بسمه تعالی

دانشکده علوم و فنون نوین

گروه بین رشته ای فناوری (بخش علوم و فناوری شبکه)

پیشنهاد

احراز هویت غیرحضوری متقاضیان خدمات الکترونیک انتظامی بر مبنای سنجه‌های بیومتریکی

ارائه شده به: نیروی انتظامی جمهوری اسلامی ایران، معاونت فناوری اطلاعات و ارتباطات، مرکز تحقیقات کاربردی

نسخه ۲.۰.۰

شهریور ۱۳۹۹

فهرست مطالب

۱) فصل اول: مقدمه و خلاصه طرح

۱-۱) مقدمه

با توسعه روزافزون فضای مجازی و رشد سرویس‌های برخط (آنلاین)، گرایش عمومی مردم نیز به عدم مراجعه حضوری و انجام کارها از راه دور، روز به روز بیشتر می‌شود. این موضوع برای دریافت سرویس‌های مختلف مرتبط با پلیس هم به وضوح دیده می‌شود و بخش عمده‌ای از این فعالیت‌ها که امروزه به صورت حضوری و با مراجعه افراد به دفاتر خدمات الکترونیک انتظامی (پلیس +۱۰) انجام می‌شود، می‌تواند توسط خود افراد و در منزل یا محل کار آنها و به صورت برخط صورت پذیرد، کاری که در حوزه‌های حساسی مانند امور بانکی نیز انجام شده و روز به روز بر تعداد خدمات غیرحضوری و مجازی مالی و بانکی افزوده می‌شود و بسیاری از کارها که قبلا توسط کارمندان بانک انجام می‌شد، امروزه توسط خود مشتریان انجام می‌شود. این موضوع، علاوه بر کاهش هزینه‌های مختلف سازمانی برای ارائه دهنده خدمت، آسایش و راحتی بیشتری را برای گیرنده خدمت هم فراهم می‌کند، به ویژه در شرایطی مانند بحران کرونا (Covid 19) که گرایش به عدم حضور و تجمع افراد در مکان‌های سرپوشیده مانند دفاتر خدمات الکترونیکی در حال افزایش است.

برای عملیاتی کردن خدمات غیرحضوری، یکی از اصلی‌ترین چالش‌های پیش‌رو، موضوع امنیت و اعتبارسنجی هویت مشتریان (KYC) است. این مساله در رویکرد سنتی، با مراجعه حضوری افراد به دفاتر و پیشخوان‌های پلیس حل می‌شود، این در حالی است که برای ارائه خدمات مجازی باید از احراز هویت الکترونیکی (eKYC) بهره گرفت. هرچند برخی راهکارهای eKYC در دنیا (در کشورهای مختلفی مانند سوئیس، آلمان، انگلستان و هند) راه‌اندازی شده و در امور مختلف مانند خدمات مالی، بیمه و اپراتورهای تلفن همراه در حال استفاده است، اما با توجه به نوظهور بودن آن، در ایران، هنوز یک چالش محسوب می‌شود و مشتری را وادار به حضور فیزیکی در یکی از دفاتر می‌کند. الزام برای مراجعه حضوری از یک طرف منجر به نارضایتی افراد و از طرف دیگر منجر به افزایش هزینه‌های پلیس می‌شود. از این رو، احراز هویت از راه دور یکی از نیازمندی‌های حیاتی برای همه سازمان‌های ارائه دهنده خدمات مانند پلیس است و یکی از سرویس‌های جذاب برای مردم محسوب می‌شود. بدیهی است که این به معنی عدم استفاده از دفاتر و مراکز حضوری نیست و در مواردی که لازم است (مانند ارائه برخی سرویس‌های حساس که الزاما باید احراز هویت حضوری صورت پذیرد) می‌توان از دفاتر حضوری هم بهره گرفت.

۲-۱) بیان مسئله و تشریح ضرورت اجرای طرح

برای ارائه خدمات انتظامی غیرحضوری و از راه دور به افراد جامعه، لازم است امنیت ارائه خدمات به ویژه احراز هویت افراد با اطمینان مطلوب تامین شود. هدف این طرح ارائه یک راهکار احراز هویت غیرحضوری افراد متقاضی دریافت خدمات الکترونیک انتظامی است که برای این کار از ویژگی‌های زیست‌سنجی (بیومتریک) چهره آنها به عنوان معیار شناسایی استفاده می‌شود. بدین صورت که فرد متقاضی با بیان یکی از شناسه‌های هویتی خود مانند کد ملی، شماره گواهینامه یا گذرنامه و همچنین ارائه تصویری از خود (در قالب ویدئو) به صورت برخط درخواست تایید هویت (Verification) می‌کند که برای این کار تصویر چهره داخل ویدئو با تصویر چهره مرتبط با آن شناسه هویتی (که از سامانه‌های مرتبط مانند سامانه ثبت احوال استعلام گرفته می‌شود) مقایسه شده و در صورت تطابق، مورد تایید قرار می‌گیرد. علاوه بر تایید هویت مبتنی بر چهره، موضوع مهم دیگر این طرح، تشخیص زنده بودن (Liveness) است که در آن زنده بودن ویدئوی دریافتی بررسی می‌شود. موضوع دیگر، تامین امنیت اطلاعات رد و بدل شده بین کلاینت (متقاضی) و سرور (مرکز ارائه دهنده خدمت) است که باید در نظر گرفته شود.

