دانشگاه اصفهان

دانشکده مهندسی کامپیوتر

گزارش فاز اول پروژه تحلیل و طراحی سیستم‌ها

سامانه ادله دیجیتال

گروه شماره ۱۵

گردآورندگان:

محمد محمدی

حیدرعلی الدیرانی

علی بهرامی

مهدی غفوری

سهیل کریمیان خوزانی

پارسا مظاهری

استاد راهنما: جناب دکتر محمدرضا شعرباف

دستیار آموزشی: خانم شیما مغزی

نیم‌سال دوم سال تحصیلی ۱۴۰۳ – ۱۴۰۴

فهرست مطالب

فاز اول: مقدمات و شناسایی نیازها

۱ – مقدمه

در این فصل قصد داریم به تعیین و تبیین نیازمندی‌های یک سامانه ادله دیجیتال بپردازیم. از دیرباز شاکیان برای اثبات حق از دست رفته‌شان به یک مدرک و سند قابل‌اعتماد و محکمه‌پسند احتیاج داشتند و تا کنون هم این نیاز پابرجاست. امروزه با پیشرفت علم‌وفناوری[۱] نوع اسناد و مدارک نیز تغییر یافته‌اند. به همین دلیل اهمیت استفاده از ادله دیجیتال در اثبات برخی ادعاها اهمیت بسیار زیادی به خود جلب کرده است.

۱-۱- هدف

در این سامانه[۲] قصد داریم برای افراد سکویی[۳] امن بنا کنیم تا ابتدا افراد احراز هویت[۴] شوند و سپس فرد شاکی مدارک و مستندات خود در زمینه جرائم اینترنتی[۵] به مقامات قضایی ارائه کند. سپس مدارک وی در کمال حفاظت و نگهداری صحیح در فرایندهای جمع‌آوری و ذخیره‌سازی، با ابزارهای به‌روز هوش مصنوعی و به‌دور از خطاهای انسانی یا بعضاً سوءنیت پالایش شده و در اختیار حکام قضایی قرار گیرد.

۱-۲- قلمرو

این سامانه به‌منظور تسهیل فرایند بارگذاری، احراز صحت ادله، حفظ و نگهداری و در نهایت دادرسی در اماکن قضایی ایجاد شده است. این سامانه در دستگاه قضایی، نیروی انتظامی و پلیس فتا تعبیه می‌شود و شاکیان و قضات در بستر اینترنت می‌توانند فرایند دادخواهی یا رسیدگی به شکایات را رصد کنند. همچنین این در این سامانه قصد داریم تمامی مدارک و ادله دیجیتال من‌جمله متن، تصویر و صدا را پشتیبانی کرده و در کمال حفاظت در اختیار مراجع ذی‌صلاح قرار دهیم تا از برخی مسائل همچون جعل یا سرقت اسناد نیز جلوگیری لازم به عمل آید.

۱-۳- بیان مسئله

از دیرباز ارائه مدارک برای اثبات دعاوی حقوقی یک مسئله بسیار حیاتی بوده است که در بسیاری از موارد معرفی یک الی چند شاهد به دادگاه از چالش‌های اثبات حق یک فرد شاکی است. امروزه اما با پیشرفت تکنولوژی این فرایند با ارائه برخی مدارک همچون فیلم و عکس بسیار آسان‌تر شده است. از سوی دیگر این پیشرفت باعث ایجاد روش‌های نوین در زمینه جرائم اینترنتی مانند کلاهبرداری‌های آنلاین یا جعل اسناد با کمک هوش مصنوعی[۶]

[1] Technology
[2] System
[3] Platform
[4] Authentication
[5] Cybercrime
[6] AI (Artifical Intelligence)

شده است که پیچیدگی‌های خاص خود را دارند و دیگر روش‌های سنتی تحلیل شواهد به نسبت ناکارآمد شده است. از این‌سو این سامانه قصد دارد تا با کمک گرفتن از هوش مصنوعی روی به هوشمندسازی، تحلیل و بررسی و درنهایت تصمیم‌گیری در خصوص ادله دیجیتال بیاورد.

۱-۴- تعاریف، واژگان و کوته‌نوشت‌ها

مخفف یا معادل فارسی	معادل انگلیسی	توضیح کلمه
فناوری	Technology	مجموع تکنیک‌ها و روش‌هایی است که در تولید کالاها یا تحقق اهداف معمولاً علمی استفاده می‌شود
سامانه	System	مجموعه‌ای متشکل از عناصر مرتبط با یکدیگر که مسئول انجام کار خاصی هستند؛ دستگاه.
سکو	Platform	محل ارائه خدمات و ارتباطات همگانی
جرائم سایبری	Cybercrime	جرائمی که در محیط مجازی رخ می‌دهند
سرور	Server	مرکز ارسال پاسخ به درخواست‌های سیستم
هوش مصنوعی	AI	سیستم‌های کامپیوتری که با شبیه‌سازی برخی کارهای انسان‌ها را با منطق پیاده‌سازی شده‌اش انجام می‌دهد
رابط کاربری	UI	بخشی که انسان می‌توانند با کامپیوتر تعامل کند
HTTPS	Hypertext markup language	به معنای پروتکل انتقال ابرمتنی است و وظیفهٔ ارسال و دریافت داده‌ها بین کاربر و سرور را بر عهده دارد
HTML	Hypertext markup language	زبان ساخت اسکلت اجزای یک سایت است
CSS	Cascading style sheets	زبان استایل دادن و ویرایش ظاهری اجزای سایت است
JavaScript		زبان برقراری ارتباط بین اجزای سایت و دستورات کاربر
Captcha		سؤالی کوچک برای تمایز دادن بین انسان و کامپیوتر
RAM	Random-Access Memory	حافظه‌ای کوتاه‌مدت برای ذخیره موقت داده‌ها
SSD	Sold State Drive	حافظه‌ای برای ذخیره داده‌ها که کار با آن سریع است

