به نام خدا

پروپوزال پروژه Safe Drive

درس مهندسی نرم‌افزار

دانشکده مهندسی کامپیوتر - دانشگاه صنعتی اصفهان

نیمسال اول تحصیلی 1403-1404

نام تیم:

App Mipokhteam

نام پروژه:

Safe Drive

اعضای تیم و اطلاعات تماس:

1. **فاطمه خلیلی**
   - ایمیل: f.khalili@ec.iut.ac.ir
2. **دانیال هادی‌زاده**
   - ایمیل: d.hadizadeh@ec.iut.ac.ir
3. **امیررضا قلی‌زاده**
   - ایمیل: a.gholizadeh@ec.iut.ac.ir
4. **علیرضا گلستان هاشمی**
   - ایمیل: a.golestan@ec.iut.ac.ir

معرفی کلی پروژه

پروژه Safe Drive یک سامانه نوین برای ذخیره‌سازی فایل‌های رمزنگاری‌شده به صورت کاملاً غیرمتمرکز است. با پیشرفت فناوری و دیجیتالی شدن اطلاعات، نیاز به محافظت از حریم خصوصی افراد بیش از پیش احساس می‌شود. امروزه، افراد و سازمان‌ها حجم وسیعی از اطلاعات شخصی، حساس و مالی خود را به صورت دیجیتالی ذخیره می‌کنند. این اطلاعات ممکن است شامل اسناد حقوقی، اطلاعات مالی، داده‌های محرمانه‌ی شرکت‌ها و حتی فایل‌های شخصی کاربران باشد. از این رو، امنیت این داده‌ها اهمیت زیادی پیدا کرده است.

پروژه Safe Drive قصد دارد فضایی را فراهم کند که کاربران بتوانند فایل‌های خود را به صورت کاملاً امن و رمزنگاری‌شده ذخیره کنند، بدون اینکه نیازی به اعتماد به یک سرویس‌دهنده متمرکز داشته باشند. این سیستم به گونه‌ای طراحی شده است که با توزیع اطلاعات در بین چندین سرور و استفاده از تکنولوژی‌های رمزنگاری پیشرفته، امکان دسترسی غیرمجاز به فایل‌ها عملاً غیرممکن شود. بنابراین، حتی اگر یکی از سرورها دچار نفوذ شود، هیچ اطلاعات مفیدی از کاربران به سرقت نخواهد رفت.

همچنین Safe Drive با بهره‌مندی از تکنیک End to End Encryption به گونه‌ای طراحی خواهد شد که تضمینی دائمی از دسترسی به فایل ها فقط توسط کاربر خواهد داد.

تکنیک End to End Encryption در Safe Drive به گونه‌ای طراحی خواهد شد که هر فایلی که قصد آپلود شدن در شبکه را دارد قبل از خروج از سیستم میزبان (شخصی که میخواهد فایلی را آپلود کند) به طور کامل رمزنگاری می شود و سپس در دیتابیسی غیر متمرکز ذخیره خواهد شد و رمزگشایی فایل فقط توسط خود کاربر امکان پذیر خواهد بود. (encryption & decryption at client side)

بدین گونه حتی اگر تمام شبکه توسط سازمانی یا دولتی کنترل شود، هیچ اطلاعاتی (حتی metadata از فایل ها) استخراج نمی تواند بشود.

علاوه بر این، Safe Drive قابلیت مقیاس‌پذیری بالایی دارد و می‌تواند برای هر دو گروه کاربران فردی و سازمانی راه‌حل مناسبی ارائه دهد.

نوآوری‌های پروژه

پروژه Safe Drive شامل چندین نوآوری منحصر به فرد است که آن را از سایر پلتفرم‌های ذخیره‌سازی فایل متمایز می‌کند:

استفاده از رمزنگاری پیشرفته: در Safe Drive، هر فایل پیش از بارگذاری روی سیستم به صورت محلی توسط دستگاه کاربر رمزنگاری می‌شود. این به این معناست که فایل‌ها هرگز بدون رمزنگاری به سرورها ارسال نمی‌شوند. رمزنگاری فایل‌ها بر اساس الگوریتم‌های رمزنگاری مدرن انجام می‌شود که باعث می‌شود حتی اگر فایل‌ها در دسترس افراد غیرمجاز قرار گیرد، هیچ‌گونه اطلاعات مفیدی از آن‌ها استخراج نشود.

