Capítulo I – CÉSAMO: Aplicativo de gerenciamento de fechaduras inteligentes

Giovane Antônio Garrido Bego [1]
Heitor Almeida Boscariol [2]
Rafael Ribeiro Felix [3]
Camila Fogaça de Oliveira [4]
Daniel Almeida Colombo [5]

RESUMO

O presente artigo apresenta a construção de um aplicativo para gerenciamento de fechaduras inteligentes, levando em consideração a praticidade e a segurança do acesso. O objetivo é proporcionar uma melhor experiência para o usuário, oferecendo comodidade e praticidade sem comprometer a segurança. É realizado um levantamento de tecnologias e ferramentas que serão utilizadas para o desenvolvimeno do aplicativo e dentre elas podemos citar Internet das coisas, bluetooth, wi-fi, linguagem Java, autenticação Single Sign On com Oauth 2.0, Figma para prototipação, SQLite para banco de dados local. Apresenta-se nesse artigo o protótipo do artefato que possibilitará acesso remoto a fechaduras inteligentes e criações de grupos de acesso à ferramenta.

Palavras-chave: Aplicativo, fechadura inteligente, segurança, Internet das coisas.

CÉSAMO – Smart lock management application

ABSTRACT

This article presents the development of an application for managing smart locks, taking into consideration convenience and access security. The objective is to provide a better user experience by offering convenience and practicality without compromising security. A survey of technologies and tools that will be used for the development of the application is carried out, including Internet of Things, Bluetooth, Wi-Fi, Java language, Single Sign-On authentication with OAuth 2.0, Figma for prototyping, SQLite for the local database. This article presents the prototype of the artifact that will enable remote access to smart locks and the creation of access groups for the tool.

[1] Estudante UniSenaiPR - Campus Londrina, giovanebego@outlook.com
[2] Estudante UniSenaiPR - Campus Londrina, heitorbosc@gmail.com
[3] Estudante UniSenaiPR - Campus Londrina, rafaelfelix.cod@gmail.com
[4] Docente UniSenaiPR - Campus Londrina, camila.oliveira@sistemafiep.org.br
[5] Docente UniSenaiPR - Campus Londrina, daniel.colombo@sistemafiep.org.br

Keywords: Application, smart lock, security, Internet of Things.

1 INTRODUÇÃO

Com os avanços na área de tecnologias inteligentes nos últimos anos várias soluções inovadoras envolvendo softwares vêm surgindo no âmbito de facilitar o gerenciamento de dispositivos. Dentre os vários dispositivos envolvendo essas tecnologias encontramos as fechaduras inteligentes.

Através de aplicativos de controle de fechaduras inteligentes o usuário pode abrir sua fechadura remotamente de maneira segura e prática bem como controlar os acessos de usuários terceiros ao dispositivo.

O desafio para o gerenciamento de fechaduras inteligentes é unir a praticidade com a segurança ao acesso, o aplicativo precisa ser intuitivo, porém precisa ser arquitetado de forma segura para que o usuário extraia a melhor experiência ao utilizar. Nesse relatório trazemos como se dará a construção do nosso aplicativo de acordo com os requisitos levantados e quais as tecnologias que utilizaremos nesse processo.

Acreditamos que um aplicativo para fechaduras inteligentes construído de forma segura pode facilitar e trazer vários benefícios à vida do usuário impactando positivamente o cotidiano proporcionando comodidade e praticidade nunca deixando de lado o fator segurança crucial para esse tipo de aplicação.

2 REFERENCIAL TEÓRICO

2.1 Dispositivos Móveis - *Android*

O Android é um sistema operacional voltado para dispositivos móveis, baseado em Linux (DEVELOPERS, 2011). O sistema oferece várias bibliotecas em C/C++ usadas por vários componentes e acesso ao seu Framework para simplificar a reutilização de componentes (DEVELOPERS, 2011). Entre as vantagens do Android está a possibilidade de modificações profundas no sistema, notificações rápidas de SMS, multitarefa e recomendação de desenvolvedores (ADEKOTUJO et al., 2020). Contudo, sua característica de

código aberto torna o Android propenso a ataques e capaz de executar programas nocivos no dispositivo, além da grande maioria dos aplicativos requerer acesso à internet para funcionar (ADEKOTUJO et al., 2020). A Google fornece suporte para o sistema operacional e atualizações de grande porte são disponibilizadas a cada seis ou doze meses (DEVELOPERS, 2011).

2.2 Internet das coisas (Internet Of Things - IOT)

IoT é um novo avanço que lidera a indústria da tecnologia para uma nova revolução industrial, a “Indústria 4.0” (GAZIS, 2021).

Não há uma definição única disponível para IoT que seja aceitável, inclusive há variados e distintos grupos que dominaram o termo, que tende a ser definido como: “Uma rede aberta e compreensível de objetos que tem a capacidade de se auto-organizar, compartilhar informação, dados e recursos, agindo e reagindo com as situações e mudanças no ambiente.” (MADAKAM, RAMASWAMY, TRIPATHI 2015).

Adicionalmente, a Internet das Coisas (IoT) pode ser empregada como uma ferramenta para ajudar as empresas a atingir a "transformação digital". Esse conceito refere-se à necessidade de reduzir os pontos de contato ao longo do fluxo de operações de negócios, visando diminuir o tempo e o custo de entrega. Em geral, essa meta é alcançada por meio da adoção de serviços em nuvem para substituir processos de negócios e pela substituição de aplicativos monolíticos por sistemas mais inteligentes (GAZIS, 2021).

2.3 Tecnologias e conceitos utilizados

2.3.1 ESP WROOM 32

O ESP WROOM 32 é um microcontrolador de baixo custo fabricado pela empresa chinesa Espressif Systems (MIRANDA, 2019).

Esse dispositivo possui Bluetooth e Wi-fi integrados e foi lançado em 2016 com uma produção em larga escala já disponibilizada no mesmo ano. Esse modelo é um dos mais robustos e notórios do mercado tendo características que trazem um diferencial para seu uso como o tamanho compacto e sua conexão com a internet (NETO, COSTA, 2022).

Por esses motivos esse tipo de modelo de microcontrolador se torna bastante atrativo para projetos que envolvam internet das coisas pela facilidade no acesso remoto e possibilidade de realizar diferentes tarefas (NETO, COSTA, 2022).

2.3.2 Bluetooth

O Bluetooth é uma tecnologia muito importante quando observamos o cenário de comunicações sem fio em IoT. Desenvolvida na Suécia em 1994 pela empresa de telecomunicações Ericsson, é amplamente utilizada pela sua facilidade de aplicação e praticidade (LONZETTA et. al., 2018).

