

SPHYNX – Sistema de Controle de Acesso
Escolar e Domiciliar

SPHYNX – School and Home Access Control System

SPHYNX – Sistema de Control de Acceso Escolar y
Domiciliario

Kaik Mendes¹
kaik.mendes@fatec.sp.gov.br

Natã Martins Duarte de Freitas¹
nata.freitas@fatec.sp.gov.br

Pedro Henrique Vidal dos Santos¹
pedro.santos229@fatec.sp.gov.br

Mickael Leite Pereira Batista¹
mickael.batista@fatec.sp.gov.br

Daisy Éboli¹
daisy.eboli@fatec.sp.gov.br

Palavras-chave:
Segurança Escolar.
Controle de Fluxo.
Proteção Domiciliar.
Sistema de Controle de
Acesso.

Keywords:
School Security.
Flow Control.
Home Protection.
Access Control System.

Palabras clave:
Seguridad Escolar.
Control de Flujo.
Protección.
Sistema de control del
acceso.

Apresentado em:
05 dezembro, 2024

Evento:
7º EnGeTec

Local do evento:
Fatec Zona Leste

Avaliadores:
Edson Company Colalto
Junior
Gerson Gonçalves Silva



Resumo
Este trabalho apresenta uma solução e prototipação de um projeto para problemas muito presente nos tempos atuais: O aumento de casos de invasões, furtos e roubos em propriedades privadas e instituições públicas. Todos esses casos derivam das mesmas circunstâncias: a falta de uma segurança pública eficaz, um controle de fluxo adequado e a negligência da importância de tal controle. Tal solução, apelidada de Projeto Sphynx, se trata de um sistema de segurança feito corrigir essa defasagem, o deixando mais intuitivo e com novos módulos adicionais, tendo como função reduzir casos de invasão, controlar fluxo de pessoas e auxiliar na segurança de locais públicos, destacando instituições de ensino. Para o desenvolvimento adequado de um projeto que cumpra todas as expectativas, foram estudadas diversas tecnologias controle de acesso, por meio do método de revisão sistemática, além da utilização de linguagens de programação C++, JavaScript e Java para a criação de um protótipo web que se conecta com um microcontrolador ESP32.

Abstract:
This work presents a solution and prototype for a project addressing a prevalent issue in modern times: the increase in cases of break-ins, thefts, and robberies in private properties and public institutions. All these cases stem from similar circumstances: the lack of effective public security, inadequate flow control, and neglect of the importance of such control. This solution, named Project Sphynx, is a security system designed to bridge this gap, making it more intuitive with additional modules aimed at reducing intrusion incidents, controlling the flow of people, and enhancing the security of public spaces, especially educational institutions. For the successful development of a project that meets all expectations, various access control technologies were studied using a systematic review method. In addition, programming languages C++, JavaScript, and Java were employed to create a web prototype that connects with an ESP32 microcontroller.

Resumen:
Este trabajo presenta una solución y un prototipo de un proyecto para abordar un problema muy presente en la actualidad: el aumento de casos de intrusiones, hurtos y robos en propiedades privadas e instituciones públicas. Todos estos casos derivan de las mismas circunstancias: la falta de una seguridad pública eficaz, un control de flujo adecuado y la negligencia hacia la importancia de dicho control. Esta solución, denominada Proyecto Sphynx, es un sistema de seguridad diseñado para corregir esta deficiencia, haciéndolo más intuitivo y con módulos adicionales, con el objetivo de reducir casos de intrusión, controlar el flujo de personas y mejorar la seguridad de espacios públicos, destacando las instituciones educativas. Para el desarrollo adecuado de un proyecto que cumpla con todas las expectativas, se estudiaron diversas tecnologías de control de acceso mediante el método de revisión sistemática. Además, se emplearon los lenguajes de programación C++, JavaScript y Java para crear un prototipo web que se conecta con un microcontrolador ESP32.

¹ Fatec Ferraz de Vasconcelos

1. Introdução

Com o aumento dos índices de violência e insegurança, a necessidade de soluções de segurança pública se tornou crítica, tanto para o governo quanto para a população. Em particular, a proteção de instituições educacionais e residências em áreas de baixa renda tem se mostrado urgente, principalmente na região metropolitana leste de São Paulo. A falta de controle e monitoramento em tempo real de acessos a esses ambientes aumenta o risco de invasões e, consequentemente, de episódios trágicos que ultrapassam a perda de bens materiais e colocam vidas em risco. Além disso, instituições educacionais, como universidades e escolas carecem de medidas para rastrear a presença e movimentação de alunos e funcionários, deixando lacunas preocupantes na gestão de segurança interna (Zagonel; Machado; Mônico, 2017).

Em São Paulo, a prevenção de invasões e o controle de acesso têm se destacado como um desafio constante. Crimes patrimoniais, como furtos e roubos, embora ainda prevalentes, são apenas um dos problemas. As invasões, que se mantêm em crescimento, apontam para a necessidade de soluções preventivas mais eficazes, sobretudo no contexto escolar. Entre 2019 e 2021, dados do SAEB revelaram um aumento significativo em registros de vandalismo e invasões em escolas. Eventos trágicos, como o ataque a uma escola na zona leste de São Paulo (SP) e a uma creche em Blumenau (SC), ambos em 2023, expõem as limitações das medidas utilizadas atualmente, evidenciando a necessidade de uma abordagem integrada para a segurança educacional (Soares et al., 2024).

Diante dessa realidade, desenvolvemos o Sphynx, uma solução de controle de acesso voltada para garantir segurança e praticidade de residências até pequenos negócios. Construído com foco em acessibilidade e eficiência, o sistema utiliza a placa ESP32, integrada a um módulo RFID (Radio Frequency Identification) para autenticação por cartões e dispositivos que suportem o protocolo NFC (Near Field Communication), como celulares e relógios inteligentes, oferecendo também módulos opcionais, como leitura de impressão digital e reconhecimento facial utilizando técnicas de aprendizado de máquina populares disponíveis no mercado.

O sistema é gerido por um software robusto, desenvolvido na linguagem de programação Java, que oferece recursos de gerenciamento de usuários, definição de permissões de acesso e armazenamento seguro dos dados com criptografia. A interface web responsiva em múltiplas plataformas permite o monitoramento em tempo real e configuração de novos parâmetros de segurança. Com essas funcionalidades, o Sphynx visa ser uma solução escalável e acessível, que atende desde pequenas residências até grandes instituições educacionais, promovendo o controle de fluxo e um ambiente seguro para todos os envolvidos.

