پروپوزال فنی "سامانه مستندساز ادله الکترونیکی"	
کارفرما : معاونت نظارت بر فضای مجازی دادستانی کل کشور	**شرکت فناوری های تنظیم یار شریف**

عنوان محصول

فناوری های مستندساز ادله الکترونیکی

چکیده

در این پروپوزال، پیشنهاد فنی سامانه مستندساز ادله الکترونیکی خدمت **معاونت محترم نظارت بر فضای مجازی دادستانی کل کشور** ارائه می گردد. سامانه مستند ساز ادله الکترونیکی عدالت یار، بستری جهت گردآوری و دسترسی به ادله الکترونیکی اشخاص حقیقی و ارائه آن ها به دادگاه می باشد. به کمک این سامانه می توان تمامی مدارک الکترونیکی لازم را جمع آوری نمود که مدیریت آن طبق آئین نامه مذکور به صورت امن توسط اشخاص حقیقی و با امکان مشاوره از سمت **مرکز آمار و فناوری اطلاعات قوه قضائیه** انجام می‌گیرد. اپلیکیشن این سامانه کمک بسیاری به دسترس پذیری اطلاعات در لحظه و اعتمادسازی به فرآیند شکایت می کند و می تواند در دو جهت جامعه را هدایت و یاری نماید:

۱. افزایش آگاهی جامعه در مورد طرح شکایات و کمک به حفظ هویت افراد و افزایش آسایش در جامعه
۲. افزایش سرعت رسیدگی به پرونده ها و بازرسی آن ها و کمک به قضاوت

شرح نیاز

امروزه با گسترش فناوری های مبتنی بر اینترنت، توسعه نرم افزارها، سخت افزار ها و بهبود فرآیند های آنلاین، تمامی امکانات و مسائل موجود به شکل آنلاین مطرح و حل و فصل می گردند. همچنین پس از همه گیری بیماری ویروس کرونا، مردم بیش از پیش به ترکنش های آنلاین و حل مسائل خود بدون مراجعه حضوری روی آوردند که در نهایت موجب پدیدار شدن خدمات الکترونیکی از جمله ادله الکترونیکی شامل گفتگوها، خرید و فروش ها، مبادلات، انتقال اطلاعات و ... شده است .

(کاربرد و نیاز جامعه) در این دوران، بیشتر مسائل و مشاجرات و تهدید و توهین ها در فضای مجازی و در قالب چت و یا انتشار مطلب به صورت پست در گروه ها، صفحات وب و کانال ها شکل گرفته است. بنابراین داده گاه ها نیز در پرونده های حقوقی، کیفری و تجدیدنظر به استفاده از این ادله تمایل پیدا می کنند و با درخواست شاکیان و متشاکیان در قبال رسیدگی به این ادله الکترونیکی مواجه می شوند. همچنین مردم امروزه بر اساس وقایع و شواهد در دسترس خود که معمولا اطلاعات موجود در فضای مجازی در قالب های مذکور می باشد، شکایت خود را مطرح می کنند و یا از خود در مقابل شکایت دفاع می کنند. این مدارک به صورت کلی شامل اسکرین شات از چت ها و پست ها،اطلاعات حساب های مجازی، انتشار غلط اطلاعات، مدارک و حساب های سواستفاده از هویت افراد، و همچنین اطلاعات سایت ها و وبلاگ ها می باشد. رسید های مالی و پرداخت ها نیز از جمله این مدارک می باشند.

(حذف پیام) همچنین در بسیاری از پیام رسان ها پس از ارسال پیام، امکان حذف آن چه برای خود فرستنده و چه حتی برای گیرنده وجود دارد که باعث می شود هیچ رد و اثری از گفتگو باقی نماند و شاکی و متشاکی به دلیل فرصت از دست رفته جهت اثبات شواهد خود، نتوانند هیچگاه به آن استناد کنند و احقاق حق نمایند. همچنین دادگاه ها، مراجع قضائی و پلیس فتا نیز با وجود امکانات متعدد جهت استعلام اطلاعات افراد، دسترسی به این داده ها ندارند. وجود این سامانه و در دسترس قرارگیری سامانه آن برای عموم مردم، موجب جمع آوری سریع و بهینه ادله الکترونیکی می شود و امکان حل بسیاری مسائل و رفع دغدغه ها را به مردم می دهد.

(پیام رسان ها) نتایج نظرسنجی مرکز افکارسنجی دانشجویان ایران (ایسپا) حاکی از این است که ۶۴.۱ درصد از افراد بالای ۱۸ سال کشور از پیام‌رسان واتس‌اپ استفاده می‌کنند، اینستاگرام با ۴۵.۳ درصد در رتبه دوم و تلگرام با ۳۶.۳ درصد در رتبه سوم قرار دارد. پس از تلگرام، ۴.۸ درصد از ایتا، ۴ درصد از سروش، ۴ درصد از بله، ۳.۳ درصد از فیس‌بوک و ۲ درصد افراد بالای ۱۸ سال کشور از توییتر استفاده می‌کنند.

همچنین طبق نتایج نظرسنجی این مرکز در مردادماه ۱۴۰۰، در پاسخ به این پرسش که "در حال حاضر، شما از کدام رسانه‌های اجتماعی استفاده می‌کنید؟" ۴۸.۴ درصد پاسخگویان اعلام کردند که فقط از رسانه‌های اجتماعی خارجی مثل تلگرام، واتس‌اپ و اینستاگرام استفاده می‌کنند؛ در مقابل ۱.۸ درصد پاسخگویان فقط از رسانه‌های اجتماعی داخلی مثل سروش، روبیکا و... استفاده می‌کنند. همچنین ۲۲.۸ درصد پاسخگویان، هم از رسانه‌های اجتماعی داخلی و هم خارجی استفاده می‌کنند. ۲۷ درصد پاسخگویان نیز در حال حاضر کاربر هیچکدام از رسانه‌های اجتماعی داخلی یا خارجی نیستند.

(پیام رسان های داخلی) طبق گفته های کمیسیون مشترک طرح حمایت از حقوق کاربران و خدمات پایه کاربردی فضای مجازی در آبان ۱۴۰۰، تعداد کاربر ثبت‌نام‌شده در ایتا ۱۱ میلیون و ۶۰۰ هزار نفر و تعداد کاربران فعال ماهانه ۳ میلیون و ۳۸۰ هزار نفر است. همچنین اطلاعات تعداد کاربران ثبت‌نام‌شده در پیام‌رسان سروش پلاس ۱۲ میلیون و ۲۰۰ هزار نفر و کاربران فعال ماهانه ۲ میلیون و ۳۰۰ هزار نفر است؛ تعداد کاربر ثبت‌نام‌شده در پیام‌رسان بله ۸ میلیون و ۴۴۵ هزار نفر و کاربران فعال ماهانه آن ۱ میلیون و ۳۸۲ هزار نفر برآورد می‌شود. تعداد کاربر ثبت‌نام‌شده در پیام‌رسان گپ ۶ میلیون و ۳۰۰ هزار نفر و کاربران فعال ماهانه این پیام‌رسان ۴ میلیون و ۴۰۰ هزار نفر هستند. بر اساس برآوردهای مرکز ملی فضای مجازی با حذف کاربران مشترک، حدود ۲۰ میلیون نفر کاربر منحصربه‌فرد از مجموع این پیام‌رسان‌ها استفاده می‌کنند. میزان ترافیک مصرفی سرویس‌های اینترنت و IXP پیام‌رسان‌ها در مرکز داده شبکه ملی اطلاعات در شکل ۱ آمده است:

• **میزان ترافیک مصرفی سرویس های اینترنت و IXP پیام رسان ها در مرکز داده شبکه ملی اطلاعات**

ردیف	نام	اینترنت				IXP			
		ترافیک ماهانه		ترافیک روزانه		ترافیک ماهانه		ترافیک روزانه	
		ماکزیمم	میانگین	ماکزیمم	میانگین	ماکزیمم	میانگین	ماکزیمم	میانگین
۱	سروش	19 M	10 M	19.5 M	9.4 M	9.3 G	1.2 G	5.7 G	2.4 G
۲	ایتا	235 M	25 M	47 M	26 M	5 G	2.9 G	4.6 G	3 G
۳	گپ	810 M	306 M	576 M	324 M	0	0	0	0
۴	آی گپ	35 K	4 K	37 K	4 K	0	0	0	0

شکل ۱. میزان ترافیک مصرفی سرویس‌های اینترنت و IXP پیام‌رسان‌ها در مرکز داده شبکه ملی اطلاعات

کاربردها و چالش ها

هدف ازاین پروپوزال، تولید سامانه ای جهت ثبت و نگهداری داده های دیجیتال به صورت امن و ایجاد توکن تراکنش جمع آوری ادله برای کارفرما و کد رهگیری برای کاربر به عنوان خروجی(محصول) می باشد تا قابلیت استفاده در محاکم قانونی را دارا باشد. این سامانه برای پیام رسان های خارجی و داخلی اعم از واتس‌اپ، تلگرام، اینستاگرام، بله، ایتا، سروش پلاس و آی گپ توسعه داده می شود. در ادامه، چالش و راهکار برای هرکدام از قسمت های پیام رسان ها ذکر می گردد. ذکر این چالش ها و مطالعه دقیق پیام رسان ها از بابت اطمینان از تسلط کامل به چالش ها و مشکلات در این راه به جهت دستیابی به راهکار بهینه موردتوجه قرار گرفته است.

۱. تلگرام

این اپلیکیشن پیام رسان متمرکز بر سرعت و امنیت می باشد. رایگان بودن خدمات برای عموم کاربران در عین سرعت و سادگی کاربری موجب استقبال از آن شده است. با توجه به ذخیره داده ها بر روی سرور خود اپلیکیشن که خارج از کشور قرار دارد و جهت استنادپذیری دسترسی به منابع داده ها میسر نمی باشد، و همچنین با آگاهی از فرآیند ورود کاربر و توصیه تلگرام به استفاده کاربران از تایید دو مرحله ای، لازم است تا چالش ها و راهکارهای ممکن برای این اپلیکیشن به دقیق ترین صورت ممکن بررسی شود.

موجودیت ها: این اپلیکیشن دو نسخه اپ موبایل و نسخه دسکتاپ اپ دارد که هردو عملکرد مشابهی دارند. هرکدام از موجودیت هایی که قابلیت ثبت اطلاعات دارند، به تفکیک به همراه چالش های هرکدام ذکر می گردند:

- ✓ **صفحه خانه اپلیکیشن:** این صفحه شامل تمامی چت های شخصی و گروه ها، کانال ها می باشد.
- ✓ **گروه ها :** یک گروه معمولی تلگرام می‌تواند نهایتا ۲۰۰ عضو را داشته باشد. در گروه معمولی هر یک از اعضا قادر به تغییر نام گروه، تغییر عکس گروه و همچنین اضافه کردن اعضای جدید به آن خواهند بود. اما سوپر گروه تلگرام قادر است تا ۵۰۰۰ عضو را در خود جای دهد. همچنین سوپر گروه تلگرام از تاریخچه یکپارچه (Unified History) بهره می‌برد، بنابراین پیام‌هایی که از گروه حذف شوند در تلگرام تمام کاربران گروه حذف خواهند شد. قابلیت پین یا سنجاق کردن پیام‌های مهم به بخش فوقانی صفحه هم از دیگر ویژگی‌های منحصر به فرد یک سوپر گروه تلگرام است.
- ✓ **کانال ها:** امکان ارسال پیام و اظهار نظر در مورد پست‌های ارسال‌شده در کانال‌های تلگرامی وجود ندارد. این یک ویژگی بخصوص کانال‌های تلگرامی است که آن‌ها را از دیگر گروه‌های ارتباطی جدا می‌کند. در یک کانال، پیام‌ها توسط مدیران کانال قابل‌ارسال بوده و کاربران معمولی تنها قادر به خواندن آن‌ها هستند. این نوع عملکرد به منظور بهینه‌سازی در ارسال پست‌های انبوه ایجاد شد. اعلان پست جدید به صورت خودکار به همه افراد دنبال‌کننده کانال ارسال می‌شود.
- ✓ **صفحه شخصی:** این ویژگی، حالت خاص "گروه ها" محسوب می شود که طی آن افراد با یکدیگر مبادله داده انجام می دهند. تمامی اطلاعات و دسترسی ها مانند گروه های ساده می باشند.
- ✓ **چت های آرشیو شده:** این چت ها در صفحه خانه اپلیکیشن قابل مشاهده نیستند و به منظور عدم نیاز کاربر به حضور در صفحه اصلی تعریف می شوند.
- ✓ **صفحه پیام های ذخیره شده:** این صفحه که حالت خاصی از صفحه شخصی می باشد ، برای ذخیره اطلاعات توسط کاربر استفاده می گردد. از نظر ماهیت فنی هیچ تفاوتی با صفحات چت شخصی ندارند.

- ✓ **چالش های موجودیت های تلگرام:**
  - **(صفحات اطلاعات کانال)** در این صفحات، اطلاعات کانال شامل لینک کانال، بیوی کانال، تعداد هرکدام از اطلاعات به تفکیک نوع داده، امکان خروج از کانال و گزارش کانال وجود دارد.
  - **(صفحات اطلاعات گروه)** در این صفحات، اطلاعات گروه شامل لینک گروه ، بیوی گروه ، تعداد هرکدام از اطلاعات به تفکیک نوع داده، امکان خروج از گروه و همچنین تعداد و پروفایل کاربران وجود دارد.
  - **(امکان خروجی گرفتن از تاریخچه تلگرام)** این امکان در صورت نیاز می تواند به کمک سامانه مستندساز ادله الکترونیک بیاید. این امکان از تمامی تاریخچه تلگرام با ذکر انواع داده ها نسخه دریافت می کند که شامل عکس ها، خروجی پیام ها با اموجی های محدود در قالب HTML ، فایل ها(MP3 و JPG)، عکس ها در پوشه photos، استیکرها در قالب tgs و tgs_thumb در پوشه stickers، صوت ها در قالب ogg و در پوشه voice_messages، ویدیوها و تصویر شروع ویدیو در قالب MP4 و JPG همگی توسط این خدمت قابل بازیابی هستند. **ولی پیام های پاک شده چه برای خود شخص و چه برای بقیه افراد را ذخیره نمی کند.**

انواع داده ها: در تلگرام، قابلیت مبادله داده های متنی، داده های قابل تبدیل به متن(اموجی ها) و داده های کدگذاری شده (استیکرها)، داده های صوتی، گیف ها، عکس و ویدیو موجود می باشد. این داده ها هرکدام حجم مشخصی دارند و در سرور های تلگرام در امانت شخصی کاربر حفظ شده و در صورت نیاز فراخوانی می گردند. بنابراین هرکدام از این داده ها آدرس های مشخصی برای فراخوانی دارند. همچنین امکان بررسی داده ها در هر روز و دسترسی مستقیم به داده های هر تاریخ وجود دارد. تمامی داده ها در ساعت و دقیقه مشخصی ارسال شده اند که در پیام ها مشخص هستند.

