



UNIP- Araçatuba

Instituto de Ciências Exatas e Tecnologia

APS - ATIVIDADES PRÁTICAS SUPERVISONADAS

**“DESENVOLVIMENTO DE UM SISTEMA DE IDENTIFICAÇÃO E
AUTENTICAÇÃO BIOMÉTRICA”**

NOME: LEONARDO LEITE DE MORAES

R.A: T0152D9

ORIENTADOR: PROF.ALDRIANO JOSÉ DA SILVA

Sumário

1- OBJETIVO DO TRABALHO	2
2- INTRODUÇÃO	3
3- FUNDAMENTOS DAS TÉCNICAS BIOMÉTRICAS.....	5
3.1- Tipos de identificações biométricas	6
4- PLANO DE DESENVOLVIMENTO DA APLICAÇÃO	12
4.1- Java	12
4.2- Firebase	13
4.2- AndroidStudio	15
5- PROJETO DA APLICAÇÃO.....	16
6- CONSIDERAÇÕES FINAIS	23
BIBLIOGRAFIA	24

1. OBJETIVO DO TRABALHO

O objetivo do trabalho é o desenvolvimento de uma ferramenta de identificação e autenticação biométrica em Java ou C# que foi proposta pelo orientador da disciplina de sistemas operacionais abertos e mobile, sendo formado por um grupo de 3 alunos, podendo ter quantidade de integrantes alterado com a aprovação do coordenador do curso.

A atividade tem objetivo de criação de uma aplicação que realize a identificação e autenticação biométrica e que restrinja o acesso a uma rede com banco de dados do Ministério do Meio Ambiente. A ferramenta criada tem intuito de priorizar o meio ambiente fazendo que os possam visualizar informações estratégicas de propriedades rurais que utilizam agrotóxicos proibidos por causarem grandes impactos nos lençóis freáticos, rios e mares. O sistema será subdividido em três níveis, onde, o primeiro nível todos os usuários podem ter acesso, o segundo nível é restrito para os diretores de divisões e o terceiro nível somente é acessado pelo ministro do meio ambiente.

2. INTRODUÇÃO .

Antes mesmo do início dos estudos de biometria, partes do nosso corpo e aspectos do nosso comportamento foram usados como uma forma de identificação, lembramo-nos e identificamos uma pessoa de acordo com seu tom de voz e seu rosto. Entretanto, a assinatura foi uma forma muito utilizada para a como um método de identificação em bancos, contratos e entre diversas ocasiões.

Francis Galton é considerado um dos fundadores da biometria, suas pesquisas em capacidade e disposições mentais, que incluíam estudos de gêmeos idênticos, foram as pioneiras em demonstra que há vários traços que são genéticos. Sua paixão por esta área que permitiu que ele abrisse seu Laboratório de Antropométrica na Exibição Internacional de Saúde em impressões digitais, que logo foi adaptado por departamento de polícia, onde, naquela época, as impressões digitais eram a formar mais confiável de identificação, até a chegada do ADN (ácido desoxirribonucleico, nome da molécula de dupla hélice que contém informações únicas que está presente nas células do corpo).

Os avanços na área da biométrica começaram na década de setenta. Durante este período, foi instalado um sistema chamado Identimat em locais secretos para controle de acesso. Este sistema media a forma da mão e principalmente o tamanho dos dedos. A sua utilização foi pioneira na aplicação de geometria da mão e abriu um caminho para a tecnologia biométrica como um todo. A produção dos Identimat foi parada na década de oitenta.

Imagem 1: Identimat



Fonte: The Driver

Durante as décadas de sessenta e setenta, algumas companhias estavam envolvidas com a identificação automática das digitais para auxiliar as forças policiais, pois o processo manual de comparação era muito extenso e necessitava de muito trabalho manual. No final dos anos sessenta, o FBI começou a verificar as digitais automaticamente e em meados de setenta já havia uma grande quantidade de scanners automáticos. Desde então os Automated Fingerprint Identification Systems (AFIS) são utilizados por um grande número de forças policiais em todo o mundo.

Existem dois tipos de biometria: a fisiológica, que possui como referências traços característicos de nosso corpo convertendo-os em parâmetros ou indicadores, e a do comportamento, que recorre a outros aspectos derivados de uma ação concreta, como escrever ou caminhar, por exemplo.