Dessa forma, combinando componentes de baixo custo, linguagens de programação e tecnologias robustas, a solução pretende democratizar o acesso a tecnologias avançadas de segurança para as comunidades mais vulneráveis, muitas vezes desprovidas de recursos para adotar sistemas tradicionais de alto custo. Iremos abranger comunidades de baixa renda e instituições tanto públicas quanto privadas que buscam uma solução segura e econômica para controlar o acesso em suas propriedades imobiliárias. O nome "Sphynx" foi escolhido em referência à raça felina de mesmo nome e ao monumento histórico "Grande Esfinge de Gizé", uma figura mitológica que representava proteção e vigilância no antigo Egito.

2. Fundamentação teórica

Como forma de buscar entender melhor o problema em questão e explorar suas necessidades, uma pesquisa utilizando o método de revisão sistemática. Analisaremos projetos que propuseram soluções semelhantes, além de investigar a urgência no aprimoramento das soluções de segurança utilizando tecnologia no país. Por fim, iremos relacionar os principais pontos identificados com nossa proposta e avaliar sua relevância.

2.1. Revisão Sistemática

“A revisão sistemática é um tipo de investigação científica que tem por objetivo reunir, avaliar e conduzir uma síntese dos resultados de múltiplos estudos primários” (Cordeiro et al., 2007, p. 2). Utilizando métodos sistemáticos e explícitos para identificar, selecionar e analisar dados relevantes, uma revisão sistemática exige rigor metodológico para garantir a confiabilidade das conclusões.

Para auxiliar na obtenção e organização dos dados, utilizamos o software StArt (State of the Art through Systematic Review). Este software foi desenvolvido pelo Laboratório de Pesquisa em Engenharia de Software (LaPES) da Universidade Federal de São Carlos (UFSCar) e oferece funcionalidades que tornam o processo de revisão mais eficiente e estruturado. O StArt é uma ferramenta que facilita a condução de revisões sistemáticas ao nos permitir importar e organizar referências bibliográficas, as filtrando de acordo com critérios de inclusão e exclusão predefinidos. Além disso, a ferramenta permite rastrear a evolução das revisões, facilitando a criação de um histórico de buscas e filtrações que tornam o processo mais transparente e rigoroso, garantindo a qualidade e a confiabilidade dos dados obtidos.

Com o StArt, reunimos as referências inicialmente selecionadas, classificamos os estudos relevantes para nossa pesquisa e avaliaremos cada fonte. O software também permite o registro dos dados extraídos e a sumarização das informações obtidas, gerando relatórios que auxiliam na análise dos resultados. Essa funcionalidade contribui para garantir exatidão e organização ao longo de todo o processo de revisão sistemática, auxiliando o desenvolvimento de uma base sólida de evidências para nossa proposta.

2.2. Segurança Pública

De Lima, Minguard, Marques e Carvalho (2024, p. 259) destacam como, em São Paulo, a segurança pública tem se voltado progressivamente para crimes patrimoniais, como furtos e roubos, respondendo a uma percepção crescente de insegurança. Em locais emblemáticos como a Cracolândia, o crime patrimonial e a complexidade social agravam o quadro de insegurança, exigindo soluções que transcendem a abordagem policial tradicional. Já Soares et al. (2024) destacam a violência escolar e as limitações das instituições educacionais em prevenir tais incidentes.

Spaniol, JR e Rodrigues (2020) analisam como a falta de continuidade nas políticas de segurança pública no Brasil prejudica o combate efetivo à criminalidade, destacando a centralização excessiva das políticas e a falta de integração entre os diversos níveis do governo. Essas limitações, incluindo a baixa articulação entre órgãos federais, estaduais e municipais, resultam em políticas desatualizadas e pouco eficazes.

Esse contexto reforça a relevância do Sphynx ao oferecer uma solução de controle de acesso com foco em acessibilidade e prevenção de invasões, roubos e furtos. Projetado para áreas de vulnerabilidade, nosso projeto se alinha à necessidade identificada pelos autores de abordar a segurança de forma integrada, contribuindo para a inclusão de comunidades de baixa renda em soluções tecnológicas que normalmente estariam fora de alcance. Ao possibilitar um controle rígido e em tempo real sobre acessos, atenderemos à demanda por soluções preventivas e não intrusiva, aplicável em residências e ser particularmente útil em escolas, ajudando a minimizar invasões e vandalismo, ao mesmo tempo que rastreia entradas e saídas.

Além disso, a escalabilidade do sistema facilitaria sua adaptação e adoção. Essa independência de um mecanismo de segurança centralizado permite que residências e escolas protagonizem suas próprias medidas de segurança, complementando o papel das políticas públicas com um controle direto e simples.

O artigo Tecnologias na Segurança Pública: prospecção sobre o uso de inteligências artificiais e outros dispositivos (De Lima et al., 2020) explora a aplicação de Inteligência Artificial (IA) e Internet das Coisas (IoT) na segurança pública. A utilização de IA e RFID, como discutido, confirma o potencial que nosso projeto possui ao adotar tais tecnologias para realizar o controle eficaz, além da tecnologia de reconhecimento facial, que pode ser integrada em solução utilizando Edge AI, como explicado por

Singh e Gill (2023), aproveitando os recursos IoT de forma otimizada e padronizada. Além disso, preocupação com a privacidade e a regulamentação de dados discutidas são essenciais para a implementação responsável de um sistema que lida com informações sensíveis, destacando a importância da criptografia, um ponto chave para qualquer sistema de segurança.

2.3. Tecnologias de controle de acesso

Os estudos sobre o uso de RFID para controle de acesso em escolas (Zagonel; Machado; Mônico, 2017) e desenvolvimento, implantação e acompanhamento de sistema de controle de acesso em escola pública (Santiago; Sousa; Oliveira, 2020) oferecem observações práticas para a proposta do Sphynx, especialmente em ambientes de grande circulação. A tecnologia RFID permite o monitoramento eficiente de entradas e saídas, sendo um ponto crucial para sistemas de controle de acesso, onde a automação do controle e a minimização de erros humanos são objetivos centrais. O uso de leitores RFID para acompanhamento em tempo real e o armazenamento dos dados de frequência em banco de dados são práticas relevantes para simplificar e agilizar o controle de entrada e saída, garantindo uma experiência segura e integrada para o usuário final. A pesquisa de Zagonel, Machado e Mônico também destacam as limitações dos leitores RFID, pontos que podem ser melhorados na proposta do Sphynx ao considerar tecnologias de biometria como módulos complementares para garantir uma cobertura de monitoramento robusta.