- ✓ **چالش های داده ها:**
  - **(ویرایش و برنامه ریزی داده ها)** امکان ویرایش اطلاعات برای پیام های متنی وجود دارد. البته در صورت انجام ویرایش، کلمه "Edited"ذکر می گردد. همچنین، امکان برنامه ریزی (Schedule) برای فرستادن اطلاعات وجود دارد که طی آن در زمان مشخصی ارسال آن ها انجام می گیرد. این امکان برای همه انواع داده ها می باشد. این دو دسته از اطلاعات، در صورتی که جهت ثبت و ارسال اطلاعات استفاده شوند، شامل هر محتویاتی که باشند، **قابل استفاده و ارجاع برای استنادپذیری نمی باشند.**
  - **(حذف داده ها)** اطلاعات ارسال شده قابلیت حذف شدن از سمت ادمین کانال برای کانال ها، از سمت فرستنده برای تمامی کاربران در گروه ها و سوپرگروه ها، توسط ادمین گروه ها و سوپرگروه ها، توسط هردوی فرستنده و گیرنده در صفحه شخصی دارند. همچنین امکان حذف پیام برای خود کاربر حذف کننده و در عین حال برای تمامی کاربران وجود دارد که بنابر اجازه اشخاص مورد استفاده قرار می گیرد. **در این صورت نیاز است تا این سامانه با کاربری مناسب و در زمانی سریع فراخوانی گردد تا پیش از حذف احتمالی توسط کاربر دیگر، مورد استفاده قرار گیرد.**
  - **(نوع داده ها)** خروجی این داده ها بنا به استفاده و محل ذخیره تغییر می یلبد. در حللت کلی، خروجی های مدنظر PDF و JSON می باشد. پس از ثبت داده ها، و بررسی خروجی های مدنظر، میزان حجم و نوع داده ها مشخص می گردد.

- (**پیام های دوباره ارسال شده یا Forward**) این پیام ها در هر قالبی که ارسال شوند، با ذکر منبع می باشند و قابلیت بازیابی را مهیا می کنند که از چه شخص/کانالی ارسال شده است.

۲. واتس‌اپ

اپلیکیشن واتس‌اپ، پیام‌رسانی ساده و قابل اطمینان است که از طریق **گفتگوهای گروهی**، می‌توان پیام‌ها، عکس‌ها و ویدیوها را **با حداکثر ۵۱۲ نفر** در آن واحد به اشتراک گذاشت. همچنین می‌توان برای گروه نام تعیین کرد، آن را بی‌صدا نمود یا اعلان‌ها را تنظیم نمود. همچنین با تماس‌های صوتی و تماس‌های ویدئویی رایگان، می‌توان به صورت رو در رو صحبت کرد. می توان پی دی اف‌ها، اسناد، برگه‌ها و اسلایدها با حجم حداکثر ۱۰۰ مگابایت ارسال نمود.

وقتی شخصی با استفاده از پیام‌رسان واتس‌اپ به شخصی پیام می‌دهد، **رمزگذاری سرتاسری** واتس‌اپ مورد استفاده قرار می‌گیرد. رمزگذاری سرتاسری تضمین می‌کند که فقط شما و مخاطبی که با او در حال ارتباط هستید، می‌توانید آنچه را که فرستاده شده بخوانید و نه هیچ کس دیگر در این میان، حتی واتس‌اپ. دلیل آن این است که با رمزگذاری سرتاسری، پیام‌های شما با قفلی محافظت می‌شود که تنها گیرنده و شما کلید لازم برای باز کردن و خواندن آن را دارید. همه اینها به طور خودکار اتفاق می‌افتد: نیازی به فعال‌سازی تنظیمات یا راه اندازی گفتگوهای محرمانه خاصی برای محافظت از پیام‌های خود ندارید.

موجودیت ها: این اپلیکیشن سه نسخه اپ موبایل، نسخه واتس‌اپ بیزینس و نسخه وب/دسکتاپ دارند. هرکدام از موجودیت هایی که قابلیت ثبت اطلاعات دارند، به تفکیک به همراه چالش های هرکدام ذکر می گردند:

- ✓ **صفحه خانه اپلیکیشن:** این صفحه شامل تمامی چت های شخصی و گروه ها، می باشد.
- ✓ **صفحه وضعیت:** این صفحه شامل پروفایل اشخاص و وضعین های آن ها در قالب های مختلف به اشتراک گذاشته شده است.
- ✓ **گروه ها** : یک گروه معمولی تلگرام می‌تواند نهایتا ۵۱۲ عضو را داشته باشد. در گروه معمولی هر یک از اعضا قادر به تغییر نام گروه، تغییر عکس گروه و همچنین اضافه کردن اعضای جدید به آن خواهند بود. اما سوپر گروه تلگرام قادر است تا ۵۰۰۰ عضو را در خود جای دهد. همچنین سوپر گروه تلگرام از تاریخچه یکپارچه (Unified History) بهره می‌برد، بنابراین پیام‌هایی که از گروه حذف شوند در تلگرام تمام کاربران گروه حذف خواهند شد. قابلیت پین یا سنجاق کردن پیام‌های مهم به بخش فوقانی صفحه هم از دیگر ویژگی‌های منحصر به فرد یک سوپر گروه تلگرام است.
- ✓ **صفحه شخصی:** این ویژگی، حالت خاص "گروه ها" محسوب می شود که طی آن افراد با یکدیگر مبادله داده انجام می دهند. تمامی اطلاعات و دسترسی ها مانند گروه های ساده می باشند.
- ✓ **چت های آرشیو شده:** این چت ها در صفحه خانه اپلیکیشن قابل مشاهده هستند و به منظور عدم اطلاع رسانی در هنگام دریافت پیام در اختیار کاربر قرار گرفته اند.
- ✓ **واتس آپ بیزنس (حساب تجاری رسمی):** یکی از نسخه های فرعی واتس‌اپ اصلی می باشد که همانند واتس‌اپ معمولی برای ارسال پیام، ارسال محتوا، ایجاد تماس صوتی و تصویری، معرفی کسب و کار، ساخت کاتالوگ محصولات، ارتباط موثر با مشتری و... مورد استفاده قرار می گیرد. قابلیت های آن عبارتند از:
  - امکان درج مشخصات کسب و کار مثل آدرس، موقعیت روی نقشه، ساعات کاری و...

- امکان ساخت کاتالوگ برای معرفی محصولات و خدمات
- امکان ارسال پیغام های خودکار
- پیام های خوشامدگویی خودکار به مخاطبین جدید
- امکان آماده سازی متن های از پیش تعریف شده برای پاسخ به سوالات پرتکرار
- امکان ساخت برچسب برای مخاطبین ویژه (مثل برچسب تخفیف، برچسب مخاطب وفادار و...)
- ارسال پیام خودکار در واتس اپ بیزینس
- **(ارسال پیام خودکار در واتس اپ بیزینس)** قابلیتی تحت عنوان Auto respond ارائه شده که به واسطه آن امکان ارسال پیام خودکار در واتس اپ بیزینس فراهم شده است. زمانی که با سوالات پرتکرار مواجه می شویم و می خواهیم جواب آماده ای تنظیم و به کاربران خود ارسال کنیم، قابلیت Quick Replays کاربردی خواهد بود. بدین ترتیب می توانیم به وسیله امکان quick replays برنامه واتس‌اپ بیزنس به کاربران جواب های از پیش تعیین شده ارائه دهید.
- **(لینک پروفایل در واتس‌اپ)** می توانیم لینک کوتاهی از پروفایل خود ایجاد نموده و آن را در اختیار عموم قرار دهیم. قابلیت لینک سازی اکانت واتس‌اپ بسیار جذاب است و می توان برای جذب مخاطب از آن بهره جست. این امکان که Short links نام دارد، برای زمانی که تصمیم داریم پروفایل خود را با کسی به اشتراک بگذاریم مناسب است. بدین ترتیب برای معرفی خود به اشخاص، لینکی کوتاه شده ارائه می کنیم.
- **(آمارگیری در واتسپ)** در هر حساب اینترنتی بررسی میزان تعاملات اکانت با مخاطبین بسیار ارزشمند است و به واسطه آن می توان آمار دقیقی بدست آورد و میزان بازدهی و عملکرد کسب و کار را بهبود بخشید. این مورد در اینستاگرام تحت عنوان اینگیجمنت ارائه شده که در مقاله آموزشی روش های بالا بردن بازدهی پیج اینستاگرام به شرح مفصل آن پرداختیم. جالب است بدانید قابلیت مشابهی نیز در واتس‌اپ بیزینس ارائه شده که به واسطه آن قادر به آمارگیری در واتس‌اپ خواهید بود. به واسطه قابلیت statistics یا آمار می توانید آمار کلی تعاملاتی که با پیج شما صورت گرفته را مشاهده کنید. در این قسمت آمار مربوط به موارد زیر ارائه شده است:
  - تعداد پیام های ارسال شده
  - پیام های تحویل داده شده
  - پیام های خوانده شده
  - پیام های دریافت شده توسط مخاطب

✓ **واتس‌اپ وب:** واتس‌اپ وب، واتس‌اپ مجزا نیست و نمی‌توان با ورود به وبسایت واتس‌اپ، به یک صفحه ثبت نام (sign up)، صفحه لاگین یا ورود (login) دسترسی داشته باشید یا اصلاً نمی‌توان یک نسخه رسمی از نرم افزار دستکتاپ واتس‌اپ را روی رایانه نصب کرد و یک اکانت مجزا ساخت. واتس‌اپ وب بستری است که رایانه و تلفن همراه را اصطلاحاً سینک (sync) یا همگام می‌کند.

- **(اتصال اینترنت)** برای اتصال واتسپ وب اینترنت موبایل را نباید خاموش نمود. تا زمانی می‌توان از واتس‌اپ وب استفاده کرد که تلفن همراه هم به اینترنت متصل باشد. به محض خاموش کردن اینترنت در

تلفن، ارتباط با واتسپ وب نیز قطع خواهد شد! باید توجه داشت که در هنگام اتصال، می‌توان از طریق دو آی اس پی مختلف (ISP) (شرکت خدمات ارائه دهنده اینترنتی)، به اینترنت متصل بود اما همچنان دسترسی داشته داشت.

- **(محدودیت ها)** واتس‌اپ وب دسترسی ما را به برخی از بخش‌ها محدود و عملاً اجازه چنین کاری را از ما سلب کرده است. با وجود چنین تمهیداتی، ما کماکان قادر به ایجاد گروه، مشاهده وضعیت مخاطبین خود و یا تغییرات پروفایل هستیم؛ اما به طور کلی امکان تغییر در تنظیمات حساب (Account) وجود ندارد.
- **(مرورگرها)** کلیه مرورگرها به غیر از اینترنت اکسپلورر (internet explorer) از این قابلیت پشتیبانی می‌کنند. پس حالا با خیال راحت اتصال خود را ایجاد کنید.
- **(حالت روح در واتس‌اپ وب)** با استفاده از این حالت، ما پیام فرستاده شده از سمت مخاطب خود را دریافت و آن را می‌خوانیم اما تنها دو تیک خاکستری برای فرد مقابل نمایان می‌شود و دو تیک آبی که نشان می‌دهد ما پیام را خوانده‌ایم برای او به نمایش در نمی‌آید، به این ترتیب ما به یک روح مبدل خواهیم شد. اگر هنوز سردرگم هستید به نوشتار "چگونه بفهمیم در واتس‌اپ بلاک شدیم" مراجعه کنید و انواع وضعیت‌های پیام‌های ارسالی و دریافتی در واتس‌اپ را مطالعه نمایید.

✓ **چالش های موجودیت های واتس‌اپ:**

- **(ابزارهای کنترلی اولیه)** برای کمک به ایمن ماندن، آن‌ها را متناسب با شرایط تنظیم می کنیم که از تنظیمات حریم خصوصی می‌توان با گزینه‌های زیر آخرین بازدید، تصویر نمایه، درباره یا وضعیت خود را تنظیم نمود:
  - همه: آخرین بازدید، تصویر نمایه، درباره یا وضعیت شما در دسترس همه کاربران واتس‌اپ خواهد بود.
  - مخاطبان من: آخرین بازدید، تصویر نمایه، درباره یا وضعیت شما فقط در دسترس مخاطبان دفترچه تلفنتان شما خواهد بود.
  - مخاطبان من به استثناء...: آخرین بازدید، تصویر نمایه، درباره یا وضعیت شما در دسترس مخاطبان دفترچه تلفنتان خواهد بود، به‌جز آن‌هایی که مستثنی می‌کنید.
  - هیچ‌کس: هیچ‌کس به آخرین بازدید، تصویر نمایه، درباره یا وضعیت شما دسترسی نخواهد داشت.
  - می‌توانید رسید خواندن را نیز غیرفعال کنید. اگر رسید خواندن را غیرفعال کنید، خود شما هم دیگر رسید خواندن ارسال یا دریافت نمی‌کنید.
- **(چالش های واتس‌اپ بیزینس)** قابلیتی تحت عنوان Auto respond ارائه شده که به واسطه آن امکان ارسال پیام خودکار در واتس اپ بیزینس فراهم شده است. زمانی که با سوالات پرتکرار مواجه می شویم و می خواهیم جواب آماده ای تنظیم و به کاربران خود ارسال کنیم، قابلیت Quick Replays کاربردی خواهد بود. بدین ترتیب می توانیم به وسیله امکان quick replays برنامه واتس‌اپ بیزنس به کاربران جواب های از پیش تعیین شده ارائه دهید.

