طرح‌نامه پروژه های تحقیقاتی

«فرم پیشنهاد(پروپوزال)طرح تحقیقات دفاعی»

عنوان طرح کسر خدمت

فارسی:

راه‌اندازی و ریزتوسعه یک پروتکل متن‌باز برای ارتباطات لحظه‌ای غیرمتمرکز با پشتیبانی ذاتی از E۲EE

لاتین:

Deploy and micro development an open source protocol for decentralized real-time communications with native support E۲EE

نام مجری

علی رحیمیان

نام استاد راهنما

میثم محمدی

(الف) اطلاعات مربوط به مجری طرح

۱) مشخصات مجری

الف) نام و نام خانوادگی: علی رحیمیان ب) شماره شناسنامه و محل صدور: ۴۵۶۰۲۱۵۹۷۹ سمنان

ج) نام پدر: حمیدرضا د) سال تولد: ۱۳۷۷ ه) شماره ملی: ۴۵۶۰۲۱۵۹۷۹

و) رشته تحصیلی: کامپیوتر ز) گرایش: مهندسی نرم افزار ح) آخرین مدرک تحصیلی: کارشناسی ارشد

.....

۲) نشانی محل سکونت : تهران جنت آباد جنوبی – بلوار لاله شرقی – خیابان مجاهد کبیر – کوچه بنفشه ۱۱ – پلاک ۶/۱ واحد ۸

الف) نشانی محل کار: کارمند شرکت خصوصی (برنامه نویس)

ب) منزل: تهران جنت آباد جنوبی – بلوار لاله شرقی – خیابان مجاهد کبیر – کوچه بنفشه ۱۱ – پلاک ۶/۱ واحد ۸

شماره تلفن: ۰۹۳۶۲۳۶۸۷۵۱

.....

(ب) طرح تحقیق پروژه

۱) عنوان طرح:

راه‌اندازی و ریزتوسعه یک پروتکل متن‌باز برای ارتباطات لحظه‌ای غیرمتمرکز با پشتیبانی ذاتی از E2EE

۲) مقدمه:

۲–۱) اطلاعات کلی پروژه:

نوع پروژه:	☐ محصول محور نیست (مطالعاتی/ دانشی)	☑محصول محور هست
پروژه در کدام مرحله قرار دارد:	☐ امکان‌سنجی	☐ طراحی ☑ طراحی، ساخت و تست
وضعیت نیاز به پروژه:	☐ نیازی اخذ نگردیده	☑ نیاز وجود دارد* (کابر مورد نظر: نیاز وجود دارد – ارتباط امن بین کاربران مختلف در اینترنت و اینترانت
وابستگی یا ارتباط پروژه با پروژه‌های دیگر:	☐ بخشی از یک پروژه دیگر است. (نام پروژه: .....)	☑ یک موضوع مستقل از پروژه‌های دیگر است.

* اعلام نیاز پیوست گردد.

۲–۲) مدت اجرای طرح*: ۱۰ ماه شمسی

ارزیابی میزان فعالیت محقق در هر ماه به میزان ۱۵۰ ساعت است

مدت اجرا: ۱۰ ماه شمسی

توضیح: معادل نفر-ساعت تخمینی: ۱۰ ماه × ۱۵۰ ساعت/ماه = ۱۵۰۰ نفر-ساعت

۲–۳) کل بودجه مورد نیاز*: ۰ میلیون ریال

۳) بیان مسأله و هدف از انجام طرح:

۳–۱) اهداف پروژه

با اجرای این پروژه، چه نیازمندی‌هایی پاسخ داده خواهد شد؟

با اجرای این پروژه، نیازهای زیر برآورده می‌شود:

- ارتباط امن بین کاربران.
- پیاده‌سازی نمونه‌ی نرم‌افزاری (کلاینت/سرور) که از پروتکل مذکور پشتیبانی می‌کند.
- ارائه مستندات فنی، کد منبع نمونه، و گزارش تست امنیتی و ارزیابی.