جدول ۱

۱-۵- مراجع

Kung, David C. Object-oriented software engineering: an agile unified methodology. McGraw-Hill, 2014

۱-۶- طرح کلی

در این سند ابتدا اهداف و ویژگی‌های این سیستم را بیان کرده و سپس به بیان شرح کلی، چشم‌انداز محصول و بیان واسط‌های مختلف سیستم از جمله واسط‌های کاربر، واسط‌های نرم‌افزار و سخت‌افزار و... می‌پردازیم. سپس کارکردهای محصول، قیود، مفروضات و وابستگی‌های سیستم مورد بررسی قرار می‌گیرند و نهایتاً به نیازمندی‌های محصول می‌پردازیم تا یک تصویر جامع و کامل از سیستم ارائه شود.

۲- شرح کلی

در دنیای امروز، با پیشرفت فناوری و گسترش استفاده از اینترنت، نقش ادله دیجیتال در تحقیقات کیفری و روند دادرسی‌های قضائی افزایش‌یافته است. ازآنجاکه جرایم سایبری روزبه‌روز پیچیده‌تر و نوآورانه‌تر می‌شوند، در این سیستم قصد داریم تا با کمک گرفتن از تکنولوژی‌های نوین مانند هوش مصنوعی و یادگیری ماشین در شناسایی و پیگیری مجرمان سایبری بپردازیم و از سیستم‌های سنتی که عمدتاً زمان‌بر و کم‌دقت هستند به یک سیستم بسیار سریع، آسان و با دقت بالا برسیم و دخالت‌های انسانی را تاحدامکان کاهش دهیم. در این سیستم یک بخش پرسش از هوش مصنوعی بدون ورود به سایت تعبیه شده که بهترین پاسخ‌ها را در خصوص سؤالات حقوقی به افراد می‌دهد. در داخل سامانه پس از تحلیل ادله و صحت سنجی توسط هوش مصنوعی، مراجع قضایی می‌توانند به روند پرونده ورود کرده و احکام را اجرا کنند. این فرایند برای کاربران (قضات، شاکیان و متهمان) قابل‌مشاهده است. حکام می‌توانند نوبت دادگاه تعیین کنند یا به شاکی یا متهم نامه بزنند. هر فرد تنها یک حساب کاربری یکتا دارد. همچنین یک پایگاه‌داده کلان داریم که ادله در آنجا ثبت و ضبط می‌شوند و در زمان نیاز استفاده می‌شوند.

۲-۱- چشم‌انداز محصول

سامانه مذکور با هدف فراهم‌آوردن سیستم‌های هوشمند برای تحلیل و شناسایی صحت ادله ارسالی توسط شاکی یا متهم به دنبال جلوگیری از جعل اسناد و مدارک، ایجاد شفاف‌ترین ادله برای دستگاه‌های قضایی و درنهایت فراهم‌کردن ایده‌آل‌ترین شرایط برای تصمیم‌گیری مراجع قضایی با کمک هوش مصنوعی است. در این سامانه ما یک پاسخگوی هوش مصنوعی آنلاین برای رفع شبهه در خصوص برخی قوانین نیز تعبیه کرده‌ایم که افراد در هر ساعت از شبانه‌روز می‌توانند برای سؤالات خود پاسخی با دقت بالا دریافت کنند.

۲-۱-۱- واسط‌های سیستم

واسط‌های سیستم به تبادل اطلاعات و ارتباط بین سیستم فعلی و سیستم‌های خارجی کمک می‌کنند و به چگونگی ارتباط با محیط خارج می‌پردازد.

- دسترسی سامانه به سیستم دریافت سوءپیشینه افراد برای تصمیم‌گیری بهتر
- دسترسی به یک سامانه ارسال پیامک دارای زمان انقضا برای دریافت کد احراز هویت ارسال شده به شماره‌تلفن به نام شخص حقیقی یا شرکت حقوقی
- دسترسی به یک سامانه تأیید کد کپچا[1] برای تعیین انسان بودن کاربر
- ارتباط با سیستم‌های ارتباطات صوتی و تصویری برای فراهم‌کردن امکانات تماس و ویدئوکنفرانس بین کاربران.

[1] Captcha

- دسترسی به سیستم‌های پردازش تصویر برای شناسایی و اعتبارسنجی اسناد هویتی مانند کارت ملی یا پاسپورت.
- ارتباط با سیستم‌های هشداردهنده و امنیتی برای شناسایی تهدیدات سایبری

۲-۱-۲- واسط‌های کاربری[1] (UI)

واسط کاربری نقطه تعامل و ارتباط بین انسان و کامپیوتر در یک دستگاه است. این واسط باید آن‌قدر خوب باشد تا کاربر پس از اتصال به اینترنت و ورود به سامانه، بدون نیاز به آموزش جدی و تنها از طریق تجربه‌کردن بخش‌های مختلف دستگاه به‌خوبی به نیازهای خود جامه عمل بپوشاند. توجه کنید که بر اساس میزان سطح دسترسی به اطلاعات سامانه سطح رابط کاربری افراد با یکدیگر متفاوت است. یعنی برای مثال کارهایی که یک قاضی در سامانه می‌تواند انجام دهد بسیار بیشتر از دسترسی‌های شاکی یا متهم است. این واسط‌ها باید ایمن، سریع، مقیاس‌پذیر و کاربرپسند باشند تا فرایند مدیریت، تحلیل و تبادل شواهد دیجیتال به‌راحتی و ساده‌ترین نحو انجام شود.