É uma tecnologia de comunicação que é capaz de realizar uma troca de dados a certas distâncias (de 0,5m a 100m dependendo do modelo). Usando ondas de rádio de baixa frequência podendo emitir e receber informações (GAIKWAD, KALSHETTY, 2015).

Atualmente o Bluetooth está presente nos mais variados aparelhos do nosso dia a dia como celulares, computadores, fones de ouvido, teclados, brinquedos e é também utilizado em sistemas de casa inteligente podendo controlar luzes, termostatos, televisões e até fechaduras inteligentes (LONZETTA et. al., 2018).

2.3.3 Wi-fi

O termo Wi-fi vem do inglês “Wireless Fidelity” ou "Fidelidade sem fio". Esse tipo de tecnologia permite aparelhos se comunicarem e trocar informações sem a necessidade de cabos. A tecnologia wi-fi é amplamente utilizada em casas, escritórios e mais variados estabelecimentos (YINAN, SHUGUO, DAWEI, 2012).

Esse tipo de tecnologia é baseado no protocolo IEEE 802.11 e é bastante popular podendo oferecer os mais variados tipos de serviços por sua alta capacidade de transferência de dados (KAUSHIK, 2012).

As aplicações do Wi-fi são muito flexíveis e eficientes podendo conectar diversos aparelhos a uma rede e podendo se conectar com qualquer aparelho que esteja conectado à internet, tornando o uso da tecnologia uma poderosa ferramenta (YINAN, SHUGUO, DAWEI, 2012).

2.3.4 Autenticação com Single Sign-On (SSO)

As infraestruturas de autenticação são cada vez mais comuns nas aplicações atualmente. Esse tipo de sistema facilita implementações e as torna menos custosas se formos considerar que desse modo não é necessário o desenvolvimento de um sistema de autenticação próprio para cada novo produto criado (De CLERCQ, 2022).

O Sistema de autenticação por Single Sign-On ou SSO permite o usuário realizar o login em uma aplicação e utilizar essa autenticação para acessar diversos outros sistemas sem a necessidade de estabelecer vários usuários e senhas para cada aplicação. Esse tipo de autenticação facilita o acesso e experiência do usuário (MICULAN, URBAN, 2011).

A utilização desse tipo de sistema de autenticação também terceiriza o risco do gerenciamento e criptografia de senhas, pois elas não serão guardadas na aplicação que utiliza o modelo de acesso por SSO, mas sim onde o usuário tem seu usuário e senha registrados (De CLERCQ, 2022).

2.4 Ferramentas de desenvolvimento

2.4.1 Android Studio

Android Studio é a ferramenta oficial de desenvolvimento para aplicações em Android. Essa IDE (Integrated Development Environment) é baseada na IntelliJ IDEA da JetBrains. A ferramenta é disponibilizada gratuitamente para desenvolvedores sob a licença Apache 2.0. (ANDROID, 2023).

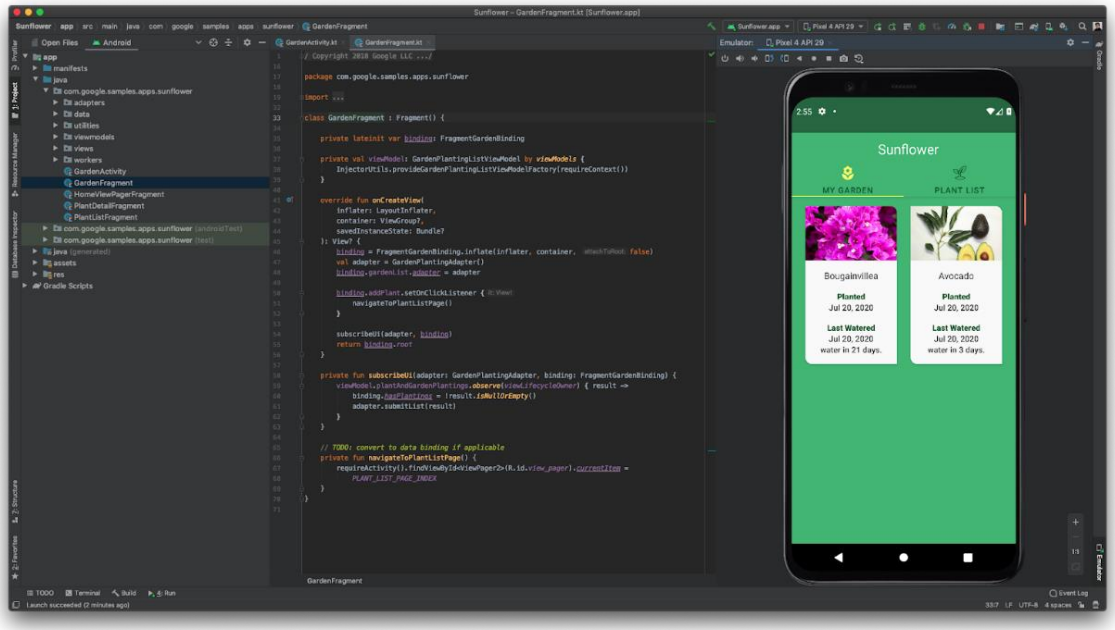
A IDE possui várias facilidades para o desenvolvedor criar e testar a sua solução, ela conta com ferramentas para emular uma aplicação incluindo escolha de diversos dispositivos, podendo assim ser testada a portabilidade e como o aplicativo será exibido em vários aparelhos como tablets, celulares e computadores (ANDROID, 2023).

A IDE já vem com diversos templates prontos o que torna a inicialização de projetos mais rápida e prática. O Android Studio possui também diversas integrações com outras aplicações como o GitHub o que facilita o monitoramento

do versionamento do código e possibilita a programação em grupo (ANDROID, 2023).

Na Figura 1 podemos observar uma tela da aplicação emulando um código que pode ser editado e suas alterações refletidas em tempo real para o desenvolvedor.

Figura 1 - Android Studio emulando um código.



Fonte: ANDROID, 2023.

2.4.2 Github

O GitHub é uma plataforma de hospedagem de código-fonte e colaboração para desenvolvimento de software amplamente utilizada por desenvolvedores. Ele permite criar e gerenciar repositórios de código-fonte, controlar versões de código, colaborar em equipe, rastrear problemas e integrar ferramentas de integração contínua para garantir a qualidade do código. Além disso, a comunidade ativa e os projetos de código aberto hospedados na plataforma fornecem aos desenvolvedores a oportunidade de contribuir e compartilhar conhecimentos (JOSEPH, MARGARET-ANNE, ALEXEY, 2016).