- **(پاک شدن خودکار پیام ها)** تمامی پیام ها در چت های شخصی و گروه ها قابلیت پاک شدن به شکل خودکار در بازه های زمانی ۲۴ ساعته، ۷ روزه، و ۹۰ روزه دارند که باید حتما در زمان بررسی، مورد توجه قرار گیرند.
- **(صفحات اطلاعات گروه)** در این صفحات، اطلاعات گروه شامل نام و عکس گروه، توانایی جستجو و تماس در گروه ، بیوی گروه ، دسترسی به داده های صوت و تصویر، شخصی سازی اطلاع رسانی وقایع گروه برای هر کاربر، امکان خروج از گروه و همچنین تعداد و پروفایل کاربران وجود دارد.
- **(ادمین گروه)** هر گروهی به محض تاسیس، خالق خود را به عنوان ادمین می شناسد که توانایی اضافه کردن دیگر افراد یا حذف آن ها را دارد. همچنین دسترسی به اضافه کردن دیگر ادمین ها و یا دعوت با استفاده از لینک دعوت دارد.
- **(امکان خروجی گرفتن از تاریخچه واتسپ)** این امکان تنها در واتس‌اپ موبایل وجود دارد و با امکان Export chat می توان تمام داده های آن گروه(چت) را شامل و یا بدون عکس و ویدئو خروجی گرفت. این امکان در صورت نیاز می تواند به کمک سامانه مستندساز ادله الکترونیک بیاید. **ولی پیام های پاک شده چه برای خود شخص و چه برای بقیه افراد را ذخیره نمی کند.**

انواع داده ها: در واتسپ، قابلیت مبادله داده های متنی، داده های صوتی، داده های قابل تبدیل به متن(اموجی ها) و داده های کدگذاری شده (استیکرها)، گیف ها، عکس و ویدیو موجود می باشد. این داده ها هرکدام حجم مشخصی دارند و روی دستگاه خودمان ذخیره می‌شوند. همچنین امکان بررسی داده ها در هر روز و دسترسی مستقیم به داده های هر تاریخ وجود دارد. تمامی داده ها در ساعت و دقیقه مشخصی ارسال شده اند که در پیام ها مشخص هستند.

✓ **چالش های داده ها:**

- **(رمزگذاری)** همه پیام‌های واتس‌اپ با همان پروتکل رمزگذاری Signal محافظت می‌شوند که پیام‌ها را قبل از ترک دستگاه محافظت می‌کند.
- **(حساب تجاری واتسپ)** وقتی به حساب تجاری واتس‌اپ پیام می‌دهید، پیام شما ایمن به مقصد منتخب آن کسب‌وکار تحویل داده می‌شود. واتس‌اپ فرض می‌کند گفتگو با کسب‌وکارهایی که از برنامه واتس‌اپ تجاری استفاده می‌کنند و پیام‌های مشتریان را خود مدیریت کرده و ذخیره می‌کنند، رمزگذاری سرتاسری شده است. وقتی پیامی دریافت شد، مشمول شیوه‌های حریم خصوصی آن کسب‌وکار می‌شود. صاحب کسب‌وکار ممکن است تعدادی از کارمندان یا حتی سایر فروشندگان را برای پردازش و پاسخ به پیام، انتخاب کند.
- **(دسترسی با پیامک)** هرگز نباید کد تایید حساب واتس‌اپ خود را با دیگران به اشتراک گذاشت. اگر کسی در تلاش است تا اختیار حساب را در دست بگیرد، به کد تایید پیامکی که به شماره تلفن کاربر فرستاده شده است، نیاز دارد. بدون این کد هر کاربری که بخواهد شماره را تایید کند، نمی‌تواند مرحله تایید حساب را انجام دهد و از شماره تلفن شخص در واتس‌اپ استفاده کند. این یعنی کنترل حساب واتس‌اپ شخص در دست او باقی می‌ماند.

- **(ذخیره داده بر روی دستگاه)** واتس‌اپ اطلاعات کافی را برای شناسایی شخصی که در تلاش برای تایید حساب واتس‌اپ ماست، ندارد. واتس‌اپ سرتاسر رمزگذاری شده است و پیام‌ها روی دستگاه خودمان ذخیره می‌شوند، بنابراین شخصی که از دستگاه دیگری به حسابتان دسترسی پیدا کند، نمی‌تواند مکالمات قبلی ما را بخواند.
- **(پرداخت ها)** پرداخت‌ها در واتس‌اپ که در بعضی از کشورها در دسترس است، انتقال بین حساب‌ها در موسسات مالی را ممکن می‌کند. شماره کارت‌ها و حساب‌های بانکی بصورت رمزگذاری شده و در شبکه‌ای با امنیت بالا ذخیره می‌شوند. اما چون موسسات مالی نمی‌توانند بدون دریافت این اطلاعات مربوط به این پرداخت‌ها، تراکنش انجام دهند، این پرداخت‌ها رمزگذاری سرتاسری نشده‌اند.
- **(پشتیبان گیری)** گفتگوهای ما در واتس‌اپ به طور خودکار هر روز در حافظه گوشی شما پشتیبان‌گیری و ذخیره می‌شوند. همچنین بسته به تنظیمات، می‌توانیم بطور دوره‌ای از گفتگوهایمان در واتس‌اپ روی گوگل درایو پشتیبان‌گیری کنیم. اگر میخواهیم واتس‌اپ را از گوشی خود پاک کنیم اما نمی‌خواهیم هیچ‌کدام از پیام‌ها را از دست بدهید، اطمینان حاصل شود که پیش از حذف واتس‌اپ به طور دستی از گفتگوها پشتیبان‌گیری کرده باشیم. هنگام صدور با پیوست رسانه‌ها، می‌توانید حداکثر تا ۱۰،۰۰۰ پیام اخیر را بفرستیم. بدون رسانه‌ها، می‌توانیم تا ۴۰،۰۰۰ پیام بفرستیم. این محدودیت به خاطر حداکثر اندازه ایمیل است.

۳. اینستاگرام

اینستاگرام یک شبکه اجتماعی با تمرکز فراوان بر المان‌های بصری است. هر بار که اپلیکیشن باز می شود، یک فید اصلی به نمایش درمی‌آید که شامل آخرین پست‌های افرادی است که آن‌ها را فالو کرده‌ایم. اینستاگرام به صورت رایگان روی موبایل‌های هوشمند مبتنی بر دو سیستم عامل iOS و اندروید در دسترس قرار گرفته است. از سوی دیگر، با مراجعه به وب‌سایت رسمی اینستاگرام، نسخه تحت وب هم در دسترس است، ولی آپلود تصویر و ویدیو و اشتراک‌گذاری محتوا با دیگر کاربران ایستاگرام تنها روی اپلیکیشن موبایل اینستاگرام امکان‌پذیر است.

موجودیت ها: این اپلیکیشن سه نسخه اپ موبایل، نسخه واتس‌اپ بیزینس و نسخه وب/دسکتاپ دارند. هرکدام از موجودیت هایی که قابلیت ثبت اطلاعات دارند، به تفکیک به همراه چالش های هرکدام ذکر می گردند:

- ✓ **صفحه خانه اپلیکیشن:** در اینجا می‌توانیم میان پست افراد و اکانت‌هایی که دنبال کرده‌اید اسکرول کنیم.
- ✓ **اکسپلور:** ما را به صفحه‌ای با همین نام برده و پست‌های متعلق به اکانت‌هایی که شاید به آن‌ها علاقه‌مند باشیم را نمایش می‌دهد.
- ✓ **اتاق‌های لایو (Live Rooms) :** محلی برای آنلاین استریمینگ افراد با فالوورهایشان می باشد.
- ✓ **ریلز :** در قسمت Reels ویدیوهای کوتاه، سرگرم‌کننده و ترندی را مشاهده می کنیم. اساساً، Reels پست‌های عمودی تمام صفحه هستند که می‌توانند از ۱۵ ثانیه تا ۱ دقیقه طول بکشند. این عملکرد همچنین به شما امکان می‌دهد چندین فیلم کوتاه را در یک فیلم ترکیب کنید. علاوه بر این، Reels را می‌توان به انواع مختلفی از امکانات اضافی مجهز کرد تا محتوا را جذاب‌تر کند:

- قابلیت Voiceover: در جدیدترین تغییرات اینستاگرام، شما می‌توانید صدای خود را روی ویدیو ضبط کنید.
- قابلیت Doodles: در جدیدترین تغییرات اینستاگرام، می‌توانید روی ویدیوی خود نقاشی بکشید.
- استیکرها: یکی ازویژگی و قابلیت های جدید اینستاگرام ۲۰۲۲ (۱۴۰۱) این است که بعد از اینکه ویدیوی خود را اپلود کردید، می‌توانید یک استیکر به آن اضافه کنید.
- تایمر: در جدیدترین تغییرات اینستاگرام، با وجود تایمر نیازی به نگه داشتن گوشی در حین ضبط ویدیو ندارید.

✓ داستان ها: بااستفاده از «داستان‌ها»، می‌توانیم عکس‌ها و ویدیوهایی را به اشتراک بگذاریم که از نمایه، «فید» و پیام‌ها پس از ۲۴ ساعت حذف خواهند شد، مگراینکه آن‌ها را به‌عنوان داستان‌های برگزیده به نمایه‌تان اضافه کنیم.

✓ **پیام ها:** در بخش Direct Message می‌توان تاریخچه فعالیت‌ها را در میان پیام‌های خصوصی را مشاهده کرد.

✓ **ایجاد پست:** در بخش Compose هم می‌توانید پیامی تازه ایجاد کرده و پس از انتخاب گیرنده، آن را ارسال کرد.

✓ **صفحه شخصی:** این ویژگی، حالت خاص "گروه ها" محسوب می شود که طی آن افراد با یکدیگر مبادله داده انجام می دهند. تمامی اطلاعات و دسترسی ها مانند گروه های ساده می باشند.

✓ **چت های آرشیو شده:** این چت ها در صفحه خانه اپلیکیشن قابل مشاهده هستند و به منظور عدم اطلاع رسانی در هنگام دریافت پیام در اختیار کاربر قرار گرفته اند.

✓ **چالش های موجودیت های اینستاگرام:**

- در صفحه پست ها، ایدی صفحه، یکتا می باشد و پروفایل و ساختار صفحه مورد توجه می باشد. در حالی که عکس پروفایل، بیوی صفحه و وضعیت استوری ها(هایلایت) می تواند مشابه دیگر صفحات باشد.
- خوشبختانه، به دلیل ماهیت سرور محور بودن این اپلیکیشن، امکان ثبت نام و اطلاعات از سمت کاربر وجود ندارد و به اطلاعات موجود در آن می شود اعتماد کرد.
- **(عکس یا ویدیوی ناپدید شونده)** به عنوان یک پیام گروهی یا تکی، پس از اینکه شخصی یک عکس یا ویدیویی ناپدید شونده‌ای را باز کرد که برای او ارسال کرده‌ایم، پیام دیگر در صندوق دریافتش قابل مشاهده ،نخواهد بود، مگر اینکه بازپخش پیامتان را مجاز کرده باشیم. توجه داشته باشیم زمانی که یک پیام گروهی ارسال می‌کنیم، یک Thread گروه را شروع می‌کند که هر شخصی در گروه می‌تواند مشاهده کند و به آن پاسخ دهد. می‌توانیم یک بازدید را انتخاب کنید تا به شخص یا گروهی که عکس یا ویدیو را دریافت می‌کند، فقط یک بار اجازه مشاهده آن را بدهیم. همچنین می‌توانیم عکس‌ها یا ویدیوهای ناپدید شونده را فقط برای افرادی ارسال کنیم که ما را دنبال می‌کنند یا قبلاً پیام‌های تأیید شده را از ما تأیید کرده‌انم. توجه: زمانی که موارد دیگری را با استفاده از Instagram Direct (مانند: پست‌ها از فید، متن، هشتگ‌ها) ارسال می‌کنیم، آن پیام‌ها ناپدید نخواهند شد و در گفتگو قابل مشاهده خواهند ماند.
- حتما زمانی که داستان یک شخص را مشاهده می‌کنیم، او می‌تواند مشاهده کند که ما آن را دیده‌ایم. فقط ما می‌توانیم ببینیم که چه کسانی داستانمان را دیده‌اند. می‌توانیم تا ۴۸ ساعت پس از پست کردن داستان، ببینید که چه کسانی آن را مشاهده کرده‌انم.

انواع داده ها: در اینستاگرام، قابلیت مبادله داده های متنی، داده های صوتی، داده های کدگذاری شده (استیکرها)، عکس و ویدیو موجود می باشد. این داده ها هرکدام حجم مشخصی دارند و سمت سرور ذخیره می‌شوند. همچنین امکان بررسی داده ها در هر روز و دسترسی مستقیم به داده های هر تاریخ وجود دارد. تمامی داده ها در ساعت و دقیقه مشخصی ارسال شده اند که در پیام ها مشخص هستند.

✓ **چالش های داده ها:**

- **(ذخیره داده ها توسط اینستاگرام)** آنتیگون دیویس، مدیر امنیت جهانی متا، گفته است که چت‌ها در اینستاگرام تا سال ۲۰۲۳ به طور کامل رمزگذاری نخواهند شد. دیویس قبلاً قول داده بود که چت‌ها را در هر دو پلتفرم به صورت پیش‌فرض رمزگذاری شده انجام دهد. آخرین گزارش نشان می دهد که ممکن است به این زودی اتفاق نیفتد. این نشان می‌دهد که تا زمانی که چت‌ها در این پلتفرم رمزگذاری نشوند، احتمال لو رفتن آنها بیشتر است.
  - اینستاگرام در مرورگر و تاریخچه جستجو، موقعیت مکانی، داده‌های استفاده، شناسه‌ها و آشکارا محتوای ارسال شده به پلتفرم شما را ردیابی می‌کند و می‌فروشد.
  - یک لایه پنهان از داده‌ها در همه چیز، از جمله عکس‌هایی که آپلود می‌کنید، وجود دارد. این‌ها حاوی داده‌های EXIF data (Exchangeable Image File Format) هستند، شامل تاریخ و ساعت عکس‌برداری و دستگاه مورداستفاده. همچنین می‌تواند افرادی را که می‌شناسید ردیابی کند و به فهرست مخاطبین شما دسترسی پیدا کند تا شما را با دوستان خود به طور مشابه با استفاده از اینستاگرام پیوند دهد.
  - دسترسی به متون و خواندن آنها دو چیز متفاوت هستند. اینستاگرام متن های ما را نمی خواند. همانطور که گفته شد، iMessages به هر حال رمزگذاری شده است و فراتر از آن، متا به کاربران اطمینان می دهد که "این ویژگی محتوای تماس ها یا پیام های متنی شما را جمع آوری نمی کند." آنچه می تواند جمع آوری شود فقط ابرداده (متادیتا) است، نه آنچه ما در واقع می نویسیم یا درباره آن صحبت می کنیم. متا معتقد است که این یک سرویس انتخابی است، هر گونه داده ایمن است و به اشخاص ثالث فروخته نمی شود.
- **(رمزگذاری سرتاسری)** درحالت عادی، پیام ها رمزگذاری نشده اند. گپ رمزگذاری سرتاسری‌شده در Instagram، صرفاً برای ما و فردی که با او صحبت می‌کنیم طراحی شده است. توجه داشته باشید که این امر فقط در گپ با یک حساب دیگر قابل دسترسی است. ویژگی encrypted را روی گپ‌هایی که رمزگذاری سرتاسری شده هستند میبینیم. هر گفتگوی دیگری که با آن حساب داشته باشید، به‌صورت یک گپ مجزا در فهرست «گپ‌های» شما نشان داده می‌شود.
- **(پاک شدن پیام ها)** اینستاگرام قابلیتی مانند واتس اپ دارد که به کاربران اجازه می دهد پیام هایی را که ارسال کرده اند حذف کنند. در حالی که واتس‌اپ ادعا می‌کند پیام‌ها را برای «همه» حذف می‌کند، اینستاگرام واقعاً پیام‌هایی را که «ارسال نمی‌کنید» را از پایگاه داده خود حذف نمی‌کند.
- **(دخالت در ترافیک)** برنامه‌های فیس‌بوک و اینستاگرام هنگامی که وسایل SG/ASG Proxy ترافیک را قطع می‌کنند کار نمی‌کنند. کاربران نمی توانند در این شرایط به این برنامه ها دسترسی داشته باشند زیرا

رمزهای پروکسی SSL با لیست رمزهای مشتری ورودی همپوشانی ندارند. برنامه‌های تلفن همراه فیس‌بوک/اینستاگرام فقط از TLS 1.3 استفاده می‌کنند که تنها دارای سه مجموعه رمزگذاری است. در حال حاضر، دستگاه‌های ProxySG/ASG تنها در صورتی از TLS 1.3 پشتیبانی می‌کنند که اتصال و پردازش را به عنوان TLS 1.2 کاهش دهند. برنامه فقط سه رمز ارسال می کند که به پروکسی اجازه نمی دهد از TLS 1.3 به TLS 1.2 تنزل دهد.

