Мэдээллийн сүлжээ,
аюулгүй байдлын салбар

Кибер аюулгүй байдал
мэргэжил

Прокси дахин шифрлэх схемд суурилсан туршилтын систем хөгжүүлэх нь

Гүйцэтгэсэн: А.Мягмарцэрэн (B190970106)

Удирдагч: В.Нямсүрэн (Доктор Ph.D)
Зөвлөх багш: В.Нямсүрэн (Доктор Ph.D)
Ц.Манлайбаатар (Магистр)

Агуулга

Зорилго

Прокси дахин шифрлэх схемийг ашиглан шифрлэсэн файл хуваалцах туршилтын системийн систем хөгжүүлэх.

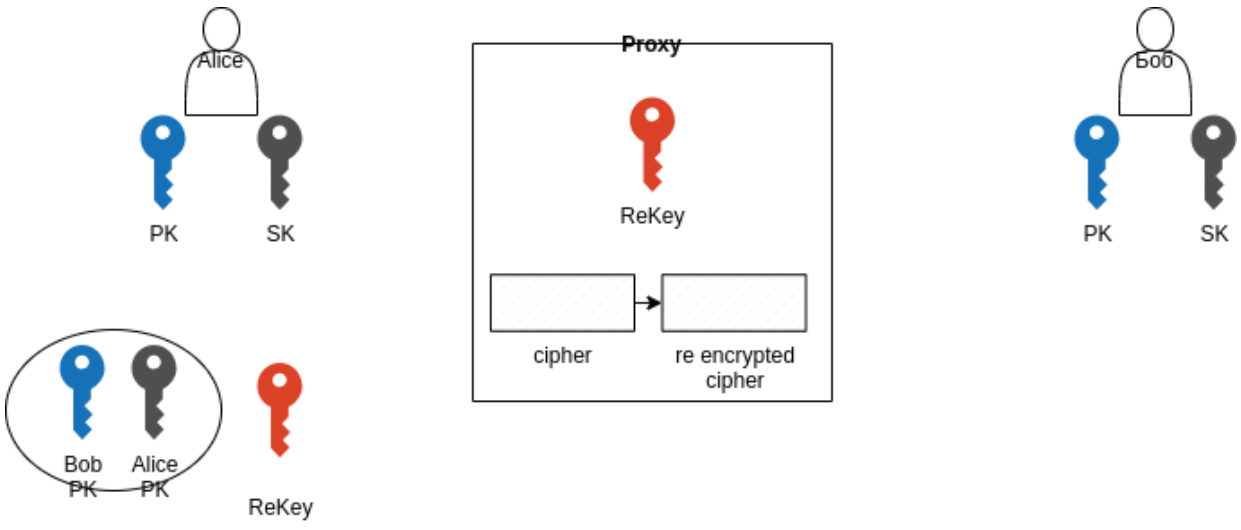
Файл хуваалцахад учрах аюулгүйн байдлын эрсдэл

Шифрлэх схемүүд

- Танилтад суурилсан шифрлэлт
- Шинж чанарт суурилсан шифрлэлт
- Гомоморф шифрлэлт
- Прокси дахин шифрлэлт

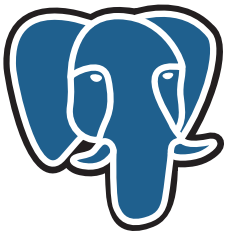
Прокси дахин шифрлэх схем

1. Алис өөрийн PK -ээр шифрлэнэ.
2. Боб-ын PK болон өөрийн SK-г ашиглан ReKey үүсгэнэ.
3. Прокси Алис-ын шифрийг ReKey-р дахин шифрлэнэ
4. Боб шифрийг өөрийн SK-г тайлна.



Ашигласан технологи

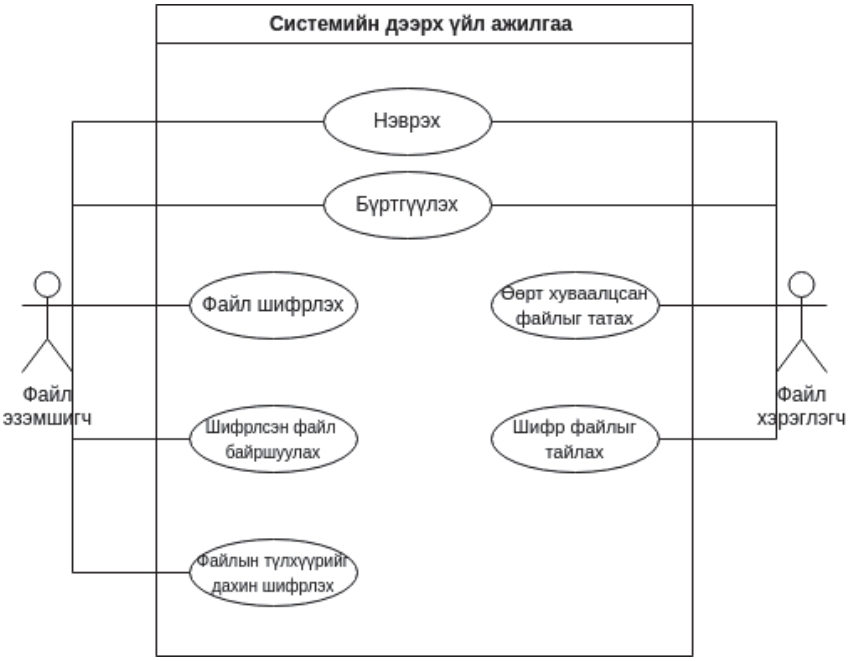
- Flask
- Tkinter
- PyUmbral
- PostgreSQL