Figura 2 – Tabela de termos resumidos da ferramenta GitHub

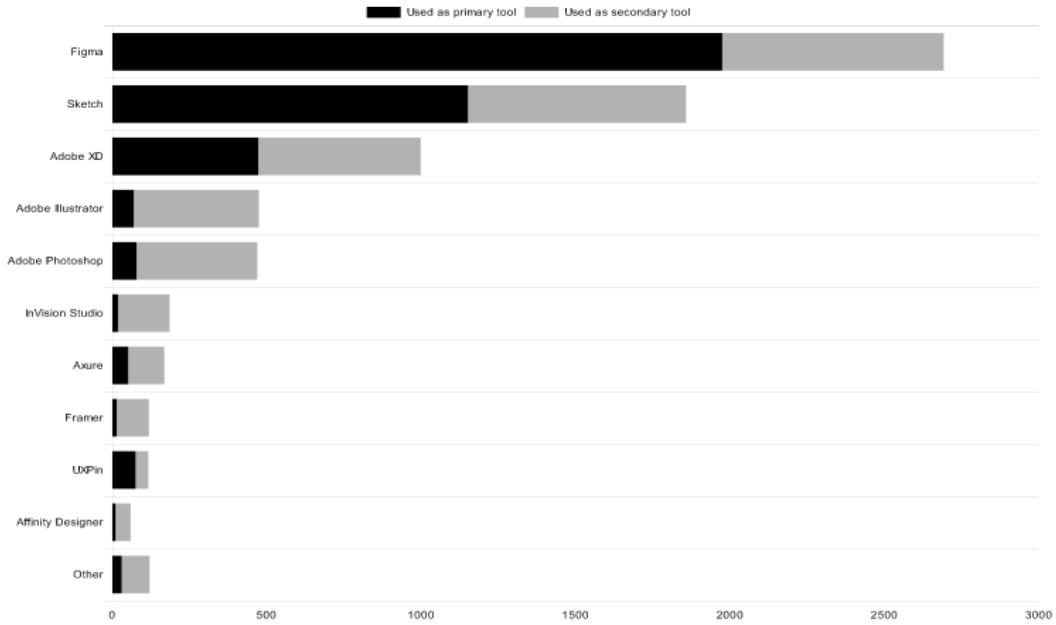
Tópico	Resumo
Repositórios	Coleções de arquivos e pastas que compõem um projeto de software, usados para versionar e gerenciar o código-fonte de um projeto, permitindo rastrear alterações, colaborar em diferentes ramos de desenvolvimento e reverter alterações indesejadas, se necessário.
Controle de versão	O GitHub é baseado em um sistema de controle de versão distribuído chamado Git, que permite a várias pessoas trabalhar em um projeto colaborativamente, mantendo um histórico detalhado de todas as alterações no código-fonte, possibilitando a coordenação de mudanças e a revisão de código eficiente.
Colaboração em equipe	Recursos avançados para colaboração em equipe, como criação de branches para diferentes recursos ou correções de bugs, capacidade de mesclar mudanças de volta ao branch principal do projeto após revisão e aprovação, atribuição de tarefas a membros da equipe para facilitar a coordenação de esforços.
Rastreamento de problemas	Sistema de rastreamento de problemas (issues) permite registrar e acompanhar problemas, bugs ou solicitações de recursos relacionados a um projeto, facilitando a comunicação entre a equipe de desenvolvimento e os usuários ou contribuidores do projeto, permitindo a discussão e a resolução de problemas estruturadamente.
Integração contínua	O GitHub é frequentemente integrado a ferramentas de integração contínua, automatizando a construção, teste e implantação de código. Isso permite que a equipe de desenvolvimento verifique continuamente a qualidade do código e detecte problemas de forma rápida, garantindo a estabilidade do projeto.
Comunidade e código aberto	O GitHub é conhecido por sua comunidade ativa e abundância de projetos de código aberto, permitindo que os desenvolvedores acessem uma ampla gama de projetos, contribuam para eles e compartilhem seu próprio código com outros desenvolvedores em todo o mundo.

Fonte: GITHUB, 2023.

2.4.3 Figma

O Figma é um programa de design de aplicações ou sites que se encaixam nos padrões UX, é um “placeholder” do que será sua aplicação no futuro. Nele é possível ajustar todos os mínimos detalhes e criar algo da forma que o desenvolvedor desejar. Em uma pesquisa feita pela equipe do UXTools em 2020, o Figma foi a ferramenta preferida por usuários para a realização de interfaces de design (figura 3). Podendo customizar desde resoluções de telas de variados dispositivos, até mesmo uma pequena demonstração de como o site ou aplicação funcionaria.

Figura 3 - gráfico de preferência do mercado



2.5 Pesquisa de produtos similares no mercado

2.5.1 Produtos similares da empresa

Durante uma busca de **Fechadura Digital Inteligente** da marca **"Pado"** localizamos os diversos modelos relacionados a busca desejada, porém, os modelos escolhidos para análise, foram, ("**FDE-600W**" e "**FDE-300W**"), sendo os modelos mais completos da marca, com diversas características relacionadas a funcionalidades como, por exemplo: integração com Alexa, opções de autenticação diversas, aplicativo móvel disponível para Android e IOS, resistente a aguá, função não perturbe, compartilhamento de senha temporária, gerenciar os dispositivos via App, conexão via Wifi utilizando um gateway, conexão via Bluetooth e gerenciamento de um ou mais dispositivos através do App.

O aplicativo "Pado Digital Locking" foi localizado na plataforma "Google Play" e ele foi analisado por meio de uma engenharia reversa do APK, assim identificando ser possível adicionar diversos dispositivos para o mesmo usuário e gerenciá-los pelo aplicativo, é possível abrir e fechar a porta através do App remotamente, a autenticação pode ser feita no App a distância ou diretamente na fechadura, criação de senhas temporárias.

2.5.2 Produtos similares no mercado

Com base na pesquisa de mercado feita com foco em apenas uma empresa, foi feita uma segunda pesquisa visando localizar produtos do mesmo segmento, porém, de outras marcas, mas com o mesmo padrão de tecnologia e qualidade, localizamos alguns modelos de diversas marcas como (“ **IFR 3000+ e IFR 7000+**”) da marca “**IntelBras”**, onde localizamos uma diferença em questões de tecnologia, ambos modelos das fechaduras smart fazem parte do ecossistema IZY de casa inteligente da Intelbras, você conta com a fechadura + hub de automação smart, para deixar sua casa ainda mais moderna e conectada.