- **(تلاش غیرعادی برای ورود به سیستم)** تقریباً همیشه، هنگامی که از طریق موبایل های مختلف به اکانت اینستاگرام دسترسی پیدا می کنی!، یک پیام هشدار برای ما ارسال می کند که می گوید تلاشی برای ورود انجام شده است، این اتفاق می افتد، زیرا اینستاگرام آدرس IP را که به طور مرتب از اینستاگرام استفاده می کنید، ردیابی می کند. . هنگامی که به وای فای ناشناس متصل می شویم، در آن زمان سیستم امنیتی اینستاگرام نیز فعال می شود و احتمالاً همان پیام هشدار را برای ما ارسال می کند. پس باید سعی کنیم از اینستاگرام روی داده موبایل یا بالعکس استفاده کنیم.
- **(حفظ داده ها نزد اینستاگرام)** هر زمان که داده‌ها را از سرویس‌های آنلاین حذف می‌کنیم، معمولاً یک تاخیر زمانی نامشخص قبل از حذف کامل داده‌ها از سرورهای سایت وجود دارد. برای اینستاگرام، این شرکت می‌گوید معمولاً حدود ۹۰ روز طول می‌کشد تا اطلاعات به طور کامل حذف شوند. اما محققان امنیتی مشکلات مشابهی را با سایر سرویس‌ها در گذشته پیدا کرده‌اند، از جمله توییتر، که پیام‌های مستقیم بین کاربران را تا سال‌ها پس از ظاهراً حذف آن‌ها حفظ می‌کرد.

۴. بله

این اپلیکیشن، پیام‌رسان رسمی بانک ملی ایران است که امکان خرید، پرداخت و ارسال رسید در بستر گفتگو(چت) را مهیا می کند. راهی برای پرداخت وجوه خرد و کلان برای انواع خدمات و محصولات در گروه‌ها و کانال‌های فروشگاهی و امکان به اشتراک گذاری فاکتورهای پرداخت با امکان پرداخت سریع و راحت در این بستر وجود دارد. اهدا به کانال‌های خیریه معتبر، جذب سرمایه جمعی (جمع‌سپاری تأمین مالی)، اتصال به انواع بسترهای خدمات اداری ـ سازمانی. مدیریت آسان و دقیق پرداخت‌ها (گزارش‌دهی، امکان ارسال رسیدها به دیگران و...) از دیگر خدمات این پیام رسان می باشد. خدمات پایه کاربری دیگری شامل خرید سریع شارژ و پرداخت راحت قبض، پرداخت بسیار سریع و آسان همه قبوض، دریافت ساده شارژ برای خود، خانواده و دوستان، و پرداخت وجه سرویس‌های آنلاین در این اپلیکیشن وجود دارد.

بله یک شبکه اجتماعی پیام‌رسان با قابلیت دسترسی از طریق دستگاه های مختلف(مولتی پلتفرم) است. نسخه اندروید و iOS بله از طریق فروشگاه های مختلف اپلیکیشن قابل دانلود است. نسخه وب بله بصورتی ریسپانسیو قابل دسترسی از طریق مرورگرهای مختلف بر روی دستگاه های مختلف است.

موجودیت ها: این اپلیکیشن دو نسخه اپ موبایل و نسخه دسکتاپ اپ دارد که هردو عملکرد مشابهی دارند. هرکدام از موجودیت هایی که قابلیت ثبت اطلاعات دارند، به تفکیک به همراه چالش های هرکدام ذکر می گردند:

- ✓ **منوی اپلیکیشن:** منوی اپلیکیشن پیام‌رسان بله شامل دو بخش «پیام‌رسان» و «خدمات مالی و اجتماعی» است.
  - **پیام‌رسان**

- **گفتگوی فردی و گروهی:** از طریق قسمت پیام‌رسانی اپلیکیشن بله می‌توانیم با دوستانمان گفتگو کنیم. گروه و یا کانال ایجاد کنیم.
- **ارسال و دریافت عکس، فیلم و فایل:** با استفاده از پیام‌رسان بله می‌توانیم برای دوستانمان عکس، فیلم و فایل با کیفیت بالا بفرستیم.

- **خدمات مالی و اجتماعی**

- **کارت‌به کارت (انتقال پول):** امکان کارت به کارت از مبدأ بانک‌های ملی ایران، کشاورزی، پست بانک، آینده، شهر و انصار به همه کارت‌های عضو شتاب در این اپلیکیشن وجود دارد.
- **پرداخت قبض:** با واردکردن «شناسه قبض» و «بارکد اسکنر» و اطلاعات رمز دوم کارت، می‌توانیم قبضمان را پرداخت کنیم.
- **خرید شارژ:** برای ما یک رسید تراکنش که در آن «مبلغ»، «شماره موبایل»، «کد شارژ»، «سریال»، «شماره پیگیری» و «تاریخ خرید» تراکنش انجام شده است ارسال می‌شود.
- **درخواست پول:** امکان «درخواست پول ثابت و یا متغیر»، بدین صورت که در گروه و یا در صفحه گفتگوی شخصی با فردی می‌توانیم با کلیک روی شکل گیره‌ای که در پایین صفحه قرار دارد و انتخاب گزینه «بانک» و کلیک روی گزینه «درخواست پول» و با وارد کردن مبلغ موردنظر، شماره کارت و توضیحی برای این درخواست، درخواست پول کنیم.

✓ **منوی کشویی:**

- **استیکرهای بله:** در این قسمت استیکرهای بله نشان داده می‌شود که با کلیک روی یک استیکر، می‌توانیم بسته آن استیکر را مشاهده کنیم و در صورت تمایل، با کلیک روی گزینه «افزودن بسته»، آن بسته را به مجموعه استیکرهای خود اضافه کنیم.
- **ایجاد گروه:** از طریق این قسمت می‌توانید گروه ایجاد کنیم. برای این کار باید نام و شناسه گروه را مشخص کنیم و همین‌طور می‌توانید یک عکس هم برای گروه انتخاب کنیم.
- **ایجاد کانال:** از طریق این قسمت نیز می‌توانید کانال ایجاد کنیم.
- **مخاطبین:** از طریق این قسمت می‌توانیم این اپلیکیشن را به دوستان خود معرفی کنیم که برای این کار کافی است روی گزینه «بله را به دوستان خود معرفی کنید» کلیک کنیم. همچنین می‌توانید دوستانمان را به این اپلیکیشن اضافه کنیم.
- **بانک من:** از طریق این قسمت می‌توانید کارت‌های بانکی خود را ذخیره کنیم.
- **دعوت‌نامه:** با استفاده از این بخش می‌توانید با ارسال «کد دعوت‌نامه» به دوستانتان و پس از نهایی شدن ثبت‌نام آن‌ها در «بله»، امتیاز بگیریم و شانس خود را برای برنده شدن جوایز افزایش دهیم.
- **تنظیمات:** در این قسمت می‌توانیم اطلاعات خود را وارد کنیم و پس‌زمینه گپ، زبان، اعلان‌ها، لیست مسدود شده‌ها و... را مشاهده و تنظیم کنیم.
- **گزارش و بازخورد:** در این بخش می‌توانیم بازخوردها و گزارش‌های خود از این اپلیکیشن را ارسال کنیم.

✓ **جایگاه تبلیغاتی در پیام‌رسان بانکی بله:**

- **تبلیغات تب گفتگو:** جایگاه تبلیغات تب گفتگو، به‌صورت پیام سنجاق‌شده، در اولین سطر در قسمت گفتگو قرار دارد. درصورتی‌که کاربران روی تبلیغ تب گفتگو کلیک کنند، به لینک این تبلیغ هدایت می‌شوند. این جایگاه از نظر میزان نمایش و بازدید بسیار ویژه است.
- **تبلیغات بنری ویترین:** کاربر در این بخش کاربردی می‌تولند کلنال‌های موجود در بله را با دسته‌بندی موضوعی مشاهده کند. به کمک دسته‌بندی‌های ویترین بله، کاربران می‌توانند به‌راحتی و بدون اتلاف وقت، موضوعات دلخواه خود را پیدا و دنبال کنند. روزانه میلیون‌ها کاربر، برای دیدن بهترین کلنال‌های بله، از ویترین بله دیدن می‌کنند؛ این حجم از بازدید، ویترین بله را به یکی از پربازدیدترین مکان‌ها در اپلیکیشن تبدیل کرده است.

✓ **چالش های موجودیت های بله:**

- **(عدم وجود ورود دو مرحله‌ای)** نبود این امکان در بله می‌تواند منجر به اتفاقات بد امنیتی شود که قطعا اعتماد کاربران را به این پیام رسان داخلی از بین می‌برد. در مواقعی که کاربران نتوانند امنیت اولیه خود را برای ورود به محیط کاربریشان در پیام رسان بله حفظ کنند، قطعا با نبود امکان ورود دو مرحله‌ای ضررهای فراوانی را تجربه خواهند کرد.
- **(عدم وجود چت ایمن)** این امکان امنیتی در بعضی از پیام رسان‌های داخلی نیز وجود دارد که از جمله آن می‌توان به آی‌گپ اشاره کرد که حتی برای شکستن رمزنگاری‌های گفتگوهایش جایزه یک میلیارد تومانی تعیین نموده که نشان از اطمینان بالای مدیران آن برای امنیت پیام رسانشان دارد ولی پیام رسانی مانند بله که مراودات مالی میلیاردی روزانه در آن جریان دارد، باید از الگوریتم‌های رمزنگاری پیشرفته برای کاربرانی که به دنبال امنیت بیشتر هستند، استفاده شود.

انواع داده ها: در اپلیکیشن بله، قابلیت مبادله داده های متنی، داده های قابل تبدیل به متن(اموجی ها) و استیکرها، داده های صوتی، ، عکس و ویدیو موجود می باشد. این داده ها هرکدام حجم مشخصی دارند و در سرور های بله حفظ شده و در صورت نیاز فراخوانی می گردند. بنابراین هرکدام از این داده ها آدرس های مشخصی برای فراخوانی دارند. همچنین امکان بررسی داده ها در هر روز و دسترسی مستقیم به داده های هر تاریخ وجود دارد. تمامی داده ها در ساعت و دقیقه مشخصی ارسال شده اند که در پیام ها مشخص هستند.

✓ **چالش های داده ها:**

- **(نسخه ویندوز ندارد)** نبود نسخه ویندوز که در پیام رسان‌های دیگر مانند: پیام رسان سروش، پیام رسان ایتا، آی‌گپ و... ضعف این اپلیکیشن است و طبق آمار درصد قابل توجهی از کاربران، برای ورود به محیط کاربری خود از نسخه ویندوز استفاده می‌کنند که نبود آن در پیام رسان بله یک اشکال بزرگ محسوب می‌شود و قطعا شانسش را برای جایگزین شدن با تلگرام کم می‌کند.

۵. ایتا

ایتا یک برنامه پیام‌رسان است که تمرکز خود را بر روی سرعت و امنیت گذاشته است. ما می‌توانید بطور همزمان بر روی تمامی دستگاه‌ها و وسایل خود از آن استفاده کنیم. پیام‌های ما در تلفن همراه، تبلت یا رایانه‌مان بصورت یکپارچه همگام‌سازی می‌گردند. می‌توانیم به مخاطبان خود پیام بفرستیم و با استفاده از نام کاربری افراد، آنها را بیابیم.

برخلاف واتس‌اپ، ایتا بر مبنای فضای ابری بنا نهاده شده و همگام‌سازی در آن یکپارچه است. یعنی ما می‌توانیم همزمان از دستگاه‌های متعدد مانند گوشی اندرویدی و وب سرویس به پیام‌های خود دسترسی داشته باشیم و می‌توانید تعداد زیادی عکس، فیلم و فایل (MP3، Doc، Zip و...) به اشتراک بگذاریم یا آنها را در فضای ابری ذخیره کنیم. پیام رسان ایتا از نظر ظاهری شبیه تلگرام است. زیرا رابط کاربری تلگرام توانسته است رضایت نسبی کاربران ایرانی را جلب کند و مخاطبان با ورود به ایتا با محیط غریبه‌ای مواجه نمی‌شوند. علاوه بر این‌ها خدماتی افزون بر تلگرام برای ایتا پیش‌بینی شده است که به تدریج و بصورت رایگان به کاربران عرضه خواهد شد.