A aplicação de fechaduras inteligentes utilizando IoT em cacifos universitários (Margarho, 2019) exemplifica o uso de tecnologia de controle de acesso em espaços altamente compartimentados. A implementação usa fechaduras inteligentes que também aproveitam a tecnologia NFC, ao permitir o uso do smartphone para autenticação. O artigo também sugere o uso de protocolos de autorização seguros, como o OAuth 2.0, uma medida importante para garantir a proteção de dados dos usuários e a segurança nas transações de entre o dispositivo, interface web final do usuário e API (Application Programming Interface) do sistema, reforçando a conformidade com a LGPD (Lei Geral de Proteção de Dados).

O reconhecimento da rotina escolar e a análise dos processos internos propostos por Santiago, Sousa e Oliveira (2020) se demonstra particularmente interessante para sistemas customizados e escaláveis. A melhoria na segurança e controle de fluxo, além da geração de relatórios estatísticos, é uma característica desejável para o Sphynx, que também visa oferecer dados precisos para a tomada de decisão.

Peixer (2023, p. 9) destaca o RFID como uma solução econômica para controle de acesso, confirmando que a base do projeto é uma alternativa viável para o público que pretendemos atingir. O sucesso do protótipo como solução prática e eficiente reafirma a viabilidade do uso, junto a microcontroladores como o ESP32, que pretendemos utilizar. A discussão sobre tecnologias de controle de acesso e a importância do protocolo MQTT (Message Queuing Telemetry Transport) para IoT pode ser relevante para a arquitetura do Sphynx, permitindo comunicação eficiente em ambientes diversos.

2.4. Sistema e Usabilidade

A ênfase em usabilidade para melhorar a experiência do usuário é crítica para o Sphynx, que deve garantir que sua interface seja intuitiva e fácil de usar, pois pretende atingir diversos públicos de diferentes faixas etárias e habilidades tecnológicas. A adaptação das heurísticas de Nielsen para o contexto da Web, utilizada por Maciel et al. (2004) poderia ser utilizada no Sphynx para identificar e corrigir problemas de usabilidade na interface do usuário. Complementar a Avaliação Heurística com outros métodos pode ser um ponto a considerar futuramente, durante a implementação, garantindo que a experiência do usuário seja constantemente aprimorada.

O foco na usabilidade do sistema Visit Card (Martins; Lima, 2019) para controle de acesso pode fornecer ideias valiosas, especialmente na criação de uma interface que maximize a facilidade de uso

e segurança. A avaliação de diferentes heurísticas, como "Estética e Design Minimalista", indica que devemos priorizar uma interface visualmente agradável, facilitando a interação do usuário.

A combinação de análises qualitativas e quantitativas propostas pelos autores pode ser uma abordagem eficaz para avaliar a aceitação do Sphynx entre usuários finais, garantindo que todas as necessidades sejam atendidas.

O sistema de segurança residencial integrado ao controle via smartphone proposto por VOLPATO, L. (2012) oferece exemplos práticos de usabilidade e interação usuário-dispositivo que são aplicáveis ao Sphynx. Ao facilitar o controle de acesso remoto por um aplicativo, o autor evidencia como uma interface intuitiva pode elevar a eficácia do sistema de segurança, garantindo acessibilidade e rapidez no gerenciamento das ocorrências. Essa perspectiva reforça a nossa proposta de incorporar uma interface amigável, fornecendo uma navegação simples para o usuário e uma comunicação eficiente com o sistema e hardware.

As notificações e alertas propostas por VOLPATO também são relevantes, pois permitem que o usuário esteja sempre ciente de todas as tentativas de acesso.

3. Método

3.1. Revisão Sistemática

Para pesquisa e revisão sistemática, utilizamos o software StArt mencionado anteriormente, com ele conseguimos selecionar, classificar e avaliar os estudos selecionados, possibilitando a obtenção de resultados satisfatórios. A plataforma foi utilizada para encontrar diversos artigos onde os autores propuseram soluções semelhantes e destrincharam o tema de forma aprofundada, de forma que, ao analisarmos, pudéssemos desenvolver uma ideia mais crítica e assertiva ao redor da solução.

3.2. Software e Sistema

Após pesquisarmos e nos aprofundarmos no tema e problema, iniciamos o desenvolvimento da solução. Utilizamos tecnologias de controle de acesso como bancos de dados e sistemas embarcados. O servidor será configurado para atender requisições HTTP (Hypertext Transfer Protocol), garantindo a comunicação entre os dispositivos. O sistema empregará microcontroladores ESP32, sensores de RFID e cabos Jumpers para monitoramento e controle de acesso. As linguagens de programação C++, Javascript e Java serão usadas para o firmware do microcontrolador, o servidor web e o software de integração, respectivamente.

Quanto aos módulos adicionais, para o reconhecimento facial utilizamos tecnologias como a linguagem de programação Python para adotar modelos e técnicas de machine learning utilizando DLib e Google Mediapipe para garantir a precisão, praticidade e otimização do sistema, de modo que ele possa ser executado em qualquer dispositivo atual. O módulo de impressão digital será integrado ao código em C++ do dispositivo embarcado como uma biblioteca adicional que oferecerá suporte a componentes populares como SFM v1.7 e HLK-ZW101, buscando integrar as informações ao banco de dados. Além disso, Técnicas de criptografia como Fernet e AES serão utilizadas para garantir a segurança dos dados de todos os usuários.

4. Resultados e Discussões

4.1. Resultados da Revisão Sistemática

A partir da revisão sistemática conduzida na plataforma StArt, foi possível gerar uma nuvem de palavras-chave para ajudar na identificação dos pontos centrais do projeto. Esta visualização nos deu um parâmetro para compreendermos melhor os aspectos mais importantes da pesquisa realizada.

Com isso, adquirimos uma visão mais abrangente do problema e ideias de aprimoramento para a solução.