O aplicativo Izy Smart (anteriormente Izy Home) foi desenvolvido para que você possa controlar todos os seus produtos Smart Home da Intelbras de onde estiver, com somente um aplicativo, da maneira mais fácil.

Na Figura 4 temos um comparativo entre os modelos de fechaduras smart com valores e características de cada produto.

Figura 4 – Tabela comparativa de modelos de fechaduras smart

Marca/Modelo	Tipos de Autenticação	Conexão	App	Tela de Toque	Resistência a Água	Quantidade Máxima de Usuários	Preço Aproximado
Yale YMF 40	Senha numérica, chave mecânica	N/A	N/A	Sim	Não	20 senhas e 20 cartões RFID	R$ 5.300,00
Samsung SHS-P718	Senha numérica, cartão RFID, chave mecânica	N/A	N/A	Sim	Não	30 senhas e 70 cartões RFID	R$ 4.387,95
Advance Milre 7800	Senha numérica, cartão RFID, chave mecânica	N/A	N/A	Não	Sim, IPX7	100 senhas e 100 cartões RFID	R$ 1.675,00
Intelbras FR 300 D	Senha numérica, chave mecânica	N/A	N/A	Não	Sim, IP65	4 senhas e 50 cartões RFID	R$ 2.070,05
Yale YDM 4109 RL	Senha numérica, cartão RFID, chave mecânica	Wi-Fi	Sim	Sim	Não	20 senhas e 20 cartões RFID	R$ 3.011,45
G-Locks Vitro 50	Senha numérica, cartão RFID, chave mecânica	Wi-Fi, Bluetooth	Sim	Sim	Sim, IP65	100 senhas e 100 cartões RFID	R$ 1.519,05
FDE-600W	Senha numérica, cartão RFID, chave mecânica	Wi-Fi	Sim	Sim	Sim, IP65	200 senhas e 200 cartões RFID	R$ 3.096,24
FDE-300W	Senha numérica, cartão RFID, chave mecânica	Wi-Fi	Sim	Sim	Sim, IP65	200 senhas e 200 cartões RFID	R$ 2.101,92
IFR 3000+	Senha numérica, cartão RFID, chave mecânica	N/A	N/A	Não	Não	100 senhas e 100 cartões RFID	R$ 1.049,00
IFR 7000+	Senha numérica, cartão RFID, impressão digital, chave mecânica	Wi-Fi	Sim	Sim	Não	100 senhas e 100 cartões RFID	R$ 2.189,00

3 METODOLOGIA

O desenvolvimento do protótipo foi planejado no primeiro semestre de 2023 e conduzido no segundo semestre. A metodologia adotada foi a metodologia Agile com sprints de 15 dias, realizando encontros semanais e entregas quinzenais.

O esboço e prototipação foi feito pelo Figma pelo fato de já termos familiaridade com a plataforma devido aos trabalhos da jornada de outros anos no decorrer do curso.

O aplicativo foi desenvolvido em Java, utilizando o Android Studio como IDE pela facilidade de emular dispositivos móveis na ferramenta, todo o desenvolvimento e versionamento do projeto foi registrado na plataforma GitHub pelo seu fácil manuseio e familiaridade dos integrantes.

O hardware em que a implementação do app foi testada foi um ESP modelo WROOM 32. O microcontrolador traz as opções de conexão via WiFi e Bluetooth e a simulação da abertura da fechadura foi sinalizada por um led instalado na placa que acende e apaga quando se é enviado o comando de “Abrir” e “Fechar”.

3.1 Principais requisitos e limitações

A partir do documento inicial da jornada e de informações extraídas do nosso contato com a Pado em uma visita ao SENAI realizamos um levantamento de requisitos funcionais e não-funcionais que a aplicação deveria conter, esses requisitos serão mais bem detalhados na seção de Desenvolvimento.

Algumas limitações técnicas foram encontradas no decorrer do projeto como conhecimento limitado na linguagem Java e como utilizá-la no Android Studio bem como falta de experiência na aplicação de autenticações via biometria, reconhecimento facial e Single Sign-On (SSO).

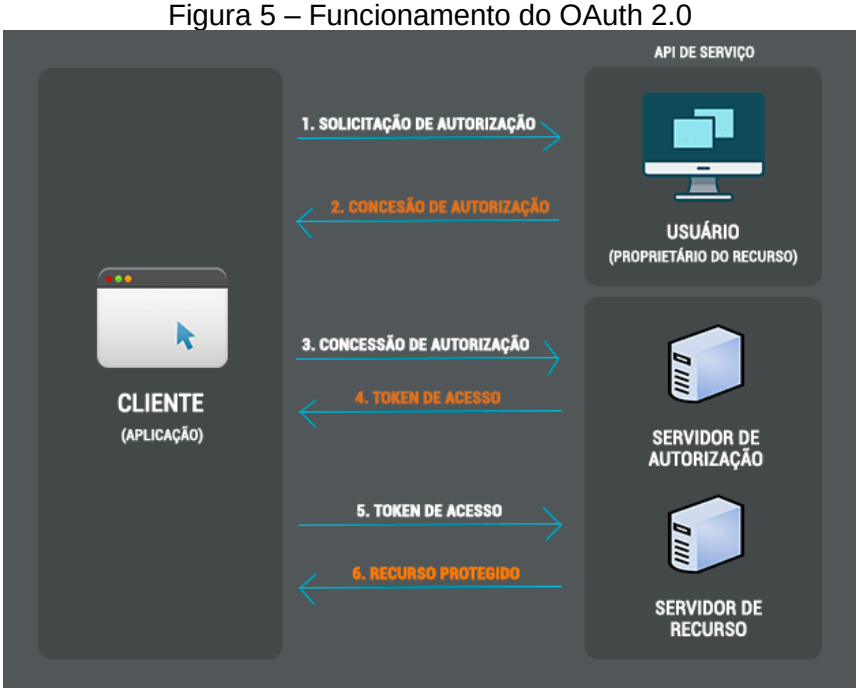
Outro desafio foi termos trabalhado uma boa parte da construção do protótipo do software sem ter acesso a um protótipo de hardware da fechadura em mãos não sendo possível um teste mais detalhado de funcionamento. Sendo assim uma placa micro controladora ESP WROOM 32 foi disponibilizada para provar o conceito do funcionamento da abertura da fechadura através de um led se acendendo e apagando quando enviados comandos de abrir e fechar.