موجودیت ها: این اپلیکیشن دو نسخه اپ موبایل و نسخه دسکتاپ اپ دارد که هردو عملکرد مشابهی دارند. هرکدام از موجودیت هایی که قابلیت ثبت اطلاعات دارند، به تفکیک به همراه چالش های هرکدام ذکر می گردند:

- ✓ **گروه‌ها:** در فاز نخست می‌توانند تا ۵۰۰ عضو داشته باشند. برخی ویژگی‌های گروه در ایتا:
  - تاریخچه یکپارچه: قابلیت ویرایش (و حذف) پیام‌ها پس از انتشار
  - دسترسی آنی به پیام‌های خود در هر زمان، از هر تعداد دستگاه موبایل اندروید و یا نسخه ویندوز
  - جستجو در پیام‌ها: امکان پاسخ به پیام دیگران و بکارگیری هشتگ
  - دنبال کردن آسان یک مکالمه بدون در نظر گرفتن اندازه گروه
  - قابلیت پین کردن یک پیام (فقط در ابرگروه ها)
  - ابزارهای مدیریتی: برای گروه مدیر انتخاب کنید تا پیام‌ها را به صورت جمعی پاک، عضویت را کنترل و پیام‌های مهم را سنجاق کند.
  - اشتراک فایل: هر نوع فایلی را، می توانیم ارسال یا دریافت کنیم و به صورت آنی در تمام دستگاه‌های خود دسترسی داشته باشیم.
- ✓ **چالش های موجودیت های بله:**
  - **(تفاوت میان گروه‌ها، ابرگروه‌ها و کانال‌ها)** گروه‌های ایتا برای اشتراک مطلب بین دوستان و خانواده یا همکاری بین تیم‌های کوچک ایده‌آل هستند. آن‌ها می‌توانند تا سقف ۵۰۰ عضو داشته باشند و به صورت پیش فرض هر کسی می‌تواند اعضای جدید را به گروه اضافه کند و نام و عکس گروه را تغییر دهد. با امکان ابرگروه(سوپر گروه) می‌توانیم گروه خود را به یک ابرگروه ارتقا دهیم. تعداد اعضا در ابرگروه ایتا نامحدود است. ابرگروه‌ها یک تاریخچه یکسان دارند، بنابراین پیام‌های حذف شده از دید همه اعضاء پنهان خواهند شد. همچنین ما می‌توانیم پیام‌های مهم را به بالای صفحه سنجاق کنیم تا تمام اعضا آن‌ها را ببینند، حتی اعضایی که به تازگی عضو شده‌اند. همچنین کانال‌ها ابزاری برای انتشار پیام‌های عمومی برای تعداد بالایی مخاطب هستند.
  - **(نام کاربری)** هیچ کدام از طرفین شماره تلفن دیگری را نخواهد دید. شبیه وقتی که شما به شخصی که در یک گروه ایتا می‌بینید، پیام می‌فرستید. یک استثنا برای این هست: مانند حالتی که در همه پیام‌های ایتا برقرار است. اگر ما شماره کسی را به عنوان یک مخاطب ذخیره کرده باشیم و به او پیامی بفرستیم، صرفنظر از این که چگونه چت با آن شخص را باز کرده باشید، شماره ما نیز برای او نمایان می‌گردد. درست مانند پیامک. چه از طریق منوی مخاطبان باشد، چه جستجوی سراسری با نام کاربری، چه پیوند eitaa.com و یا از صفحه‌ی اعضای گروه.

- **(کانال های تلگرامی)** تمام کانال‌های تلگرام که در سامانه صدور شناسه الکترونیکی محتوای دیجیتال (شامد) وزارت ارشاد ثبت شده‌اند پیش از این در ایتا رزرو شده و در اختیار سازندگان آن‌ها قرار می‌گیرند. شناسه سایر کانال‌های پرمخاطب تلگرام هم تا مدت زمان محدودی پس از عرضه ایتا، در صورت تقاضای سازنده (creator) در اختیار آن‌ها قرار خواهند گرفت.

انواع داده ها: با ایتا ما می‌توانیم انواع پیام، عکس، ویدیو، گیف، استیکر و هر نوع فایل (MP3، Doc، Zip و...) را بفرستیم.

✓ **چالش های داده ها:**

- **(عدم افشا اطلاعات)** هیچ شخص، گروه و جریانی نمی‌تواند ایتا را مجبور به حذف اطلاعات کاربران و فعالیت‌های آن‌ها در نرم افزار نماید. در عین حال ایتا تابع قوانین و مقررات رسمی جمهوری اسلامی ایران و احکام مراجع صالح قضایی است و نسبت به حذف ربات‌ها و کانال‌هایی که مطالب خشونت آفرین و تروریستی را نشر دهند یا حاوی مطالب مستهجن باشند اقدام خواهد کرد. تا به این روز به اندازه ۰ بایت دیتا در اختیار اشخاص ثالث از جمله دولت‌ها قرار داده اند.
- **(پروتکل امنیتی)** ایتا بر پروتکل Mtproto و از درگاه https بر روی الگوریتم‌های آزمایش شده در طول زمان برای سازگار کردن امنیت با ارسال سریع و حتی پشتیبانی اتصال‌های ضعیف پایه ریزی شده است. رمزنگاری امن را پشتیبانی می‌کند. رمزنگاری Client-Server در چت‌های روی ابر (چت‌های خصوصی و گروهی) همه داده‌ها، صرف‌نظر از نوع (نوشته، رسانه یا فایل‌ها)، به یک روش رمزنگاری می‌شوند.
- رمزنگاری‌ها بر روی رمزنگاری AES سیمتریک ۲۵۶ بیتی، رمزنگاری RSA ۲۰۴۸ می‌باشد
- **(انتقال داده‌ها و تبادل اطلاعات امن)** ایتا می‌تواند هنگام انتقال داده‌ها و تبادل اطلاعات امن، کمک کند. یعنی همه داده‌ها (شامل رسانه‌ها و فایل‌هایی) که ما از طریق ایتا می‌فرستیم یا دریافت می‌کنیم، برای ISP ما، مدیر شبکه یا دیگر اشخاص ثالث قابل دسترسی نیستند. ولی اگر شخصی به گوشی ما یا رایانه‌ای که به نسخه وب وصل می‌شوید دسترسی روت پیدا کند، نمی‌توانند ما را در برابر آنها محافظت کند.

راهکار حل مسئله

در این قسمت از پروپوزال، پس از تشریح نیازها و چالش های گفته شده، راهکارهای پیشنهادی خود را مطرح می کنیم. این راهکار ها با توجه و به کارگیری آخرین تکنولوژی های شبکه و امنیت و همچنین علم تنظیم گری و سیاستگذاری فناوری محور با اولویت دهی به حفظ حریم خصوصی می باشد. حسب بهینه بودن از نظر قابلیت استنادپذیری، حفظ حریم خصوصی و داده های هویتی افراد، و در نهایت استقبال کاربران بررسی و طرح شده است. امید است راهکارهای تشریح شده مورد توجه کارفرمای محترم قرار گیرد و در جهت حفظ منافع مردم کارساز باشد. سوالات مهم و تعیین کننده که راهکار موردنظر را تثبیت می کنند و باعث استنادپذیری راهکار مدنظر می گردند عبارتند از:

۱. چگونگی **جمع آوری اطلاعات (ادله الکترونیکی)** که ناظر به بعد فناوری می باشد.
۲. چگونگی **نگهداری و حفظ اطلاعات** که ناظر به بعد فناوری می باشد.
۳. مشخص شدن **سازمان/شرکت جمع آوری کننده اطلاعات** که ناظر به بعد سیاستگذاری می باشد.
۴. مشخص شدن **سازمان/شرکت نگهداری کننده اطلاعات** که ناظر به بعد سیاستگذاری می باشد.

(نحوه تعامل این سامانه با دادستانی کل کشور/ مرکز آمار وفناوری اطلاعات قوه قضائیه) متعاقبا نحوه تعامل سازمان های حاکمیتی با بسیاری از شرکت های خصوصی جهت ارائه خدمات الکترونیک از نوع "خرید خدمت/محصول" بوده است. در این حالت، این محصول یک خدمت داخلی دادستانی کل کشور به حساب می اید و مانند web archive تلقی می گردد. اما باید در نظر داشت که می توان با شیوه جدیدی از تعامل، محصولی را در خارج از دادستانی کل توسعه داد و خدمت به این سازمان و یا به پلیس فتا ارائه گردد. علت این امر چالش هایی است که در ادامه ذکر می گردد:

۱. نگهداری و پشتیبانی از این سرویس با توجه به نیاز بالا به اپراتور ها جهت CRM سامانه ، بررسی هویت و درخواست‌های کاربران
۲. هزینه راه‌اندازی سامانه و نگهداری سخت افزار و داده ها
۳. دشواری شخصی سازی محصول با توجه به ظهور ویژگی های جدید در پلتفرم ها که با فرآیند های موجود در تناقض است و یا ویژگی جدیدی محسوب می شود که استنادپذیری را زیر سوال می برد. (مانند ویژگی چت ایمن)
۴. دشواری شخصی سازی محصول با توجه به ظهور پلتفرم های جدید که همواره در حال وقوع است.
۵. امکان به روزرسانی سریع فرآیند و استفاده از تکنولوژی ها در صورت ظهور امکان جدید برای استنادپذیری ادله الکترونیک (مانند خروجی گرفتن از چت ها)
۶. امکان تعامل و مکاتبه با شرکت های پیام رسان خارجی در صورت نیاز که به استنادپذیری کمک می کند.
۷. ایجاد رقابت در بخش خصوصی که باعث افزایش کیفیت خدمات، کاهش هزینه های خدمات، تعامل بهتر بخش خصوصی و بخش حاکمیتی جهت انجام خدمات منافع عمومی، و درآمدزایی برای بخش خصوصی و دانش بنیان می شود.

با توجه به این چالش ها، فرصت دادن به بخش خصوصی جهت توسعه این محصول و ارائه خدمت به ذی نفع موردنظر به صورت پایه کاربری راهکار مناسبی به شمار می آید. پیشنهاد شرکت فناوری های تنظیم‌یار شریف در این راستا شامل دو بعد راهکار فنی و راهکار سیاستی می باشد. ابتدا راهکارهای فنی را با توجه به سوالات موردنظر شرح می دهیم:

راهکار فنی اول: طراحی و توسعه سامانه مستندساز ادله الکترونیکی

این راهکار شامل توسعه سامانه مستتندساز ادله الکترونیکی و رابط کاربری مناسب و ارائه سرویس به کارفرمای محترم می‌باشد.این راهکار در پاسخ به چگونگی حل سه بخش شامل فرآیند تجمیع اطلاعات، نحوه نگهداری اطلاعات و فرآیند ارجاع اطلاعات به دادستانی کل کشور/پلیس فتا می‌باشد. طرح سامانه مستتندساز ادله الکترونیکی با بهره گیری از مفهوم طرف سوم و با هدف اعتماد سازی بین مردم، استنادپذیری فضای مجازی و تسهیل فرآیند دادرسی پرونده ها پیشنهاد می‌شود. با توجه به موارد پیش گفته برای تهیه مستندات قابل ارجاع و اتکا با سه نوع محتوا روبه‌رو هستیم:

۱. محتوای نوع اول: در دسترس عموم بدون نیاز به احرازهویت وجود دارد مانند: محتوی یک وب سایت یا وبلاگ
۲. محتوای نوع دوم: نیاز به ورود یا شرایط خاصی برای مشاهده دارد مثلا محتوی داخل پیام رسان‌ها، وب سایت‌هایی که نیاز به ورود (Login) دارند. (محتوای موردنظر که برای آن راهکار ارائه شد)
۳. محتوای نوع سوم: محتوای دیجیتال مالی مانند رسیدهای دیجیتالی، فاکتورها، و اطلاعات پرداخت ها (مخصوصا در توالی تراکنش ها به قصد کشف فیشینگ و استنادپذیری مدارک)

جهت تهیه مستند از محتوای نوع اول نیاز به سامانه‌ای داریم که پس از دریافت آدرس از کاربر، محتوا را مشاهده و ذخیره کند. جهت تهیه مستند از محتوای نوع دوم و نوع سوم راهکار پیشنهادی ما ذکر می‌شود. در این فرآیند، طبق شکل ۲، ابتدا تعهدنامه ای جهت توضیح قوانین و اعطای دسترسی به سامانه جهت اخذ داده ها به کاربر نمایش داده می شود که در صورت پذیرش آن، کاربر به داخل فرآیند راهنمایی می شود. درباره این تعهدنامه و محتوای آن در پیوست الف توضیحاتی ارائه می گردد. کاربر به سامانه وارد می شود و پس از وارد کردن اطلاعات هویتی و ثبت درخواست، احراز هویت انجام می دهد. سپس از بین اپلیکیشن ها و پلتفرم های موجود، گزینه مورد نظر خود را انتخاب می کند. سپس به پلتفرم مورد نظر تحت وب خود که توسط سامانه توسعه داده شده است، راهنمایی می شود. جمع آوری ادله الکترونیک توسط کاربر انجام می گیرد. این سامانه با الگوگیری از سایت Zone-H طراحی می‌شود. بنابراین لازم است تا سامانه ای طراحی شود تا قابلیت تطبیق پذیری و شمول تمامی انواع اپلیکیشن های ذکر شده مخصوصا واتس‌اپ وب و اینستاگرام تحت وب را داشته باشد.

(**فرآیند تجمیع و نگهداری اطلاعات**) کاربر جهت ورود، نام کاربری و رمز خود را وارد می‌کند. جهت انجام جمع آوری ادله الکترونیکی، از دکمه های تعبیه شده "اسکرین بگیر"، "ضبط ویدئو از ادله"، و "اپلود فایل(صوت، فایل PDF، و ...)" استفاده می‌کند. در جهت شفافیت فرآیند ثبت ادله الکترونیکی، عملیات را برای کاربر به صورت زنده (Live stream) نمایش می دهیم که درون موجودیت های (Agent) توسعه یافته سلنیوم اجرا می شود که موقت هستند. Session های فعال نیز پس از اتمام فرآیند حذف می گردند که این مورد نیز به صورت زنده به کاربر نمایش داده می شود. همچنین جهت افزایش اطمینان کاربران، از آن ها درخواست می شود که تمامی session های فعال خود را پس از پایان کار به صورت دستی حذف کنند و پس از آن رمز خود را نیز تغییر دهند که در شکل ۲ نیز شرح داده شده است.

مهم ترین بخش، پایگاه داده و فرآیند نگهداری داده است که باید به صورت امن، بهینه و غیرقابل دستکاری و تخریب طراحی شود. در این راستا، دو دیدگاه و نحوه پیاده سازی جهت تحقق این امر وجود دارد:

۱. **نگهداری همه داده ها در سرور**، که این سرور می تواند با توجه به ملاحظات سیاستی و هویتی سرور های سامانه مستندساز ادله الکترونیکی(کارگزار) و یا سرورهای مرکز آمار و فناوری اطلاعات قوه قضائیه باشند.
۲. **نگهداری تنها Hash تبدیل شده از داده ها** (مانند SHA256) که به کاربر اعطا می گردد(کد رهگیری)، تشکیل **گواهی مبنی بر استناد پذیری ادله الکترونیکی** با شرح حداقل اطلاعات هویتی، نوع درخواست و اطلاعات موردنیاز که توسط سامانه مستندساز تولید شده است و قابلیت ارائه به دادگاه جهت پیگیری دارد(مانند گزارش های پلیس فتا به دادستانی کل کشور)، و **تحویل فایل‌های ادله الکترونیکی** به کاربر (در این مدل هیچ داده ای از کاربران ذخیره نمی گردد و پس از تولید Hash، داده ها پاک می گردند.)