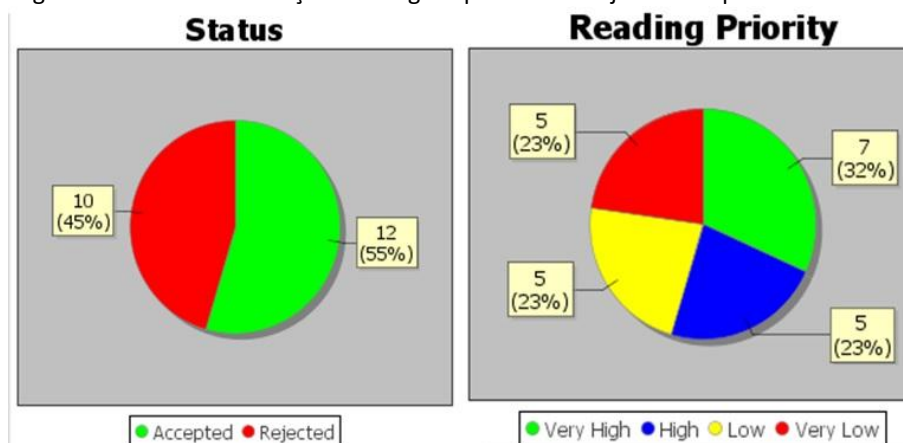
Figura 1 – Nuvem de palavras



Fonte: StArt (2024)

O software também possibilitou organizar os estudos selecionados de acordo com a prioridade, os classificando em níveis que vão desde baixíssima prioridade a altíssima prioridade. Por fim, a ferramenta gerou relatórios indicando os percentuais de aprovação e rejeição na seleção manual de artigos, assim como os mais importantes para a continuidade da pesquisa. Esse recurso foi essencial para focar nos estudos mais relevantes para o avanço da pesquisa, pois nos permitiu organizar de forma aprimorada a pesquisa por temas de relevância.

Figura 2 – Gráficos de relação de artigos aprovados e rejeitados e prioridade leitura



Fonte: StArt (2024)

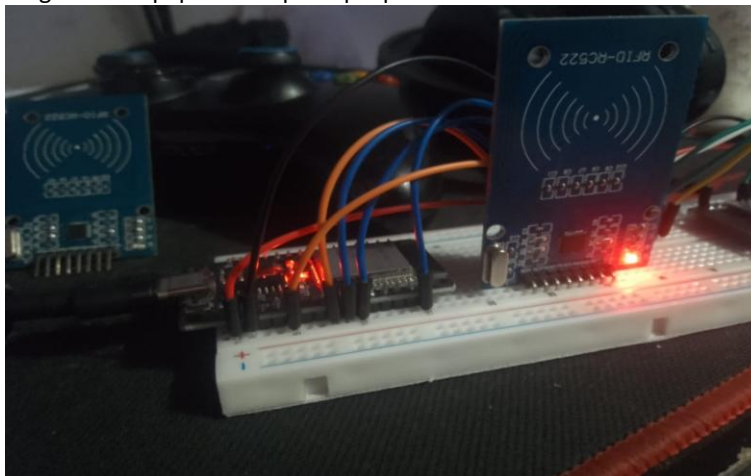
4.2. Sistema

O sistema principal do projeto consiste em uma API escrita em Java, integrada ao dispositivo que utiliza o SoC ESP32. Inicialmente, foi implementado o código em C++ para o dispositivo, possibilitando o desenvolvimento de um sistema similar aos encontrados em dispositivos automatizados para casas inteligentes, como lâmpadas. Esse sistema conta com uma lógica de gerenciamento de redes Wi-Fi, acessível enquanto o dispositivo está em modo de pareamento, permitindo o usuário gerenciar as redes salvas, definindo senhas e prioridade de conexão. Assim, ele tenta automaticamente se conectar a redes salvas, caso estejam disponíveis, otimizando a conexão e comunicação com outros dispositivos de forma integrada.

Em seguida, foi implementada a lógica de controle de acesso utilizando RFID, com o módulo RC522 e cartões MiFare. O dispositivo lê os dados do cartão, os encapsula em um objeto JSON, juntamente com as informações da rede, e os envia para a API Java, que processará esses dados, verificando se são válidos, e, se as informações cadastradas do cartão, juntamente com as do usuário, possuem permissão para acessar o local especificado. Além disso, há um modo de “Cadastro de TAG” acessível via website,

onde o administrador do sistema pode selecionar qualquer dispositivo registrado no sistema para cadastrar novos cartões e dispositivos NFC para os usuários.

Figura 3 – Equipamento principal para controle de acesso com RFID



Fonte: Elaborado pelos autores (2024)

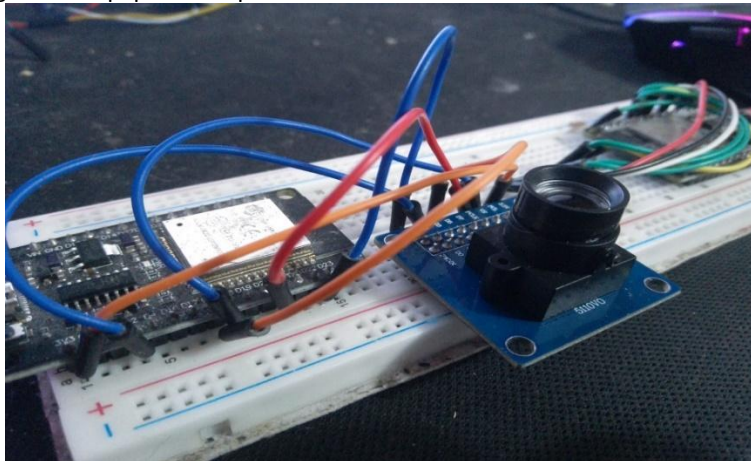
A API, desenvolvida em Java usando o framework Spring Boot, centraliza toda a lógica de monitoramento e controle. Por meio de endpoints (endereços de serviço acessíveis via HTTP), permite o cadastro de usuários, grupos de usuários e locais (dispositivos com ESP32), além de realizar o gerenciamento automático e em tempo real das tentativas de acesso. O sistema de grupos segue uma lógica básica de permissões, permitindo relações de muitos-para-um entre grupos e usuários e de muitos-para-muitos entre locais e grupos, promovendo personalização e escalabilidade nas permissões para os diferentes locais cadastrados.