۲-۱-۳- واسط‌های سخت‌افزاری

- هر شخص باید حداقل یک تلفن همراه یا کامپیوتر شخصی[2] جهت اتصال به اینترنت و ورود به سایت داشته باشد.
- به یک بخش پایگاه‌داده و سرور جهت ارسال و دریافت اطلاعات به کاربران احتیاج است.
- در اماکن قضایی به دستگاهی برای تمبر زدن و پلمب کردن نامه‌های ارسالی نیاز داریم.
- جهت احراز هویت، هر کاربر (قضات، شاکیان و متهمان) نیازمند حداقل یک تلفن همراه یا رایانه شخصی دارای سیم‌کارت، به‌منظور دریافت پیامک و استفاده از امکانات سامانه است.

۲-۱-۴- واسط‌های نرم‌افزاری

برای استفاده از سامانه، کاربران ملزم به استفاده از مرورگرهایی نظیر Chrome، Mozilla Firefox و Microsoft Edge یا هر مرورگری که از ابزارهای توسعه سایت مثل HTML، CSS و JavaScript پشتیبانی می‌کند استفاده کنند. برای ذخیره، پردازش و... اطلاعات نیز به یک پایگاه‌داده مانند MySQL نیاز داریم.

۲-۱-۵- واسط‌های ارتباطی

این سامانه از پروتکل HTTPS[3] برای برقراری ارتباط امن با سرور بهره‌مند می‌شود. برای ورود به سایت، از سامانه پیامکی که به شماره تماس که به نام خود شخص است ارسال می‌شود. برخی اطلاع‌رسانی‌ها از طریق خود

[1] User Interface
[2] PC (Personal Computer)
[3] HyperText Transfer Protocol Secure

سیستم به کاربر نمایش داده می‌شوند و برخی از اطلاع‌رسانی‌ها از طریق نامه رسمی به دست شخص مورد نظر می‌رسند. افراد حتی می‌توانند با ایمیل خود ثبت‌نام مقدماتی کنند.

۲-۱-۶- واسط‌های حافظه

- استفاده از حافظه RAM[1] جهت تسریع در فرایند پاسخگویی به کاربران
- استفاده از برنامه‌نویسی بهینه و ساختمان داده‌های مناسب و سریع برای افزایش سرعت و کاهش مصرف حافظه
- استفاده از حافظه SSD[2] برای پردازش، ذخیره و بازیابی اطلاعات در سریع‌ترین زمان ممکن

۲-۱-۷- واسط‌های عملیاتی

- این سامانه نیاز به یک پایگاه‌داده قدرتمند دارد که بتواند داده‌های مختلف مانند فیلم، عکس، صدا و متن را به صورت لحظه‌ای ذخیره و به‌روزرسانی کند. این پایگاه‌داده باید قابلیت مدیریت حجم بالای داده‌ها را داشته باشد.
- این سامانه نیاز به ابزارهایی دارد که داده‌های پاک شده را برای ما بازیابی کند (مثل پیام‌های پاک شده یا تاریخچه مرورگر پاک شده).
- این سامانه نیاز به ابزارهایی برای تشخیص داده‌های جعلی دارد. برخی از این ابزارها عبارت‌اند از:
  - PhotoDNA: برای تشخیص تصاویر جعلی یا غیرمجاز.
  - Triage-G2: ابزار پیشرفته برای تحلیل و تشخیص جعل در داده‌های دیجیتال.
- این سامانه نیازمند یک سیستم پیامکی برای اطلاع‌رسانی به شهروندان به‌خصوص شاکیان و متهمان جهت اطلاع‌رسانی است.
- این سامانه نیاز به یک سیستم احراز هویت خودکار دارد تا بتواند کاربران را به‌صورت ایمن شناسایی و تأیید کند. این سیستم می‌تواند از روش‌هایی مانند احراز هویت دومرحله‌ای[3] استفاده کند.

۲-۱-۸- نیازمندی‌های سازگاری با محل نصب

ازآنجایی‌که سیستم ما بر روی یک سایت پیاده‌سازی خواهد شد، افراد برای دسترسی و استفاده از سایت لازم دارند ابزارهایی همچون تلفن همراه، رایانه و در کل هر وسیله‌ای که بتوان یک مرورگر را روی آن نصب کرد در اختیار داشته باشند تا پس از اتصال به اینترنت وارد سایت شوند و از امکانات تعبیه شده استفاده لازم را به عمل بیاورند.

۲-۲- کارکرد محصول

- این سامانه با شناسایی کلاهبرداران باعث ایجاد فضایی امن برای کاربران فضای مجازی می‌شود.

[1] Random Access Memory
[2] Sold State Drive
[3] Two-Step Verification

- این سامانه با استفاده از ابزارهای مختلف در تشخیص مدارک جعلی به کاربران کمک می‌کند که اخبار دروغین را تشخیص بدهند.
- این سامانه با استفاده از هوش مصنوعی گنجانده شده در خود می‌تواند بدون نیاز به ورود به سیستم قضایی به سؤالات و ابهامات قانونی شما در سریع‌ترین زمان ممکن بهترین پاسخ را ارائه دهد.
- این سیستم‌ها می‌توانند با قراردادن اطلاعات در اختیار پلیس کار نیروهای پلیس را تسهیل ببخشد.
- این سیستم‌ها می‌توانند با شناسایی حملات ddos از آسیب به سرورها جلوگیری کنند.
- این سامانه با ویژگی غیرحضوری بودن خود می‌تواند حتی‌الامکان از ایجاد ترافیک جلوگیری کرده و ردپای کربن[1] را نیز به طرز چشمگیری کاهش دهد.
- این سامانه قابلیت مشاهده و رصد لحظه‌ای پرونده را نیز فراهم می‌کند.