Por fim encontramos alguns problemas na integração do software com o hardware através de Wi-fi e bluetooth durante o desenvolvimento o que nos trouxe alguns desafios para realizar essa tarefa através do Android Studio e conseguir emular corretamente o protótipo.

3.2 Arquitetura e componentes da plataforma

Os usuários podem acessar a aplicação mediante autenticação por meio de diversos métodos. A autenticação pode ser efetuada através da criação de um registo, composto por um nome de usuário e palavra-passe, os quais serão armazenados numa base de dados local em SQLite. Alternativamente, a autenticação pode ser realizada através de biometria ou reconhecimento facial. Por fim, a autenticação também é possível usando Single Sign-On (SSO), implementado através do protocolo OAuth 2.0.O Funcionamento do OAuth pode ser observado na Figura 5.

Figura 5 – Funcionamento do OAuth 2.0



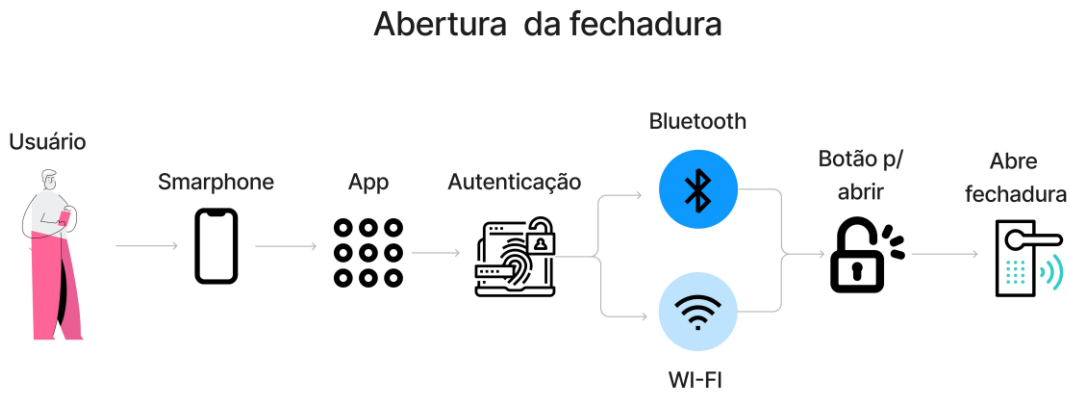
Fonte: TUTORIALSPOINT, 2023.

Ao acessar a aplicação o usuário poderá escolher entre as formas de conexão Wi-fi ou Bluetooth para se conectar com o hardware da fechadura. Após isso ele poderá rastrear e adicionar dispositivos ao aplicativo.

Entrando em um desses dispositivos o usuário pode então “Abrir” e “Fechar” o dispositivo através de um botão no app.

O funcionamento da aplicação ou, jornada do usuário, é demonstrado na Figura 6 que demonstra os tipos de conexão com o hardware e a funcionalidade principal do protótipo que é abrir a fechadura através do aplicativo.

Figura 6 - Jornada do usuário do aplicativo



Fonte: Produzido pelo autor.

O aplicativo permitirá também a criação e gerenciamento de grupos hierárquicos onde usuários podem ser adicionados. Para se tornar administrador desses grupos no dispositivo o usuário deve ler um QR code que deve vir junto com a fechadura no manual do usuário. Assim o administrador pode gerenciar grupos relacionados a uma fechadura específica atribuindo dias da semana e horários que cada grupo pode utilizar o dispositivo.

3.3 Segurança em aplicações

As ferramentas que utilizaremos para garantir a segurança da aplicação são o OAuth 2.0 e criptografia com SHA-1.

As informações armazenadas no banco local serão criptografadas com SHA-1 garantindo, segurança, privacidade dos usuários e conformidade da aplicação com a LGPD.

O OAuth 2.0 é um protocolo de autorização amplamente utilizado para autenticação segura em aplicativos. Ao implementar o OAuth 2.0, o aplicativo pode se integrar com provedores de identidade confiáveis, como Google, Facebook ou Microsoft, para autenticar os usuários de forma segura. Isso elimina a necessidade de armazenar senhas localmente e protege contra ameaças

como ataques de força bruta. Além disso, o OAuth 2.0 permite que os usuários concedam permissões específicas ao aplicativo, garantindo que apenas as informações necessárias sejam compartilhadas.

Em conjunto, essas ferramentas fornecem uma abordagem abrangente para a segurança de um aplicativo. O SHA-1 garante a segurança do armazenamento de dados, o OAuth 2.0 protege a autenticação dos usuários. Essa combinação permite que desenvolvamos medidas de segurança sólidas no nosso app, oferecendo aos usuários uma experiência confiável e protegida.

4 DISCUSSÃO DE RESULTADOS

Após análise do documento elaborado para o desafio da Jornada de aprendizagem e de informações levantadas com o funcionário da PADO reunimos uma lista de requisitos funcionais e não funcionais para o aplicativo que são descritos a seguir.

4.1 Requisitos Funcionais

- Desenvolver a solução em Java
- Utilizar sistema de autenticação SSO com o OAuth 2.0
- Usar autenticação com biometria e/ou reconhecimento facial
- Utilizar o SQLite para armazenar dados localmente
- Botão para rastrear os dispositivos e cadstrá-los
- Leitura de QR code para cadastro do administrador da fechadura
- Na tela de desbloqueio da fechadura somente um botão para destravar e trancar a fechadura e botões de gerenciamento para analisar logs de acesso e grupos relacionados ao dispositivo
- Local para criação e gerenciamento de grupos de acesso ao dispositivo com possibilidade de escolha de períodos (dias e horário de acesso)