Foi também desenvolvida uma segunda API, em Node.js, com o objetivo de monitorar e varrer a rede em busca de novos dispositivos. Essa API filtra os dispositivos usando requisições HTTP com websockets e notifica a API principal.

4.3. Reconhecimento Facial

O sistema de reconhecimento facial, desenvolvido em Python, se tornou uma outra API para o projeto, utilizando o framework Flask para facilitar a comunicação com os dispositivos e website. A aplicação realiza um mapeamento do rosto do usuário e armazena um registro criptografado dos dados biométricos, utilizando o método Fernet. O usuário pode conectar uma câmera IP via rede local (padrão com o módulo OV7670 junto ao ESP32) ou utilizar uma câmera própria, como uma webcam.

Figura 4 – Equipamento para controle de acesso com reconhecimento facial



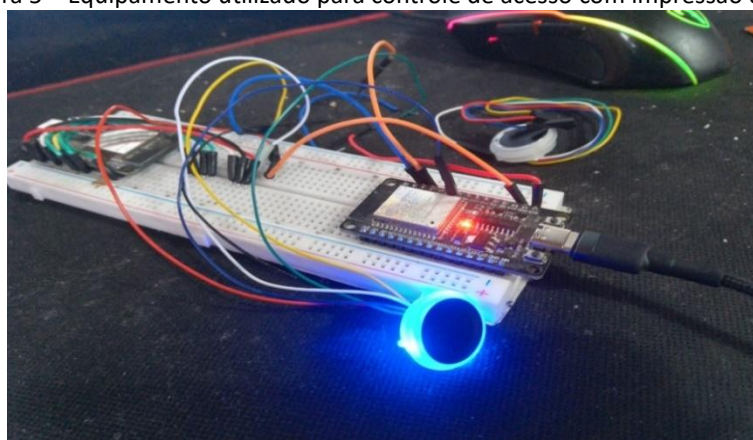
Fonte: Elaborado pelos autores (2024)

Ao iniciar, o sistema de reconhecimento facial busca rostos a cada 5 segundos e, ao encontrar um, realiza rapidamente o mapeamento e compara com os dados cadastrados, retornando um resultado positivo ou negativo. As bibliotecas Google MediaPipe, OpenCV e DLib foram essenciais para o desenvolvimento, permitindo uma solução de baixa demanda computacional, rápida e eficiente, onde a verificação facial ocorre em menos de um segundo.

4.4. Impressão Digital

O módulo de impressão digital foi separado em uma biblioteca externa ao sistema principal embarcado. Testamos os módulos SFM v1.7 e HLK-ZW101 para leitura biométrica, ambos demonstrando excelente desempenho, mesmo com baixo custo. Na interface web, o usuário pode ativar o modo de cadastro, inserindo o dedo no leitor algumas vezes para o mapeamento completo da biometria. Similar ao leitor RFID, o módulo de impressão digital coleta e encapsula os dados obtidos pelo leitor, enviando-os ao sistema principal em Java para processamento da solicitação de acesso.

Figura 5 – Equipamento utilizado para controle de acesso com impressão digital



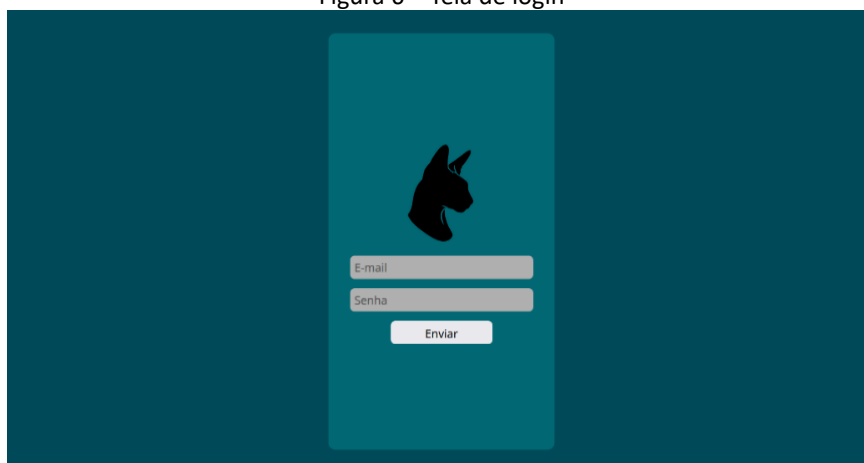
Fonte: Elaborado pelos autores (2024)

4.5. Interface Web

A interface web foi projetada para ser responsiva tanto em desktops quanto em dispositivos móveis, permitindo que o usuário role horizontal e verticalmente para cadastrar, editar e visualizar informações. Inclui também um menu interativo que se expande, exibindo todas as opções de navegação para uso.

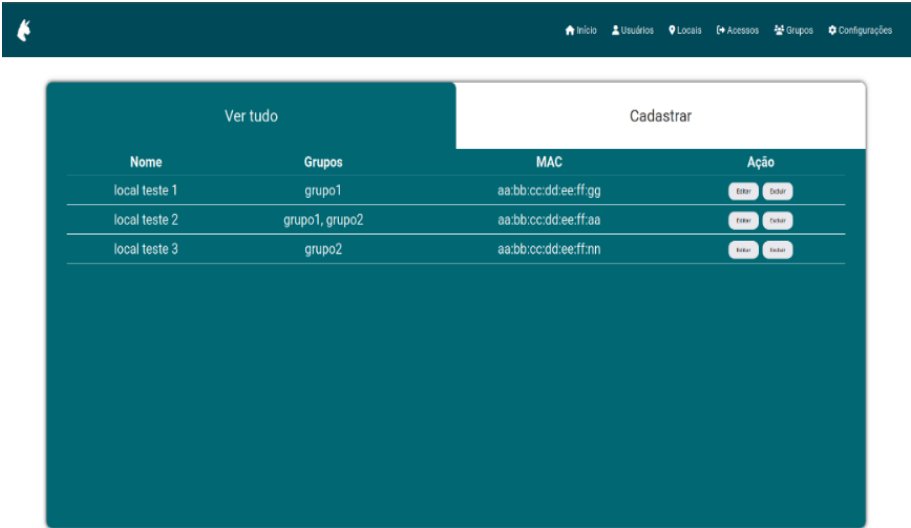
A aplicação web serve como uma interface para uma interação intuitiva entre o usuário e as diversas APIs que o projeto possui, integrando todas as ferramentas em um único software para o usuário.