As principais vantagens na aplicação da biometria são:

- A possibilidade de associar um indivíduo específico (ao contrário de uma senha, que pode ser usado por alguém sem autoridade).
- Sua facilidade de uso, uma vez que não tem necessidade de lembrá-la ou ter uma.
- Sua segurança, pois é um método que tem uma alta resistência a fraudes.

Um dos maiores usos atualmente da biometria se trata dos múltiplos benefícios proporcionados às empresas, que auxiliam a reduzir os custos de manutenção em seus sistemas de autenticação, aumenta a eficiência do controle de

horário. Mas há diversos outros usos que são aplicados, como: controle de acesso a locais restritos, controle de presença para empregados, luta contra fraudes em instituições bancárias e diversas outras.

3. FUNDAMENTOS DAS TÉCNICAS BIOMÉTRICAS.

Para termos um aprofundamento melhor das utilizações de técnicas biométricas, é importante ressaltar inicialmente alguns conceitos como: captura, extração e comparação. Abaixo você terá uma curta explicação de como funcionam estes conceitos.

- **Captura:** Nesta fase é necessário um scanner ou sensor que fica responsável por obter uma amostra biométrica, ou seja, uma imagem que permite realizar a identificação do indivíduo, podendo ser digitais e geometria da mão, íris, retina, expressões faciais etc.
- **Extração:** Após realizar a captura, com um software biométrico a amostra é analisada e as suas características mais relevantes são extraídas. Por exemplo: se a amostra biométrica é a palma da mão, a característica relevante será as linhas que dão forma às digitais.
- **Comparação:** Com as características extraídas é realizada a última etapa, a comparação. Ela realiza uma comparação entre a amostra obtida e as amostras do banco de dados. Esta verificação é feita com o auxílio de diversos algoritmos, cada um trabalhando da sua maneira para obter os resultados de comparação para definir à quem possui esta identidade.

Após verificar estes conceitos, podemos estar falando sobre algumas técnicas biométricas presentes.

As técnicas dependem de características únicas de cada indivíduo, tais como impressões digitais, traços faciais ou até mesmo seu timbre de voz. Os métodos biométricos são utilizados para realizar autenticações em diversas situações. Por exemplo, uma empresa pode realizar o uso de técnicas biométricas para garantir que algumas informações privilegiadas sejam para alguém esteja em um alto nível de gestão. Bancos e instituições financeiras podem usar deste método para limitar acesso a cofres de caixas de banco ou empregados e permitir acesso apenas a

clientes. Além disso, os indivíduos podem usar técnicas de biometria para garantir restrição de pertences pessoais.

Segundo a Biometric Consulting Inc., a melhor maneira de garantir a proteção de informações e pertences é realizando o uso de diversos dispositivos de reconhecimento biométrico, tais como impressões digitais e dispositivos de reconhecimento de íris.

Todos os dados biométricos são registrados em um banco de dados, onde, cada uma é tratada com unicidade, pretendendo assim manter a segurança contra possíveis fraudes. Existem diversas maneiras de garantir que os dados biométricos estejam seguros. Primeiro, deve-se realizar backups destes dados em um local separado, centralizado que estejam seguros. Segundo, organizações que utilizam de cartões de identificação biométricos, devem-se usar imagens ocultadas ou números do cartão que pode ser reconhecido apenas pelo scanner biométrico. Isso reduz o risco de fraudes, mesmo que o cartão de identificação biométrico foi copiado, as imagens ou números escondidos estariam faltando, impedindo que a autenticação seja completa.

3.1- Tipo de identificações biométricas.

Existem diversos tipos de biometrias, desde as que se baseiam na geometria da mão à análise de assinaturas, que realiza a autenticação de acordo pressão e maneirismos. Podem-se citar seis tipos que são mais populares, utilizados em uma série de soluções, mais ou menos seguras ou com estudos mais avançados que outras.

- Impressões Digitais: É o método de mais antigo e de menor custo para implementação. É uma das mais confiáveis, por conta da baixíssima instabilidade dos dados ao longo de muito tempo, dada que as digitais se mantem as mesmas por toda a vida, tendo a possibilidade de apresentar problemas somente se o indivíduo perder sua digital, independente do motivo. A captura das digitais teve sua migração suavemente dos meios analógicos para o digital.