ضرورت ارائه خدمات غیرحضوری با رشد روزافزودن خدمات برخط و افزایش تقاضای مردم برای آن، به ویژه در شرایطی مانند بحران بیماری کرونا، موضوعی بدیهی است که همه سازمان‌ها و نهادهای ارائه دهنده خدمات را به سمت بهره‌گیری از آن سوق داده است و مورد تاکید نهادهای بالادستی کشور شامل قانون‌گذاران و سیاست‌گذاران است. این طرح پیش‌نیاز ارائه هرگونه خدمات غیرحضوری توسط پلیس است و لازم است افراد قبل از دریافت خدمات، احراز هویت شوند. بنابراین، همه سرویس‌های ارائه شده به مردم، قبل از دریافت توسط افراد، با فراخوانی سرویس احراز هویت، فرد گیرنده خدمات را شناسایی می‌کنند. خلاصه ضرورت‌های انجام این طرح عبارتنداز:

- تقاضای روزافزون ارائه خدمات الکترونیکی و غیرحضوری از سمت مردم و لزوم بهبود تجربه مشتری (User Experience) به دلیل سادگی و سرعت کار
- تاکید نهادهای قانون‌گذار بر ارائه خدمات الکترونیکی و غیرحضوری به مردم به ویژه با تشدید موضوع در شرایط بحران کرونا
- نیاز به کاهش مراجعات حضوری افراد (از نظر سلامتی، ترافیک، ....)
- ضرورت افزایش امنیت و اشراف اطلاعاتی پلیس با تکمیل پایگاه‌های داده افراد به ویژه در تکمیل اطلاعات زیست‌سنجی، تهیه زیرساخت‌های استفاده از آنها، یکپارچه‌سازی و پیگیری (شفافیت)

- لزوم کاهش خطاهای انسانی و سواستفاده افراد از اطلاعات و اسناد

۳-۱) معرفی کاربردها/کاربران

احراز هویت برای ارائه بسیاری از خدمات الکترونیکی انتظامی در کاربردهای مختلفی مانند حوزه گواهینامه، گذرنامه، وظیفه عمومی، کارت سوخت، اعلام سرقت، دریافت سابقه عدم سو پیشینه و ... ضروری است، به گونه‌ای که از تعداد زیاد خدمات الکترونیکی قابل ارائه در دفاتر ارائه خدمات الکترونیکی انتظامی، در حال حاضر تعداد بسیار محدودی از آنها (بر اساس اطلاعات موجود در سایت http://epolice.ir) به صورت غیرحضوری و برخط ارائه می‌شود چراکه ارائه این خدمات به صورت غیرحضوری نیاز به احراز هویت افراد دارد. از این رو، با راه‌اندازی این سرویس، ارائه خدمات غیرحضوری در بسیاری از کاربردهای الکترونیکی انتظامی ممکن خواهد بود.

کاربران این سرویس دو گروه هستند: ارائه دهنده‌های خدمات الکترونیکی (پلیس) و گیرندگان خدمات الکترونیکی (عامه مردم). در سمت ارائه دهنده، هر کدام از سرویس‌های الکترونیکی انتظامی در هر کدام از حوزه‌های فعلی (گذرنامه، گواهینامه و ....) می‌توانند با فراخوانی این سرویس و در صورت تایید هویت افراد توسط آن، به ارائه خدمت مرتبط به افراد بپردازند. از طرف دیگر، همه افراد متقاضی استفاده از خدمات غیرحضوری، می‌توانند با انجام دستورالعمل احراز هویت در بستر فراهم شده برای دریافت خدمات (مانند اپلیکشن موبایل یا نسخه تحت وب)، ابتدا کار احراز هویت خود را انجام داده و پس از آن، خدمت مربوطه را دریافت کنند.

۴-۱) بیان مزایا و فواید عملیاتی طرح

اجرای طرح مزایا و دستاوردهایی عملیاتی مختلفی را برای گروه‌های مختلف دخیل در طرح به همراه خواهد داشت. در ادامه این مزایا به تفکیک دو گروه ارائه دهنده خدمات (پلیس) و دریافت خدمات (مردم) ذکر می‌شود.

۱-۴-۱) منافع برای ارائه دهنده خدمات (پلیس)

- کمک به تحقق پلیس هوشمند و ارائه خدمات غیرحضوری توسط نیروی انتظامی

- همراستایی با اهداف بالادستی کشور و در راستای تحقق دولت الکترونیک
- تصویرسازی نوآورانه و به‌روز بودن مبتنی بر فناوری از پلیس
- کمک به تحقق مسئولیت‌های پلیس در ارائه ساده و آسان خدمات با رعایت سلامتی شهروندان به ویژه در بحران‌هایی مانند شیوع کرونا
- کمک به اشراف اطلاعاتی پلیس و فراهم شدن امکان اعمال کنترل‌های امنیتی قوی‌تر و دقیق‌تر بر اساس روش‌های فناورانه مبتنی بر بیومتریک و در نتیجه ارتقاء امنیت
- کاهش مراجعات حضوری به دفاتر و کم کردن مشکلات ناشی از آن
- کاهش احتمال خطای انسانی و یا کم‌توجهی نیروهای انسانی
- فراهم کردن دسترسی ۲۴*۷ و حتی در روزهای تعطیل به خدمات
- فراهم کردن امکان نگاشت اطلاعات مختلف افراد به همدیگر در پایگاه داده‌های مختلف (کد ملی، اطلاعات گذرنامه، اطلاعات گواهینامه و ...)
- تسریع در تطبیق‌پذیری: با تغییر مقررات، سیستم‌های کنترل دسترسی باید به طور متناوب تغییر کنند. فرایندهای احراز هویت در مواردی که نیاز به تغییر سریع دارد، می‌تواند به سادگی در سامانه به‌روز می‌شود و خیلی سریع با شرایط جدید سازگار شود.
- یکپارچه‌سازی: eKYC در بیشتر موارد، با استفاده از APIها، قابلیت احراز هویت را به آسانی به سایر سامانه‌ها اضافه می‌کند. همچنین، داده‌های مشتری، اسناد و اطلاعات به طور ایمن در سوابق الکترونیکی او ذخیره می‌شوند و در صورت لزوم در سایر سامانه‌ها قابل استفاده هستند.
- پیگیری/گزارش: داده‌های دیجیتالی جمع‌آوری شده در فرایند احراز هویت قابل انتقال به سیستم‌های تحلیل، ممیزی، پیگیری و گزارش‌دهی هستند و فرصت‌هایی را برای بهینه‌سازی و تحلیل استراتژیک ایجاد می‌کنند.