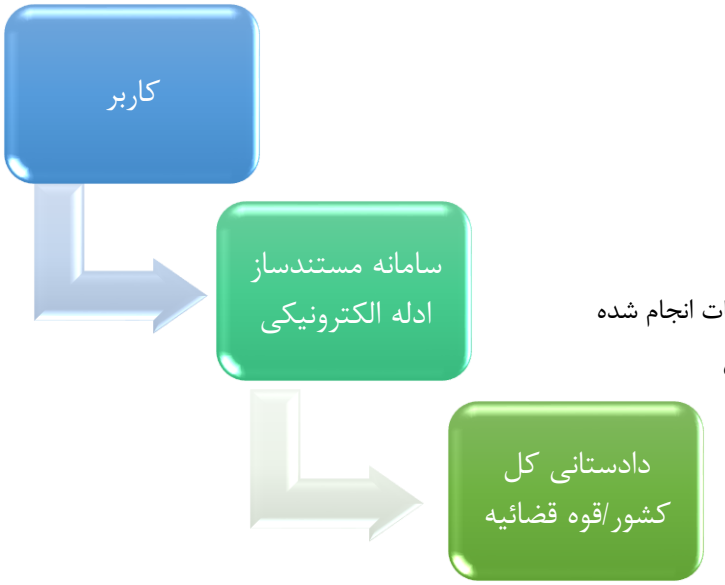
در هر دو این حالات، پس از تایید و ثبت داده ها، پرداخت توسط کاربر به ازای داده ها با تعرفه گذاری انجام گرفته صورت می گیرد و سپس به ازای فرآیند اتمام یافته، کد رهگیری (و یا در صورت صلاحدید، گواهی مبنی بر استناد پذیری ادله الکترونیکی) به کاربر اعطا می گردد. بنابراین فرآیند نگهداری، اولین دوراهی موردنیاز جهت تصمیم گیری برای پیاده سازی می باشد.

در پایان فرآیند، جهت تایید اصالت مدارک و قابلیت استنادپذیری آن‌ها با توجه به عدم امکان ویرایش ادله الکترونیکی و ویژگی برگشت ناپذیری فرآیند، از کاربر تایید اخذ می گردد. پس از اتمام فرآیند، ادله الکترونیکی استخراج شده به هر فرمت و حجمی که باشند،

به همراه برخی متغیرهای مهم در استنادپذیری ادله الکترونیکی شامل خروجی HTML از پیام ها، تصویر با فرمت مشخص، اطلاعات دقیق فرستنده و گیرنده پیام و یا محتوا، و زمان ثبت داده، ثبت می گردند.

(فرآیند ارجاع اطلاعات) در فرآیند کنونی، خدمت های گوناگون گزارش گیری های دیجیتال بنابر صلاحدید قاضی و درخواست قاضی از پلیس فتا می باشد که دسترسی های لازم از سمت دادستانی کل کشور به پلیس فتا ارائه می گردد. این دسترسی ها دارای چهارچوب شناسایی دستگاه کاربران و آخرین اطلاعات ورود کاربران (در اپلیکیشن های ایرانی) می باشد. با توجه به اینکه استنادپذیری ادله الکترونیک در اپلیکیشن های خارجی نیازمند تایید از سمت سرورهای پیام رسان موردنظر است، این فرآیند دچار اختلالات بسیار در این مورد بوده است. بنابراین، دوراهی دوم این فرآیند نحوه ارجاع به پلیس فتا می باشد. در این راستا نیز، دو دیدگاه جهت تحقق این امر وجود دارد:

۱. اعلام کد رهگیری به دادگاه، دادستانی کل کشور و معاقبا قاضی پرونده با API از سامانه مستندساز الکترونیکی
۲. ارائه فایل های ادله الکترونیکی، Hash و گواهی استنادپذیری توسط کاربر به دادگاه، سپس دادگاه در صورت نیاز با API، Hash ارائه شده را اعتبارسنجی می نماید.



شکل ۲. فرایند ثبت ادله در سامانه مستتندساز ادله الکترونیکی طبق راهکار اول

طی این فرآیند، پس از مستندسازی و گردآوری اطلاعات، به کاربر یک گواهی مبتنی بر Hash ایجاد شده به همراه اطلاعات شخص حقیقی با فرمت قابل قبول بخش فنی معاونت نظارت بر فضای مجازی دادستانی کل و معاونت فنی مرکز فناوری اطلاعات و ارتباطات قوه قضائیه ارائه می شود. به این گواهی، تاییدیه الکترونیکی از سامانه مستندساز ارائه می شود که به کاربر اطمینان جهت استنادپذیری را می دهد. تمامی اطلاعات فرد در سرورهای سامانه می باشد و پس از ارائه گواهی و hash به کاربر و بررسی API آن توسط دادستانی کل و تایید نهایی، اطلاعات کاربران پاک می گردد. مستندات خروجی سامانه قابلیت ارائه در محاکم قانونی را خواهد داشت و جایگزین استعلام های کنونی از پلیش فتا خواهد بود. این پیاده سازی با موجودیت های سلنیوم و یا ابزار مشابه آن برای ایجاد session های موقت می باشد. بدین ترتیب، این فرآیند زیر نظر دادستانی کل کشور و مرکز آمار و فناوری اطلاعات قوه قضائیه و توسط

سامانه مستندساز ادله الکترونیکی پیاده سازی می گردد. طبق این راهکار، یک وبسایت با اتصال امن به سامانه های مشخص پلیس فتا و با استفاده از پروتکل امن انتقال اطلاعات HTTPS توسعه داده می شود.

(بلاکچین خصوصی) جهت افزایش اطمینان از نحوه نگهداری اطلاعات، ما می‌خواهیم افرادی که می‌توانند داده‌ها را در این بلاک چین بنویسند، کنترل کنیم و همچنین می‌خواهیم افرادی را که می‌توانند داده‌ها را از این بلاک چین بخوانند، کنترل کنیم. به منظور انجام این امر، اولین اقدام شناسایی است. لازم است بدانیم که چه کسی بخشی از این شبکه بلاک چینی است. اگر ما ندانیم که چه کسی کاربر این شبکه است، تعریف کردن قوانین در مورد اینکه چه داده‌هایی را می‌توان به سامانه مستندساز تحویل داد و چه داده‌هایی را می‌توان از آن مصرف کرد، اگر نگوییم غیر ممکن می شود، قطعا بسیار دشوار خواهد شد.

این شبکه بلاک چین خصوصی نیاز به یک دعوتنامه دارد و باید توسط مدیر شبکه یا با مجموعه‌ای از قوانین که توسط او وضع می‌شود مورد تایید قرار بگیرد. بنابراین زمانی که یک گره به شبکه وارد می‌شود، نقشی در حفاظت از بلاکچین به شیوه غیر متمرکز خواهد داشت. سامانه مستندساز ادله الکترونیکی ممکن است به سطحی از امنیت، حریم خصوصی، انطباق، عملکرد و بسیاری از خصوصیات دیگر که یک بلاک چین خصوصی می‌تواند فراهم کند، نیاز داشته باشد. تراکنش‌ها به طور عمومی در بلاک چین قابل رویت نیستند و تنها نودهای انتخاب شده در این بلاک چین‌های خصوصی می‌توانند به دفتر کل دسترسی داشته باشند. مزایای بلاک چین های خصوصی موردنظر عبارتست از: کنترل منابع و دسترسی به بلاک چین توسط سازمان، عملکرد سریعتر به دلیل توزیع محلی نودها، امکان اضافه کردن نودها و سرویس‌های قابل دسترسی، و کنترل کردن زیر ساخت توسط خود سازمان

بلاکچین های خصوصی تضمین می‌کنند که بر تمام کسانی که می‌توانند جزییات اطلاعات موجود در زنجیره را بنویسند و بخوانند، کنترل کامل دارند. در بحث سطح اجازه دسترسی به شرکت کنندگان در شبکه، بلاکچین خصوصی مورد توسعه، متمرکز است زیرا فقط به افراد خاصی امکان می‌دهد تا در یک شبکه بسته شرکت کنند. در این مدل، تمام تاییدکننده ها یکدیگر را می‌شناسند و به عنوان بخشی از شبکه منتصب می‌شوند و قابلیت تغییر یا اصلاح تراکنش ها بر اساس نیازهای خود را دارند. گرچه این مدل برای حمله مستعدتر است؛ زیرا نودهای مخرب آسانتر می‌توانند کنترل شبکه را در دست بگیرند.

همچنین در این راستا با توجه به تعداد کاربران استفاده کننده از سامانه که تخمین زده شده‌اند، مقیاس پذیری نیز حائز اهمیت است. در بلاکچین خصوصی موردنظر نیازی نیست که تراکنش ها از صدها یا هزاران نود عبور کند تا اطلاعات آنها تایید شود. بنابراین، این تراکنش ها می‌توانند با سرعت بیشتری پشتیبانی و پردازش شوند. ممکن است مفهوم غیرمتمرکزسازی برای ارائه شفافیت، امنیت و کاهش هزینه ها باشد، اما در آخر تمام این موارد به اهداف دادستانی کل کشور و مرکز آمار و فناوری اطلاعات قوه قضائیه بستگی دارد که این فناوری را چگونه می‌پذیرد.

راهکار فنی مطرح شده، بنابر مصاحبه با شرکت های دارای محصول امنیت، کارشناسان رمزگذاری، و مدیران فنی پیام رسان های داخلی دارای قابلیت توسعه در پیاده سازی با تغییراتی در ساختار می باشد. از جمله این قابلیت ها، پیاده سازی این سامانه در ماشین مجازی می باشد. در زیر به توضیح آن می پردازیم.

پیاده سازی توسعه ماشین مجازی سمت کارفرما در راهکار اول

در این قسمت، راهکار مذکور را بر روی ماشین مجازی با الهام از ساختار VDI توسعه می دهیم. برای اجرای سیستم‌عامل مدنظر نیازی به دسترسی به سخت‌افزارهای خاص طراحی‌شده برای اجرای آن سیستم‌عامل نداریم و می توانیم با هر سخت‌افزاری سیستم‌عامل‌ها را اجرا کنیم. پس از نصب ماشین مجازی توسط کاربر، محیطی فراهم می‌شود که ماشین می‌تواند سیستم‌عامل خود را در

آن بدون وابستگی به دستگاه میزبان (دستگاه فیزیکی نصب‌شده روی آن) یا سایر ماشین‌های مجازی، اجرا کند. سیستم‌عامل در حال اجرا در ماشین‌های مجازی به‌عنوان «سیستم‌عامل مهمان (Guest OS) شناخته می‌شود. در این راهکار، می توان با توسعه این محصول، راه حل مناسبی برای تمامی اپلیکیشن ها در محیط یک مرورگر یا اپلیکیشن با دسترسی مناسب از سمت دادستانی کل و با نظارت مستمر اپراتور، با وارد کردن اطلاعات ورود به حساب شاکی و یا متهم، تشخیص اصالت انجام گیرد و تمامی فرآیندها سمت سرور صورت پذیرد.

(ساختار) سیستم‌عامل مهمان می‌تواند با سیستم‌عامل دستگاه میزبان یا سایر ماشین‌های مجازی ایجادشده روی دستگاه میزبان یکسان باشد یا با آن‌ها تفاوت داشته باشد. یک دستگاه میزبان می‌تواند هم‌زمان از چند دستگاه مجازی در حال اجرای سیستم‌عامل‌ها و اپلیکیشن‌های مختلف میزبانی کند و در صورت استفاده هم‌زمان از چند ماشین مجازی تداخلی بین فعالیت سیستم‌عامل‌های آن‌ها ایجاد نمی‌شود و در فرآیند فعالیت این ماشین‌ها هیچ مشکلی به وجود نمی‌آید. سیستم‌عامل‌های در حال اجرا در ماشین‌های مجازی و اپلیکیشن‌های موجود در آن‌ها می‌تواند درست مانند سیستم‌عامل‌ها و اپلیکیشن‌های حقیقی به‌روزرسانی شوند و حذف یا نصب اپلیکیشن‌ها روی این سیستم‌عامل‌ها نیز به‌راحتی امکان‌پذیر است؛ انجام این فرآیندها به‌هیچ‌وجه سیستم‌عامل دستگاه میزبان یا سیستم‌عامل سایر ماشین‌های مجازی را تحت تأثیر قرار نمی‌دهد.

(نوع مورد استفاده) میزبانی از ماشین‌های مجازی توسط کامپیوتر نیازمند استفاده از یک نرم‌افزار هایپروایزر (hypervisor) است (کلمه هایپروایزر به معنی ناظر ارشد یا فرا ناظر است). این نرم‌افزار سی‌پی‌یو، رم، هارد، شبکه و سایر قطعات نرم‌افزاری کامپیوتر را به‌صورت مجازی شبیه‌سازی می‌کند و با این روش منابع سخت‌افزاری لازم را متناسب با نیاز ماشین‌های مجازی در اختیار آن‌ها قرار می‌دهد. این نرم‌افزار می‌تواند از چند پلتفرم سخت‌افزاری مجازی پشتیبانی کند که هر یک از آن‌ها به‌صورت کاملاً مستقل و مجزا از یکدیگر عمل می‌کنند. هایپروایزر با استفاده از این پلتفرم‌ها اجرای هم‌زمان سیستم‌عامل‌هایی مانند لینوکس و ویندوز سرور (مجموعه سیستم‌عامل‌های سرور که توسط مایکروسافت طراحی و تولید می‌شود) روی یک دستگاه فیزیکی را امکان‌پذیر می‌کند. هایپروایزر منابع موجود را مدیریت می‌کند و آن‌ها را به ماشین یا ماشین‌های مجازی در حال کار روی دستگاه اختصاص می‌دهد. در ضمن این نرم‌افزار در زمان‌بندی تعیین روش اختصاص منابع بر اساس نحوه پیکربندی هایپروایزر و ماشین‌های مجازی را نیز بر عهده دارد و قادر است منابع اختصاص‌داده‌شده به هر یک از ماشین‌های مجازی را بر اساس تغییر نیازهای آن‌ها تغییر دهد. هایپروایزر مدنظر برای دادستانی کل بسته به سیاست های موجود می تواند یکی از دو نوع هایپروایزر برهنه که مستقیماً روی دستگاه فیزیکی میزبان اجرا می‌شود و به سخت‌افزار آن دسترسی مستقیم دارد، باشد و یا از نوع هایپروایزر میزبانی‌شده باشد که این نوع هایپروایزر روی سیستم‌عامل دستگاه میزبان نصب و برای مدیریت فراخوانی‌های مختلف برای دسترسی به منابع سخت‌افزاری مختلف استفاده می‌شود.