Figura 6 – Tela de login



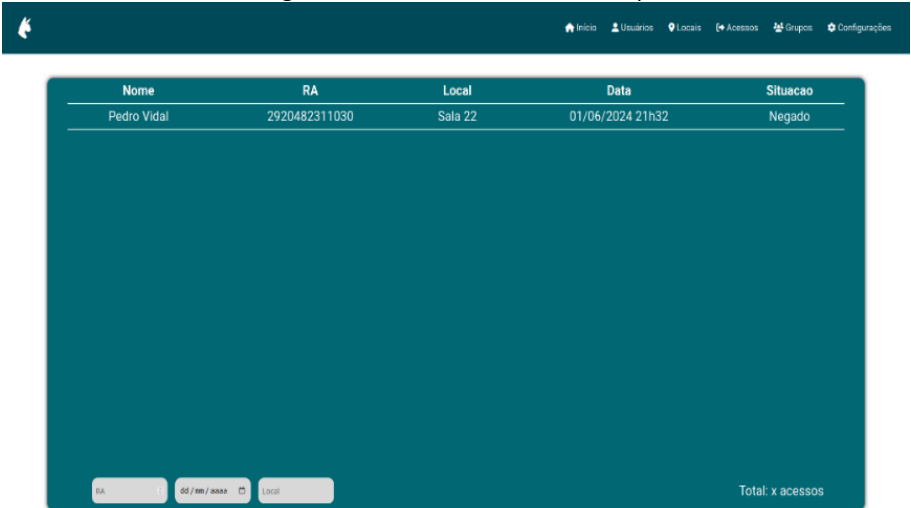
Fonte: Elaborado pelos autores (2024)

Figura 7 – Aba de locais - Desktop



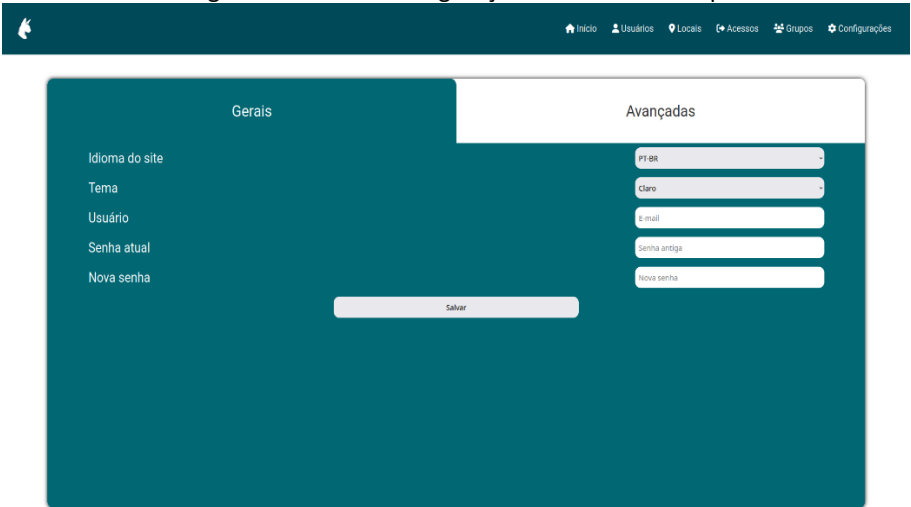
Fonte: Elaborado pelos autores (2024)

Figura 8 – Aba de Acessos - Desktop



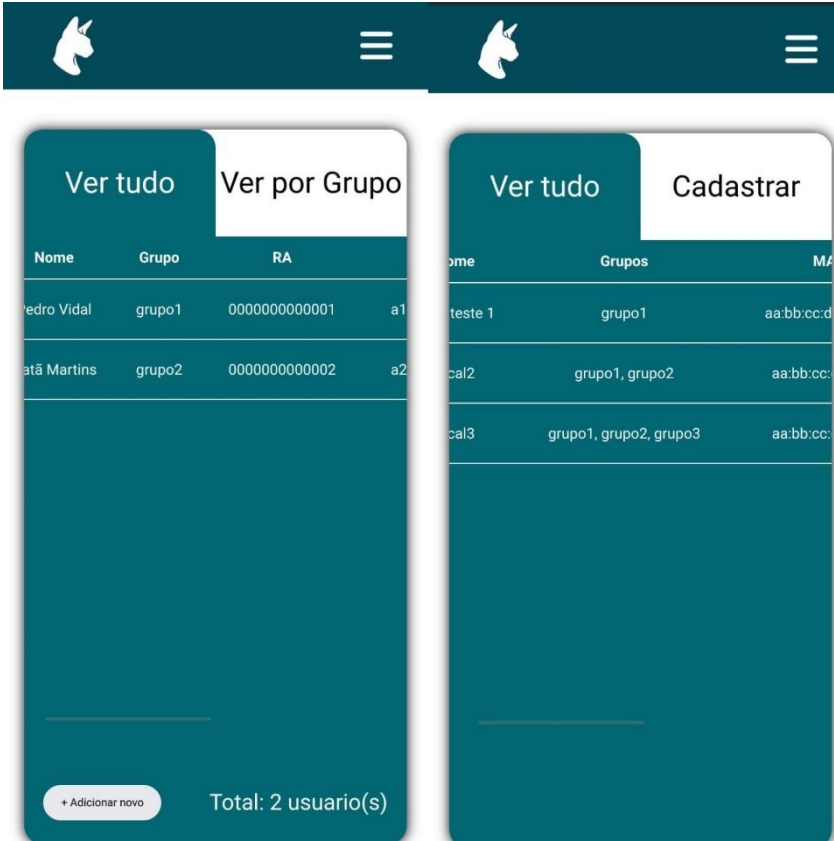
Fonte: Elaborado pelos autores (2024)