۲-۴-۱) منافع برای دریافت کننده خدمات (مردم)

- افزایش سرعت دریافت خدمات
- کاهش مراجعات حضوری به دفاتر و دستیابی به مزایای ناشی از آن (ترافیک، زمان، سلامتی و ...)
- فراهم کردن دسترسی شبانه‌روزی و حتی در روزهای تعطیل به خدمات انتظامی
- امکان دریافت خدمات به صورت ساده و آسان

- صرفه جویی در زمان افراد با حذف مراجعه حضوری و منتظر ماندن در دفاتر
- صرفه جویی در هزینه با توجه به کاهش تردد
- کمک به سلامتی و جلوگیری از شیوع در مواردی مانند بحران کرونا
- ایجاد اختیارات سلف‌سرویس و تسهیل فرایندها
- بهبود تجربه مشتری در دریافت خدمات

۱-۵) تحلیل راهبردی طرح

طرح احراز هویت غیرحضوری از نظر راهبردی دارای اهمیت زیادی است چرا که اجرای آن منجر به تحقق بسیاری از اهداف کلان سازمانی نیروی انتظامی و حتی ملی می‌گردد. این سرویس پیش نیاز ارائه خدمات مختلف غیرحضوری است و تجربه موفق آن در پلیس راهگشای فعالیت‌های مشابه در سطح ملی خواهد بود. برخی از راهبردهای ملی و سازمانی که با اجرای طرح eKYC محقق و یا تقویت می‌گردند، عبارتند از:

- توسعه پلیس هوشمند و فناور
- فراهم کردن بستری برای توجه به سلامت شهروندان در شرایط ویروس کرونا
- ارتقاء منزلت شهروندی و رعایت حداکثری حقوق آنها
- ارتقاء امنیت ملی و افزایش اشرافیت اطلاعاتی پلیس
- توسعه خدمات الکترونیک انتظامی
- کاهش اصطکاک و روبرویی ملموس پلیس با مردم
- ارتقاء اعتبار و جایگاه پلیس

۱-۶) خلاصه سوابق طرح

احراز هویت غیرحضوری موضوعی است که است در دهه گذشته مورد توجه بوده است و تاکنون در دنیا به چهار صورت کلی زیر در کشورهای مختلف ارائه شده است:

- احراز هویت و تطبیق هویت (مدل هنگ‌کنگ): در این مدل، احراز هویت به صورت خودکار و با بهره‌برداری از تکنولوژی‌های هوش مصنوعی شامل تطبیق چهره و تشخیص زنده بودن انجام می‌شود. این مدل اگرچه در استارتاپ‌ها و شرکت‌های نوپا به صورت پراکنده در سراسر دنیا به ویژه کشورهای

دارای تکنولوژی دنبال می‌شده اما در سطح ملی، توسط هنگ کنگ ارائه شده و در سال ۲۰۱۹ انواع دیگر این مدل شامل مالزی و اتحادیه اروپا نیز مورد استفاده بوده است.

- تأیید ویدیو (مدل آلمانی): در این مدل برای جلوگیری از جعل هویت در فرآیند e-KYC، تماس‌های ویدیویی دو طرفه با عامل انسانی جایگزینی جلسات حضوری شده است. این مدل از آلمان در سال ۲۰۱۴ شروع شده و در کشورهای دیگر مانند سنگاپور نیز مورد توجه بوده است.
- شناسه دیجیتالی (مدل‌های سوئدی و هندی): در این رویکرد یک سامانه متمرکز ملی برای ایجاد یک شناسه ملی دیجیتال برای هر فرد ایجاد می‌شود که از تکنولوژی‌های زیست سنجی نیز بهره می‌برد. معروف‌ترین نمونه این خانواده، سامانه Aadhaar کشور هند است که از سال ۲۰۰۹ راه‌اندازی شده و حدود ۱.۲ میلیارد نفر از شهروندان هندی کاربر آن هستند.
- ارزیابی جدی در مقابل ارزیابی ساده (مدل انگلستان): در این مدل که در انگلیس و برای مسائل مالی ارائه شده است، مشتریان کم‌ریسک واجد شرایط خاصی می‌توانند شامل ارزیابی ساده (در مقابل ارزیابی جدی) شوند و موسسات مالی می‌توانند با جمع‌آوری نام، تاریخ تولد و اطلاعات آدرس مسکونی و تأیید اطلاعات ارائه شده توسط منابع رسمی (به عنوان مثال ثبت‌نام در انتخابات، احکام دادگاه، اطلاعات موجود در مؤسسات اعتباری) هویت مشتریان را تأیید کنند.

احراز هویت غیرحضوری در ایران نیز اگرچه چند سالی سال است که بر سر زبان‌ها افتاده است اما شاید احراز هویت راه دور در سجام (برای دریافت کد بورسی) را که در تیرماه ۱۳۹۹ ارائه شده، مهم‌ترین کار در این حوزه دانست که از مدل هنگ کنگ پیروی می‌کند و در آن از تکنولوژی‌های تشخیص چهره و تشخیص زنده بودن در کنار عامل انسانی استفاده می‌کند.