۲-۳- قوانین کسب‌وکار

قوانین کسب‌وکار شامل مجموعه‌ای از مقررات و قوانین حقوقی است که باید رعایت شوند. در ادامه به برخی از این قوانین به‌کارگرفته‌شده در این سامانه پرداخته می‌شود.

- هر شخص برای ورود به سامانه باید شماره همراهی به نام خود داشته باشد که پیامک تأیید کاربر برای آن شماره ارسال شود.
- مقامات قضایی باید مجوز و مدرک لازم را برای قضاوت و اجرای احکام داشته باشند و آن را بارگذاری کنند.
- برای پذیرش ادلهٔ دیجیتال در محاکم، لازم است که صحت و تمامیت آنها حفظ شود. این امر معمولاً از طریق استفاده از تکنیک‌های درهم‌سازی[2] و ارائهٔ شواهدی مبنی بر عدم تغییر یا دست‌کاری داده‌ها انجام می‌شود.
- جهت حفظ امنیت اطلاعات کاربر، اگر کاربر به مدت ۱۵ دقیقه از سامانه استفاده نکند و خارج نشود، سامانه به طور خودکار باید کاربر را از دسترس خود خارج کند.
- در صورت سه بار بی‌توجهی به نامه ارسالی از سمت دادگاه، قاضی می‌تواند حکم جلب شخص را صادر کند.
- اطلاعات کاربران را به‌دقت محافظت کرده و از هرگونه سوءاستفاده یا نقض حریم خصوصی آنها جلوگیری شود.
- به شواهد دیجیتالی که توسط پلیس ضبط شده است به‌عنوان شواهد شخص اول و شواهد دیجیتالی که از منابع دیگر گرفته شده است به‌عنوان شواهد شخص ثالث اشاره خواهیم.
- سیستم باید برای ذخیره و جلوگیری از ازدست‌رفتن داده‌های کاربران به طور منظم از پایگاه‌داده.
- اطمینان از انطباق سیستم با استانداردها و مقررات ملی و بین‌المللی مرتبط با مدیریت ادله دیجیتال.

[1] Carbon Footprint
[2] hashing

- تنظیم سطوح دسترسی برای کاربران مختلف بر اساس نقش‌ها و مسئولیت‌هایشان، به‌منظور جلوگیری از دسترسی غیرمجاز به داده‌ها.

۲-۴- مشخصات کاربران

سامانه ادله دیجیتال توسط گروه‌های مختلفی از کاربران مورد استفاده قرار می‌گیرد که هر یک نقش‌ها و مسئولیت‌های خاصی در فرایند مدیریت، تحلیل و استفاده از این ادله دارند. در ادامه، انواع کاربران این سامانه‌ها و توضیح مختصری درباره هر یک ارائه شده است:

- کاربران عمومی (شاکیان و متهمان): در برخی موارد، افراد عادی ممکن است نیاز به استفاده از سامانه‌های مدیریت ادله دیجیتال داشته باشند، مثلاً برای ارائه شواهد در پرونده‌های مدنی یا پیگیری مسائل حقوقی شخصی.
- وکلای مدافع: وکلای مدافع از این سامانه‌ها برای بررسی شواهد دیجیتال مرتبط با موکلان خود استفاده می‌کنند. آنها می‌توانند با تحلیل این شواهد، دفاعیات مؤثرتری ارائه دهند و از حقوق موکلان خود دفاع کنند.
- قضات و دادستان‌ها: این گروه از کاربران برای بررسی و ارزیابی شواهد دیجیتال در فرایندهای قضایی از سامانه‌های مدیریت ادله دیجیتال بهره می‌برند. دسترسی به شواهد معتبر و مستند به آنها کمک می‌کند تا تصمیمات قانونی دقیق‌تری اتخاذ کنند.
- مأموران اجرای قانون: پلیس و سایر مأموران اجرای قانون از سامانه‌های مدیریت ادله دیجیتال برای دسترسی سریع و مؤثر به شواهد الکترونیکی استفاده می‌کنند. این سامانه‌ها به آنها امکان می‌دهد تا در تحقیقات خود به داده‌های مورد نیاز دسترسی داشته باشند و روند پیگیری پرونده‌ها را تسریع کنند.

۲-۵- قیود

در این بخش به محدودیت‌های پیشرو می‌پردازیم:

C1. سیستم باید توانایی مدیریت و پردازش حجم زیادی از داده‌های دیجیتال را از جمله عکس، ویدئو و صدا را داشته باشد.

C2. هر کاربر (قضات، شاکیان و متهمان) فقط با یک کد ملی و یک شماره تماس می‌تواند ثبت‌نام کند.

C3. داده‌هایی که از طریق هوش مصنوعی تحلیل می‌شوند باید دقت بالایی داشته باشد و بتواند نوع جرایم را تشخیص دهد.

C4. سیستم باید از رمزنگاری‌های قوی همچون RSA و AES-256 استفاده کند تا بتواند از نفوذ و دست‌کاری جلوگیری کند.