۳–۲) بیان مسئله (یا مسائل):

- هر تحقیق، تلاش برای رسیدن به پاسخ یک یا چند سوال است. پروژه حاضر به چه سوالات و نیازهایی پاسخ می‌دهد؟

- ❖ چگونه می‌توان یک پروتکل سبک، کارا و امن را برای ارتباط میان کاربران مختلف طراحی کرد که مناسب سکوهای مختلف باشد؟
- ❖ چه مکانیزم‌های امنیتی پایه باید گنجانده شوند تا از دستکاری و شنود داده‌های بین کاربران جلوگیری شود؟
- ❖ پروتکل طراحی‌شده در برابر کدام حملات آسیب‌پذیر است و چه راه‌حل‌هایی برای کاهش این آسیب‌پذیری‌ها وجود دارد؟
- ❖ چطور و تا چه اندازه امنیت نرم‌افزار را تضمین می‌کنیم؟
- ❖ امنیت پایگاه داده تا چه اندازه است و چطور و تا چه اندازه آن را تضمین می‌کنیم؟
- ❖ پروتکل طراحی شده در برابر کدام حملات و تا چه اندازه امنیت دارد؟
- ❖ نتایج تست نفوذ در برابر حملات و تحلیل آن‌ها

۳-۳) ویژگی های کاربردی و عملیاتی

نسخه اندروید :

راه‌اندازی کلیه‌ی قابلیتهای استاندارد پروتکل پیام‌رسان به علاوه قابلیتهای جدید زیر :

- **تماس صوتی و تصویری- در اتاق‌های دونفره (چت خصوصی)، طرفین میتوانند تماس صوتی و یا تصویری یک به یک برقرار نمایند و همچنین امکان سوییچ بین تماس صوتی و تصویری و بالعکس (استفاده از المنت کال به جای جیتسی)**
- **جلسات تصویری- امکان برگزاری جلسات تصویری در اتاق‌های بیش از دو عضو (کنفرانس صوتی و تصویری) (استفاده از المنت کال به جای جیتسی)**
- **قابلیت Multi Account و جابه‌جایی کاربر در اکانت‌هایش به نحوی که کلیدهای اتاق‌ها نیز مدیریت شود. (اکانت ها در سرورهای جداگانه و یا یک سرور باشند.)**
- **قابلیت نمایش وضعیت (ماجرا) توسط کاربر در اپلیکیشن.**
- **قابلیت مشاهده میزان درصد دانلود یا آپلود انجام شده همه رسانه‌ها (عکس، فیلم، صوت و فایل‌های دیگر)**
- **امکان ادامه پخش فایل‌های صوتی و تصویری در صورت خروج از گروه و اپلیکیشن**
- **در صورت امکان انتخاب چند پیام و ارسال آنها به شخص یا گروه دیگر** (Forwarding)
- **امکان پاسخ به نظرسنجی در کانال توسط اعضا**
- **فعال بودن پیش‌فرض امکان** push notification
- **پس زمینه صفحات گفتگو مانند پیام‌رسان‌های استاندارد باشد (دارای شکلک های زیبا در پس زمینه)**
- **هنگام ورود به صفحه گفتگو (شخصی، کانال، گروه) کاربر را به اولین پیام خوانده نشده هدایت کند. و از دکمه پرش به خوانده نشده استفاده نشود.**
- **در بازارسال (پاسخ** replay**) به متن، فقط یک مرحله متن قبلی درج شود**

پنل داشبورد مدیریت سامانه :

- **امکان تعریف سطوح دسترسی برای کاربران مختلف**
- **امکان راه‌اندازی نرم‌افزار بر بستر معماری غیرمتمرکز فدریشن**
- **امکان اضافه کردن کاربر**