۷-۱) هدف و قلمرو طرح

۱-۷-۱) اهداف طرح

هدف اصلی این طرح، مطالعه و بررسی روش‌های احراز هویت غیرحضوری مبتنی بر تشخیص چهره به همراه پیاده‌سازی نسخه پایلوت از آن است. بنابراین اهداف طرح را می‌توان به صورت خلاصه شامل موارد زیر دانست:

- مطالعه روش‌ها و مبانی احراز هویت مبتنی بر چهره و تشخیص زنده بودن
- پیاده‌سازی ماژول تایید هویت مبتنی بر چهره (Face Verification) به صورت پایلوت

- پیاده‌سازی ماژول تشخیص زنده بودن (Liveness Detection) به صورت پایلوت
- پیاده‌سازی مسائل مرتبط با امنیت اطلاعات و تبادل اطلاعات در فرایند احراز هویت
- راه‌اندازی سرویس احراز هویت غیرحضوری در یکی از خدمات موردنظر کارفرما

۲-۷-۱) قلمرو طرح

مفهوم احراز هویت غیرحضوری می‌تواند گسترده در نظر گرفته شود و شامل رویکردهای مختلف و استفاده از زیست‌سنجی‌های مختلف یا روش‌های متنوع تشخیص زنده بودن (Liveness Detection) باشد اما با توجه به اهداف طرح جاری، قلمرو این طرح در این مرحله، فقط شامل احراز هویت از روی تایید هویت با چهره (Face Verification) و تشخیص زنده بودن از روی ویدئو است و محدود به استفاده از آن به صورت یک سرویس در یکی از کاربردهای مدنظر کارفرما است.

۲) فصل دوم: نیازسنجی

۲-۱) شرح نیازمندی‌های عملیاتی و مشخصات محصول (از نگاه کاربر)

همان‌گونه که بیان شد، هدف این طرح، مطالعه و بررسی روش‌های احراز هویت غیرحضوری به همراه پیاده‌سازی یک نسخه پایلوت از این سرویس در یکی از سامانه‌های مورد نظر کارفرما است. مشخصات محصول این طرح (سرویس eKYC) از نگاه کاربر عبارتنداز:

- امکان استفاده آسان از سرویس
- امکان تعامل راحت استفاده کننده با سرویس
- سرعت پاسخگویی مناسب سرویس
- دقت مطلوب در پردازش درخواست‌ها
- امکان ارائه سرویس به طیف وسیعی از استفاده کنندگان
- امکان اتصال استفاده کننده به ناظر انسانی در صورت لزوم
- امن و قابل اعتماد بودن سرویس

برای رسیدن به هدف پروژه، نیازمندی‌های عملیاتی پروژه به شرح زیر است:

- تحلیل وضعیت موجود کارفرما و تعیین دقیق یک نمونه کاربرد (Case Study) با نهایی کردن جزئیات راه حل پیشنهادی با کارفرما (شامل فرایند انجام کار و نحوه استفاده از ماژول‌های احراز هویت غیرحضوری)
- تامین زیرساخت سخت‌افزاری و شبکه‌ای لازم برای اجرای پروژه توسط کارفرما برای نصب و راه‌اندازی سرویس احراز هویت غیرحضوری
- فراهم کردن امکان دسترسی سرویس eKYC پیاده شده به یکی از سامانه‌های موردنظر کارفرما که در نمونه کار برد تعیین شده است
- همکاری و هماهنگی لازم در اجرای پروژه

۳) فصل سوم: توجیهات منطقی برای اجرای طرح

۳-۱) مبانی علمی و فنی

بر اساس قوانین و فرآیندهای ملی و سازمانی، سه نوع سیستم eKYC می‌توان راه‌اندازی کرد [1] :

- **eKYC غیر خودکار (مبتنی بر عامل انسانی):** این روش مبتنی بر تماس (ویدئویی) مشتری با یک عامل انسانی است که در تمام مراحل مشغول فعالیت است. این روش توسط سرویس‌های نویسه‌خوان نوری (OCR) برای تبدیل اطلاعات روی سند هویتی فرد (مانند کارت ملی) به متن و زیست‌سنجی چهره (برای تایید هویت) پشتیبانی می‌شود. در این فرایند، مشتری به یک وب‌سایت/اپ مراجعه کرده است و فرم درخواست را به صورت آنلاین تکمیل می‌کند. پس از آن، این فرایند توسط یک عامل انسانی از سازمان، نهایی می‌شود.
- **eKYC نیمه خودکار:** مشتری کلیه اسناد و مدارک لازم را از طریق سرویس آنلاین و موبایل ارائه می‌کند و سپس با یک مشاور انسانی که به نهایی کردن روند کمک می‌کند، متصل می‌شود. از مشتری خواسته می‌شود یک عکس/ویدئو از خود و یک عکس از کارت شناسایی ارائه کند.
- **eKYC کاملاً خودکار:** این فرآیند کاملاً بدون پشتیبانی انسانی انجام می‌شود. در این حالت نیز در صورت بروز هرگونه مشکل، در نهایت یک مشاور انسانی وارد فرایند می‌شود.

در شکل ۳-۱ مراحل کلی eKYC نشان داده شده است که در آن بعد از ارائه درخواست، تصویر یکی از کارت‌های شناسایی فرد دریافت شده تا توسط سرویس OCR اطلاعات آن استخراج شود، سپس، تصویر چهره فرد برای بررسی توسط الگوریتم‌های احراز هویت مبتنی بر چهره و همچنین تشخیص زنده بودن تصویر، دریافت می‌شود. در هر کدام از مراحل فرایند، می‌تواند پشتیبانی توسط اپراتور انسانی انجام شود. با توجه به اینکه تصویر کارت شناسایی، مخصوصا در حالت راه دور که امکان اعتبارسنجی فیزیک سند (ویژگی‌های امنیت فیزیکی نظیر گیلوش، میکروتکست، هولوگرام و ...) وجود ندارد، به سادگی قابل جعل است، ارزش افزوده ناشی از اسکن کارت و OCR عمدتا آرشیو کردن آن برای بازبینی احتمالی و ورود خودکار اطلاعات (به جای ورودی دستی اطلاعات توسط متقاضی) است.