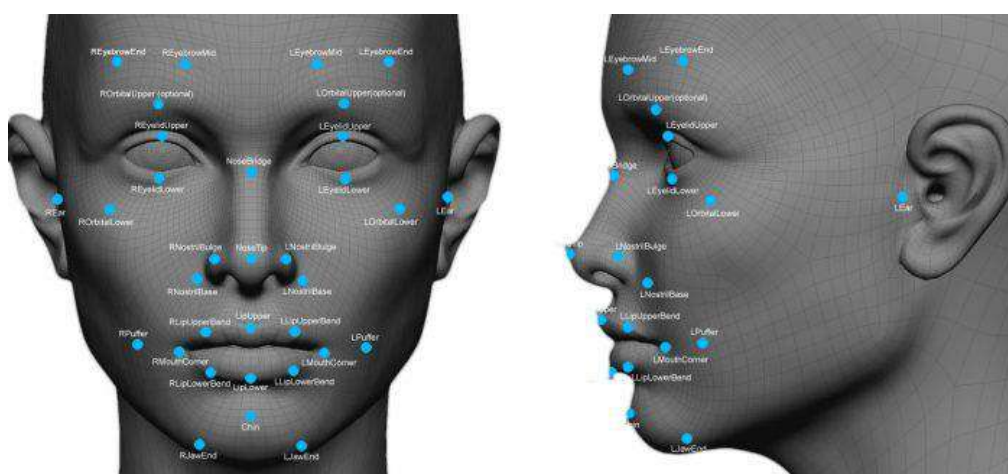
Imagem 2: Símbolo da impressão digital.



Fonte: Tecnoblog.

- **Reconhecimento Facial:** Presente até em celulares, consiste em mapear um rosto, tanto em 3D (como o FaceID da Apple) ou em 2D (como a maioria dos smartphones). Esta técnica cria uma imagem da pessoa que será utilizada para autenticação, permitindo acesso aos dados. Alguns argumentos contra a mesma, está o fato de não ser uma técnica permanente, ao passo o usuário envelhece, pode haver mudanças em seu rosto e também a possibilidade de ter um irmão gêmeo faz que ele não tenha esta segurança. A coleta em 2D também não é precisa, e mesmo que haja um mapeamento profundo costuma ocorrer falhas.

Imagem 3: Reconhecimento facial.



Fonte: Tecnoblog.

- Reconhecimento de íris: A íris (parte colorida do olho humano, responsável por controlar a entrada e saída de luz) é extremamente confiável, já que a membrana permanece a mesma durante toda a vida. Embora tenha um extremo nível de confiança, é um método caro, embora se cogite que a leitura de íris será a mais usada em médio prazo, superando a impressão digital.

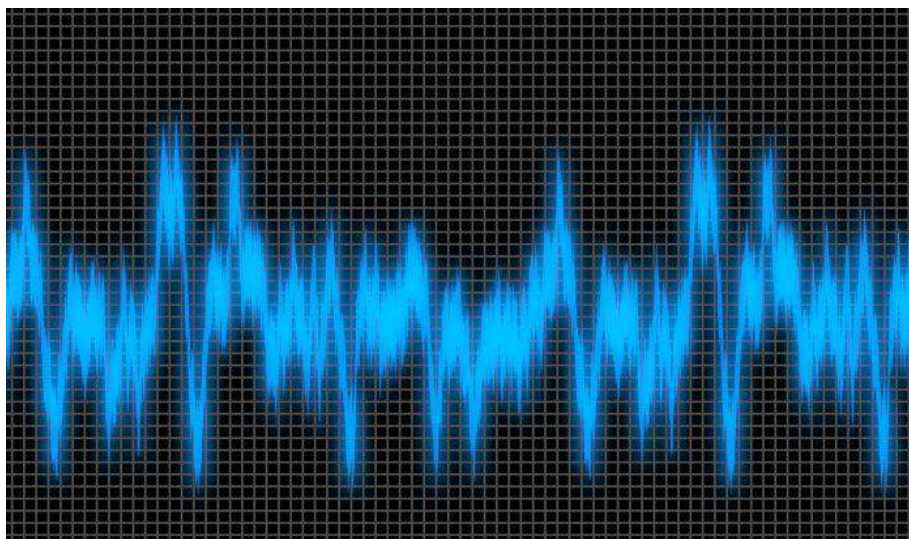
Imagem 4: Reconhecimento de íris.



Fonte: Tecnoblog.

- Reconhecimento de voz: Este método realizar uma análise dos parâmetros físicos (cordas vocais, laringe etc.) e comportamentais, como sotaques, entonação etc. O seu resultado é um perfil sonoro único, que em tese pode ser usado como uma assinatura biométrica. Por ter um custo baixo, a sua confiabilidade é baixa, já que qualquer ruído pode comprometer a coleta e análise da voz. Alterações causadas por problemas de saúde e pelo próprio envelhecimento também atrapalham a validação destes métodos.