- **ارائه راهکار مبتنی بر اکسل در پنل ادمین جهت ساخت کاربران (Bulk List)**
- **امکان خروجی گرفتن از لیست کاربران به شکل فایل اکسل یا pdf و ... .**
- **ارسال هشدار به کاربران به شکل تک پخشی یا چند پخشی یا همه پخشی.**
- **نمایش کاربران آنلاین (ip و مشخصات دستگاه موبایل) به صورت لحظه‌ای**
- **نمایش مقدار منابع سخت‌افزاری در حال استفاده سامانه به تفکیک، ساعت، روز، هفته و ماه در قالب نمودار گرافیکی به صورت لحظه‌ای و تجمیعی**
- **امکان تعریف گروه کاری برای کاربران و مدیران و اضافه یا حذف کردن کاربران مختلف به گروه.**
- **اخراج یا اضافه کردن کاربر به اتاق**
- **امکان تنظیم مقدار حجم فایل‌های ارسالی**

سرور

- **طراحی و پیکربندی سرویس‌ها به شکل داکرایز**
- **مدیریت کانتینرها به وسیله کوبرنتیس**
- **امکان اتصال به سرورهای دیگر به شکل فدراسیون**
- **مجهز به پنل داشبورد مدیریت**

۳-۴) فرضیات

این پروژه صرفاً یک نمونه‌پیاده‌سازی تحقیقاتی/نمونه‌اولیه است و برای استفاده در ابعاد بزرگ نیاز به بررسی‌های عملکردی و تأیید بیشتر خواهد داشت.

۳-۵) جزئیات و روش‌های فنی انجام پروژه (چگونگی اجرای کار؟)

فاز تحلیل و طراحی : بررسی الزامات، مطالعه وضعیت موجود، بررسی پایگاه داده Postgresql، بررسی الگوریتم‌های E۲EE.

فاز پیاده‌سازی اولیه سرور : طراحی و پیکربندی سمت سرور (داکرایز) کردن سرویس‌ها ، مدیریت کانتینرها با استفاده از کوبرنتیس و هاردنینگ سیستم‌عامل سرور بر اساس دستورالعمل‌های امنیتی CIS Benchmark و تنظیم سند.

فاز پیاده‌سازی اولیه کلاینت‌ها : طراحی و پیاده‌سازی کلاینت نسخه اندروید.

فاز بهینه‌سازی و مستندسازی : مستندسازی پروتکل، تهیه راهنمای پیاده‌سازی و گزارش نتایج.

فاز نهایی و ارائه : آماده‌سازی گزارش نهایی، ارائه شفاهی/جلسه دفاع، انتشار کد نمونه در مخزن Git (در صورت مجاز بودن).

روش‌های ارزیابی : تست‌های عملکردی، تست‌های استرس سرور، تست‌های امنیتی کلاینت و سرور و بررسی تطابق خروجی با مشخصات ارایه شده.

در شکل زیر یک نمای کلی از بلوک دیاگرام پروژه نشان داده شده است :

۶–۳) کلمات کلیدی

واژگان کلیدی : دیتابیس ، postgresql، سیستم عامل ، اندروید ، E۲EE ، غیرمتمرکز

keywords: DataBase, Postgresql, Operating system, Android, End to End Encryption, Decentralized

۴) اهمیت و ضرورت انجام پروژه:

علل اصلی انجام پروژه بایستی در اینجا مورد بحث قرار گیرد که به عنوان مثال شامل موارد زیر هستند:

- افزایش نیاز به راهکارهای امن و کارا برای ارتباط بین کلاینت‌های سکوهای مختلف.
- فراهم آوردن مستندات و نمونه‌کد برای تیم‌های توسعه که می‌خواهند ارتباطات امن بین سرور و کلاینت‌های سکوهای مختلف برقرار کنند.

۵) پیشینه تحقیق (با ذکر مشخصات کامل منابع) و جمع بندی پیشینه‌های مرتبط با پروژه

۵–۱) مرور پیشینه

۵–۲) پژوهش‌ها یا محصولات مشابه موجود در سطح کشور و دنیا

چند مورد از پژوهش ها یا محصولاتی که به تحقیق حاضر بسیار نزدیک هستند در جدول زیر ذکر شود.

