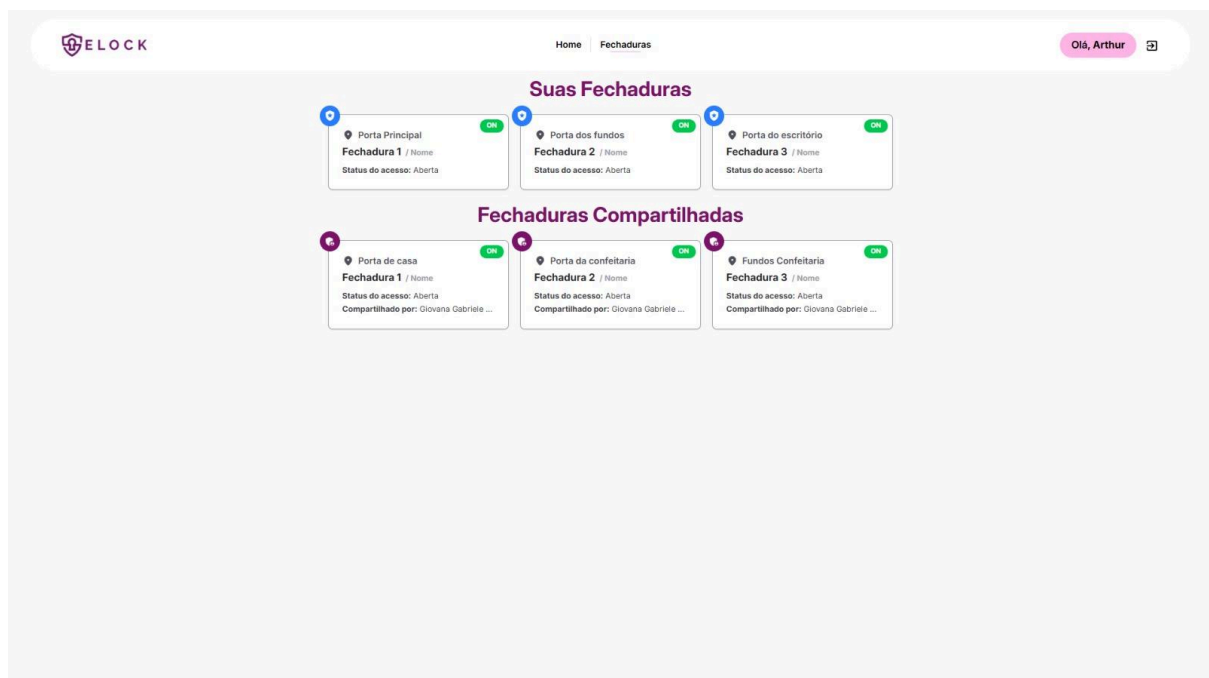
a) Desktop



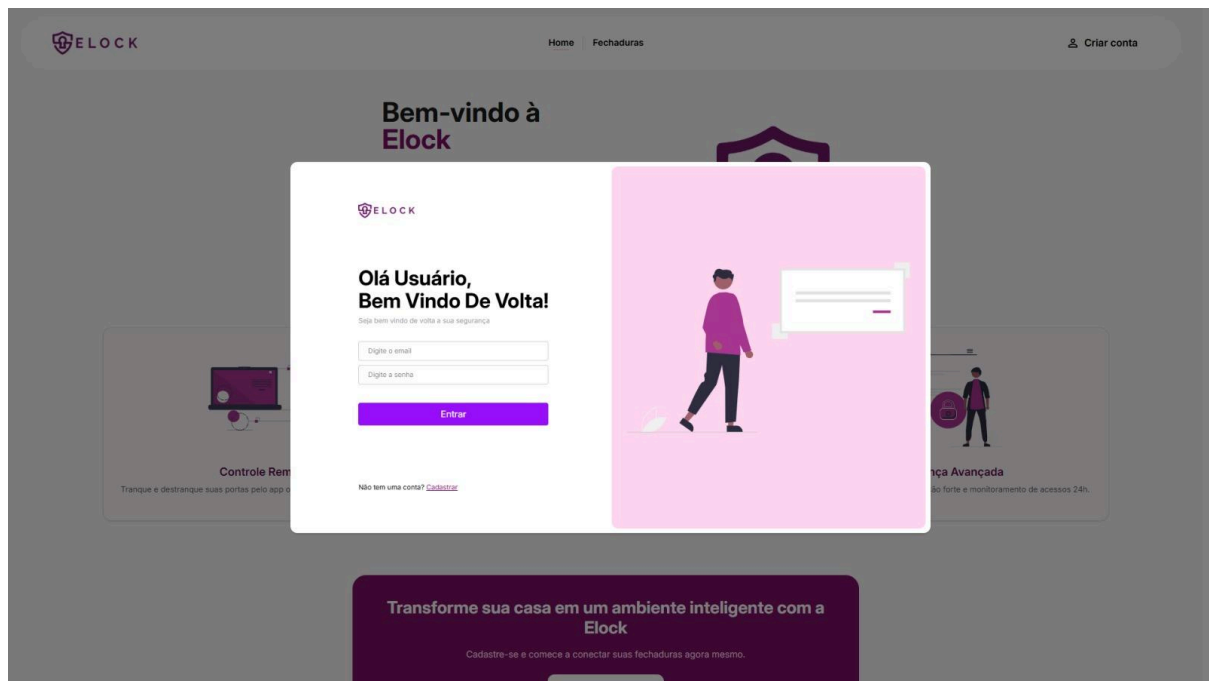
Tela inicial do Elock, com as principais informações do site, conteúdos, acesso a tela de cadastro/login e etc.