شکل ۳-۱- مراحل کلی یک سامانه eKYC

فرایند زیست‌سنجی و تشخیص چهره در این روند باید از به روزترین تکنولوژی‌های تجاری بهره‌مند باشد. در این فناوری باید راه‌های جلوگیری از ورود و یا دسترسی افراد غیر مجاز و تقلب نیز در نظر گرفته شده باشد. یکی از مهم‌ترین ویژگی‌های سیستم‌های احراز هویت افراد از راه دور با استفاده از فناوری چهره، تشخیص زنده بودن فرد است. تشخیص زنده بودن معمولا بعد از تایید هویت و یا همزمان با آن انجام می‌شود (شکل ۳-۲).

شکل ۳-۲ احراز هویت راه دور و استفاده از تکنولوژی‌های تایید هویت با تطابق چهره و تشخیص زنده بودن

در راهکار مورد استفاده در این طرح، دو ماژول اصلی تشخیص چهره (Face Recognition) و تشخیص زنده بودن (Liveness Detection) را استفاده می‌کند که در ادامه به بررسی مختصر این دو ماژول پرداخته می‌شود.

۳-۱-۱) تشخیص چهره

شناسایی افراد با توجه به چهره عملی است که اکثرا ما انسان‌ها در زندگی روزمره نیز برای تشخیص هویت استفاده می‌کنیم. توانایی انسان برای انجام این کار قابل توجه بوده و تشخیص چهره‌ی افراد بسیاری که در طول عمر خود دیده‌ایم را حتی با وجود تغییراتی در چهره و یا پس از گذشت سال‌ها انجام می‌دهیم. در بین زمینه‌های زیست‌سنجی نیز، احراز هویت به کمک چهره بسیار مورد توجه قرار گرفته است. مخصوصا در سه دهه‌ی اخیر، موضوع تشخیص چهره از یک موضوع تحقیقاتی علمی عبور کرده و پا به عرصه‌ی تکنولوژی و محصولات تجاری گذاشته است. کاربردهای این تکنولوژی از تشخیص هویت افراد در مرزهای بین‌المللی و جستجو به دنبال مجرمان تا نشانه‌گذاری(Tagging) صورت‌ها در شبکه‌های اجتماعی گسترده شده است.

اولین تلاش‌ها برای دسته‌بندی چهره در مقاله‌ی [1] در سال ۱۸۸۸ میلادی مورد بررسی قرار گرفت. روش پیشنهادی نویسنده در این مقاله بدین صورت است که خطوط نیم‌رخ چهره به صورت برداری ذخیره شود و با محاسبه‌ی میانگین این بردارها و محاسبه‌ی فاصله‌ی هر بردار تا بردار میانگین، دسته‌بندی خطوط انجام شود. در سال‌های اخیر نیز شناسایی و تشخیص چهره در یک تصویر توسط کامپیوتر بسیار مورد توجه قرار گرفته است. علت این امر آن است که تشخیص هویت به کمک چهره مزیت‌هایی نسبت به سایر روش‌های زیست‌سنجی دارد که به صورت مختصر به برخی از آن‌ها اشاره می‌شود.

- بسیاری از دیگر روش‌های زیست سنجی نیازمند قرار گرفتن کاربر در حالتی خاص می‌باشد؛ به عنوان مثال برای ثبت اثر انگشت و یا هندسه‌ی دست نیاز است که کاربر دست خود را در محلی مشخص قرار دهد و همچنین برای اسکن عنبیه و شبکه‌ی چشم نیاز است که فرد در موقعیت مشخصی نسبت به دوربین قرار گیرد. اما در تشخیص چهره (مخصوصا حالت دو بعدی) بدون نیاز به قرار گرفتن کاربر در حالتی خاص می‌توان با دوربین‌هایی از فاصله‌ی دور نیز چهره‌ی افراد را شناسایی کرد.
- روش‌های تشخیص عنبیه‌ی چشم و شبکیه‌ی چشم نسبت به حرکت فرد بسیار حساس هستند. در صورتی که تصویر برداری از چهره با وجود یک دوربین ثابت از فاصله‌ی دور امکان‌پذیر است. با

وجود الگوریتم‌های مناسب برای تشخیص چهره و پیش‌پردازش‌های مناسب، می‌توان مدلی ارائه داد که تا حدی نسبت به تغییرات زاویه‌ی دید، اندازه و روشنایی مقاوم باشد.

- برای دریافت بسیاری از اطلاعات زیست‌سنجی نیاز است که همه‌ی افراد از یک دستگاه استفاده کنند و در طول دریافت این اطلاعات نیاز است که بدن آن‌ها با دستگاه تماس پیدا کند. این امر می‌تواند موجب انتقال میکروب بین افراد شود (به ویژه در بحران‌هایی مانند کرونا). اما تشخیص چهره هیچ نیازی به برخورد فیزیکی با فرد مورد نظر نداشته و استفاده از آن هیچ خطری برای سلامتی انسان ندارد.
- برای احراز هویت از راه دور، استفاده از چهره نیاز به تجهیزات متفاوت (مانند اسکنر اثرانگشت و اسکنر عنبیه) ندارد و دریافت چهره با دوربین‌های تلفن همراه و لپ تاپ‌ها که عمومی‌تر و رایج‌تر هستند، امکان‌پذیر است.

