Všeobecný popis aplikácie

1.1 Účel a vlastnosti:
Aplikácia predstavuje zašifrované online úložisko súborov, kde:
- Šifrovanie a dešifrovanie prebiehajú výlučne na strane klienta (End-to-End).
- Privátne kľúče (alebo seed/tajné dáta) nikdy neopúšťajú zariadenie používateľa.
- Na serveri sú uložené len zašifrované súbory a verejné kľúče používateľov.
- Verejné kľúče sú dostupné pre jednoduchú výmenu súborov medzi používateľmi (klient automaticky získava verejný kľúč príjemcu zo servera).

Hlavný cieľ - zabezpečiť dôvernosť údajov (server nedokáže dešifrovať súbory), a zároveň zjednodušiť výmenu kľúčov (server funguje ako “Key Directory”).

1.2 Cieľová skupina:
- Študenti, učitelia, výskumní pracovníci, ktorí potrebujú bezpečne zdieľať dokumenty.
- Firmy a freelanceri, ktorí si cenia dôvernosť údajov (obchodné ponuky, zmluvy).
- Široká verejnosť, ktorej záleží na bezpečnom ukladaní a zdieľaní súborov.

1.3 Použitie na rôznych zariadeniach:
- Desktop (Windows/Linux/macOS): prístup cez webový prehliadač (Chrome, Firefox, Edge).
- Mobilné zariadenia (iOS, Android): responzívny dizajn

Požiadavky používateľov
2.1 Používateľské role:
2.1.1) Hosť (neprihlásený):
- Môže prezerať niektoré súbory, ak vlastník vytvoril verejný odkaz.
- Nemôže nahrávať nové súbory a dešifrovať súkromné súbory.

2.1.2) Registrovaný používateľ:
- Pri registrácii generuje pár kľúčov (verejný + privátny) lokálne.
- Server ukladá iba verejný kľúč pre jednoduché zdieľanie.

- Môže nahrávať súbory (šifruje lokálne pomocou verejného kľúča alebo hybridne).
- Môže zdieľať súbory s inými používateľmi.
- Dešifruje len tie súbory, ku ktorým má privátny kľúč.

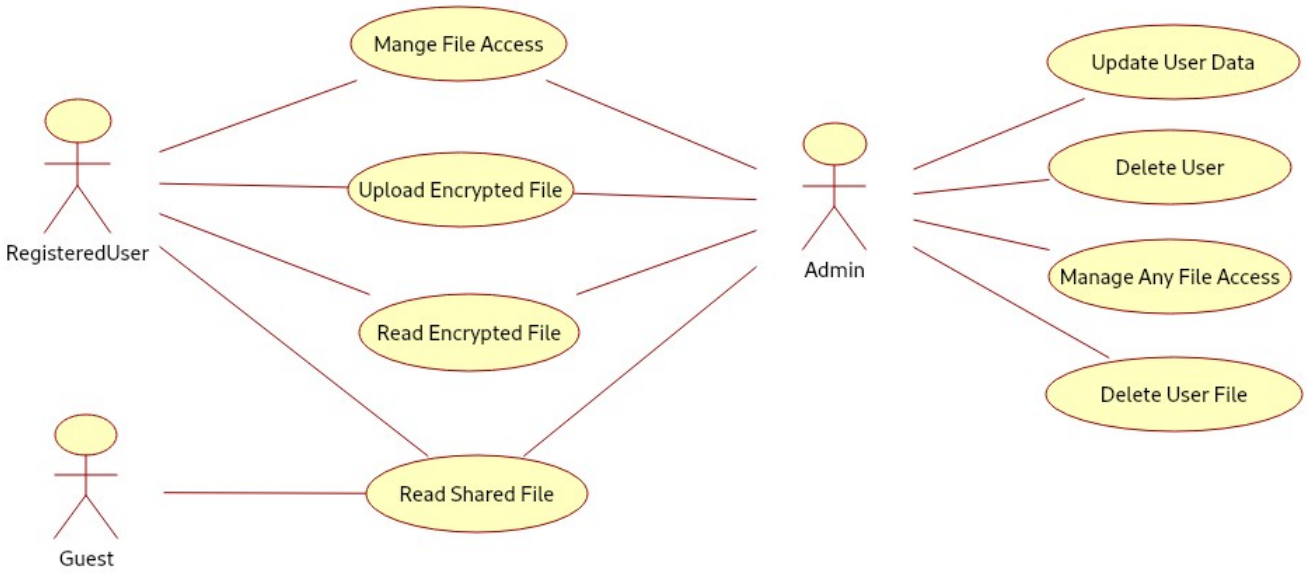
2.1.3) Administrátor:
- Spravuje používateľské účty (aktivácia, blokovanie, kvóty).
- Vidí metadáta súborov (veľkosť, hash, vlastník) a verejné kľúče.
- Nemôže dešifrovať súbory (nemá privátne kľúče).