4.1 Requisitos Não-funcionais

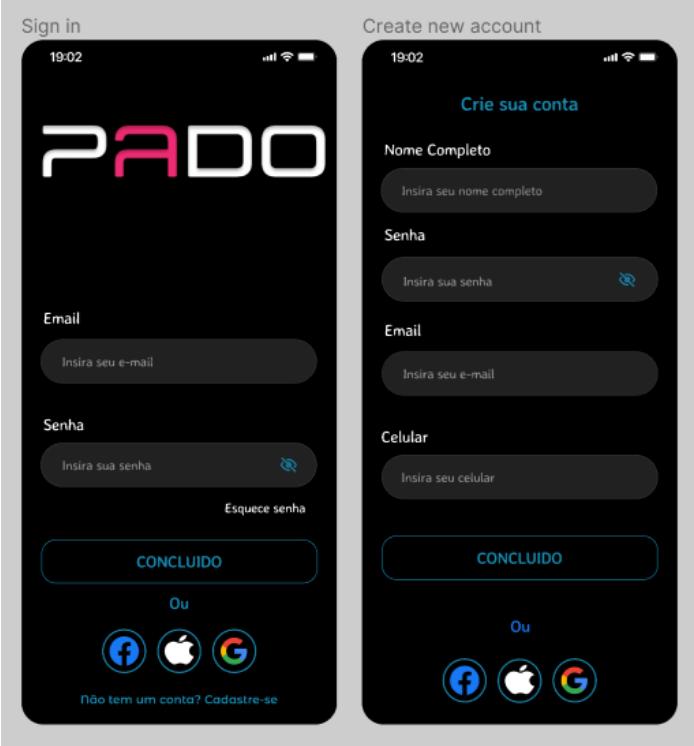
- Ser multiplataforma (portabilidade entre Android e IOS)

- UX intuitiva (user friendly)
- Funcionar através de bluetooth e wi-fi
- Velocidade: tempo de resposta curto
- Confiabilidade (estar sempre disponível)
- Fornecer privacidade de acordo com a LGPD

4.3 Comparação da Prototipação versus Resultado

Para a prototipação das telas do aplicativo utilizamos o Figma. Na figura 7 apresentamos a tela inicial de acesso que possibilita o usuário acessar com SSO ou criar uma conta com usuário e senha para acesso.

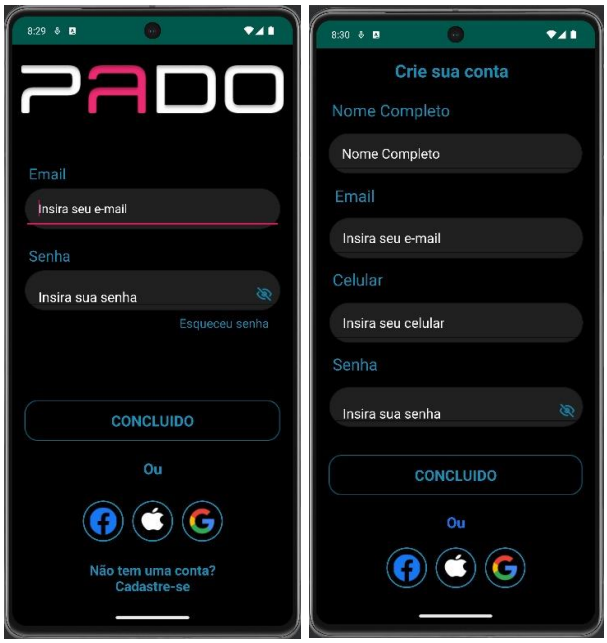
Figura 7 – Telas de cadastro de usuário e acesso ao aplicativo – Protótipo



Fonte: Produzido pelo autor.

Na Figura 8 apresentamos o resultado das telas implementadas no aplicativo.

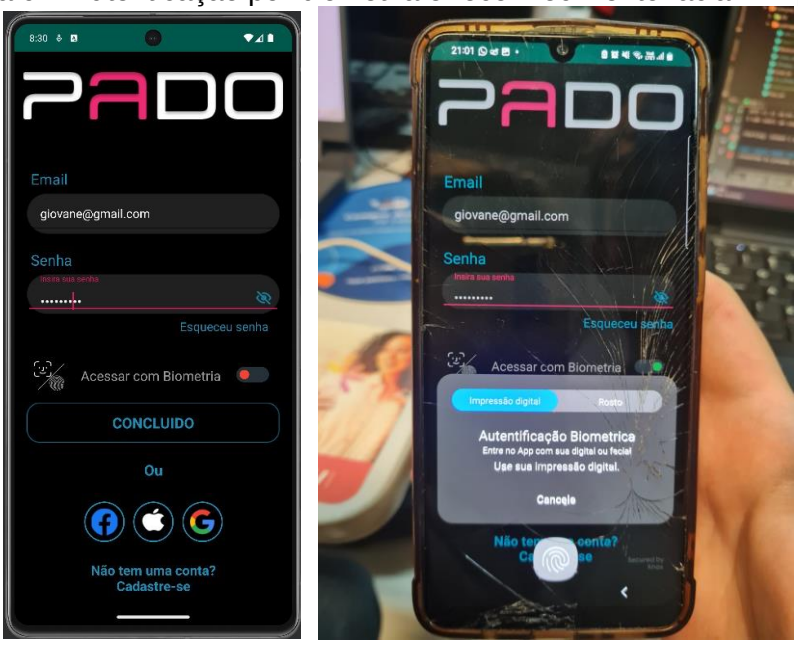
Figura 8 – Telas de cadastro de usuário e acesso ao aplicativo - Implementação



Fonte: Produzido pelo autor.

O usuário também tem a opção de realizar o login através de biometria ou reconhecimento facial, após o primeiro login é possível selecionar a opção de ativar esse tipo de autenticação como mostra a figura 9.

Figura 9 – Autenticação por biometria e reconhecimento facial - Implementação

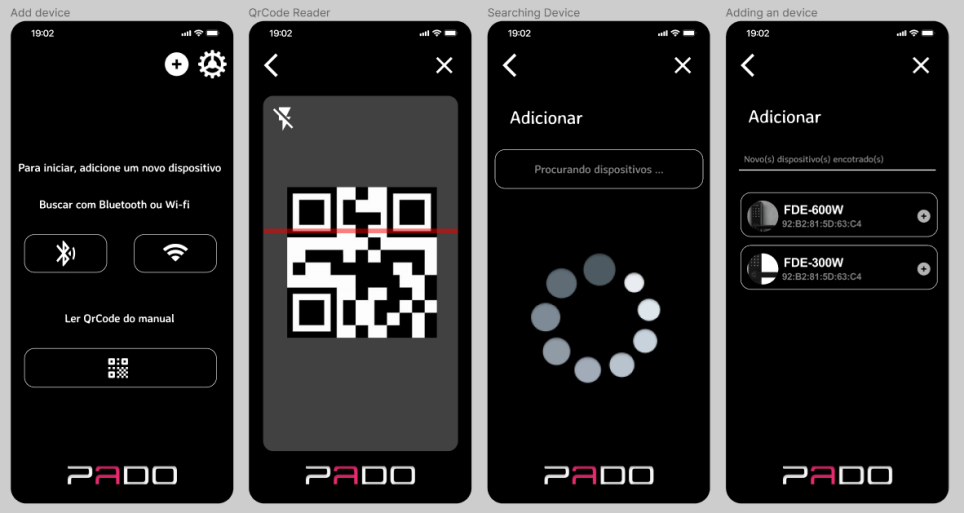


Fonte: Produzido pelo autor.