C5. باید اطلاعات خصوصی کاربر در سیستم مطابق استانداردهای بین‌المللی و تابع حفاظت از داده‌ها و حریم خصوصی ایران حفظ شود.

C6. برای پردازش داده‌های حجیم ما نیازمند زیرساخت قوی هستیم که می‌توان به سرور و پردازنده‌های سریع اشاره کرد.

C7. سیستم باید قابلیت اتصال به پایگاه‌داده‌های پلیس و نهادهای قضایی را داشته باشد.

C8. سیستم باید شواهد و مدارک دیجیتالی را به‌گونه‌ای غیرقابل‌تغییر و ویرایش کند که نهادهای پلیس و قوه قضاییه به این سیستم اعتماد داشته باشند.

C9. برخی از پرونده‌ها نیازمند پردازش سریع اطلاعات هستند پس باید مدت‌زمان پردازش تاحدامکان کم باشد.

C10. باید سیستمی طراحی کرد که به‌صورت لایه‌ای باشد و دسترسی کاربران محدود باشد.

C11. سیستم باید بتواند بدون کاهش کارایی، هجمه‌ای را از کاربرانی که به‌صورت هم‌زمان از آن سیستم استفاده می‌کنند به‌خوبی مدیریت کند.

۲-۶- مفروضات و وابستگی‌ها

مفروضات:

- کاربر باید کد ملی و یک شماره همراه به نام خودش داشته باشد.
- کاربر باید از حداقل سواد خواندن و نوشتن برخوردار باشد.
- کاربر باید از روش‌های کار با وسایل هوشمند مثل کامپیوتر یا گوشی دارای حداقل‌های یادگیری باشد.

وابستگی‌ها:

- برای کار با سامانه به یک بستر اینترنت پرسرعت نیازمندیم.
- به یک سامانه ارسال پیام کوتاه برای احراز هویت کاربران احتیاج است.
- سامانه به یک سیستم پرداخت آنلاین نیاز دارد.
- برای ثبت، حفاظت و بازیابی اطلاعات کاربران به یک پایگاه‌داده کلان نیازمندیم.

۳- نیازمندی‌ها

۳-۱- تبیین نیازمندی‌های کارکردی

۳-۱-۱- ثبت‌نام کاربران (مراجع قضایی، شاکیان و متهمان)

R1. در سامانه باید یک بخش دادرسی توسط هوش مصنوعی ایجاد شود که شخص بدون ورود به سامانه سؤالات و ابهامات خود را از آن بپرسد و درگیر فرایند شکایت نشود. همچنین بهترین و دقیق‌ترین پاسخ خود را دریافت کند.

R2. سامانه باید شرایط ثبت‌نام با شماره تماس منطبق با کد ملی و ایجاد رمز را فراهم کند.

R3. سامانه باید شرایط ثبت‌نام با شماره تماس منطبق با اسم شخص را فراهم کند.

R4. سامانه باید خطا دادن در صورت رعایت‌نکردن قالب نوشتاری در واردکردن شماره و کد ملی را لحاظ کند.

R5. سامانه باید قابلیت تشخیص ربات بودن یا نبودن شخص را با کپچا داشته باشد.

R6. سامانه باید ثبت‌نام با ایمیل[1] را امکان‌پذیر کند.

R7. سامانه باید امکان ارسال پیامک تأیید به ایمیل شخص را تعبیه کند.

R8. سامانه باید قابلیت تشخیص یکتا بودن اطلاعاتی مانند شماره تماس و کد ملی را داشته باشد.

R9. سامانه باید در صورت هر گونه تکراری بودن شماره همراه به کاربر اخطار دهد.

R10. سامانه باید در صورت هر گونه تکراری بودن کد ملی به کاربر اخطار دهد.

R11. سامانه باید پس از ۳ بار اشتباه‌کردن کاربر در واردکردن رمز یا کد ملی دسترسی او را به مدت ۱۵ دقیقه محدود کند.

R12. سامانه باید تأیید کاربر با کد امنیتی از طریق پیامک را امکان‌پذیر کند.

R13. سامانه باید فیلم آموزشی نحوه ثبت‌نام باید برای کاربران فراهم کند و لینک آن در صفحه لاگین[2] قرار داده شود.

R14. سامانه باید گزینه فراموشی رمز عبور و گزینه بازیابی حساب کاربری را قرار دهد.

۳-۱-۲- مرحله پس از ورود

۳-۱-۲-۱- دستگاه‌های قضایی (قضات، وکلا، نیروی انتظامی و...)

R15. در سامانه باید امکان دریافت ادله بر اساس میزان دسترسی افراد به اسناد اعمال شود.

R16. سامانه باید امکان مشاهده نظر هوش مصنوعی در خصوص ادله ارائه شده را فراهم کند و به مرجع قضایی بدهد.

R17. سامانه باید امکان درخواست گرفتن ادله بیشتر از شاکی یا متهم را تعبیه کند.

R18. سامانه باید امکان ارسال نامه به نهادهای دیگر مانند دادگاه، دادسرا، شهرداری و... را در صورت نیاز فراهم کند.

R19. سامانه باید امکان صدور حکم جلب در صورت مراجعه‌نکردن شاکی یا متهم به دادگاه پس از ۳ نامه را در دسترس قرار دهد.

[1] Email
[2] Login

R20. سامانه باید ثبت نظر نهایی در خصوص شکایت و نشان‌دادن نتیجه به شاکی یا متهم را ایجاد کند.

R21. سامانه باید ارسال نتیجه نهایی به دست شاکی یا متهم را فراهم کند.

