Uma imagem com texto, Tipo de letra, captura de ecrã, Gráficos

Descrição gerada automaticamente

**Faculdade de Ciências da Universidade de Lisboa**

**Departamento de Informática**

**Mestrado em Engenharia Informática**

Relatório

**Privacidade e Segurança de Dados**

***Projeto (Segunda Fase)***

**Rodrigo Craveiro Rodrigues (Nº64370)**

**Diogo Serrano Sargaço (Nº58252)**

**André Filipe Diniz Belo (Nº58211)**

Professor: **Doutor** **Bernardo Ferreira**

1º Semestre Letivo 2024/2025

**dezembro 2024**

Índice

[1. Introdução 3](#_Toc181808179)

[2. Funcionalidades Adicionadas e Implementações 3](#_Toc181808180)

[2.1 Conversas em Grupo 3](#_Toc181808181)

[2.1.1 Conceitos Teóricos 3](#_Toc181808182)

[2.1.2 Implementação Técnica 3](#_Toc181808183)

[2.1.3 Desafios e Soluções 3](#_Toc181808184)

[2.2 Armazenamento de Longo Prazo e Alta Disponibilidade 4](#_Toc181808185)

[2.2.1 Conceitos de Disponibilidade e Segurança 4](#_Toc181808186)

[2.2.2 Implementação e Estrutura do Sistema 4](#_Toc181808187)

[2.2.3 Garantias de Privacidade e Segurança 4](#_Toc181808188)

[2.3 Pesquisa de Mensagens Preservando a Privacidade 4](#_Toc181808189)

[2.3.1 Técnicas de Pesquisa Segura 4](#_Toc181808190)

[2.3.2 Arquitetura da Implementação 5](#_Toc181808191)

[2.3.3 Desafios e Soluções 5](#_Toc181808192)

[2.4 Sistema de Recomendação Preservando a Privacidade 5](#_Toc181808193)

[2.4.1 Conceitos de Recomendação e Segurança 5](#_Toc181808194)

[2.4.2 Arquitetura de Implementação e Algoritmos 5](#_Toc181808195)

[2.4.3 Estratégias para Garantir Privacidade 6](#_Toc181808196)

[3. Comparação com a Primeira Fase 6](#_Toc181808197)

[4. Desafios e Soluções Implementadas 6](#_Toc181808198)

[5. Referências 6](#_Toc181808199)

# 1. Introdução

Nesta segunda fase do projeto, a aplicação foi aprimorada com a adição de novas funcionalidades que aumentam a complexidade e a utilidade do sistema. Além de suportar comunicação segura ponto-a-ponto de forma descentralizada, foi adicionado novas funcionalidades de forma a possibilitar conversas em grupo (com base em tópicos de interesse), armazenamento persistente e replicado das mensagens, funcionalidades de pesquisa rápida de palavras-chaves, e um sistema de recomendações consoante o perfil do cliente. As melhorias foram feitas com uma atenção especial à segurança, privacidade e desempenho, utilizando conceitos avançados de criptografia e estratégias de armazenamento seguro abordados em sala de aula.

# 2. Funcionalidades Adicionadas e Implementações

## 2.1 Conversas em Grupo

### 2.1.1 Conceitos Teóricos

Conversas em grupo em sistemas de mensagens seguras são desafiadoras porque requerem que uma única chave de sessão seja compartilhada entre múltiplos membros, garantindo que apenas os participantes autorizados possam desencriptar as mensagens. O objetivo é proporcionar confidencialidade, integridade e autenticação das mensagens. Técnicas como o protocolo de Troca de Chaves de Diffie-Hellman com Curvas Elípticas (ECDH) são fundamentais para estabelecer estas garantias em um ambiente descentralizado.

### 2.1.2 Implementação Técnica

Troca de Chaves Segura: Utilizamos o protocolo ECDH para gerar uma chave de sessão partilhada entre todos os membros do grupo. Cada membro do grupo gera um par de chaves (privada e pública) e troca as chaves públicas com os outros membros. O segredo compartilhado derivado é usado para gerar a chave de encriptação AES.

Encriptação AES-GCM: Para cada mensagem enviada, utilizamos o modo AES-GCM, que oferece confidencialidade e integridade. O nonce e o tag de autenticação são manipulados para garantir que cada mensagem seja única e que qualquer tentativa de manipulação seja detectada.

Gestão de Membros do Grupo: O sistema permite a criação e a gestão de grupos por tópicos de interesse. A interface gráfica facilita a visualização e a participação em diferentes grupos.

### 2.1.3 Desafios e Soluções

Distribuição Segura das Chaves: Garantir que a chave de sessão não seja comprometida foi um desafio. Resolvemos isso utilizando a criptografia ECDH para derivar chaves de forma segura.

Performance: A encriptação em tempo real de mensagens para múltiplos destinatários pode ser intensiva em termos de recursos. Optámos por otimizar o processo de encriptação utilizando a biblioteca “cryptography”.

## 2.2 Armazenamento de Longo Prazo e Alta Disponibilidade

### 2.2.1 Conceitos de Disponibilidade e Segurança

A disponibilidade de mensagens em um sistema distribuído implica garantir que as mensagens estejam sempre acessíveis, mesmo em caso de falha do dispositivo do utilizador ou de um provedor de nuvem. Para isso, é fundamental replicar as mensagens em múltiplos locais e proteger os dados contra acessos não autorizados. Adicionalmente, a criptografia de dados em repouso é crucial para garantir que mesmo que um provedor seja comprometido, os dados permaneçam protegidos.