ردیف	عنوان پژوهش یا محصول*	نوع	محل اجراء	دستاورد پژوهش	آخرین وضعیت	توضیحات	مرجع
۱	پیام‌رسان element						
۲							
۳							

* نوع پژوهش: مقاله، پایان‌نامه، کتاب، طرح پژوهشی، نمونه آزمایشگاهی، نمونه اولیه، نمونه صنعتی و...

۵–۳) وجوه تمایز:

- تمرکز بر طراحی و پیاده‌سازی پروتکل متن‌باز برای ارتباطات لحظه‌ای غیرمتمرکز.

۵–۴) منابع:

مراجع کل پیشنهادیه طرح در این قسمت آورده شود.

در صورتی که می خواهید در پروژه خود به یک مقاله، پایان‌نامه، کتاب، طرح پژوهشی، نمونه آزمایشگاهی، نمونه اولیه، نمونه صنعتی ارجاع دهید از نمونه استاندارد زیر استفاده نمایید:

۶) مراحل انجام و گام‌های تحقیق و جدول زمان‌بندی اجرای پروژه:

گام‌های اصلی در انجام پروژه و عنوان فعالیت‌هایی که در هر گام صورت می‌پذیرد را به همراه مدت زمان تقریبی هریک بیان نمایید. تعداد گام‌ها و ستون‌های زمان را تا حد نیاز اضافه نمایید. در بخش نفر ساعت کل ساعاتی که نیاز است مجری بر روی آن گام مشغول باشد را بیان نمایید.

ردیف	مراحل و گام‌های اجرای پروژه	نفر ساعت	زمان اجرا (ماه)																		
			۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸	۱۹
۱	مطالعه و تحلیل شناختی پروتکل ارتباطات لحظه‌ای غیرمتمرکز	۷۵	✓																		
۲	مطالعه پایگاه داده PostgreSQL و دستورات و امنیت این پایگاه داده و روش-های ریکاوری و concurrency آن.	۷۵	✓																		
۳	بررسی ابزارهای کلیدی Devops از قبیل داکر و کوبرنتیس	۷۵		✓																	
۴	بررسی حملات به پروتکل ارتباطات لحظه‌ای غیرمتمرکز	۷۵		✓																	
۵	بررسی الگوریتم‌های E۲EE و نقاط قوت و ضعف آنها و امکان تغییر آنها	۷۵			✓																
۶	طراحی و پیکربندی سمت سرور (داکرایز) کردن سرویس ها	۷۵			✓																
۷	مدیریت کانتینرها با استفاده از کوبرنتیس	۷۵				✓															

۸	هاردنینگ سیستم-عامل سرور بر اساس دستورالعمل‌های امنیتی CIS Benchmark و تنظیم سند.	۷۵					✓																		
۹	طراحی و پیاده‌سازی داشبورد وب جهت مدیریت سرور. (ریز امکانات در بخش ۳-۳)	۱۵۰				✓																			
۱۰	طراحی و پیاده‌سازی کلاینت نسخه اندروید (ریز امکانات در بخش ۳-۳)	۴۵۰			✓	✓	✓	✓	✓	✓															
۱۱	تست نفوذ، آزمایش و ارزیابی، رفع خطاها و باگ‌ها، و بهینه‌سازی نهایی پروژه	۱۵۰								✓															