R22. در سامانه باید ثبت و ذخیره جزئیات کامل پرونده در پایگاه‌داده برای مشاهده قاضی، متهم و شاکی ایجاد شود.

R23. سامانه باید سوابق پرونده‌ها را بایگانی کند و امکان جستجو با شماره پرونده در بین اسناد مجاز (قابل‌دسترسی توسط مرجع قضایی) پایگاه‌داده فراهم شود.

R24. سامانه باید امکان معرفی شاکی یا متهم به پلیس در صورت جعلی بودن ادله دیجیتال از جمله صدا، تصویر، متن و در کل هر نوع مدرک را پشتیبانی کند.

R25. سامانه باید امکان نظر دادن در خصوص رفتار سامانه و دیدن نظرات بقیه به‌صورت پیام متنی را در اختیار کاربران (قضات، شاکیان و متهمان) قرار دهد.

R26. سامانه باید امکان ثبت نوبت دادگاه برای مراجع قضایی و اطلاع‌رسانی به شاکی و متهم را فراهم کند.

R27. در سامانه باید مرجع قضایی بتواند به سامانه دریافت سوءپیشینه، سامانه وضعیت سلامت جسم و روان و... دسترسی داشته باشد تا بهتر بتواند تصمیم بگیرد.

R28. سامانه باید کتاب قوانین جمهوری اسلامی ایران را در قالب یک فایل قابل‌جستجو در دسترس مرجع قضایی قرار دهد.

R29. سامانه باید به سامانه معاینه فنی، تعویض پلاک و... فرد متهم دسترسی داشته باشد تا در خصوص شکایت بتواند بهتر تصمیم بگیرد.

R30. سامانه باید امکان جریمه‌کردن آنلاین فرد خاطی توسط پلیس راهنمایی‌ورانندگی را پس از اثبات جرم فراهم کند.

۳-۱-۲-۲-شاکی و متهم

R31. سامانه باید ثبت و ویرایش ادله دیجیتال برای شاکی یا متهم را فراهم کند.

R32. در سامانه باید ثبت تاریخ و ساعت ادله ارائه شده برای دسترسی بهتر مراجع قضایی تعبیه شود.

R33. سامانه باید طبقه‌بندی ادله توسط هوش مصنوعی پس از بارگذاری توسط متهم یا شاکی را انجام دهد.

R34. سامانه باید تشخیص جعلی بودن یا نبودن صوت و تصویر و متن توسط هوش مصنوعی را انجام دهد و نتیجه نهایی به دست مرجع قضایی برسد.

R35. سامانه باید امکان بررسی فرایند قضایی و مشاهده پرونده در جریان را فراهم کند.

R36. سامانه باید امکان نظر دادن در خصوص رفتار سامانه و دیدن نظرات بقیه به‌صورت پیام متنی را در اختیار افراد قرار دهد.

R37. در سامانه باید درگاه پرداخت آنلاین برای بررسی شکایات شاکیان تعبیه شود تا از پرداخت حضوری یا رشوه جلوگیری شود.

R38. سامانه باید شرایطی فراهم کند تا شاکی بتواند هر زمان که خواست از شکایت خود صرف‌نظر کرده و پرونده به بایگانی رود.

R39. سامانه باید شرایطی فراهم کند تا متهم بتواند هر زمان که خواست اظهارات شاکی را تأیید کند و پرونده مختومه گردد.

R40. سامانه باید به برخی لهجه‌های داخلی مثل لری، کردی و... مسلط باشد تا برخی از هم‌وطنانمان بتوانند از سامانه به‌درستی استفاده کنند.

۳-۲- تبیین نیازمندی‌های غیرکارکردی

۳-۲-۱- امنیت

- سامانه باید داده‌های ذخیره‌شده را با الگوریتم‌های رمزنگاری قوی (AES-256, RSA) محافظت کند.
- در سامانه باید مدارک هویتی مثل آدرس منزل، شماره تماس، کد ملی و... شاکی و متهم از دسترس یکدیگر خارج شود و تنها با اجازه مرجع قضایی این مدارک در اختیار متهم یا شاکی قرار گیرند
- سامانه باید امکان شناسایی و جلوگیری از حملات سایبری مانند DDoS، SQL Injection و XSS را فراهم کند.
- سامانه باید قابلیت ردیابی تغییرات را داشته باشد.
- سامانه باید در صورت تشخیص فعالیت مشکوک، هشدارهای امنیتی فوری صادر کند و به طور خودکار قفل شود.
- سامانه باید قابلیت کنترل سطح دسترسی کاربران بر اساس نقش و مسئولیت آن‌ها را فراهم کند.

۳-۲-۲- کارایی و عملکرد

- سامانه باید تأخیر پاسخگویی به درخواست‌های کاربران را بیش از حد طولانی نکند.
- سامانه باید حداقل ۱۰۰۰ پرونده را به طور هم‌زمان بدون افت کارایی پردازش کند.
- سامانه باید توانایی پردازش حداقل ۱۰ ترابایت داده در ماه را داشته باشد.
- سامانه باید از رایانش توزیع‌شده برای پردازش سریع‌تر داده‌ها استفاده کند.
- سامانه باید پردازش و تحلیل داده‌های چندرسانه‌ای (تصویر، ویدئو، صوت) را در کمترین زمان ممکن انجام شود.
- سامانه باید بهینه‌سازی مصرف منابع سخت‌افزاری برای افزایش بهره‌وری سیستم را اعمال کند.