اما تشخیص چهره دارای پیچیدگی‌هایی نیز می‌باشد که باعث می‌شود استفاده از آن سختی‌هایی را نیز به همراه داشته باشد. علت اصلی این امر شباهت فرم کلی چهره‌ی انسان‌هاست و این که ایجاد تمایز بین افراد در دسته‌ای از چهره‌ها که شباهت زیادی با یکدیگر دارند دشوار است. علاوه بر این، چهره‌ی انسان‌ها در طول زندگی حالت ثابتی ندارد. عوامل بسیاری می‌توانند باعث ایجاد تغییرات ظاهری چهره شوند؛ این عوامل را می‌توان به دو دسته تقسیم کرد: عوامل درونی و عوامل بیرونی

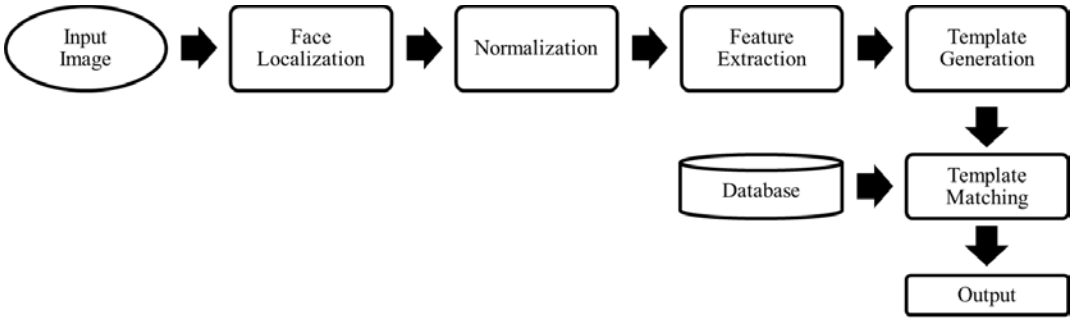
- عوامل درونی به ماهیت فیزیکی چهره مرتبط هستند. عواملی مانند سن، حالت چهره، موهای چهره، عینک، آرایش و... که گاهی می‌توانند در مدت کوتاهی تغییرات زیادی در چهره‌ی فرد ایجاد کنند.
- عوامل بیرونی نیز موجب می‌شوند که ظاهر چهره در مقابل نورهای متفاوت و یا با توجه به مکان ناظر تغییر پیدا کنند. از جمله‌ی تغییراتی که به این صورت ایجاد می‌شود می‌توان به تغییرات نور، ژست صورت، اندازه، وضوح تصویر، تمرکز تصویر، نویز و... می‌باشد.

تحقیقات انجام شده نشان‌دهنده‌ی این موضوع است که سه عامل تغییراتی که به واسطه‌ی سن، تغییرات نور و تغییرات زاویه‌ی تصویربرداری ایجاد می‌شوند، مهم‌ترین مشکلاتی است که سیستم‌های تشخیص چهره با آن مواجه هستند.

می‌توان با صرف نظر از روش‌هایی که بر پایه‌ی دنباله‌ای از تصاویر کار می‌کنند، روش‌های تشخیص چهره را با توجه به مدل چهره و روش جمع‌آوری داده‌ی آن می‌توان به دو دسته تقسیم کرد: ۱) روش‌هایی با محوریت عکس (دوبعدی) و ۲) روش‌های مبتنی بر ساختار سه بعدی چهره. هر دوی این روش‌ها در وهله‌ی اول نیازمند

دریافت تصویر فرد هستند. از آنجا که در این طرح تشخیص چهره دو بعدی مدنظر است، این رویکرد در ادامه بررسی می شود.

عملیات مقایسه در فرآیند تشخیص چهره با استفاده از یک عکس مانند هر سیستم زیست‌سنجی دیگر، مراحلی مشابه شکل ۳-۳ طی می‌شود. به این صورت که ابتدا سیستم یک عکس حاوی چهره دریافت می‌کند، مکان چهره‌ی انسان را در عکس تشخیص می‌دهد، قسمت چهره از عکس بریده شده، نرمال می‌شود و ویژگی‌های آن استخراج می‌شود و بدین ترتیب الگوی تصویر صورت تشکیل می‌شود. در هنگام تشخیص هویت، همان‌طور که در این شکل ملاحظه می‌شود، این الگوی دریافت شده با الگوهای موجود در پایگاه داده مقایسه می‌شود.



شکل ۳-۳ ساختار یک روش تشخیص چهره

بدین ترتیب دو بخش اصلی این الگوریتم ۱) مکان‌یابی چهره و ۲) تشخیص هویت چهره خواهد بود. در ادامه، جزئیات بیشتری در مورد الگوریتم‌های این دو بخش ارائه می‌شود. الگوریتم‌هایی که هر دو بخش را در برمی‌گیرند، الگوریتم‌های تشخیص چهره‌ی تمام اتوماتیک و الگوریتم‌هایی که تنها بخش دوم را شامل می‌شوند الگوریتم‌های نیمه اتوماتیک نامیده می‌شوند.

مکان‌یابی چهره در عکس (Face Detection)

همان‌طور که گفته شد در یک سیستم شناسایی چهره لازم است که مکان یک چهره در تصویر دریافت شده تعیین شود. برای این منظور لازم است که سیستم مکان‌یابی چهره، صورت افراد را در شرایط نوری مختلف و از زوایای مختلف تشخیص دهد و محل دقیق آن را در تصویر (معمولا به وسیله‌ی یک مستطیل) مشخص کند. به این عمل مکان‌یابی چهره در عکس (Face detection) گفته می‌شود.

در کاربردهای واقعی همواره شاهد صحنه‌های پیچیده‌تری از تصویر چهره هستیم که نیاز است مکان چهره از آن استخراج شود. در این حالت الگوریتم‌هایی که در هنگام آموزش تصاویری با پس‌زمینه‌ی ساده را دریافت کرده‌اند به اشتباه می‌افتند و ممکن است بخشی از پس‌زمینه را به عنوان یک چهره تشخیص دهند.
امروزه عمل مکان‌یابی چهره در تصویر در بسیاری از کاربردهای تجاری به صورت بلادرنگ بر روی تصویر انجام می‌شود. الگوریتم‌های مکان‌یابی چهره در دو بخش «بر پایه‌ی تصویر» و «بر پایه‌ی ویژگی» مورد بررسی قرار گرفته است که در ادامه الگوریتم‌های مهم این دسته‌ها بررسی خواهد شد.