ذخیره‌سازی غیرمتمرکز: برخلاف بسیاری از سیستم‌های ذخیره‌سازی ابری که فایل‌ها را در یک یا چند سرور متمرکز ذخیره می‌کنند، Safe Drive از یک معماری کاملاً غیرمتمرکز استفاده می‌کند. این بدان معناست که فایل‌های کاربران در چندین مکان و سرور توزیع شده و ذخیره می‌شوند. این سیستم باعث افزایش امنیت و دسترسی‌پذیری فایل‌ها می‌شود؛ زیرا در صورت بروز خرابی یا نفوذ در یک سرور، سایر سرورها می‌توانند داده‌ها را بازیابی کنند.

ناشناسی کاربران: در اکثر سرویس‌های مختلفی که در فضای اینترنت به ارائه خدمات می‌پردازند، نیاز به ساخت یک اکانت وجود دارد که به صورت متعارف نیاز به ایمیل یا شماره تلفن یا حتی اطلاعات شخصی تری شامل محل زندگی، کد ملی و... وجود دارد. اما در Safe Drive به لطف ایده نوآورانه Mnemonic Phrase، نیازی به هیچکدام از این اطلاعات وجود ندارد.

پلتفرم کاربرپسند: Safe Drive یک رابط کاربری ساده و کاربرپسند ارائه می‌دهد که کاربران به راحتی می‌توانند فایل‌های خود را مدیریت، بارگذاری و دانلود کنند. این سیستم با تمام دستگاه‌های مدرن سازگاری دارد و کاربران می‌توانند به راحتی از طریق تلفن همراه، تبلت یا رایانه‌های شخصی به فایل‌های خود دسترسی داشته باشند.

همکاری با سایر سرویس‌ها: یکی دیگر از ویژگی‌های مهم Safe Drive، قابلیت همکاری با دیگر پلتفرم‌های ابری است. این ویژگی به کاربران امکان می‌دهد فایل‌های خود را بین Safe Drive و دیگر سرویس‌های ابری مانند Google Drive و Dropbox همگام‌سازی کنند و مدیریت یکپارچه‌ای بر روی تمام فایل‌های خود داشته باشند.

جامعه هدف

پروژه Safe Drive برای پاسخگویی به نیازهای گسترده‌ای از کاربران طراحی شده است. جامعه هدف این پروژه شامل افراد و سازمان‌هایی است که به دنبال یک فضای امن و خصوصی برای ذخیره‌سازی اطلاعات حساس خود هستند. این پروژه به دو دسته کلی از کاربران توجه دارد:

کاربران شخصی: این گروه شامل افرادی است که به دنبال راهکاری امن برای ذخیره‌سازی اطلاعات شخصی و خصوصی خود هستند. این اطلاعات ممکن است شامل عکس‌ها، فیلم‌ها، اسناد مهم و سایر فایل‌های حساس باشد. با استفاده از Safe Drive، این کاربران می‌توانند از امنیت فایل‌های خود مطمئن باشند و بدانند که اطلاعاتشان در برابر دسترسی غیرمجاز محافظت می‌شود.

سازمان‌ها و شرکت‌ها: بسیاری از سازمان‌ها و شرکت‌ها به دنبال راه‌حلی برای ذخیره‌سازی امن اطلاعات مالی، حقوقی و تجاری خود هستند. Safe Drive می‌تواند به این سازمان‌ها اطمینان دهد که اطلاعات حساس آن‌ها در یک فضای امن و غیرمتمرکز ذخیره می‌شود. از آنجا که فایل‌ها به صورت توزیع‌شده ذخیره می‌شوند، احتمال حملات سایبری یا دسترسی غیرمجاز به اطلاعات به شدت کاهش می‌یابد.

پیاده‌سازی و معماری پروژه

پروژه Safe Drive به گونه‌ای طراحی شده است که از چندین بخش مجزا تشکیل شده و هر کدام از این بخش‌ها وظایف خاصی را برعهده دارند. این بخش‌ها شامل موارد زیر می‌شوند:

هسته کلاینت (Client Core): هسته اصلی کلاینت Safe Drive خود شامل مواردی مانند Encryption & Decryption Handler، SD-Network Handler، Authorization Handler و موارد دیگر است که وظایفی همچون رمزنگاری فایل های در حال بارگذاری، رمز گشایی فایل های در حال دریافت، ارتباط با شبکه Safe Drive و صحت سنجی کاربر را بر عهده دارند.