Tela de cadastro onde o usuário entra com as suas informações para realizar o cadastro no site



Tela onde são mostradas as suas fechaduras cadastradas, tanto as que foram compartilhadas quanto as que não foram, onde após cadastrá-las pelo aplicativo elas automaticamente aparecerão nesta tela



Tela de login onde o usuário que já possui cadastro entre com as suas informações para a realização do cadastro

b) Aplicativo



Tela de criação de usuário, onde o usuário irá se cadastrar e criar a sua conta para acessar o aplicativo ELOCK

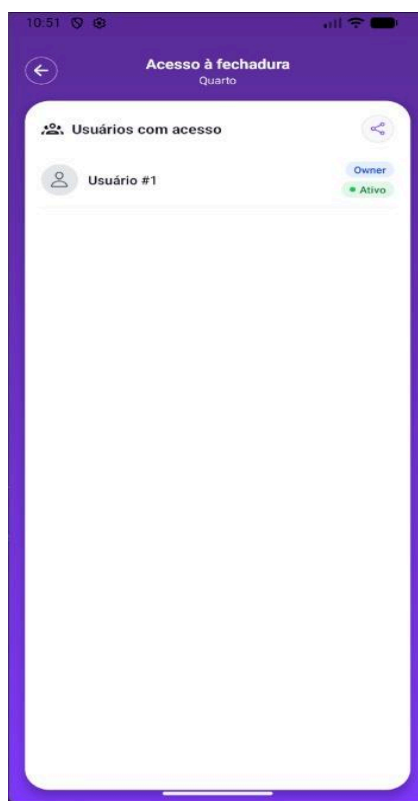


The image shows a mobile application interface for 'Elock'. At the top, there is a status bar with the time '10:49' and various icons. Below the status bar is a dark purple header with a white shield icon containing a keyhole. The word 'Elock' is written in white below the icon. Underneath, a tagline reads 'Controle suas fechaduras inteligentes com segurança e rapidez.' The main content area is a white rounded rectangle. It contains two input fields: 'E-mail' with the placeholder 'seu@email.com' and 'Senha' with a masked password '*****'. To the right of the password field is a toggle icon. Below the password field is a link 'Esqueceu a senha?'. A large purple button with the text 'Entrar →' is positioned below the inputs. Below this button is a horizontal line with the word 'ou' in the center. At the bottom of the white rectangle is a button with a user icon and the text 'Criar uma conta'. At the very bottom of the screen, in small text, it says 'Elock API • IoT Smart Locks'.

Tela de login do usuário, onde o usuário irá entrar com as suas informações para fazer o login no aplicativo



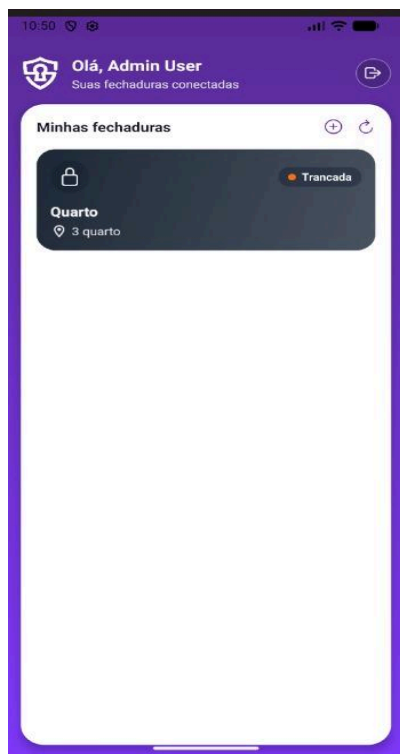
Tela de criação de fechaduras, em que o usuário poderá adicionar uma nova fechadura, colocando o nome da fechadura, a sua localização e ao clicar no botão de cadastrar fechadura, uma nova é gerada.