Figura 9 – Aba de Configurações Gerais – Desktop



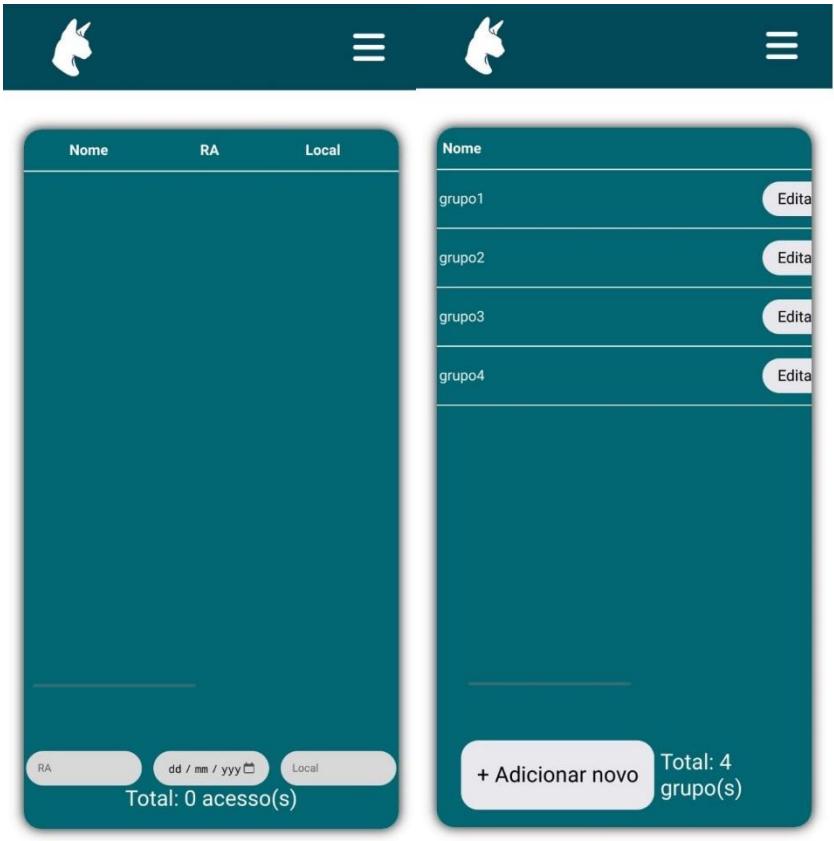
Fonte: Elaborado pelos autores (2024)

Figura 10 – Abas de usuários e locais - Mobile



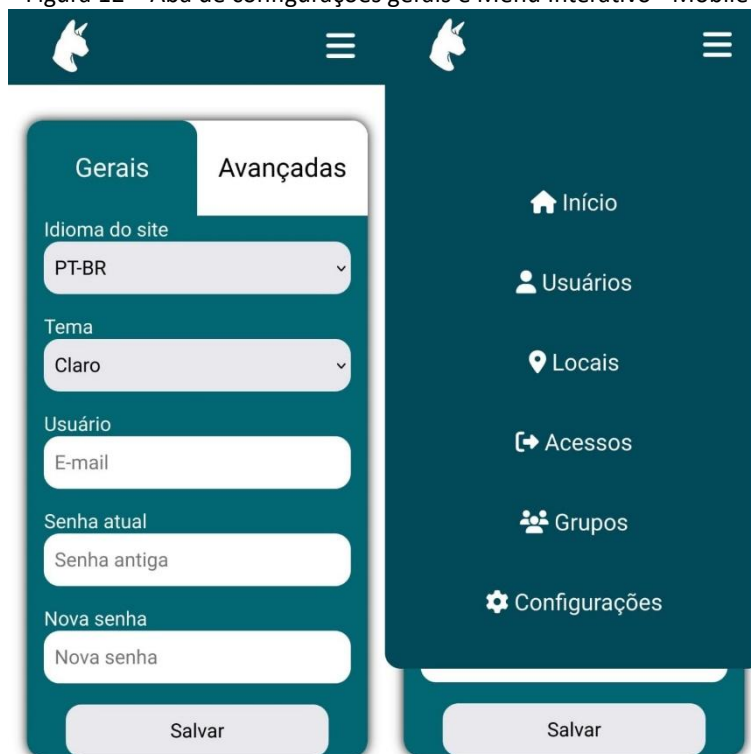
Fonte: Elaborado pelos autores (2024)

Figura 11 – Menu geral – Mobile



Fonte: Elaborado pelos autores (2024)

Figura 12 – Aba de configurações gerais e Menu Interativo - Mobile



Fonte: Elaborado pelos autores (2024)

5. Conclusão

O Projeto Sphynx, em seu estágio atual, se propõe em ser uma solução acessível e escalável para controle de acesso, utilizando tecnologias como RFID, reconhecimento facial e impressão digital integradas ao SoC ESP32. Por mais que esteja funcional e pronto para uso, planejamos melhorias futuras para maximizar o custo-benefício e incorporar tecnologias inovadoras que potencializem o sistema.

A revisão sistemática nos guiou nas escolhas das tecnológicas, garantindo que o Sphynx atenda adequadamente às demandas de segurança de diferentes ambientes. Por meio dela, notamos que ainda há pontos de aprimoramento para implementação em etapas futuras, como a aplicação das heurísticas de Nielsen, conforme sugerido por Maciel et al. (2022), para otimizar a usabilidade e garantir uma interface mais intuitiva. Além disso, pretendemos migrar a interface para a tecnologia React, o que trará maior acessibilidade, inovação e uma experiência unificada em diversas plataformas.

Em etapas futuras, exploraremos tecnologias adicionais, como Edge AI, para integrar o reconhecimento facial e possivelmente implementar o reconhecimento automatizado de comportamento, conforme discutido por Santiago, Sousa e Oliveira (2020), diretamente no dispositivo embarcado, dispensando a necessidade de serviços terceiros. Também estudaremos o uso do protocolo MQTT, conforme sugerido por Peixer (2023), para otimizar a comunicação entre dispositivos e aumentar a eficiência do sistema. Com esses aprimoramentos, o Sphynx estará cada vez mais completo e próximo de oferecer um sistema confiável de controle de acesso e fluxo em diversos contextos, beneficiando a população no geral.

Referências

CORDEIRO, Alexander Magno; OLIVEIRA, Glória Maria de; RENTERÍA, Juan Miguel; GUIMARÃES, Carlos Alberto. **Revisão sistemática: Uma revisão narrativa**. Revista do Colégio Brasileiro de Cirurgiões, Rio de Janeiro, v. 34, n. 6, p. 428-431, nov./dez. 2007. DOI: <https://doi.org/10.1590/S0100-69912007000600012>. Disponível em: <https://www.scielo.br/j/rcbc/a/CC6NRNtP3dKLgLPwcmV6Gf>. Acesso em: 22 de out. 2024.