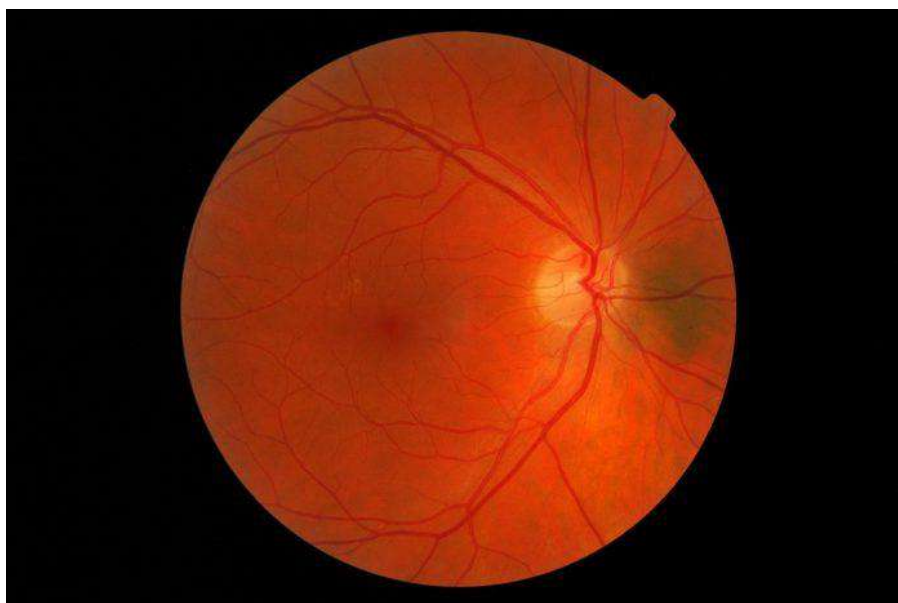
Imagem 5: Reconhecimento de voz.



Fonte: Tecnoblog.

- Reconhecimento de retina: É uma das mais seguras que existe, já que os vasos sanguíneos que irrigam a retina muda de pessoa para pessoa e não sofrem alterações durante o decorrer dos anos. Seus meios para coleta e leitura dos dados não são simples, o que dificulta a falsificação das informações. A sua captura é feita da seguinte maneira: o usuário deve olhar para um dispositivo de luz infravermelha de baixa intensidade que fara a “leitura” da retina. Embora seu alto nível de segurança, é um método desagradável e incômodo.

Imagem 6: Reconhecimento de retina.



Fonte: Tencnoblog.

- **Reconhecimento pela digitação:** Baseia-se na análise do ritmo e cadência do usuário ao digitar. Cada indivíduo possui um próprio estilo de digitação, seja a quantidade de dedos que utiliza, a velocidade de digitação, a força que aplica ao pressionar as teclas etc. Sua captação de dados não é simples e é um método de pouca confiança, já que o usuário pode mudar seu estilo de digitação, de forma inconsciente ou intencional.

Imagem 7: Reconhecimento pela digitação.



Fonte: Tecnoblog.

4. PLANO DE DESENVOLVIMENTO DA APLICAÇÃO DA APLICAÇÃO.

Após realizar análises sobre o tema apresentado, decide-se que a aplicação será desenvolvida na linguagem de programação Java através da IDE do AndroidStudio, o banco de dados se tratará do Firebase, assim, será desenvolvido o aplicativo mobile do Ministério do Meio Ambiente.

4.1- Java

A linguagem Java foi criada e comercializada pela Sun Microsystems em 1995 e atualmente mantida pela Oracle. Ela é definida como uma linguagem de programação orientada a objetos que é amplamente usada para o desenvolvimento

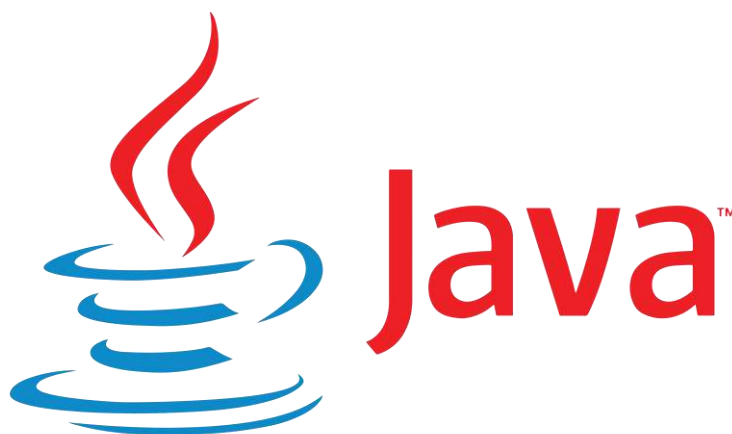
de sites e aplicativos. O Java está presente na maioria dos lugares e muitas pessoas não o conhecem ou sequer sabem que ela existe.