No planejamento inicial, após o acesso o usuário administrador da fechadura faria a leitura do QR Code que acompanharia fisicamente o manual

ou embalagem dela para cadastrar o dispositivo. Outros usuários poderiam buscar e adicionar o dispositivo através de bluetooth ou wi-fi (Figura 10).

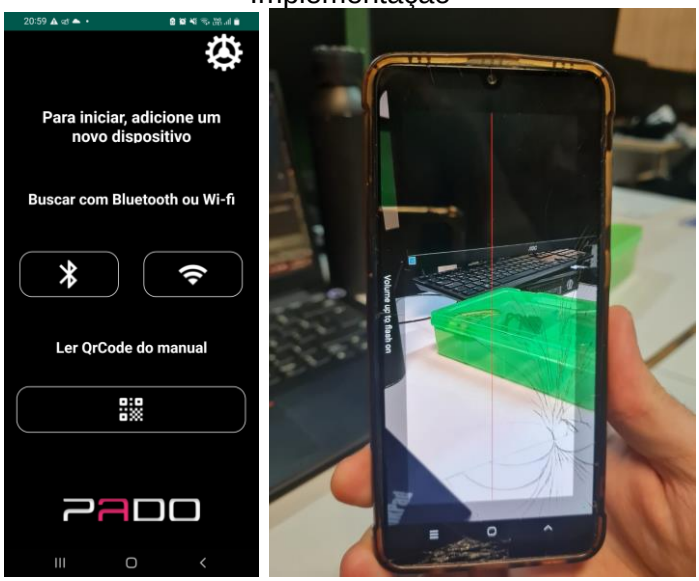
Figura 10 – Telas de busca e cadastro de dispositivos - Protótipo



Fonte: Produzido pelo autor.

Como a funcionalidade de busca por dispositivos não foi adicionada à aplicação, na figura 11 podemos observar a implementação da tela que o aplicativo mostra após o login onde é possível escolher o tipo de comunicação utilizada entre wi-fi e bluetooth e um trabalho inicial de leitura do QR code também foi implementado.

Figura 11 – Escolha de tecnologia para conexão e leitura de QR Code - Implementação

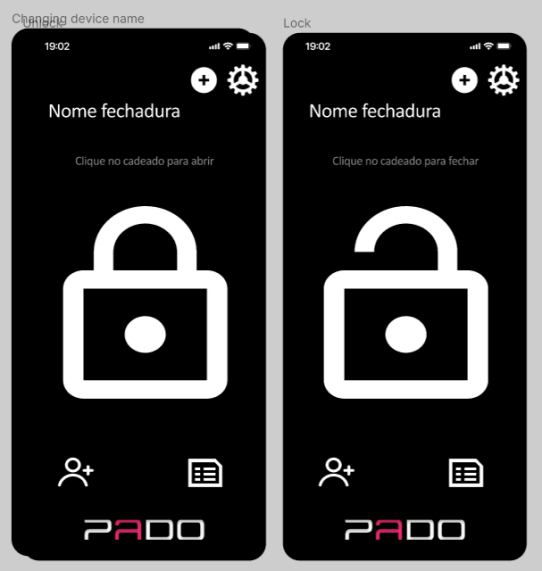


Fonte: Produzido pelo autor.

Após o acesso com a tecnologia de conexão escolhida o usuário poderá acionar o botão para abrir e fechar o dispositivo. O protótipo é exibido na Figura 12, já a implementação na Figura 13.

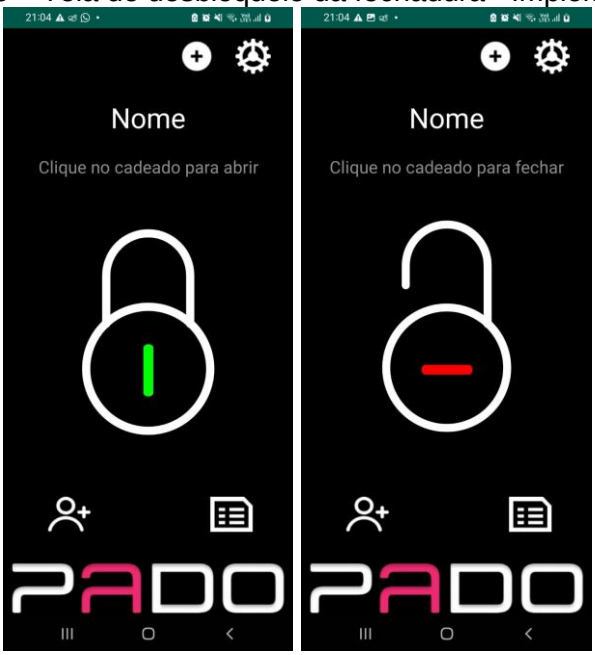
Nas telas do protótipo (Figura 12) também podemos observar um botão para adicionar usuários a essa fechadura (inferior esquerdo) e um para análise de logs (inferior direito), funcionalidade essas que não foram implementadas.

Figura 12 – Tela de desbloqueio da fechadura - Protótipo



Fonte: Produzido pelo autor.

Figura 13 – Tela de desbloqueio da fechadura - Implementação



Fonte: Produzido pelo autor.

Na Figura 14 podemos observar a tela de logs (esquerda) e a tela de análise de usuários pendentes a serem adicionados em grupos, funcionalidades planejadas, mas que não foram implementadas na aplicação.

Figura 14 – Tela de logs e análise de usuários para adição em grupos - Protótipo

Fonte: Produzido pelo autor.

Figura 15 – Criação e gerenciamento de grupos - Protótipo

Fonte: Produzido pelo autor.

Na Figura 15 podemos observar também o protótipo de como o administrador faria o gerenciamento de novos grupos de acesso determinando os dias da semana e período que os usuários acessariam o dispositivo.

A figura 16 mostra o protótipo da tela geral de configuração do aplicativo onde o usuário administrador pode realizar a restauração de uma fechadura para o padrão de fábrica e que outros usuários podem configurar algumas funcionalidades do app como ativar o leitor de biometria e facial.

Figura 16 – Restauração para o padrão de fábrica e configurações - Protótipo

Fonte: Produzido pelo autor.

