Projeto Final - Avaliação A3

VERIFICADOR PIX

Relatório técnico apresentado na UC Sistemas Distribuídos e Mobile orientado pelo Prof. MSc Flávio Henrique da Silva.

Curitiba

2025

INTEGRANTES DO GRUPO

Morrison de Oliveira -
172411130

Lucas Frozza Ramos -
172410984

Arthur Zacarias Zavadski -
172416406

Pedro Henrique Stasiak –
172411184

SUMÁRIO

1 INTRODUÇÃO

O tema e funcionalidade deste trabalho foi desenvolvido com base nos golpes que ocorrem no dia a dia da população brasileira, principalmente levando em consideração, envios de chaves Pix falsas por golpistas, mas com múltiplos outros métodos utilizados por golpistas para enganar vítimas e induzi-las a realizar pagamentos indevidos.

Este projeto foi criado com o objetivo de permitir que empresas cadastrem suas chaves Pix oficiais neste aplicativo, para que evitem possíveis futuros golpes com seus clientes, possibilitando que os mesmos verifiquem a veracidade da chave informada antes de efetuarem pagamentos — seja para cobranças, pendências financeiras ou outras finalidades.

O aplicativo funciona como uma camada adicional de segurança para a empresa, na qual um administrador ("Admin") é responsável por cadastrar todas as chaves oficiais e confiáveis do sistema. O cliente final, ao receber uma chave, pode consultar no sistema se ela realmente é legítima ou se trata de uma tentativa de golpe.

2 DESENVOLVIMENTO

Este projeto foi desenvolvido utilizando Java, com o objetivo de verificar a autenticidade de chaves Pix. Nele, um administrador cadastra previamente as chaves Pix consideradas válidas e confiáveis. O cliente final, por sua vez, pode consultar uma chave recebida para verificar se ela está registrada entre as chaves autorizadas pelo administrador.

Esta aplicação, possui basicamente duas funcionalidades internas, cadastro de chaves oficiais e confiáveis e a verificação/confirmação do cliente final, referente a chave recebida. Essa estrutura visa oferecer ao leitor uma visão clara, confiável e completa do desenvolvimento, funcionamento e aplicação prática do sistema verificador de chaves Pix.

2.1 Divisão das Tarefas

Dividimos as tarefas deste trabalho em duplas: Morrison e Pedro; Arthur e Lucas. A primeira dupla, composta por Morrison e Pedro, foi responsável pelo front-end, back end e banco de dados. Já a segunda dupla, formada por Arthur e Lucas, ficou encarregada de melhorar o front-end e fazer o relatório final.

2.2 Estrutura do Projeto

O projeto Detector Pix foi desenvolvido em Java utilizando o framework Spring Boot, que é uma ferramenta bastante usada para criar aplicações web de forma simples e organizada. O principal objetivo desse sistema é verificar se um e-mail usado em uma transação Pix é verdadeiro ou se pode ser uma tentativa de golpe. A lógica do sistema funciona da seguinte forma: ele recebe um e-mail por meio de uma API, que é um ponto de acesso que outros sistemas ou pessoas podem usar para enviar informações. Esse e-mail é enviado para uma parte do sistema chamada service, que realiza a verificação usando regras internas e um banco de dados. O banco de dados utilizado é o MySQL, onde ficam armazenados os e-mails que já foram identificados como confiáveis ou suspeitos. O sistema pode comparar o e-mail recebido com esses registros e decidir se ele representa um risco ou não. A estrutura do projeto é formada por uma classe principal que inicia a aplicação, uma classe controladora que recebe os pedidos de verificação e um serviço que executa a lógica da checagem. Para facilitar o desenvolvimento, o projeto usa algumas bibliotecas importantes, como Spring Web para criar a API, Spring Data JPA para trabalhar com o banco de dados de

forma mais simples. De forma geral, este projeto é um exemplo prático de como Java e Spring Boot podem ser usados para construir soluções úteis e seguras

2.3 Explicação da Aplicação/Software

Ao iniciar o sistema Detector Pix, a aplicação começa a funcionar como um serviço web, aguardando o recebimento de e-mails que serão verificados. O funcionamento do sistema ocorre por meio de uma API, ou seja, ele recebe as informações por uma interface que pode ser acessada por outro sistema ou até mesmo por ferramentas de teste de requisições, como o Postman.

O primeiro passo é o usuário ou sistema externo enviar um e-mail para o endereço da API de verificação. Esse envio deve ser feito por uma requisição do tipo POST, contendo o e-mail que se deseja analisar. A aplicação então recebe esse dado e encaminha para a parte responsável por verificar se o e-mail é confiável.

Em seguida, o sistema analisa esse e-mail por meio de regras internas. Ele pode comparar o e-mail recebido com uma lista de e-mails já conhecidos, armazenados no banco de dados. Essa lista inclui tanto e-mails confiáveis quanto e-mails suspeitos ou já usados em fraudes. O sistema também pode verificar se o e-mail recebido é muito parecido com algum outro confiável, o que pode indicar uma tentativa de enganar a vítima por meio de pequenas alterações no endereço.

Após realizar a verificação, o sistema retorna uma resposta automática. Essa resposta informa se o e-mail analisado é seguro ou se representa um possível risco. Essa resposta pode ser visualizada diretamente pela ferramenta que fez o envio da requisição, como o Postman, ou pelo sistema que estiver integrado com a API. Todo esse processo é feito de forma rápida, automática e segura, permitindo que instituições ou usuários validem e-mails de transações Pix antes de realizarem pagamentos, evitando cair em golpes.

2.4 Orientações de execução da Aplicação/Software

O aplicativo funciona de forma intuitiva, dividido em duas partes: uma voltada para o administrador (Admin) e outra para os consumidores/clientes finais.

Na área do administrador, é realizado o cadastro das chaves Pix oficiais da empresa, além da inclusão de chaves suspeitas ou já associadas a tentativas de golpe. Por outro lado, o cliente final utiliza a aplicação para inserir a chave Pix recebida por email e verificar se ela está registrada como oficial no sistema, garantindo assim mais segurança antes de efetuar qualquer pagamento.

2.5 Repositório

https://github.com/PedroHenrique70/verificadorpix

3 CONCLUSÃO

O desenvolvimento deste projeto teve como foco principal criar uma ferramenta simples e eficaz para combater golpes envolvendo chaves Pix falsas. A partir da identificação de um problema comum no cotidiano dos brasileiros, foi proposta uma solução que permite a verificação da autenticidade de chaves cadastradas por empresas, oferecendo mais segurança tanto para quem realiza quanto para quem recebe pagamentos.

O trabalho foi dividido de forma colaborativa entre duas duplas de um só grupo. A primeira foi responsável por estruturar a base do sistema e validar a ideia inicial em Java. A segunda dupla aprimorou a aplicação, implementando melhorias no desempenho e na interface, resultando em um produto mais próximo do que se espera de uma solução real e utilizável, realizando também, este relatório final, claro.

O projeto cumpriu seu papel de demonstrar, na prática, como a tecnologia pode ser aplicada para prevenir fraudes e proteger os usuários, além de reforçar a importância da organização e cooperação no desenvolvimento de soluções digitais.

REFERÊNCIAS

https://start.spring.io/

Linguagem JAVA para o back-end.

HTML e CSS para o front-end.

MySQL do Xampp para o banco de dados.