2.2 Scenáre použitia (Use Cases):

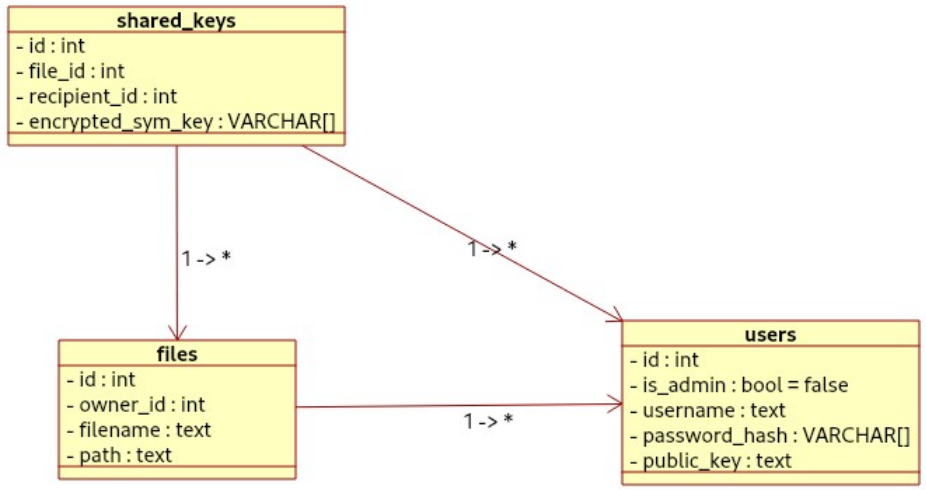
UC1: Registrácia a generovanie kľúčov:
- Aktér: Nový používateľ
- Scenár:
2.2.1.1) Vyplní registračný formulár (meno, heslo).
2.2.1.2) Aplikácia lokálne vygeneruje kľúče.
2.2.1.3) Verejný kľúč odošle na server, privátny uloží lokálne.
2.2.1.4) Server vytvorí účet s verejným kľúčom.

UC2: Nahranie zašifrovaného súboru:
- Aktér: Registrovaný používateľ
- Scenár:
2.2.2.1) Používateľ vyberie súbor.
2.2.2.2) Súbor sa lokálne zašifruje (symetrický kľúč + zašifrovanie verejným kľúčom).
2.2.2.3) Na server sa odošle už zašifrovaný súbor.
2.2.2.4) Server uloží súbor a vráti odkaz alebo ID.

UC3: Zdieľanie súboru:
- Aktér: Vlastník súboru
- Scenár:
2.2.3.1) Vyberie súbor a príjemcu.
2.2.3.2) Aplikácia získa verejný kľúč príjemcu zo servera.
2.2.3.3) Lokálne prešifruje symetrický kľúč pod verejný kľúč príjemcu.
2.2.3.4) Príjemca môže súbor dešifrovať svojim privátnym kľúčom.



Dátový model:



users (id, is_admin, username, password_hash, public_key)
files (id, owner_id -> users.id, filename, ciphertext_path)

shared_keys (id, file_id -> files.id, recipient_id -> users.id, encrypted_sym_key)

Súbor má viacero kópií kľúča, každý zašifrovaný verejným kľúčom príjemcu.

Technologické požiadavky:
4.1 Klient:
- Web API
- React, Bootstrap.
- Responzívny dizajn pre mobilné zariadenia

4.2 Server:
- Jazyk: Python 3.12
- Framework: Django 5.x
- Databáza: PostgreSQL 16
- HTTPS, hashovanie hesiel, server neukladá privátne kľúče.

4.3 Databáza: PostgreSQL, tabuľky: users, files, shared_keys

4.4 Hosting: VPS, HTTPS certifikát, zabezpečený prístup k databáze.

4.5 Podporované prehliadače: Google Chrome, Mozilla Firefox

4.6 Klient-Server rozhranie: REST API (JSON), komunikácia cez HTTPS.

Časový plán:
4 týždeň - Návrh DB, ER diagram, výber šifrovacej knižnice
5 týždeň - Registrácia, generovanie kľúčov
6 týždeň - Nahrávanie súborov (šifrovanie klienta)
7 týždeň - Zdieľanie súborov (shared_keys)
8 týždeň - UI/UX, testovanie
9 týždeň - Optimalizácia, bezpečnosť, testovanie, príprava betaverzie
10 týždeň - Dokumentácia, finalizácia betaverzie
11 týždeň - Zapracovanie spätnej väzby

Záver
Server: Uchováva verejné kľúče a zašifrované súbory bez možnosti dešifrovania.
Klient: Realizuje end-to-end šifrovanie a správu kľúčov.
Administrátor: Spravuje účty a bezpečnosť bez prístupu k obsahu súborov.