(نوع ماشین مجازی موردنظر) ماشین‌های مجازی بر اساس هایپروایزر مورداستفاده برای مدیریت آن‌ها یا میزان بار کاری که پشتیبانی می‌کنند. ماشین مجازی سیستمی (System VM) که یک محیط کاملاً مجازی‌سازی‌شده است که روی یک دستگاه فیزیکی پشتیبانی می‌شود و سیستم‌عامل خودش را اجرا می‌کند. این دسته از ماشین‌های مجازی درست مانند دستگاه‌های فیزیکی یک محیط کامل برای اجرای اپلیکیشن‌ها و سرویس‌ها ایجاد می‌کنند. آن‌ها برای مجازی‌سازی منابع سخت‌افزاری و قرار دادن آن‌ها در اختیار ماشین‌های مجازی، وابسته به یک هایپروایزر هستند. **این ماشین مجازی پیشنهادی برای توسعه می باشد.**

(معایب این راهکار) این راهکار نسبت به راهکار اول دارای پیچیدگی پیاده سازی بیشتر، ترافیک بیشتر سمت سرور و امکان هک بیشتر می باشد و برتری خاصی از نظر پیاده سازی در مقیاس جامعه نسبت به راهکار اول دارا نمی باشد.

راهکار فنی دوم: طراحی و توسعه API و کد رهگیری برای پیام رسان های داخلی

برای تمامی اپلیکیشن های داخلی، شامل ایتا، آی گپ، بله، و سروش پلاس راهکار نهایی که قابل پیاده سازی می باشد، تعبیه دکمه ای به نام ثبت در پرونده می باشد که توسط یک API تمامی اطلاعات مدنظر را برای سامانه مستندساز ارسال می‌کند. این API شماره همراه شخص حقیقی را به دلیل تشخیص هویت و log اطلاعات آن صفحه چت را برای سامانه ارسال می کند و در قبال آن یک کد رهگیری به کاربر می دهد که با استفاده از آن بتواند در سامانه ثنا پرونده خود را پیگیری کند.

به این ترتیب می‌توان به صورت در لحظه و استنادپذیر، ادله الکترونیکی را به صورت امن انتقال داد. به دلیل دسترسی به سرور های پیام رسان های داخلی، از بابت امنیت و استنادپذیری این مستندات اطمینان حاصل نمود. بدیهی است که می توان راهکارهای ذکر شده را نیز در این راستا به کار برد ولی به دلیل عدم دسترسی به سرورها در پیام رسان های خارجی، این راهکار در آن ها میسر نمی باشد. البته امید است که بتوان با ارائه مدل موفقی از این فرآیند در پیام رسان های داخلی و مکاتبه با تلگرام در آینده، این امکان را در پیام رسان های مذکور نیز مهیا نمود. این راهکار بسیار سریعتر از راهکارهای پیام رسان های خارجی به نتیجه می‌رسد و می توان به سرعت در جهت اجرایی سازی آن با توجه به گسترش روزافزون خدمات این اپلیکیشن ها (فراتر از پیام رسانی) که در کاربردها و چالش ها ذکر شد، شامل خدمات بانکی و محتوایی قدم برداشت.

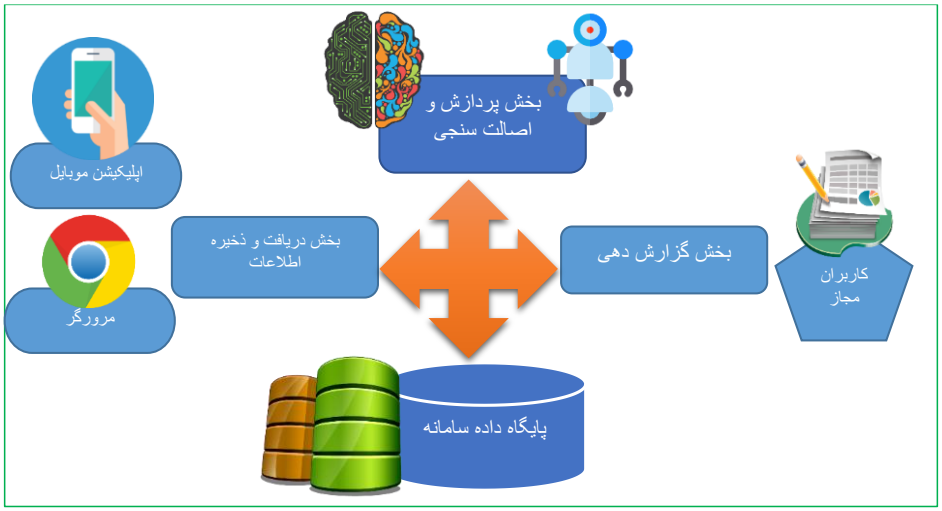
راهکار های فنی بررسی شده و مردود

مجموعه ای از راهکارهای دیگر طی تحقیق و توسعه مدنظر، بررسی شدند و بنا به دلایل مشخصی رد شدند. در جدول ۱ تمامی این موارد به همراه علت ردف مطرح و بررسی شده اند که در جدول ۱ آمده است.

جدول ۱. راهکار های فنی مردود به همراه شرح راهکار و علل ردشدن

ردیف	نام راهکار	شرح راهکار	علت رد راهکار
۱	توسعه تصویر تلگرام و تصویر اینستاگرام	راهکار به دلیل اوپن سورس بودن تلگرام و امکان خزش داده های صفحات عمومی اینستاگرام راه حل جالب و قابل اجرایی می باشد که مشابه آن بسیار تا کنون انجام شده است.	تنها صفحات عمومی اینستاگرام قابلیت خزش و جمع آوری اطلاعات دارند و صفحات شخصی و همچنین چت ها را نمی توان با بات ها مورد استفاده و بررسی قرار داد. نسخه تولید شده تلگرام برای قوه قضائیه، مقایس کوچک راهکار اول می باشد و پس از مدتی با رفتار قهری خود تلگرام مواجه شده و دچار مشکل می گردد. این راهکار برای واتس‌اپ به دلیل محوریت کلاینت، قابل بررسی نیست.
۲	تهیه اسکرین شات، ضبط ویدیو و ذخیره فایل ها انتقال به صورت امن(سرتاسر رمزگذاری	وبسایت مادر مشابه راهکار اول توسعه داده می شود که جهت بهبود دسترسی کاربران برای آن اپلیکیشن اندروید و آی اواس توسعه داده می شود. این راهکار، معمولا مورد اقبال مدیران و عموم مردم می باشد. نیاز است تا پروتکل انتقال امن اطلاعات برای آن توسعه داده شود تا پس از اخذ و ثبت	اما باید در نظر داشت که هر راهکاری که سمت کاربر توسعه داده شود، بر خلاف اقبال عمومی، استنادپذیر نمی باشد.

	شده) توسط طرف سوم سمت کاربر	داده ها از کاربر، امکان دسترسی آن وجود نداشته باشد. معماری این سامانه در شکل ۳ آمده است.	
۳	API Hooking	برای تمامی اپلیکیشن های خارجی، در صورتی که جرم یا بحث در حال وقوع باشد و یا کاربر در انتظار موقعیتی برای انجام اسکرین شات باشد (موقعیتی که در سایر موارد دیگر پوشش داده شده است ولی این راهکار برای این شرایط خاص می باشد)، این راهکار قابل استفاده می باشد. این روش، بر خلاف دیگر روش ها بدون نیاز به کاربر و یا سرور می تواند اجرایی گردد که البته بر روی تلگرام و اینستاگرام پاسخگو است. امید است تا از این طریق بتوانیم جهت تقویت سایر راهکار های مورد بحث که تمام سمت سرور می باشند، پروتکل امنی با ملاحظات حفظ حریم شخصی برای داده ها تعریف کنیم.	نیاز است تا سامانه به کلید کاربر جهت رمزگشایی پیام دسترسی داشته باشد. این روش به تحقیق و توسعه بیشتر نیازمند است. با واتس‌اپ به دلیل ذخیره داده ها بر روی دستگاه مشکل دارد.



شکل ۳. تهیه اسکرین شات، ضبط ویدیو و ذخیره فایل ها و انتقال به صورت (سرتاسر رمزگذاری شده) توسط طرف سوم سمت کاربر

زیرساخت و پروتکل اپلیکیشن ها

در جهت استفاده از هریک از راهکارها، لازم است تا پروتکل های ارتباطی پیام رسان ها را بهتر بشناسیم. راهکار منتخب، چه توسعه درون سرور باشد و چه توسعه API، لازم است تا پروتکل های گوناگون سه پیام رسان خارجی که طبق نیازسنجی انجام شده، دارای بیشترین ترافیک و کاربر هستند، مطرح گردد.

۱. تلگرام

جدول ۲. پروتکل های پیام رسان تلگرام

ردیف	تکنولوژی	نام
۱	کیفیت وبسایت	تعریف رمزگذاری کاراکتر
۲	زبان برنامه نویسی سمت سرور	JavaScript
۳	زبان برنامه نویسی سمت کاربر	Bootstrap
۴	سرور وب	Nginx 1.18.0
۵	ارائه دهنده سرویس DNS	Google
۶	مرجع صدور گواهی SSL	GoDaddy
۷	عناصر سایت	External CSS Inline CSS Cookies expiring in hours HttpOnly Cookies Secure Cookies Gzip Compression IPv6 HTTP/2 HTTP Strict Transport Security
۸	فرمت های داده های ساخت یافته	Open Graph Generic RDFa Twitter Cards
۹	زبان نشانه گذاری	HTML5
۱۰	فرمت های فایل تصویری	PNG SVG

۲. واتس‌اپ

جدول ۳. پروتکل های پیام رسان واتس‌اپ

ردیف	تکنولوژی	نام
۱	کیفیت وبسایت	تعریف رمزگذاری کاراکتر
۲	زبان برنامه نویسی سمت کاربر	JavaScript
۳	ارائه دهنده سرور ایمیل	Proofpoint
۴	مرجع صدور گواهی SSL	DigiCert
۵	شبکه های تبلیغاتی	Google Ads
۶	عناصر سایت	External CSS Embedded CSS Inline CSS Brotli Compression IPv6 HTTP/3

		HTTP Strict Transport Security
۷	فرمت های داده های ساخت یافته	Open Graph Generic RDFa
۸	زبان نشانه گذاری	HTML5
۹	فرمت های فایل تصویری	PNG SVG JPEG

۳. اینستاگرام

جدول ۴. پروتکل های پیام رسان اینستاگرام

ردیف	تکنولوژی	نام
۱	کیفیت وبسایت	تعریف رمزگذاری کاراکتر
۲	زبان برنامه نویسی سمت سرور	PHP
۳	زبان برنامه نویسی سمت کاربر	JavaScript
۴	ارائه دهنده سرور ایمیل	Proofpoint
۵	مرجع صدور گواهی SSL	DigiCert
۶	ابزار تحلیل ترافیک	Google Analytics
۷	شبکه های تبلیغاتی	Google Ads Advertising Microsoft
۸	عناصر سایت	External CSS Embedded CSS Inline CSS Gzip Compression Brotli Compression IPv6 HTTP/3 HTTP Strict Transport Security Default subdomain www Default protocol https
۹	فرمت های داده های ساخت یافته (پیوست اول)	Open Graph Generic RDFa Twitter Cards
۱۰	زبان نشانه گذاری	HTML5
۱۱	فرمت های فایل تصویری	PNG SVG

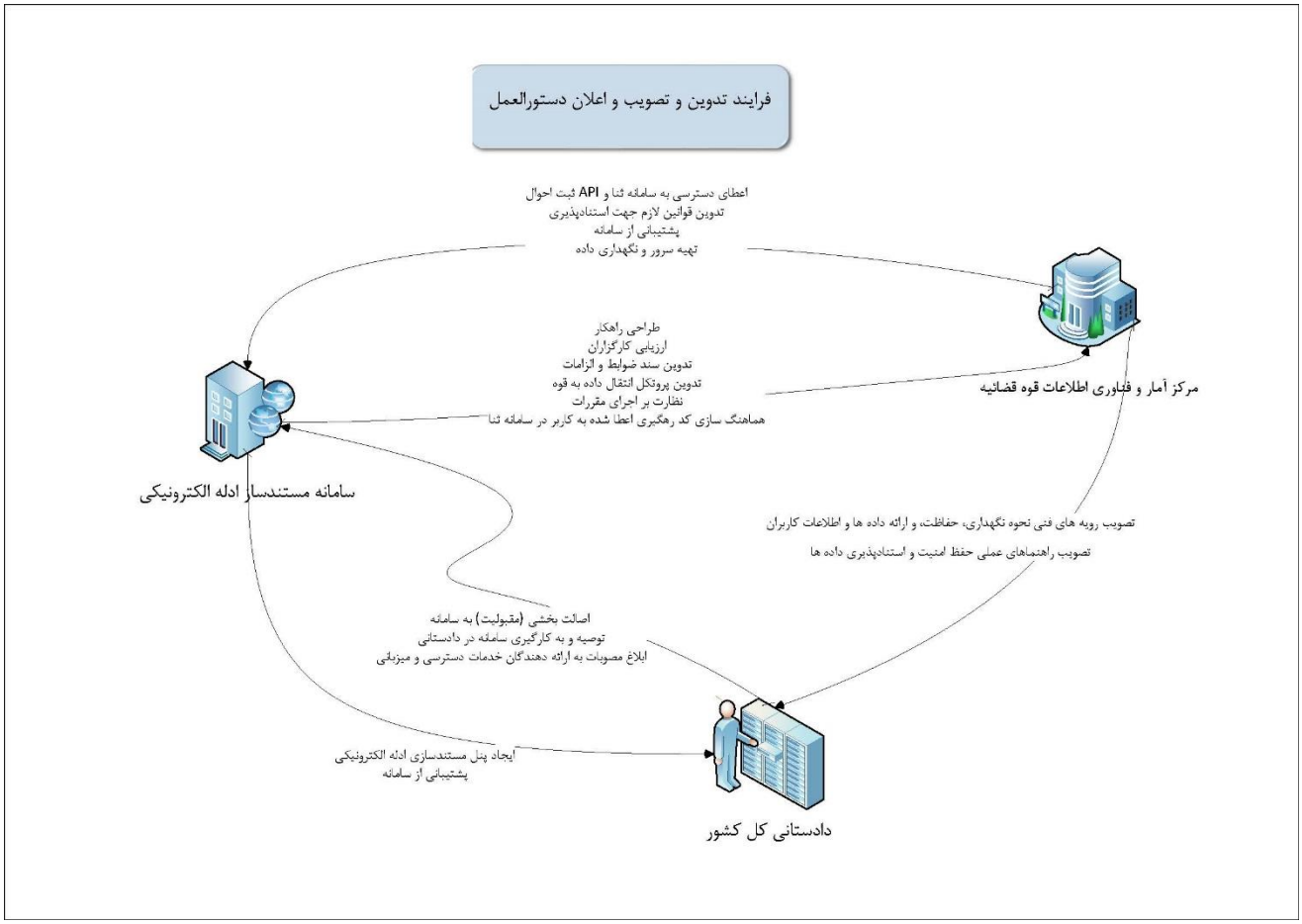
راهکار های سیاستی (نهادی)

حال با در نظر گرفتن راهکارهای فنی پیشـــنهادشـــده، به دلیل پیچیدگی بالای رویه های نگهداری داده و ارجاع به داده و همچنین اهمیت بالای داده های هویتی اشخاص حقیقی، لازم است تا راهکارهای سیاستی نیز در صورت لزوم در کنار راهکارهای فنی مطرح شود. این راهکارهای سیاستی (نهادی) شامل پیشنهاد ساز و کار مناسب برای تعریف دستورالعمل ها و شکل گیری اکوسیستم

مناسب برای پیاده سازی راهکارهای فنی و همچنین ایجاد فرآیند ارتباطی مناسب برای نگهداری و ارجاع اطلاعات بین سازمان های مرتبط و سامانه مستندساز ادله الکترونیک می‌باشد. بنابراین ابتدا باید اکوسیستم مناسب را با توجه به خلاهای قانونی کنونی پیشنهاد داد.