### 2.2.2 Implementação e Estrutura do Sistema

Firebase para Armazenamento: As mensagens são armazenadas de forma persistente na base de dados Firebase. A escolha do Firebase foi baseada na sua escalabilidade e facilidade de integração com Python.

Replicação de Mensagens: Para garantir a alta disponibilidade, as mensagens são replicadas em diferentes localizações dentro do Firebase. Esta estratégia permite que os dados sejam recuperados mesmo em caso de comprometimento de um único ponto de armazenamento.

Encriptação de Dados em Repouso: Antes de serem enviadas para a nuvem, as mensagens são encriptadas usando AES-GCM. Isso garante que o provedor de armazenamento não possa aceder ao conteúdo sem a chave de encriptação.

### 2.2.3 Garantias de Privacidade e Segurança

Proteção Contra Acessos Não Autorizados: Como os dados são encriptados antes de serem enviados para a nuvem, mesmo um ataque ao provedor não comprometerá a privacidade das mensagens.

Gestão de Chaves: As chaves privadas e de sessão são armazenadas localmente e protegidas contra acessos indevidos. Para ambientes de produção, recomendamos o uso de métodos de proteção mais robustos, como armazenamento em hardware seguro.

## 2.3 Pesquisa de Mensagens Preservando a Privacidade

### 2.3.1 Técnicas de Pesquisa Segura

A pesquisa de mensagens em sistemas criptografados representa um desafio, pois não se pode comprometer a privacidade das mensagens. Técnicas como encriptação homomórfica, índices encriptados, ou pesquisa baseada em tokens seguros são utilizadas para realizar buscas sem expor o conteúdo.

### 2.3.2 Arquitetura da Implementação

Palavras-Chave e Índices: Criamos índices encriptados para cada mensagem, facilitando a pesquisa sem revelar o conteúdo. A pesquisa é feita localmente, comparando palavras-chave fornecidas pelo utilizador com os índices armazenados.

Interface de Pesquisa: A interface permite ao utilizador inserir palavras-chave e retorna mensagens relevantes, mantendo a simplicidade de uso e a segurança.

### 2.3.3 Desafios e Soluções

Performance da Pesquisa: A busca em mensagens encriptadas pode ser lenta. Implementámos uma indexação eficiente para melhorar o desempenho.

Segurança dos Resultados: Garantimos que os resultados da pesquisa não exponham informações sensíveis, mesmo em caso de acesso não autorizado.

## 2.4 Sistema de Recomendação Preservando a Privacidade

### 2.4.1 Conceitos de Recomendação e Segurança

Sistemas de recomendação tradicionalmente analisam o comportamento dos utilizadores e fornecem sugestões com base nas suas preferências. No entanto, garantir a privacidade e anonimato dos utilizadores ao realizar este processo é um desafio. Utilizamos técnicas de anonimização e análise segura de dados para construir um sistema que não compromete a privacidade.

### 2.4.2 Arquitetura de Implementação e Algoritmos

Análise de Mensagens: As mensagens são analisadas localmente para extrair palavras-chave relevantes. O sistema gera recomendações com base em palavras como "desporto", “música” ou “viagem”.

Sistema de Recomendação Descentralizado: As recomendações são armazenadas no Firebase, mas sem associar diretamente o utilizador às suas mensagens. Isso garante que o sistema seja seguro e preserva o anonimato.

Segurança e Privacidade: Nenhum dado sensível é enviado ou armazenado sem encriptação. As mensagens são analisadas de forma local e segura.

### 2.4.3 Estratégias para Garantir Privacidade

**Anonimização:** Os identificadores dos utilizadores são substituídos por pseudónimos antes de serem enviados para a nuvem.

**Segurança de Dados:** As mensagens são processadas e analisadas em ambiente seguro, garantindo que nenhum dado sensível é exposto.

# 3. Comparação com a Primeira Fase

**Troca de Chaves:** Na primeira fase, a troca de chaves era feita de forma ponto-a-ponto. Agora, expandimos para suportar grupos de conversa.

**Armazenamento:** Na primeira fase, as mensagens eram armazenadas localmente; na segunda fase, introduzimos armazenamento persistente em nuvem.

**Interface Gráfica:** A interface foi aprimorada com suporte a grupos, pesquisa de mensagens e recomendações.

# 4. Desafios e Soluções Implementadas

**Descentralização vs. Performance:** Implementar um sistema que seja tanto descentralizado quanto eficiente foi um desafio significativo. Utilizámos um modelo híbrido que aproveita o melhor de ambos os mundos.

**Segurança e Privacidade:** Proteger os dados dos utilizadores contra acesso não autorizado enquanto se mantém a usabilidade do sistema exigiu o uso de técnicas avançadas de criptografia.

**Gerir Múltiplas Conexões:** A introdução de grupos e a necessidade de armazenamento em nuvem aumentaram a complexidade da gestão de conexões, exigindo uma gestão otimizada de threads.

# 5. Referências

**Firebase Admin SDK:** Documentação Firebase

**Referências PSD:** Link para GitHub