A linguagem de programação Java permite que você escreva instruções para serem executadas pelos computadores. Estas instruções são nomeadas de software, conhecidas como programa de computador. O software que realiza a permissão que você controle o hardware. A principal função do Java é a possibilidade de criar aplicações em rede, como jogos e programas, ou seja, um programador Java consegue projetar softwares que podem ser utilizados em múltiplas plataformas, como Mac, Windows, Linux e Android, sem ter a necessidade de modificá-los e sem necessidade de alterar a arquitetura da máquina.

Nos dias atuais, o Java está presente em nosso cotidiano, podendo encontrá-lo em:

- Supercomputadores: Responsável por realizar trilhões de cálculos por segundo feitos em supercomputadores que utilizam Java.
- GPS: O Google Maps, tecnologia de geolocalização utilizada diariamente por milhares de pessoas teve sua criação utilizando a linguagem de programação Java.
- Cartão de crédito: Os cartões Visa, por exemplo, utilizam da linguagem de programação Java.
- Jogos: O Java auxilia no desenvolvimento dos jogos, devido sua versatilidade e tamanho de conteúdo

Imagem 8: Logo do Java.



Fonte: 1000logos.

4.2- Firebase

O Firebase é uma plataforma digital da Google utilizada para facilitar o desenvolvimento de aplicativos web ou mobile. Seu objetivo principal é melhorar o desempenho de apps com a junção de diversas funcionalidades numa plataforma só. Estas funcionalidades contribuem para o desenvolvimento e para a monetização de apps, já que é possível utiliza-lo também no Marketing Digital.

A plataforma do Firebase foi desenvolvida por uma startup fundada por James Tamplin e Andrew Lee no ano de 2011. Em 2014, a plataforma foi adquirida pelo Google. Assim, possibilitou mais rapidez na criação de aplicativos, monitoramento e engajamento.

Sua base é construída na infraestrutura do Google, sendo categorizada como um programa de banco de dados NoSQL, que realizar o armazenamento dos dados em documentos de tipos JSON.

Sem o Firebase, o desenvolvedor teria que criar uma estrutura completa no back-end para desenvolver um aplicativo web ou mobile. Com essa solução, o desenvolvedor tem várias funcionalidades que pode usar de maneira mais pratica, sendo elas:

- Múltiplas plataformas: O Firebase pode ser usado em plataformas móveis, seja Android, IOS e Web.
- Várias linguagens: Tem o suporte a diversas linguagens de programação como Java, JavaScript, C++, Node.js, Swift e Objective-C. Além disso, pode ser usado também com os frameworks Angular, React e Backbone.
- Monetização: Ele gera a possibilidade de gerar dinheiro com publicidade por meio do Admob.
- Plano gratuito e pago: A plataforma permite sua utilização gratuita, sendo cobrada a partir de certo nível de experiência e funcionalidade.

Como todos os serviços que temos disponibilidade, o Firebase tem suas vantagens e desvantagens, sendo as suas principais vantagens: API pronta;

Aplicativos altamente escaláveis; Armazenamos de arquivos pelo Google Cloud Storage; Autenticação via e-mail, Google, Facebook e Github; Dados em tempo real; Hospedagem de arquivos estáticos; Segurança. Suas principais desvantagens são: Limitações de infraestrutura; Bugs de atualizações; Problemas que envolvem UI/UX.

Imagem 9: Logo do Firebase.



Fonte: Firebase.

4.3- Android Studio

O Android Studio é uma plataforma para desenvolvimento de apps mobile para o sistema operacional mais popular, ou seja, é a ferramenta responsável por criar aplicativos para Android – hoje está presente em 74,13% dos dispositivos móveis.