بخش اول راهکار سیاستی: فرآیند تدوین و تصویب و اعلان دستورالعمل

در تمامی حالت های راهکار فنی اول، نیاز به شکل‌دهی فرآیندی مابین سامانه مستندساز ادله الکترونیک، دادستانی کل کشور و مرکز آمار و فناوری اطلاعات قوه قضائیه می باشد. این مراحل، با استناد به "آیین نامه جمع آوری و استنادپذیری ادله الکترونیکی" که تنها مستند موجود برای تعریف موجودیت ها و روش ها می‌باشد، مبهم است. بنابراین، لازم است تا جهت انعقاد راهکار فنی، راهکار پیشنهادی اکوسیستمی به شرح شکل ۴ ارائه گردد. فرآیند پیشنهادی با درنظرگرفتن موجودیت های مطرح شده در آیین نامه و با توجه به فرآیند کنونی پلیس فتا برای ارائه خدمات است. شکل ۴ نشان دهنده موجودیت ها و ارتباط بین آن ها می باشد که جهت فلش نشان دهنده انجام مورد ذکر شده از سمت فرستنده به گیرنده می‌باشد.



شکل ۴. فرآیند تدوین و تصویب و اعلان دستورالعمل های استنادپذیری ادله الکترونیکی

راهکار سیاستی اول: پیاده سازی سامانه و ارائه خدمت به دادستانی کل کشور/پلیس فتا

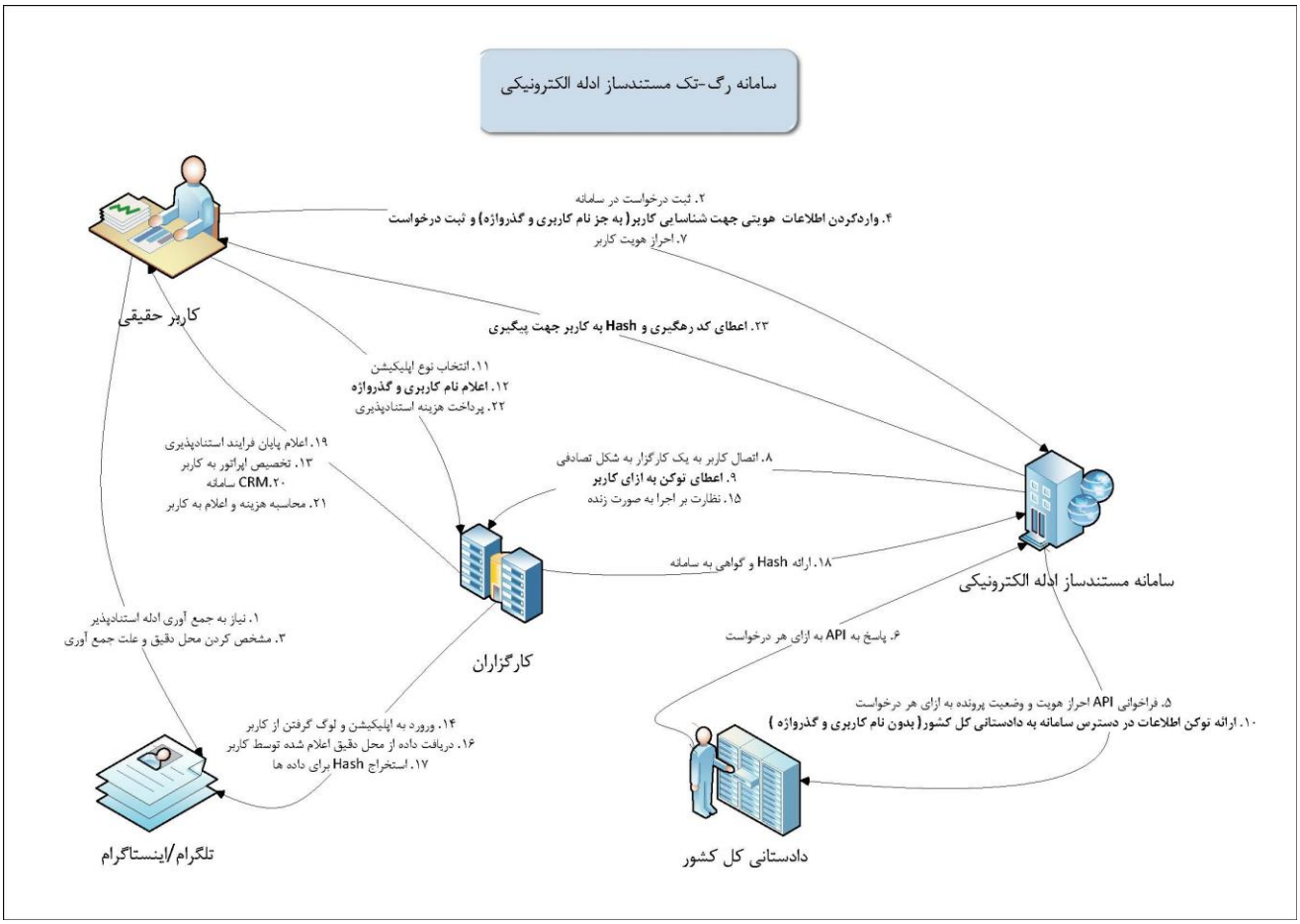
طی این راهکار، مدل کسب و کار فنی راهکار اول را پیاده سازی میکنیم و محصول نهایی به عنوان خدمت به دادستانی کل کشور/پلیس فتا ارائه می گردد. جهت شکل گیری فرآیند احراز هویت، ارائه Hash با API به پلیس فتا، و کد رهگیری به کاربر با پیامک به عنوان محصول توسط سامانه مستندساز ادله الکترونیکی ارئه می‌شود.

راهکار سیاستی دوم: فرآیند ارتباط بین نهادی در اجرای راهکار

در صورتی که طبق نظر نهادهای تصمیم گیر و بنابر آیین نامه مذکور، نیاز به حضور رگولاتور و تقسیم بندی وظایف باشد، می توان اکوسیستم را به نحوی متفاوت ایجاد نمود. در اکوسیستم جدید، سامانه مستندساز ادله الکترونیکی دیگر نقش تجمیع اطلاعات را ندارد و تمامی وظایف فنی خود را به کارگزاران اعطا می نماید. از این رو به آن سامانه نظارت بر مستندسازی ادله الکترونیکی می گوییم.

تنظیم گری و حضور فعال بخش خصوصی در حل مسائل حاکمیتی و ایجاد راه تعامل مناسب بین ذی نفع حاکمیتی و بخش خصوصی، همواره راهکاری مطمئن جهت اجرای امور فناوری محور در محیطی به دور از انحصار و در فضای رقابتی می باشد. بنابراین، با اهداف انجام فرآیند گردآوری مستندات، حفظ حریم خصوصی مخاطب حتی الامکان، عدم دسترسی ذی نفعان به تمامی داده ها (خارج از مقیاس نیاز به مستندات کاربر)، اعتماد سازی بین مردم و سامانه (مقبولیت سامانه)، و استنادپذیری مستندات(داده ها از سمت سرور جمع آوری شوند و سمت کاربر توسعه ای نباشد)، می توان راهکاری مناسب اتخاذ نمود و در این بین با ترغیب بخش خصوصی به همکاری، فرآیندی نوین در همکاری با این بخش تعریف نمود. طی این راهکار نهادی، با در نظر گرفتن روش های ارزیابی و نظارت بر فرآیند استنادپذیری و با الگوبرداری از شاپرک (شبکه الکترونیک پرداخت کارت)، شبکه الکترونیکی جدیدی به عنوان رابط میان قوه قضائیه/دادستانی کل کشور، کارگزاران فنی، پیام رسان موردنظر، و کاربران با مرکزیت سامانه نظارت بر مستندسازی ادله الکترونیک طراحی شده است. هرکدام از این موجودیت ها ارتباط هایی با یکدگیر دارند که به دقت در شکل ۵ تشریح شده است.

در این فرآیند، طبق شکل ۵ کاربر ابتدا به سامانه نظارت بر مستندسازی اتصال می یابد و مانند گذشته اطلاعات هویتی خود را وارد می‌کند، احراز هویت می شود و درخواست خود را کامل ثبت می کند. سپس مشابه با ارتباط شاپرک و پرداخت‌یارها، به صورت تصادفی به یکی از کارگزاری ها اتصال می یابد تا فرآیند تجمیع توسط پلتفرم توسعه داده شده مشابه با راهکار فنی ذکرشده مبنی بر درخواست کاربر انجام گیرد. سپس پس از اتمام کار، اطلاعات عملیات انجام شده به صورت توکن عملیات و به همراه Hash به سامانه نظارتی ارسال می گردد تا ذخیره گردد و در ادامه سامانه نظارتی بر پاک شدن session های کارگزاران نظارت می کند. بقیه فرآیند شامل ایجاد گواهی برای کاربر و اتصال Hash به دادستانی کل مانند گذشته می باشد. سامانه نظارتی، بر انجام فرآیند، کیفیت خدمات کارگزاران و مخصوصا CRM مناسب آن ها جهت ارتباط قوی و موثر با کاربران نظارت می کند. با این نحوه اجرا، نام کاربری و رمز نیز در اختیار سامانه قرار نمی گیرد و همچنین اطلاعات هویتی و ارتباط مبتنی بر نام و نام خانوادگی در اختیار کارگزاران قرار نمی گیرد و تنها نام کاربری و رمز عبور برای آن ها موجود می‌باشد.



شکل ۵. نمودار جریان فرآیند ارتباط بین نهادی در اجرای راهکار با ایجاد سامانه نظارت بر مستندسازی ادله الکترونیک

نکات غیرفنی تاثیرگذار بر راهکارها (ریسک های پروژه)

۱. همواره باید در نظر داشت در صورتی که افراد حقیقی که در پرونده مشخصی نامبرده هستند(درگیر در پرونده)، و با نیت های مختلف سعی در ایجاد شواهد الکترونیک خلاف واقع و یا جهت دهنده به پرونده را دارند، به هیچ صورتی نمی توان سوءنیت آن ها را تشخیص داد و مانند هر فرآیند الکترونیک دیگری در جهان باید به آن اعتماد نمود، چرا که مشابه این اتفاق نیر به دفعات در دادگاه ها می افتد.

۲. در صورتی که شخص حقیقی درگیر در پرونده و یا فردی مرتبط با او خواهان جعل ادله الکترونیک مانند ساختن چت جعلی، ایجاد پروفایل جعلی شامل عکس، بیو و متن جعلی، نشر اطلاعات کاذب و سپس تهیه اسکرین شات از آن باشد، راه حل مناسب در تمامی راهکارهای مذکور وجود دارد که عبارتست از احراز هویت فرد و شناسایی چت ها با اخذ اطلاعات تکمیلی مانند دریافت شماره تماس و یا ایدی یکتای فرد حاضر در چت، که این مورد در بسیاری از موجودیت های بحث شده مانند کانال های تلگرام، گروه های واتس‌اپ و اینستاگرام و ... دارای قابلیت بررسی توسط بقیه اشخاص حقیقی جهت جمع آوری ادله الکترونیک می باشد.

۳. رمزگذاری به عنوان پایه و اساس بسیاری از تکنولوژی های به شمار می آید، اما برای درخواست های HTTP و پاسخ های ایمن و همچنین احراز هویت سرورهای مبدا وب سایت از اهمیت بیشتری برخوردار است. پروتکلی که مسئولیت این امر را بر عهده دارد، HTTPS می باشد. وب سایتی که HTTPS را روی وب سایت خود پیاده سازی می کند، یک TLS certificate بر روی

سرور مبدا خود نصب می کند. این رمزگذاری سرتاسری حاضر در پیام رسان ها موجب می شود تا هیچ‌کس، حتی خود ما، به محتوای مکالمات شما دسترسی نداشته باشد. پیام رسان ها مخصوصا واتس‌اپ امکان دیدن محتوای پیام‌ها یا شنیدن تماس‌ها را ندارند. زیرا رمزگذاری و باز کردن رمز پیام‌های ارسالی ، بطور کامل روی دستگاه انجام می‌شود. پیش از اینکه پیام از گوشی شما ارسال و خارج شود، با قفل امنیتی رمزگذاری می‌شود و فقط گیرنده کلیدهای لازم را دارد. به علاوه، کلیدها برای تک‌تک پیام‌های ارسالی عوض می‌شوند. در حالیکه همه اینها در پشت صحنه اتفاق می‌افتد، واتس‌اپ می‌تواند با چک کردن کدهای امنیتی روی دستگاه از رمزگذاری سرتاسری اطمینان حاصل کند. در اینجا، این سوال مطرح می‌شود که رمزگذاری سرتاسری برای مقامات مجری قانون چه معنی دارد.. بر اساس قوانین و سیاست‌های واتس‌اپ، آن ها به دقت تقاضاهای مقامات مجری قانون را بررسی کرده، اعتبارسنجی کرده و پاسخ می‌دهند و به درخواست‌های اضطراری اولویت می‌دهند.

آدرس و اطلاعات تماس

خیابان آزادی، خیابان استاد حبیب الله، بالاتر از میدان حسینی، پلاک ۵۶، ایستگاه نوآوری شریف، ساختمان مرکز نوآوری صوت و تصویر (آومیک)

شماره تماس : ۰۹۳۹۱۸۹۷۹۷۲ تلفن : ۰۲۱۴۰۶۶۵۳۷۹ کد پستی : ۱۴۵۵۷۱۴۱۸۱