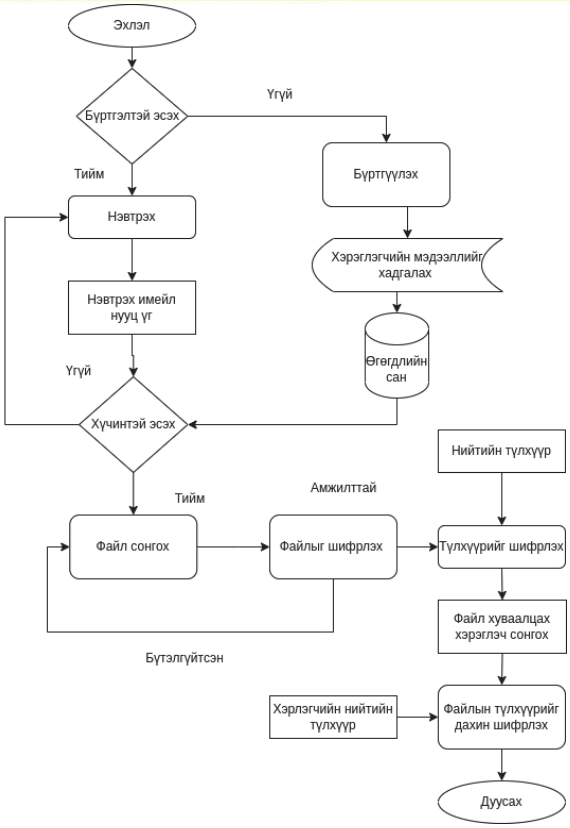
Flask

Ерөнхий загвар

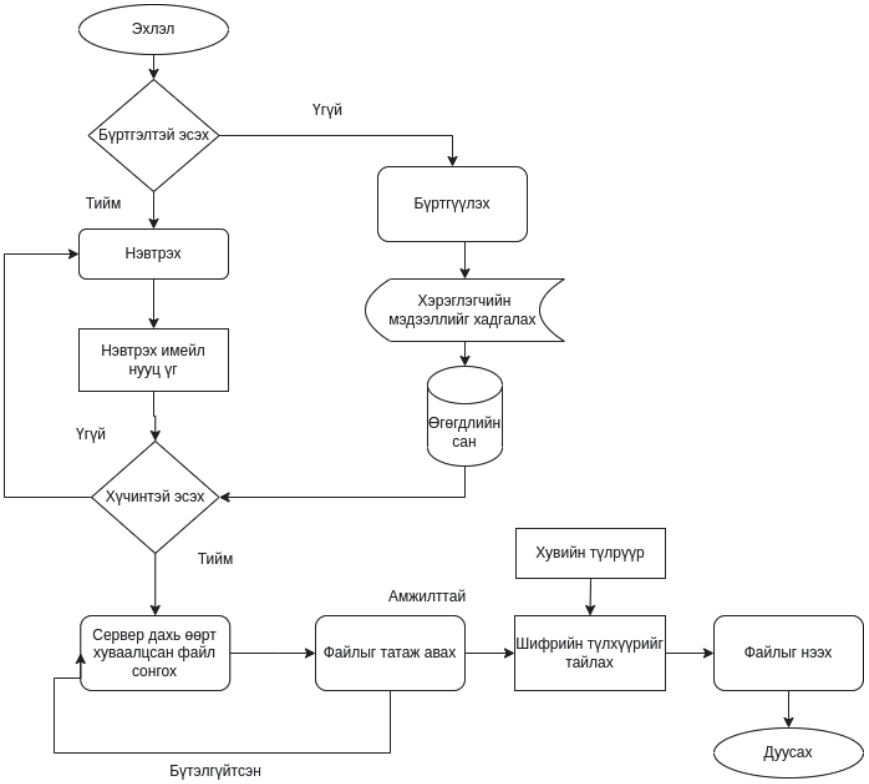
Юзкейс диаграмм



Үйл ажиллагааны диаграмм



Үйл ажиллагааны диаграмм



ДҮГНЭЛТ

- Прокси дахин шифрлэхийн схемийг талаар ойлголт авч түүнийгээ практик байдлаар өөрийн файл хуваалцах туршилтын системийг хөгжүүллээ. Бүрэн гүйцэд сайн систем болоогүй ч үргэлжлүүлэн хөгжүүлэх боломжтой.

Анхаарал хандуулсанд баярлалаа.