دانشگاه صنعتی اصفهان
دانشکده مهندسی برق و کامپیوتر

پروژه درس مهندسی نرم‌افزار

گروه نرمینو

سیستم رأی‌گیری الکترونیکی امن

نیازمندی‌ها

اعضای گروه:

نگین دشتی
محمدرضا ماجد
سید رضا موسوی
محمدصالح ناصح

استاد راهنما:

امیرارسلان یاوری

۷ آذر ۱۴۰۳

فهرست مطالب

۱ نیازمندی‌های کاربردی

۱.۱ نیازمندی‌های کاربر رأی‌دهنده

- ساده بودن و کاربرپسند بودن برنامه رأی‌گیری و مقرون به صرفه بودن آن برای کاربر
- ثبت‌نام و احراز هویت امن (register) برای ورود به سیستم رأی‌گیری (login)
- ثبت رأی به صورت امن و غیرقابل تغییر و با حفظ حریم خصوصی کاربر
- قابلیت اثبات فردی و انتها به انتهای رأی داده شده بدون افشای آن (یا با دانش صفر)
- ارتباط امن با شبکه بلاک‌چین و ارسال تراکنش بدون افشای هویت واقعی
- قابلیت ارسال سؤال برای بخش پشتیبانی و دریافت جواب در کوتاه‌ترین زمان ممکن
- قابلیت دیدن راهنمایی‌های کامل در مورد روش کار با برنامه رأی‌گیری
- دریافت اعلان‌های مرتبط با هر یک از مراحل رأی‌گیری از طریق پیامک و برنامه انتخابات
- قابلیت ناشناس بودن رأی‌گیری و عدم افشای رأی کاربر در هر یک از مراحل
- قابلیت راستی‌آزمایی رأی‌گیری توسط کاربر در پایان رأی‌گیری
- قابلیت دیدن گزارش‌ها و نتایج رأی‌گیری و تأیید عمومی و انتها به انتهای آن
- قابلیت شفاف بودن انتخابات در تمامی مراحل و متمرکز نبودن آن
- دسترسی به نتایج انتخابات به صورت شفاف و مطمئن

۲.۱ نیازمندی‌های مدیران سیستم و مسئولان برگزاری انتخابات

- قابلیت استفاده از سیستم رأی‌گیری برای همه افراد با حداقل امکانات موجود
- ایجاد یک فرآیند انتخابات به صورت امن و بدون امکان دستکاری عامل بیرونی
- چک کردن احراز هویت و واجد شرایط بودن رأی‌دهندگان به یک روش امن و مطمئن
- قابلیت جلوگیری از تقلب در انتخابات و چند بار رأی دادن افراد با هزینه کم
- قابل تأیید بودن فردی، عمومی و انتها به انتهای رأی‌گیری

- مقرون به صرفه بودن برگزاری انتخابات نسبت به روش‌های سنتی
- نظارت و حسابرسی شفاف آرا در تمامی مراحل رأی‌گیری
- محرمانه بودن رأی‌گیری
- یکپارچگی سیستم رأی‌گیری و مقاوم بودن در برابر حملات و آسیب‌پذیری‌های امنیتی
- قابل اطمینان بودن سیستم از اینکه هیچ رأیی حتی در صورت مشکلات سیستم و خرابی برخی از سرورها از بین نمی‌رود.
- مدیریت و تنظیمات انتخابات به صورت امن و مطمئن

۲ نیازمندی‌های غیرکاربردی

۱.۲ نیازمندی‌های کاربر رأی‌دهنده

- ارتباط امن و رمزنگاری شده انتها به انتها با مدیران سیستم در طی مراحل انتخابات
- قابلیت تولید کلید عمومی و خصوصی به یک روش امن برای ناشناس ماندن در فرآیند انتخابات
- قابلیت امضای قرارداد هوشمند و تولید ZKSMP برای اثبات رأی‌دهی با دانش صفر
- قابلیت ارتباط امن و رمزنگاری شده انتها به انتها با شبکه بلاک‌چین و ارسال تراکنش (برگه رأی یا توکن)

۲.۲ نیازمندی‌های مدیران سیستم و مسئولان برگزاری انتخابات

- قابلیت استفاده از برنامه در همه سیستم‌عامل‌ها و مرورگرهای مدرن
- رمزنگاری داده‌ها و محافظت از اطلاعات هویتی کاربران
- ارتباط امن و رمزنگاری شده انتها به انتها با هر یک از اجزای فرآیند رأی‌دهی مثل کاربران، سامانه ثبت احوال و غیره
- چک کردن احراز هویت و واجد شرایط بودن رأی‌دهندگان به یک روش امن و بدون امکان تقلب
- تشخیص ربات نبودن کاربر با استفاده از روش‌های مدرن و بروز مثل روش‌های هوش مصنوعی
- قابل تأیید بودن فردی، عمومی و انتها به انتهای رأی‌گیری

- مقرون به صرفه بودن برگزاری انتخابات نسبت به روش‌های سنتی
- نظارت و حسابرسی شفاف آرا در تمامی مراحل رأی‌گیری
- محرمانه بودن رأی‌گیری
- یکپارچگی سیستم رأی‌گیری و مقاوم بودن در برابر حملات و آسیب‌پذیری‌های امنیتی
- قابل اطمینان بودن سیستم از اینکه هیچ رأیی حتی در صورت مشکلات سیستم و خرابی برخی از سرورها از بین نمی‌رود.
- مدیریت و تنظیمات انتخابات به صورت امن و مطمئن
- مقیاس پذیری سیستم برای مدیریت حجم بالای کاربران و تراکنش‌ها
- استفاده از بلاک‌چین برای ثبت و ذخیره آرا
- پشتیبان‌گیری منظم از داده‌ها و تراکنش‌ها
- پیاده‌سازی CI/CD برای توسعه سریع‌تر و پایدار
- نظارت مداوم بر عملکرد سیستم (Monitoring)