۳-۲-۳- قابلیت اطمینان و دسترس‌پذیری

- سامانه باید ۷/۲۴ [1] (بدون توقف) فعال باشد.
- سامانه باید در صورت خرابی، حداکثر ظرف ۳۰ دقیقه بازیابی شود.

[1] 24 hours a day of 7 days a week

- سامانه باید از چندین سرور پشتیبان خودکار برای جلوگیری از ازدست‌رفتن اطلاعات استفاده کند.
- در سامانه اگر یک سرور از کار بیفتد، سامانه باید بدون تأخیر به سرور جایگزین منتقل شود.
- در سامانه باید قابلیت بازگردانی سریع اطلاعات حذف‌شده یا خراب‌شده وجود داشته باشد.
- سامانه باید سرویس‌ها را به‌گونه‌ای طراحی کند که در صورت افزایش کاربران، بدون افت عملکرد مقیاس‌پذیر باشد.

۳-۲-۴- مقیاس‌پذیری و توسعه‌پذیری

- در سامانه باید طراحی نرم‌افزار باید به‌گونه‌ای باشد که افزودن قابلیت‌های جدید بدون نیاز به تغییرات اساسی امکان‌پذیر باشد و بدون نیاز به توقف سرویس انجام شود.
- سامانه باید با سرویس‌های ابری[1] سازگار باشد.
- سامانه باید امکان اتصال به API[2]های سایر سیستم‌های قانونی و امنیتی را داشته باشد.
- سامانه باید هزینه نگهداری سیستم را بهینه و مقرون‌به‌صرفه کند.

۳-۳- قیود طراحی

تمامی شرایط، استانداردها و محدودیت‌هایی که به هنگام طراحی باید آنها را رعایت کرد:

- سامانه باید با قوانین داخلی مانند قانون حمایت از اطلاعات شخصی و حریم خصوصی و همچنین قوانین حقوقی جمهوری اسلامی ایران، تطابق داشته باشد.
- سامانه باید مطابق با استانداردهای بین‌المللی و داخلی امنیت اطلاعات، پیاده‌سازی شود.
- ذخیره‌سازی داده‌ها باید در سرورهای امن HTTPS مطابق با استانداردهای امنیتی باشد.
- سامانه باید به‌صورت مستمر مورد بررسی و تست‌های نفوذ قرار گیرد تا از آسیب‌پذیری‌ها و تهدیدات امنیتی جلوگیری شود.
- سیستم باید از تاریخ شمسی استفاده کند.

۳-۴- صفت‌های سیستم نرم‌افزاری

- امنیت: حفاظت از داده‌ها و اسناد در برابر دسترسی‌های غیرمجاز و تهدیدات سایبری از اهمیت بالایی برخوردار است. این سیستم باید با استفاده از مکانیزم‌های امنیتی پیشرفته، از جمله رمزنگاری و کنترل دسترسی، امنیت اطلاعات را تضمین کنند.

[1] Cloud-based solutions
[2] Application Programming Interface

- **دسترس‌پذیری[1]: اطمینان از دسترسی آسان و سریع کاربران مجاز به اسناد و داده‌ها در هر زمان و مکان ضروری است. سیستم‌های مدیریت اسناد باید امکان دسترسی آنلاین و آفلاین را فراهم کرده و با دستگاه‌های مختلف سازگار باشند.**
- **قابلیت اعتماد: سیستم باید در شرایط مختلف به‌درستی کار کند و احتمال خرابی آن کم باشد؛ همچنین سیستم باید از روش‌های پشتیبان‌گیری و بازیابی اطلاعات استفاده کند.**
- **قابلیت تعامل: سیستم باید بتواند با سایر سامانه‌های قضایی، پلیسی، و بانک‌های اطلاعاتی تبادل اطلاعات کند. استفاده ازAPIها و استانداردهای داده‌ای مانند JSON یا XML برای تبادل اطلاعات پیشنهاد می‌شود.**
- **هم‌زمانی استفاده تعداد کاربران: سیستم باید توانایی پشتیبانی از استفاده هم‌زمان چندین کاربر را داشته باشد، به‌طوری که هر کاربر بتواند بدون تداخل با دیگران به اسناد دسترسی پیدا کند.**
- **محیط کاربرپسند[2]: رابط کاربری ساده و قابل‌فهم، تجربه کاربری را بهبود می‌بخشد و نیاز به آموزش‌های پیچیده را کاهش می‌دهد. این امر باعث افزایش بهره‌وری و رضایت کاربران می‌شود.**
- **عملکرد مناسب: سیستم باید تمامی نیازمندی‌های کاربران خود را به طور کامل و دقیق پوشش دهد. برای سیستم ادله دیجیتالی، این بخش شامل ویژگی‌هایی مانند جمع‌آوری، تحلیل، و ذخیره‌سازی شواهد دیجیتال می‌شود.**
- **کارایی[3]: سیستم باید قادر به پردازش حجم بالای داده‌ها در مدت‌زمان معقول باشد. در سیستم‌های ادله دیجیتالی، سرعت جمع‌آوری و تحلیل داده‌ها به‌ویژه در شرایط اضطراری بسیار مهم است.**
- **قابلیت نگهداری[4]: سیستم باید به‌گونه‌ای طراحی شود که بتوان آن را به‌راحتی به‌روزرسانی و اصلاح کرد. برای سیستم‌های ادله دیجیتال، این بخش شامل به‌روزرسانی‌های امنیتی و اصلاحات در الگوریتم‌های تحلیلی می‌شود.**
- **قابلیت حمل‌ونقل[5]: سیستم باید قابل‌حمل باشد و امکان استفاده از آن در پلتفرم‌های مختلف و با سخت‌افزارهای مختلف وجود داشته باشد.**