DE LIMA, E. P. et al. Tecnologias na Segurança Pública: prospecção sobre o uso de inteligências artificiais e outros dispositivos. **Cadernos de Prospecção**, v. 13, n. 5, p. 1367-1367, 2020. DOI:

<https://doi.org/10.9771/cp.v13i5.33058>. Disponível em: <https://periodicos.ufba.br/index.php/nit/article/view/33058>. Acesso em: 23 de out. 2024.

LAPES. **StArt**. Disponível em: <https://www.lapes.ufscar.br/resources/tools-1/start-1>. Acesso em: 21 de outubro de 2024.

LIMA, Renato Sérgio de; MINGUARD, G.; MARQUES, D.; CARVALHO, T. Medo, violência e política na cidade de São Paulo: a quem cabe decifrar a Esfinge da Segurança Pública?. **Estudos Avançados**, v. 38, n. 111, p. 257-283, 2024. DOI: <https://doi.org/10.1590/s0103-4014.202438111.014>. Disponível em: <https://www.scielo.br/j/ea/a/ygJyf9DZfHcTNZ9qBGsMSRQ/>. Acesso em: 22 de out. 2024.

MACIEL, C.; NOGUEIRA, J.; CIUFFO, L. M.; GARCIA, A. C. B. Avaliação heurística de sítios na Web. **VII ESCOLA DE INFORMÁTICA DO SBC-CENTROOESTE**, p. 41, 2004. Disponível em: https://marcelohsantos.com/aulas/include/2022-1/projeto_Interface_Usuario/Aula7_artigo.pdf. Acesso em: 25 de out. 2024

MARGALHO, Raquel Conde. Sistema De Gestão de Fechaduras Inteligentes Usando IoT para Aplicação em Cacifos de Universidade. 2019. **Dissertação de Mestrado**. Disponível em: <https://hdl.handle.net/10316/90178>. Acesso em: 24 de out. 2024.

MARTINS, V. C.; LIMA, D. A. Heurísticas de Nielsen como Forma de Avaliação do Visitcard: Um Sistema de Controle de Fluxo em Condomínios. **Congresso Periódico de Pós-Graduação Workshop em Análise de Desenvolvimento de Sistemas**, 1 jan. 2019. Disponível em: https://www.researchgate.net/profile/Danielli-Lima/publication/362579107_Heurísticas_de_Nielsen_como_Forma_de_Avaliacao_do_Visitcard_Um_Sistema_de_Controlo_de_Fluxo_em_Condominios/links/62f26e7188b83e7320be7c0b/Heurísticas-de-Nielsen-como-Forma-de-Avaliacao-do-Visitcard-Um-Sistema-de-Controlo-de-Fluxo-em-Condominios.pdf. Acesso em: 25 de out. 2024.

PEIXER, F. M. Desenvolvimento de um protótipo de um sistema de controle de acesso via RFID. **UFSC**, 2023. Disponível em: <https://repositorio.ufsc.br/handle/123456789/252983>. Acesso em: 26 de out. 2024.

SANTIAGO, F. A. V.; SOUSA, A. B.; OLIVEIRA, M. L. S. DESENVOLVIMENTO, IMPLANTAÇÃO E ACOMPANHAMENTO DE SISTEMA DE CONTROLE DE ACESSO EM ESCOLA PÚBLICA. **Revista Docentes**, v. 5, n. 11, p. 39–49, 2020. Disponível em: <https://periodicos.seduc.ce.gov.br/revistadocentes/article/view/178>. Acesso em 23 de out. 2024.

SINGH, R; GILL, S. S. Edge AI: A survey. **Internet of Things and Cyber-Physical Systems** 3, United Kingdom, 71-92 (2023), DOI: <https://doi.org/10.1016/j.iotcps.2023.02.004>. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2667345223000196>. Acesso em: 27 de out. de 2024.

SOARES, A. P. A.; BARBOSA, J. R. G. P.; ABREU, E. A. P.; SENNA, A. ANÁLISE DA VIOLÊNCIA ESCOLAR NO BRASIL. **REVISTA ARACÊ**, São José dos Pinhais, v. 6, n.2, p.1162-1182, 2024. DOI: <https://doi.org/10.56238/arev6n2-041>. Disponível em: <https://periodicos.newsciencepubl.com/arace/article/view/693>. Acesso em: 22 de out. 2024

SPANIOL, M. I.; JR, M. C. M.; RODRIGUES, C. R. G. Como tem sido planejada a Segurança Pública no Brasil? Análise dos Planos e Programas Nacionais de Segurança implantados pós-redemocratização. **Revista Brasileira de Segurança Pública**, v. 14, n. 2, p. 100–127, 30 set. 2020. DOI: <https://doi.org/10.31060/rbsp.2020.v14.n2.1035>. Disponível em: <https://revista.forumseguranca.org.br/index.php/rbsp/article/view/1035>. Acesso em: 22 de out. 2024.

VOLPATO, L. Sistema de segurança residencial integrado com aplicativo para smartphone. **Repositório UFSC**. [s.l.] Florianópolis, jul. 2012. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/166363/PFC-20121-LuanCesarSouzaVolpato.pdf?sequence=1&isAllowed=y>. Acesso em: 22 de out. de 2024.

ZAGONEL, M. V.; MACHADO, C. C.; MÔNEGO, C. TECNOLOGIA RFID: UM ESTUDO DE CASO PARA CONTROLE DE ACESSO EM ESCOLAS. **RECeT - Revista de Engenharia, Computação e Tecnologia**, v. 1, n. 1, 2017. Disponível em: <https://revista.forumseguranca.org.br/index.php/rbsp/article/view/1035>. Acesso em: 24 de out. 2024.

“O(s) autor(es) do trabalho declara(m) que durante a preparação do manuscrito foi(foram) utilizado(as) a(s) ferramenta(s)/serviço(s) ChatGPT de Inteligência Artificial (IA) para auxiliar na revisão ortográfica e gramatical do texto desenvolvido. Após utilizar esta ferramenta/serviço, os autores editaram e revisaram o conteúdo conforme necessário e assumem total responsabilidade pelo conteúdo da publicação.”