A restauração para o padrão de fábrica se torna útil para quando o usuário precisa passar a fechadura para outra pessoa como, por exemplo, no caso de estar se mudando. Após isso as permissões são resetadas e outro usuário pode realizar a leitura do QR Code da fechadura se tornando o administrador desse dispositivo.

Na figura 17 vemos a implementação da tela de configurações do aplicativo, nela podemos notar que removemos as opções de ativação de biometria e leitor facial, essas configurações foram transferidas para a tela de login após o primeiro acesso como visto na Figura 9.

Figura 17 - Configurações e futuras features - Implementação

Fonte: Produzido pelo autor.

Tanto na prototipação (Figura 16) quanto na implementação (Figura 17) podemos observar possibilidades de futuras features a serem implementadas como integrações com alexa a google com comandos de voz e alterações de temas no app.

5 CONSIDERAÇÕES FINAIS

A elaboração de um aplicativo para fechaduras inteligentes se mostra um desafio, o encontro entre tecnologia, praticidade e segurança precisa estar bastante balanceado para fornecer a melhor experiência ao usuário da forma mais segura.

Com os requisitos levantados e estudo de outras ferramentas no mercado pudemos realizar a escolha de tecnologias a serem utilizadas na implementação dessa solução de aplicativo para uma fechadura inteligente. A prototipação das telas foi feita usando o Figma. Escolhemos trabalhar com a linguagem Java no Android Studio o que trouxe uma flexibilidade através do uso de emulação da aplicação na própria IDE.

Vários métodos de autenticação foram utilizados: cadastro de usuário com login e senha em um banco local usando o SQLite, acesso com biometria, reconhecimento facial e o acesso com SSO utilizando o protocolo OAuth 2.0.

Para simular a fechadura abrindo foi utilizado um microcontrolador ESP WROOM 32 com um led que acende e apaga conforme o usuário abre e fecha o dispositivo. Essa comunicação e envio de informação se deu através de Wi-fi e Bluetooth.

A segurança da aplicação foi garantida com o uso de autenticação SSO e a criptografia dos dados sensíveis de usuários no banco local utilizando SHA-1.

Algumas funcionalidades não foram implementadas conforme o planejado como a busca por dispositivos, a criação de grupos hierárquicos com grupos específicos onde um administrador poderia controlar o acesso de outros usuários e configurar períodos autorizados de acesso, porém essa foi uma escolha do grupo para podermos conseguir explorar mais e desenvolver com tecnologias com as quais não havíamos tido contato durante o curso como autenticação com biometria, reconhecimento facial e autenticação via SSO.

Além dos grupos hierárquicos identificamos que seria possível incluir novas features como o controle da fechadura através de assistentes de voz como a alexa e a utilização de notificações para o administrador ter maior controle em tempo real dos acessos e solicitações de acesso à fechadura.

O presente trabalho foi um desafio para o grupo e com ele tivemos a oportunidade de, pela primeira vez no curso, integrar nosso software com um hardware e testar o funcionamento da aplicação bem como entrar em contato com novas tecnologias.

REFERÊNCIAS

Adekotujo, Akinlolu, et al. **A Comparative Study of Operating Systems**: Case of Windows, UNIX, Linux, Mac, Android and iOS. International Journal of Computer Applications 176.39 (2020): 16-23.

ANDROID, 2023. Disponível em: https://developer.android.com/studio/intro. Acesso em: 17/04/2023.

Chien, Chen-Fu, Kuo-Yi Lin, and Annie Pei-I. Yu. **User-experience of tablet operating system**: An experimental investigation of Windows 8, iOS 6, and Android 4.2." Computers & Industrial Engineering 73 (2014): 75-84.

DE CLERCQ, J. **Single sign-on architectures. Infrastructure Security**: International Conference, InfraSec 2002 Bristol, UK, October 1–3, 2002 Proceedings. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002.

DEVELOPERS, Android. **What is android**. Dosegljivo: http://www. academia. edu/download/30551848/andoid--tech. pdf, 2011.

GAIKWAD, Poonam V.; KALSHETTY, Yoginath R. **Bluetooth based smart automation system using Android**. International Journal of New Innovations in Engineering and Technology, v. 7, n. 3, p. 24-29, 2017.

GAZIS, A. **What is IoT? The Internet of Things explained**. Academia Letters. 2021.

GITHUB, 2023. Disponível em: <Getting started with GitHub documentation - GitHub Docs> Acessado em 16/04/2023

JOSEPH, F.; MARGARET-ANNE, S.; ALEXEY, Z. **Student experiences using GitHub in software engineering courses**: a case study. New York, NY, United States, 2016.

KAUSHIK, S. **An overview of technical aspect for WiFi networks technology**. International Journal of Electronics and Computer Science Engineering (IJECSE, ISSN: 2277-1956), v. 1, n. 01, p. 28-34, 2012.

LONZETTA, A. M. et al. **Security vulnerabilities in Bluetooth technology as used in IoT**. Sensors and Actuators: Security Threats and Countermeasures, v. 2, p. 1-19, 2018.

MADAKAM, S.; RAMASWAMY, R.; TRIPATHI, S. Internet of Things (IoT): A Literature Review. IT Applications Group, National Institute of Industrial Engineering (NITIE), Vihar Lake, Mumbai, Índia.

MICULAN, M.; URBAN, C. **Formal analysis of Facebook Connect Single Sign-On authentication protocol**. Departamento de Matemática e Ciência da Computação, Universidade de Udine, Itália. 2011.

MIRANDA, L.A.V. **Monitoramento de parâmetros ambientais de um leito hospitalar utilizando ESP32.** Escola superior de tecnologia da Universidade do Estado do Amazonas (UEA). Manaus – AM, 2019.

NETO, J.B.C; COSTA, P.H.S. **Sistema embarcado de baixo custo utilizando oESP-32 na telemedicina.** Universidade Potiguar. Natal – Brasil, 2022.

SHAFANA, A.R.F.; ARIDARSHAN, A. **Android based Automation and Security System for Smart Homes**. International Journal of Computer Science and Information Technology Research, vol. 5, Issue 3, July 2017 – September 2017

TUTORIALSPOINT. **OAuth 2.0 – Architecture.** Disponível em: https://www.tutorialspoint.com/oauth2.0/oauth2_concepts.htm. Acesso em: 15/04/2023.

YINAN, G.; SHUGUO, Z.; DAWEI, X. **Overview of Wi-Fi Technology**. China University of Mining and Technology, 04 Aug 2012, pp. 1293-1296.