۳-۵- برنامه تکرار

نیازمندی‌ها	اولویت	وابستگی
R1	2	
R2	1	
R3	1	
R4	1	R2,R3
R5	1	

[1] Availability
[2] User-friendly
[3] Performance Efficiency
[4] Maintainability
[5] Portability

R6	1	
R7	1	
R8	1	R2,R3
R9	1	R3
R10	1	R2
R11	2	R2
R12	1	R3
R13	3	R2
R14	2	R2,R3
R15	1	
R16	2	R31
R17	1	R31
R18	1	R20
R19	2	R20
R20	1	
R21	1	R20
R22	2	R31,R20
R23	2	R22,R20
R24	3	R31,R16,R33
R25	3	
R26	1	R20
R27	2	
R28	3	
R29	2	
R30	1	R20
R31	1	
R32	1	R31
R33	2	R31
R34	1	R33
R35	1	R20
R36	3	R20
R37	1	
R38	1	
R39	1	
R40	3	

جدول 2

نیازمندی ها	تعداد هفته	تکرار
R2		
R3		
R4		
R5		
R6		
R7		
R8		
R9		

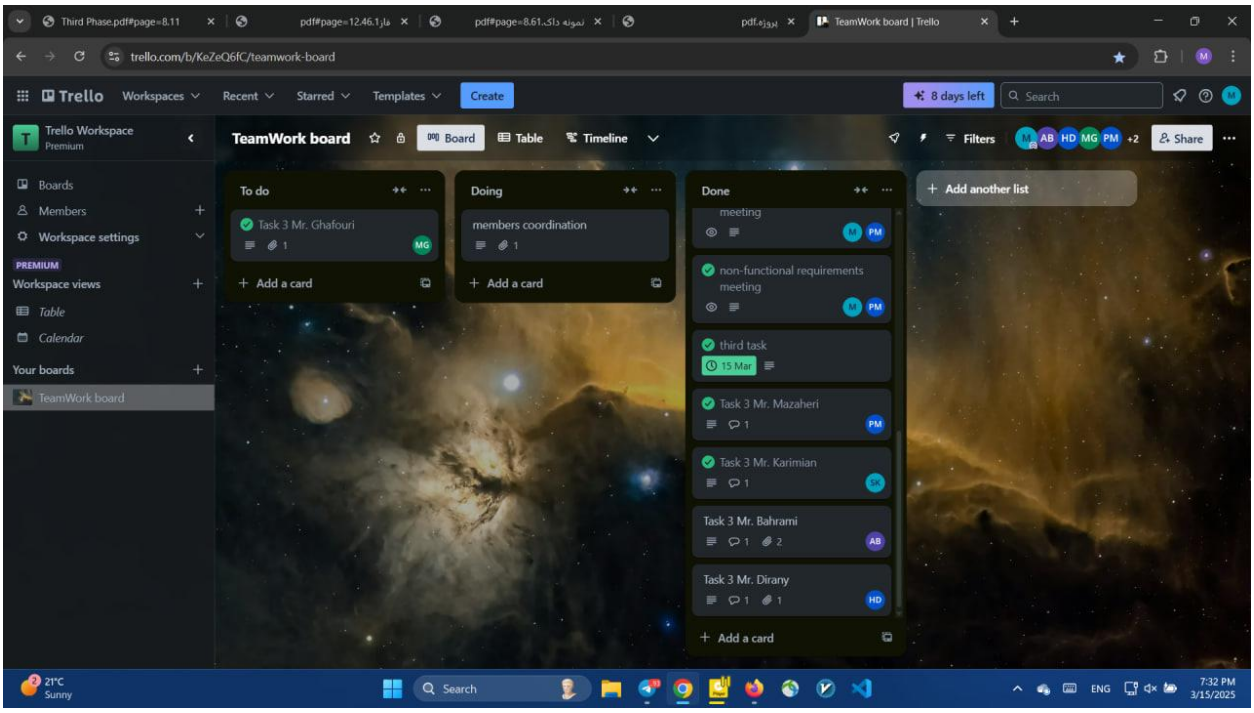
R10	چهار هفته	تکرار اول
R12		
R15		
R17		
R18		
R20		
R21		
R26		
R30		
R31		
R32		
R34		
R35		
R37		
R38		
R39		
R1	سه هفته	تکرار دوم
R11		
R14		
R16		
R19		
R22		
R23		
R27		
R29		
R33		
R13	دو هفته	تکرار سوم
R24		
R25		
R28		
R36		
R40		

جدول 3

	محمد محمدی	پارسا مظاهری	مهدی غفوری	سهیل کریمیان	علی بهرامی	حیدرعلی الدیرانی
مقدمه،هدف،قلمرو	R	R	R	R	R	R
بیان مسئله،تعاریف	R	R	C	A	C	C
طرح کلی	R	-	-	C	-	-
شرح کلی	R	R	R	A	A	A
چشم انداز محصول	A	-	-	A	-	C
کارکرد محصول	-	-	-	-	R	-
قوانین کسب و کار	-	-	A	-	-	-

مشخصات کاربران	C	-	A	-	-	-
قیود	A	R	-	-	-	-
نیازمندی‌های کارکردی	R	R	I	I	I	-
نیازمندی‌های غیرکارکردی	R	R	-	-	-	-
قیود طراحی	A	-	-	A	-	-
صفات سیستم نرم‌افزاری	I	-	R	-	-	-

جدول 4 – ماتریس RACI



تصویر 1 – Trello board