رابط کاربری کلاینت (CUI): بخش رابط کاربری کلاینت شامل نرم‌افزارهایی است که کاربران برای دسترسی به هسته کلاینت از آن استفاده می‌کنند. این نرم‌افزارها به شکل اپلیکیشن‌های وب و موبایل طراحی شده‌اند و امکان مدیریت ساده فایل‌ها، بارگذاری و دانلود آن‌ها را برای کاربران فراهم می‌کنند. کلاینت‌های Safe Drive دارای یک رابط کاربری ساده و کاربرپسند هستند که حتی کاربران غیرمتخصص نیز به راحتی می‌توانند از آن‌ها استفاده کنند.

هسته سرور (Server Core): هسته سرورهای Safe Drive مسئول مدیریت کل سیستم غیرمتمرکز و ارتباط با کلاینت‌ها هستند. این سرورها داده‌ها را دریافت و در شبکه توزیع می‌کنند. علاوه بر این، سرورها وظیفه هماهنگی بین کاربران و حفظ امنیت داده‌ها را برعهده دارند. سرورها به گونه‌ای طراحی شده‌اند که می‌توانند با افزایش تعداد کاربران و داده‌ها، به صورت پویا و مقیاس‌پذیر عمل کنند.

رابط کاربری سرور (SUI): رابطی کاربری برای ارتباط به هسته سرور برای مدیریت منابع سرور و وضعیت خواهد بود توسط مسئول مربوطه که فقط رابطی تحت وب خواهد بود.

سیستم رمزنگاری(بخشی از هسته کلاینت): یکی از مهم‌ترین بخش‌های Safe Drive، سیستم رمزنگاری آن است. این سیستم از الگوریتم‌های رمزنگاری پیشرفته برای محافظت از فایل‌های کاربران استفاده می‌کند. رمزنگاری فایل‌ها به صورت محلی و توسط دستگاه کاربر انجام می‌شود، به طوری که حتی تیم مدیریت سرور نیز به محتوای فایل‌ها دسترسی نخواهد داشت.

ذخیره‌سازی غیرمتمرکز: بخش ذخیره‌سازی پروژه به گونه‌ای طراحی شده است که فایل‌ها در چندین سرور و مکان مختلف ذخیره شوند. این سیستم توزیع شده باعث افزایش امنیت فایل‌ها و کاهش خطرات مرتبط با نفوذهای امنیتی می‌شود.

برنامه زمانی پروژه

اجرای پروژه Safe Drive به چندین فاز مجزا تقسیم می‌شود که هر فاز شامل فعالیت‌های خاصی است. برنامه زمانی پیشنهادی برای هر فاز به شرح زیر است:

فاز اول:

طراحی و پیاده‌سازی اولیه پلتفرم (1 ماه):

در این فاز، تیم توسعه‌دهنده روی طراحی کلی سیستم و پیاده‌سازی نسخه اولیه آن کار خواهد کرد. این نسخه شامل رابط کاربری پایه و زیرساخت‌های اصلی برای ذخیره‌سازی غیرمتمرکز است.

فاز دوم:

توسعه و تست سیستم رمزنگاری و ذخیره‌سازی غیرمتمرکز (2 ماه):

در این مرحله، تیم توسعه روی پیاده‌سازی و تست سیستم رمزنگاری فایل‌ها و مکانیزم ذخیره‌سازی غیرمتمرکز تمرکز خواهد کرد. این فاز شامل تست‌های امنیتی و عملکردی نیز می‌شود تا مطمئن شویم که سیستم در شرایط مختلف به درستی عمل می‌کند.

فاز سوم:

انتشار نسخه بتا و بررسی بازخورد کاربران (3 ماه):

پس از اتمام پیاده‌سازی‌های اصلی، نسخه بتا برای گروهی از کاربران منتشر می‌شود. در این فاز، بازخورد کاربران در مورد عملکرد سیستم جمع‌آوری شده و در صورت نیاز، تغییرات لازم اعمال خواهد شد.

فاز چهارم:

بهبود و ارائه نسخه نهایی (تا 6 ماه):

پس از دریافت بازخوردهای کاربران، سیستم بهینه‌سازی شده و نسخه نهایی آماده انتشار می‌شود. این نسخه شامل تمام ویژگی‌ها و امکانات نهایی است.