Ele é um Ambiente de Desenvolvimento Integrado, uma tradução para Integrated Development Environment, ou simplesmente IDE. Na sua prática, a definição é basicamente a mesma, mas parte de uma linguagem mais técnica (e correta) para se referir à ferramenta utilizada no desenvolvimento de aplicativos. Uma IDE consiste em um programa de computador que reúne todos os requisitos ideais e necessários para que seja possível criar um app para dispositivos móveis. Seu software é disponibilizado gratuitamente pela Google, dona do sistema Android, para que assim pessoas que com altos conhecimentos em programação possam elaborar soluções personalizadas aos seus clientes.

O Android Studio não é o único IDE de desenvolvimento de aplicativos mobile com sistema operacional do Google. Existem opções exclusivas, como o Eclipse e também multiplataformas, como o Xamarin.

Uma das principais vantagens do Android Studio é sua maior variedade de customização. É possível personalizar tudo na ferramenta, desde atalhos do teclado ao tema geral de apresentação. As ferramentas são iniciadas mais rápidas, fazendo a experiência de criação ser mais veloz.

Se por um lado o Android Studio tem mais recursos, isso demanda um preço maior na sua utilização. Enquanto no Eclipse o carregamento de um projeto pode levar um minuto, dependendo das configurações de sua máquina, no Studio, esse tempo pode ser facilmente dobrado. Pode parecer pouco a diferença, porém, caso tenha que fazer o carregamento uma determinada quantidade de vezes, esse tempo acabara atrapalhando sua produtividade. Outro ponto ruim para desenvolvedores mais habilidosos é a falta de possibilidade de criar mais de um app ao mesmo tempo, já que o Studio não permite a administração de projetos na mesma janela.

Imagem 10: Logo do Android Studio.



Fonte: TechCrunch.

5. PROJETO DO PROGRAMA

Foi realizada a criação do aplicativo de segurança do ministério do meio ambiente com as ferramentas citadas acima.

No início da aplicação, quando abrimos ela, temos uma breve apresentação sobre o que se trata a aplicação tendo as opções de o usuário realizar o login, caso já possua um conta cadastrada, e realizar a criação de uma nova conta caso ainda não possua.

Imagem 11: Página inicial.



Fonte: Autor próprio.

Ao clicar no botão de cadastrar novo usuário ira ser aberta a seguinte página.

Imagem 12: Página de cadastro.



MINISTÉRIO DO MEIO AMBIENTE

Cadastro de Usuário

Nome Completo

E-mail

Senha

Informe seu nível de acesso

CADASTRAR-SE

VOLTAR

Fonte: Autor próprio.

Nesta tela o usuário pode estar informando seus dados e criar sua conta para ter o acesso ao sistema. Após se cadastrar, ele será direcionado para página de login, onde poderá estar realizando o seu cadastro e verificando as informações do sistema.

Imagem 13: Página de login.

A imagem mostra a interface de login de um aplicativo. No topo, há um cabeçalho com o texto "MINISTÉRIO DO MEIO AMBIENTE" em negrito. Abaixo dele, o título "Acesso ao Sistema" também em negrito. Seguem dois campos de entrada: "E-mail" e "Senha", cada um com uma linha de texto e uma borda inferior. Na base da tela, há três botões retangulares com fundo verde e texto branco: "ACESSO COM BIOMETRIA", "LOGAR-SE" e "VOLTAR", dispostos verticalmente.

Fonte: Autor próprio.

Nesta página o usuário pode fazer o seu login com o seu e-mail e senha cadastrados anteriormente e pode realizar o acesso ao sistema com a sua impressão digital clicando em "ACESSO COM BIOMETRIA".

Após clicar em acesso com biometria, o usuário irá se deparar com a seguinte página.

Imagem 14: Página de acesso com biometria.



The image shows a mobile application interface for the "MINISTÉRIO DO MEIO AMBIENTE". The screen is titled "Acesso ao Sistema". It features two input fields: "E-mail" and "Senha". Below these fields is a section for "Autenticação Biométrica" (Biometric Authentication). This section includes the instruction "Posicione seu dedo no leitor biométrico para acessar o sistema." (Position your finger on the biometric reader to access the system.) and a green fingerprint icon. Below the icon is the text "Toque no sensor de impressão digital" (Touch the digital impression sensor). At the bottom left of the biometric section is a "CANCELAR" (Cancel) button.

Fonte: Autor próprio.

Após realizar o escaneamento da sua digital, o usuário será direcionado para a página onde consegue realizar a visualização das informações de acordo com seu nível de acesso.