مکان‌یابی چهره بر پایه‌ی ویژگی

الگوریتم‌هایی که بر پایه‌ی ویژگی‌های تصویر تشخیص چهره را انجام می‌دهند را می‌توان بر اساس نوع ویژگی‌هایی که استفاده می‌کنند به چند دسته تقسیم کرد: ۱) تحلیل‌هایی در سطح پایین، ۲) تحلیل ویژگی‌ها و ۳) مدل‌های شکل فعال (Active shape models). در تحلیل‌های سطح پایین، الگوریتم‌ها عموما عکس را بر پایه‌ی ویژگی‌های پیکسلی آن (نظیر روشنایی و رنگ آن) تقسیم‌بندی می‌کنند و طبیعت این ویژگی‌ها به گونه‌ای است که مبهم هستند. در تحلیل به کمک ویژگی‌ها، مدل با استفاده از حالت کلی هندسه‌ی صورت، به مفهومی کلی از چهره‌ی انسان دست پیدا می‌کند و ابهام آن‌ها به مراتب از ویژگی‌های سطح پایین کمتر است. در نهایت دسته‌ی مدل‌های شکل فعال است که با مدل مارها (Snakes) که در دهه‌ی ۱۹۸۰ آغاز شده و تا مدل‌های جدیدتری مانند PDM (Point Distributed Models) نیز ادامه داشته است [2] که برای ردیابی لب و مردمک چشم نیز می‌تواند به کار رود. در این کار، روش‌های مکان‌یابی چهره در تصویر در دوسته‌ی «بر پایه‌ی تصویر» و «بر پایه‌ی ویژگی» مورد بررسی قرار گرفت اما دسته‌بندی‌های دیگری نیز برای این روش‌های در برخی منابع ارائه شده که بر مبنای آن این روش‌ها به شکل‌های دیگر تقسیم‌بندی می‌شوند. به عنوان مثال در مقاله‌ی مروری ژانگ در سال ۲۰۱۰ [3] ، روش‌های مکان‌یابی چهره به چهار دسته‌ی زیر تقسیم‌بندی می‌شوند:

- بر پایه‌ی دانش: بر اساس قوانین از پیش تعریف شده، بر مبنای دانش انسان، چهره را در تصویر تشخیص می‌دهد.
- بر پایه‌ی ویژگی‌های ثابت: ساختاری از چهره را پیدا می‌کند که نسبت به تغییرات نور و زاویه‌ی دید مقاوم باشند.
- انتطباق نمونه: با مقایسه‌ی یک تصویر با نمونه‌های تصویر چهره از پیش ذخیره شده، در مورد چهره بودن یا نبودن تصویر جدید تصمیم می‌گیرد.

- بر پایه‌ی ظاهر: مدلی برای چهره بر پایه‌ی نمونه‌های تصویر دیده شده آموزش داده می‌شود و از این مدل برای مکان‌یابی در تصاویر جدید استفاده می‌شود.

مکان‌یابی چهره بر پایه‌ی تصاویر

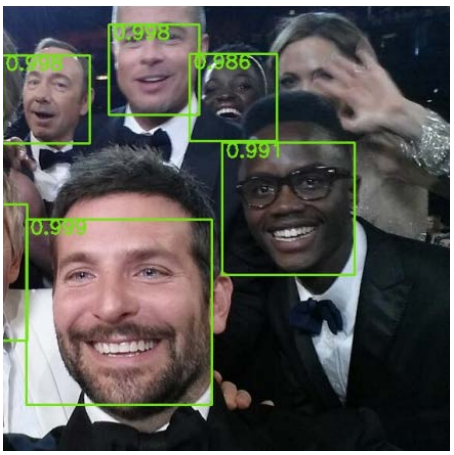
در روش‌هایی که بر پایه‌ی ویژگی‌های چهره بنا شده‌اند، در شرایط محیطی خاص و پیش‌بینی نشده شاهد کاهش شدید دقت الگوریتم‌ها بودیم. در دسته‌ی دیگری از روش‌ها نیز وجود دارند که شناسایی چهره را به عنوان یک مسئله‌ی تشخیص الگو فرموله می‌کنند و بدین ترتیب با استفاده از پایگاه داده‌ای از تصاویر چهره، مدل‌هایی را برای تشخیص چهره آموزش می‌دهند. در این‌گونه روش‌ها در صورتی که تنوع تصاویر پایگاه داده تا حد کافی باشد، حالت‌های پیش‌بینی نشده کمتر برای مدل اتفاق خواهد افتاد. روش‌های متنوعی در این زمینه مورد استفاده قرار گرفته است که از جمله‌ی آن‌ها می‌توان به روش‌های کاهش بعد، روش‌های آماری و همچنین شبکه‌های عصبی مصنوعی اشاره کرد.

یکی از تاثیرگذارترین الگوریتم‌های این زمینه الگوریتم Viola–Jones است که در سال ۲۰۰۱ میلادی توسط Viola و Jones ارائه شد [2] . این روش سه ایده‌ی کلیدی دارد که آن را به یک مکان‌یاب چهره موفق بدل کرده است و امکان مکان‌یابی چهره به صورت بلادرنگ را ممکن ساخته است: ۱) تصاویر انتگرالی ۲) استفاده از الگوریتم AdaBoost به عنوان طبقه‌بند (Classifier) و ۳) یافتن مکان‌های مهم تصویر به کمک دسته‌بندهای متوالی.

پس از این، مقالات بسیاری با الهام از ایده‌های کلیدی این پژوهش اقدام به بهبود الگوریتم‌های تشخیص چهره کردند از جمله آنها در یکی از کارهای سال ۲۰۱۴ با الهام‌گیری از ایده‌ی کلیدی سوم و دنباله‌ای ۲۲تایی از طبقه‌بندها و ترکیب آن با ایده‌های جدیدتر، به بهترین دقت در زمان خودش دست یافت [5] . در روشی دیگر [6] از هیستوگرام‌های طیفی (Spectral histograms) و ماشین بردار پشتیبانی (SVM: Support vector machine) بهره گرفته شده است.

