پروژه پایانترم: سیستم انتقال امن فایل در سازمان

هدف پروژه:

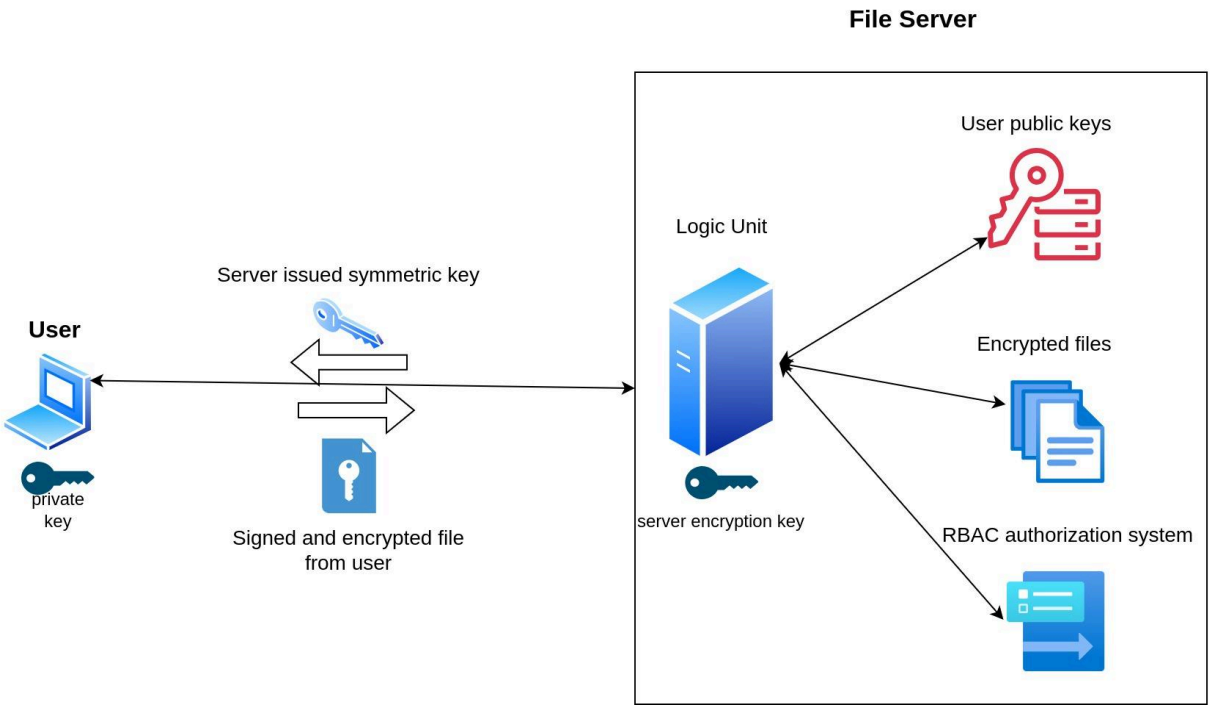
هدف این پروژه، ایجاد یک سیستم انتقال فایل بین کلاینت ها از طریف یک file server مرکزی به صورت امن است. در این پروژه شما به صورت عملی با مفاهیم زیر آشنا خواهید شد:

role-based access control, data encryption in transit, data encryption at rest, ensuring data integrity via digital signatures

پیش‌نیازها:

1. آشنایی با انواع مختلف الگوریتم های رمزنگاری
2. آشنایی با RBAC
3. آشنایی با مفاهیم شبکه و سوکت‌ها

توضیحات کلی پروژه:



فایل سرور:

- ارتباط بین کلاینت و سرور باید از طریق سوکت باشد.
- همزمان چندین کلاینت باید بتوانند با سرور تبادل اطلاعات داشته باشند.
- سه سطح دسترسی admin, maintainer و guest را ایجاد کنید.
  - دسترسی admin: ساخت، حذف و تغییر دسترسی کاربران - آپلود، دانلود و حذف تمامی فایل ها
  - دسترسی maintainer: آپلود فایل و مدیریت فایل های خود برروی سرور - دانلود تمامی فایل ها
  - دسترسی guest: دانلود تمامی فایل ها
- کلید های عمومی تمامی کاربران باید برروی سرور قرار گیرد و توسط همه کاربران قابل دسترس باشد.
- فایل های دریافتی از سمت کاربران (امضا شده) توسط server encryption key رمز میشوند و سمت سرور ذخیره میشوند. (data encryption at rest)

کاربران:

- هر کاربر پس از ثبت نام دسترسی پیش فرض guest را دارد.
- هر کاربر کلید خصوصی مخصوص به خود را دارد و در هنگام ثبت نام کاربران باید کلید عمومی خود را برای سرور ارسال کنند.

انتقال فایل:

- پس از هر ارتباط کلاینت و سرور یک symmetric key جدید، سمت سرور ایجاد شده و برای کلاینت ارسال میشود و تمامی اطلاعات ارسالی بین آن ها تا زمانی که ارتباط برقرار است ازین طریق رمز میشود.
- در صورتی که کاربر بخواهد فایلی را سمت سرور ارسال کند مراحل زیر طی میشود:
  a. کاربر با استفاده از private key خود، فایل انتخابی را امضا میکند.
  b. کاربر فایل امضا شده خود را با استفاده از کلید متقارن دریافتی از سمت سرور رمز میکند.
  c. در صورتی که کاربر دسترسی های لازم را داشته باشد، فایل بصورت امن انتقال می یابد.
- در صورتی که کاربر بخواهد فایلی را از سمت سرور دریافت کند مراحل زیر طی میشود:
  a. کاربر فایل انتخاب شده را درخواست میکند.
  b. سرور فایل را decrypt میکند و برای کاربر بصورت امن ارسال میکند.
  c. کاربر پس از دریافت فایل و رمز گشایی آن، integrity فایل دریافتی را با استفاده از امضای آن بررسی میکند.
  d. فایل به درستی برای کاربر ذخیره میشود.

نکات تکمیلی پروژه:

- انتخاب الگوریتم های رمزنگاری استفاده شده بر عهده دانشجویان است. (برای برتری انتخاب خود باید دلیلی موجه داشته باشید.)
- هر دستوری که توسط کاربر ارسال میشود ابتدا باید توسط authorization system چک شود و در صورت مجاز بودن انجام شود.
- برای ذخیره سازی داده های هویتی کاربران حتما از پایگاه داده استفاده شود.
- تمامی مراحل انجام شده پروژه باید به همراه توضیحات داکیومنت شود و به همراه پروژه آپلود شود.
- برای پیاده سازی پروژه میتوانید از زبان برنامه نویسی دلخواه استفاده کنید.

موارد نمره اضافه:

- امن سازی فرآیند دریافت کلید متقارن برای هر session.
- هر گونه خلاقیت در راستای بهبود فرآیند ذکر شده.

معیارهای ارزیابی:

- عملکرد صحیح سرور و کلاینت‌ها.
- رعایت مدیریت دسترسی.
- کیفیت پیاده سازی موارد خواسته شده در خصوص رمزنگاری و ذخیره اطلاعات.
- کیفیت مستندات و توضیحات.