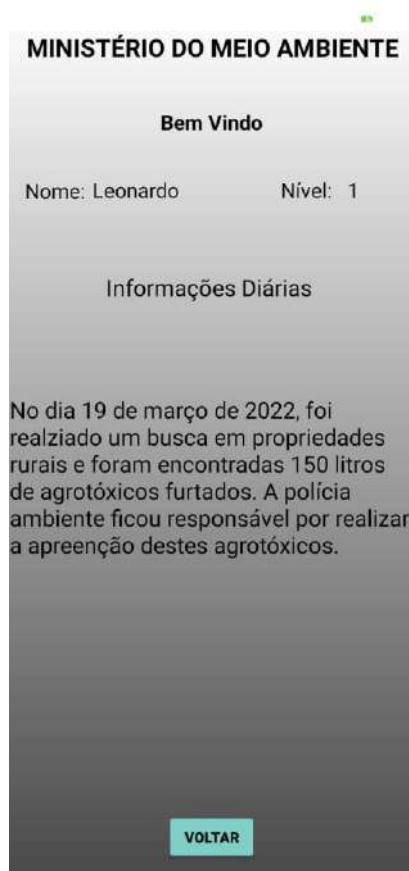
Imagem 15: Página de acesso as informações.



Fonte: Autor próprio.

Caso o usuário possua acesso ao primeiro nível, ele somente poderá acessar os dados públicos.

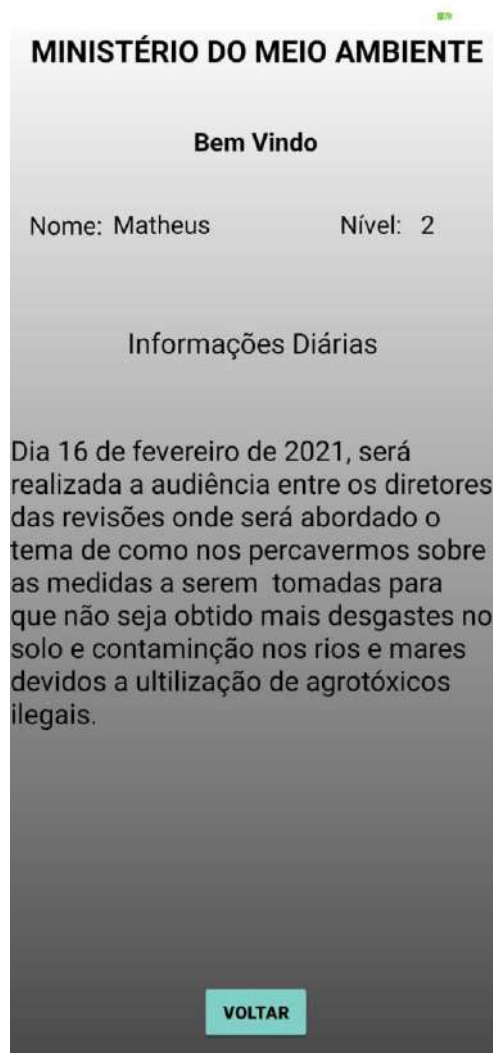
Imagem 16: Página de acesso as informações de primeiro nível.



Fonte: Autor próprio.

Caso o usuário possua acesso ao segundo nível, ele somente poderá acessar os dados públicos e os dados de segundo nível.

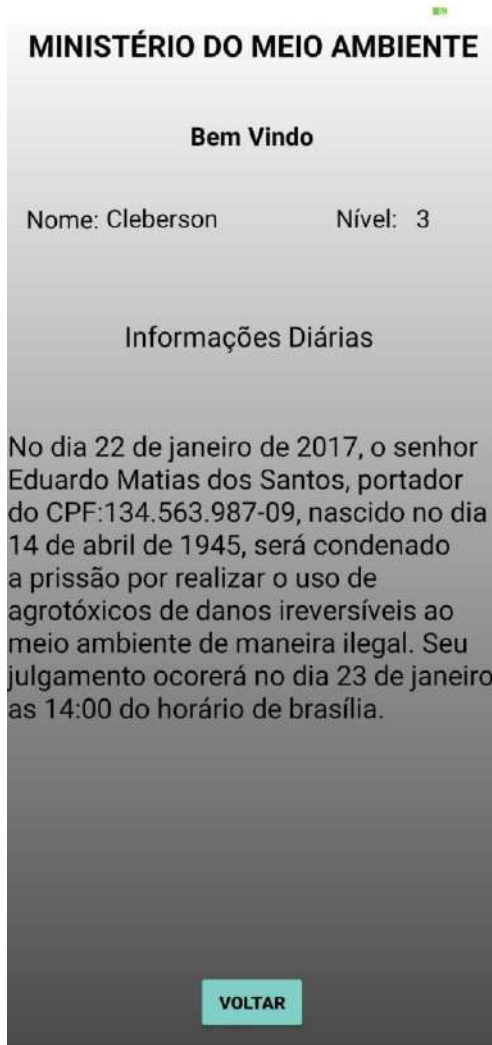
Imagem 17: Página de acesso as informações de terceiro nível.