تیم توسعه‌دهنده

پروژه Safe Drive توسط یک تیم کوچک و متخصص توسعه داده می‌شود که هر کدام از اعضای تیم دارای مهارت‌ها و تخصص‌های خاصی هستند:

علیرضا گلستان هاشمی (مسئول مدیریت زیرساخت‌های سرور و DevOps): علیرضا با تجربه در زمینه‌های مرتبط با زیرساخت‌های ابری و مدیریت سرور، نقش مهمی در پیاده‌سازی بخش‌های پشتیبانی سیستم دارد.

امیررضا قلی‌زاده (مسئول توسعه بک‌اند): امیررضا با تجربه در طراحی و توسعه بک‌اند نقش اصلی را در پیاده‌سازی و توسعه قابلیت‌های شی گرایی پروژه دارد.

فاطمه خلیلی (مسئول توسعه سیستم‌های امنیتی و رمزنگاری): فاطمه با تخصص در زمینه امنیت سایبری و رمزنگاری، سیستم رمزنگاری فایل‌های Safe Drive را طراحی و پیاده‌سازی می‌کند.

دانیال هادی‌زاده (مسئول توسعه فرانت‌اند و طراحی تجربه کاربری): دانیال با تخصص در UI/UX، وظیفه طراحی و توسعه رابط کاربری ساده و کاربر پسند Safe Drive را بر عهده دارد.

هزینه‌ها و منابع مورد نیاز

پروژه Safe Drive نیازمند منابع مالی و فنی برای توسعه و پیاده‌سازی است. برخی از هزینه‌های تخمینی به شرح زیر است:

اجاره سرورهای ابری: برای ذخیره‌سازی داده‌ها و اجرای سیستم‌های بک‌اند، نیاز به اجاره سرورهای ابری قدرتمند داریم. این هزینه به صورت ماهانه محاسبه می‌شود و بسته به میزان تقاضا و کاربران سیستم ممکن است افزایش یابد.

هزینه توسعه: توسعه و پیاده‌سازی سیستم نیازمند زمان و هزینه‌های مالی برای توسعه‌دهندگان است. همچنین هزینه‌هایی برای ابزارهای توسعه و تست سیستم نیز در نظر گرفته شده است.

تست‌های امنیتی: برای اطمینان از امنیت سیستم، نیاز به اجرای تست‌های امنیتی مستقل وجود دارد که ممکن است هزینه‌بر باشد.

بررسی ریسک‌های احتمالی

مانند هر پروژه دیگری، Safe Drive نیز با چالش‌ها و ریسک‌های مختلفی روبروست. برخی از ریسک‌های احتمالی عبارتند از:

خروج یکی از اعضای تیم: خروج یکی از اعضای کلیدی تیم می‌تواند تاثیر زیادی بر روند توسعه پروژه داشته باشد. برای کاهش این ریسک، تیم باید وظایف را به صورت متوازن تقسیم کرده و به برون‌سپاری بخشی از وظایف فکر کند.

مشکلات مالی یا قطع حمایت کارفرما: در صورت بروز مشکلات مالی یا قطع حمایت مالی، ممکن است پروژه با چالش‌هایی مواجه شود. در این صورت، باید با تنظیم قراردادهای اولیه به شکلی که شرایط فسخ مناسب در آن‌ها پیش‌بینی شده باشد، از ضررهای احتمالی جلوگیری کرد.

مشکلات امنیتی و حملات سایبری: مشکلات امنیتی و حملات سایبری شامل ریسک‌هایی است که در صورت وجود ضعف در سیستم‌های امنیتی، پروژه ممکن است با نفوذ و سرقت اطلاعات کاربران مواجه شود. برای کاهش این ریسک، پیشنهاد می‌شود از پروتکل‌های امنیتی پیشرفته استفاده شود و تست‌های امنیتی منظم برای شناسایی و رفع نقاط ضعف سیستم به صورت دوره‌ای انجام گردد.

عدم انطباق با استانداردها و قوانین: عدم انطباق با استانداردها و قوانین می‌تواند ریسک‌هایی را به همراه داشته باشد که در صورت رعایت نکردن قوانین مرتبط با ذخیره‌سازی و حفاظت از داده‌ها، پروژه با جریمه‌های حقوقی یا عدم تایید مواجه شود. برای کاهش این ریسک، پیشنهاد می‌شود از مشاوران حقوقی استفاده شود و آگاهی کاملی از قوانین مربوط به حفاظت از داده‌ها (مانند GDPR) حاصل گردد تا انطباق کامل پروژه با این قوانین تضمین شود.