۷) دستاوردهای هر گام از پروژه

ردیف	عنوان گام اصلی	شرحِ مهمترین فعالیت‌ها	دستاورد – (خروجی گام*)
۱	مطالعه و تحلیل شناختی پروتکل ارتباطات لحظه-ای غیرمتمرکز	مطالعه شناختی پروتکل ارتباطی	**شناخت پروتکل و شبکه ی غیر متمرکز آن**
۲	مطالعه پایگاه داده PostgreSQL	مطالعه شناختی، دستورات، امنیت، کار با این پایگاه داده PostgreSQL، و دستورات و امنیت و نحوه ی ریکاوری و Concurrency و...	شناخت دستورات، امنیت، کار با پایگاه داده PostgreSQL و ... .
۳	مطالعه روش های Devops از قبیل داکر و کوبرنتیس	مطالعه روش‌های Devops	شناخت روش‌های Devops
۴	طراحی و پیاده‌سازی کلاینت نسخه اندروید	طراحی UI/UX و ارتباط با سرور	**اپلیکیشن اندروید**
۵	طراحی و پیاده سازی داشبورد مدیریت	طراحی UI/UX و ارتباط با سرور	**داشبورد مدیریت سرور**
۶	تست نفوذ، آزمایش و ارزیابی، رفع خطاها و	تست امنیتی پروژه و بررسی و تحلیل امنیت کلی پروژه و گزارش‌گیری	گزارش ارزیابی خروجی پروژه

	باگ‌ها، و بهینه‌سازی نهایی پروژه		

* منظور از دستاورد، موارد تحویلی پروژه و هر نوع خروجی قابل ارائه است. بعنوان مثال: گزارش طراحی قطعات، سند آزمون محصول، قطعه، کاتالوگ، عکس و فیلم، فایل‌های شبیه‌سازی، کدهای نوشته شده، پرسشنامه‌های تحقیق، صورتجلسات و ... است.

۸) گلوگاه‌های احتمالی در اجرای پروژه و راه حل‌های عبور از آنها

منظور از گلوگاه مواردی است که سبب متوقف شدن یا کندی پروژه خواهد شد و در واقع بیان و بررسی نقاط بحرانی پروژه خواهد بود. مجری طرح سعی می‌کند در طراحی‌های خود تا حد ممکن از گلوگاه‌ها دوری کند و برای یافتن راه حل‌های مواجه با گلوگاه‌ها و بهبود آنها تلاش زیادی انجام دهند. هرچه مجری بتواند گلوگاه های احتمالی پروژه را بهتر معرفی نماید نشان از تسلط بیشتر او به موضوع پروژه دارد.

ردیف	عنوان گلوگاه	راهکار پیشنهادی	تبعات عدم رفع گلوگاه
۱	پیاده‌سازی روال push notification	استفاده از UnifiedPush	عدم اطلاع کاربر از پیام‌های دریافتی
۲	تعداد کاربران زیاد	استفاده از کوبرنتیس و داکر در پیاده‌سازی سرویس‌های سرور	پشتیبانی محدود از کاربر
۳			
۴			
۵			
۶			

۹) افراد و همکاران در اجرای پروژه:

مجری: علی رحیمیان

ناظر: میثم محمدی

۱۰) نیازمندی‌های لازم جهت اجرای طرح:

۲ hypervisor type

۱۱) سایر موارد قابل ذکر:

۱۲) توضیحات مدیر مرکز تحقیقاتی

درخصوص مجری، پروژه، ناظر پیشنهادی و... توضیحات ارائه شود. پر کردن این قسمت توسط مسئول مرکز تحقیقاتی الزامی است.

۱۳) پیوست‌ها (موارد مشخص شده با * الزامی می‌باشند)

۱- ☐ روزمه‌ی مجری* ۲- ☐ مستندات مرتبط با مشخصات فنی طرح

۳- ☐ مدارک شناسایی*

۴- ☐ فرم اطلاعات همکار

۵- ☐ پایان‌نامه کارشناسی*

۶- ☐ پایان‌نامه کارشناسی ارشد*

۷- ☐ پایان‌نامه (پروپوزال) دکتری*

۸- ☐ نامه اعلام نیاز*

۱۴) مشخصات استاد راهنما

نام و نام خانوادگی	...	مدرک تحصیلی	...
رشته و گرایش تحصیلی	...	دانشگاه محل اخذ مدرک	...

نام و نام خانوادگی مجری　　نام و نام خانوادگی استاد راهنما　　نام و نام خانوادگی مدیر مرکز تحقیقاتی

امضاء　　امضاء　　امضاء