Fonte: Autor próprio.

Caso o usuário possua acesso ao terceiro nível, ele poderá acessar todas as páginas, tendo a possibilidade de visualizar as informações sigilosas.

Imagem 18: Página de acesso as informações de terceiro nível



Fonte: Autor próprio.

6. CONSIDERAÇÕES FINAIS

Portanto, podemos concluir que minha APS (Atividade prática supervisionada), de forma que possa estar auxiliando o meio ambiente para a proteção contra a utilização de agrotóxicos.

BIBLIOGRAFIA

CBA. Consultores Biométricos Associados. História Geral da Biometria. Disponível em: < <https://www.hostinger.com.br/tutoriais/o-que-e-javascript>>. Acesso em: 08 de Novembro de 2022.

IBERDROLA. Biometria, a tecnologia que mede e analisa nossos dados biológicos. Disponível em: < <https://www.iberdrola.com/inovacao/vantagens-e-usos-da-biometria>>. Acesso em: 09 de Novembro de 2022.

SIMPLY. Biometria, entenda de vez este conceito. Disponível em: < <https://blog.simply.com.br/biometria-entenda-de-vez-esse-conceito/>>. Acesso em: 09 Novembro de 2022.

PTCOMPUTADOR. Técnicas biométricas. Disponível em: < <http://ptcomputador.com/Ferragens/computer-drives-storage/52845.html>>. Acesso em: 09 de Novembro de 2022.

GOGONI. Ronaldo Gogoni. O que é biometria? Os 6 tipos mais usados na tecnologia. Disponível em: <<https://tecnoblog.net/responde/o-que-e-biometria-tecnologia/>>. Acesso em: 10 de Novembro de 2022.

MENTORAMA. Java: o que é, para que serve e por que preciso dele?. Disponível em:< <https://mentorama.com.br/blog/java-o-que-e-para-que-serve-e-porque-preciso-dele/>>. Acesso em:10 de Novembro de 2022.

SILVA. Gizele Silva. O que é Firebase?. Disponível em: <<https://coodesh.com/blog/dicionario/o-que-e-firebase/>>. Acesso em: 12 de Novembro de 2022.


TIAGO. Tiago. Android Studio: O Que É E Como desenvolver Apps Nele. Disponível em: <<https://mundodevops.com/blog/android-studio/>>. Aceso em 12 de Novembro de 2022.

FICHA DAS ATIVIDADES PRÁTICAS SUPERVISIONADAS - APS

RA: T015209

TURNOS: Nocturno

2020/22

DATA DA ATIVIDADE	DESCRIÇÃO DA ATIVIDADE	TOTAL DE HORAS	ASSINATURA DO ALUNO	HORAS ATRIBUÍDAS (1)	ASSINATURA DO PROFESSOR
05/10	Análise sobre a proposta e busca do assunto	7 hrs	Leonardo Leite		
06/10	Estudos sobre o banco de dados Firebird	15hrs	Leonardo Leite		
07/10	Estudo sobre a linguagem Java para Android	10 hrs	Leonardo Leite		
08/10	Criação do banco de dados	5hrs	Leonardo Leite		
08/10	Criação do projeto e implementação do banco	6hrs	Leonardo Leite		
08/10	Fluxograma de implementação digital	15hrs	Leonardo Leite		
09/10	Início da documentação	9hrs	Leonardo Leite		
30/10	Montagem dos slides	3 hrs	Leonardo Leite		
18/11	montagem da ficha	5 hrs	Leonardo Leite		

(1) Horas atribuídas de acordo com o regulamento das Atividades Supervisionadas do curso

TOTAL DE HORAS ATRIBUÍDAS: 79

AValiação: Amélia

Aprovado ou Reprovado

DATA: 17/11/2022

CARIMBO E ASSINATURA DO COORDENADOR DO CURSO

Prof. Msc. Rafael Marcelino de Jesus
Coordenador Auxiliar do Curso de
Ciência da Computação
UNLP - Araçatuba/SP