Tela de usuários com acesso a fechadura, onde estão cadastrados os usuários com acessos às suas respectivas fechaduras.



Tela da fechadura onde o usuário terá acesso às informações da fechadura selecionada, e ele poderá destrancá-la e ver quem possui acesso a ela



Tela do usuário, onde ele poderá acessar cada uma de suas fechaduras cadastradas no sistema ELOCK



Tela de compartilhamento de usuários, onde o “Usuário principal” poderá compartilhar o acesso às suas fechaduras com os demais usuários que estiver cadastrados com o email.

c) lot

O sistema físico do ELOCK é composto por um conjunto de componentes eletrônicos integrados para garantir controle de acesso seguro e automatizado.

- O ESP32 atua como microcontrolador principal, responsável por processar os comandos e realizar a comunicação via Wi-Fi ou Bluetooth com o aplicativo e o servidor.
- O módulo relé é utilizado para acionar dispositivos externos, como portas ou fechaduras elétricas.
- O servo motor MG996R realiza o movimento mecânico de abertura e fechamento quando necessário.

- Um leitor NFC simples permite que o usuário destrave a porta aproximando uma tag autorizada.
- Por fim, LEDs indicadores auxiliam na sinalização visual do estado do sistema, como sucesso, erro ou operação em andamento.

7. Itens a melhorar

Durante o desenvolvimento e análise do projeto ELOCK, foram identificados alguns pontos que podem ser aprimorados nas próximas etapas de evolução do sistema:

1. Otimização da Interface de Usuário (UI/UX): Melhorar a experiência visual e a fluidez das telas do aplicativo e da plataforma web, com base em testes de usabilidade com usuários reais.
2. Atualizações Over-the-Air (OTA): Implementar um sistema automático de atualização de firmware nas fechaduras, garantindo segurança e correções sem necessidade de intervenção manual.
3. Monitoramento Energético: Incluir funcionalidades de monitoramento do consumo da bateria e alertas preditivos de substituição para o dispositivo IoT.
4. Módulo de Acesso Temporário Avançado: Permitir o agendamento de acessos com horários e datas específicas, ideal para serviços, visitantes ou locações curtas.
5. Escalabilidade do Servidor: Revisar a arquitetura de backend para suportar maior volume de usuários e fechaduras simultâneas, com balanceamento de carga e redundância.
6. Compatibilidade com Mais Protocolos IoT: Expandir o suporte além de NFC e BLE, incluindo Wi-Fi, Zigbee ou LoRaWAN, para maior flexibilidade em diferentes ambientes.

8. Considerações Finais

O projeto ELOCK representa uma inovação relevante no campo da automação residencial e corporativa, unindo hardware e software em um ecossistema seguro, escalável e de fácil utilização. Ao longo de seu desenvolvimento, buscou-se criar uma solução capaz de substituir métodos tradicionais de controle de acesso por uma alternativa mais eficiente, moderna e confiável.

A combinação de IoT, NFC e computação em nuvem proporcionou uma base sólida para atender às demandas atuais de conectividade e segurança. Através do aplicativo e da plataforma web, o ELOCK oferece gestão centralizada, monitoramento em tempo real e flexibilidade operacional, adaptando-se a diferentes contextos — residenciais, empresariais e coletivos.

Embora o sistema já apresente resultados promissores, seu potencial de evolução é amplo. Com futuras melhorias em design, integração e escalabilidade, o ELOCK poderá se consolidar como uma das soluções mais completas e acessíveis em controle de acesso inteligente.

Em síntese, o projeto cumpre seu propósito de unir segurança, praticidade e inovação tecnológica, demonstrando como a transformação digital pode tornar o cotidiano mais simples e protegido. O ELOCK não é apenas um produto tecnológico — é um passo em direção ao futuro da segurança conectada.