روش Deep Dense Face Detector (DDFD) [7] نیز نمونه‌ی دیگری از الگوریتم مکان‌یابی چهره بر پایه‌ی تصویر است که در اخیرا بر پایه‌ی یادگیری عمیق پیاده‌سازی شده و در عین سادگی نسبت به سایر روش‌ها، بسیار موفق ظاهر شده است. شبکه‌ی عصبی مورد استفاده در این مقاله، بر پایه‌ی معماری معروف AlexNet [8] بنا شده و مانند نسخه‌ی استاندارد آن ورودی‌هایی با ابعاد ۲۲۷×۲۲۷ دریافت می‌کند. در این مقاله با استفاده از روش‌های افزایش داده، در نهایت مرحله‌ی آموزش با تعداد ۲۰۰ هزار تصویر از چهره و ۲۰ میلیون تصویر

غیر چهره انجام شده است. این روش موفق شد بدون نیاز به اطلاعاتی مانند نشانه‌گذاری صورت (Facial landmarks) در دقت مکان‌یابی چهره گامی به سمت جلو بردارد. در شکل ۳-۴ یک نمونه از خروجی این الگوریتم ملاحظه می‌شود.



شکل ۳-۴ نمونه‌ای از خروجی الگوریتم مکان یابی چهره مبتنی بر یادگیری عمیق [7]

در ادامه در مورد بخش دوم (تشخیص هویت چهره) برای تصاویر دوبعدی صحبت می‌شود.

روش‌های تشخیص هویت به کمک چهره

در یک سیستم تشخیص هویت به کمک چهره، پس از مکان‌یابی چهره در تصویر و پیش‌پردازش آن، وارد مرحله‌ی بعدی یعنی استخراج ویژگی از چهره و تشکیل الگوی چهره می‌شود. الگوریتم‌های تشخیص چهره را می‌توان در یک دسته‌بندی کلی به دو بخش تقسیم‌بندی کرد:

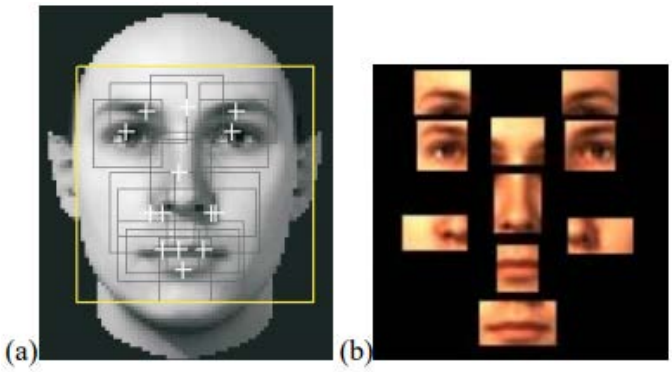
۱) روش‌های کلی

۲) روش‌های بر پایه‌ی اجزای صورت.

در روش‌های کلی، ویژگی‌های کل صورت در یک بردار ذخیره می‌شود. این بردار را می‌توان به عنوان ورودی به طبقه‌بند داد. اما در روش‌های بر پایه‌ی اجزا صورت، هر یک از اجزا به صورت جداگانه مکان‌یابی شده و ترکیب آن اجزا با یکدیگر در تشخیص هویت چهره به کار می‌روند.

به عنوان یک روش بارز که «بر پایه‌ی اجزای صورت» پیاده‌سازی شده، می‌توان به کار ارائه شده در پژوهش [1] اشاره کرد. مزیت این روش نسبت به روش‌های کلی این است که برای تغییر زاویه‌های جزئی در صورت،

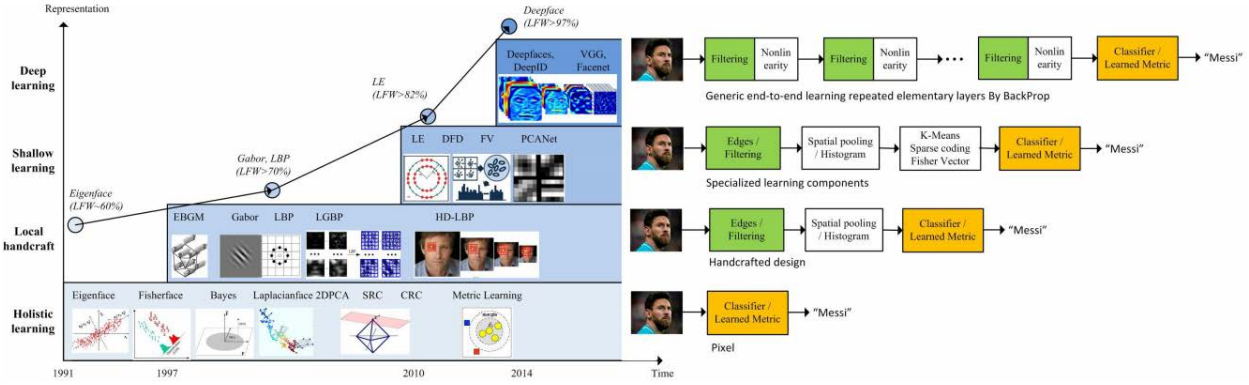
تغییرای که در هر یک از اجزا به تنهایی ایجاد می‌شود، به نسبت تغییرات کلی صورت بسیار کمتر است و بدین ترتیب سیستم نسبت به چرخش و تغییر حالت مقامت بیشتر نشان خواهد داد. شکل ۳-۵ نمایش دهنده‌ی اجزا مورد استفاده در این الگوریتم تشخیص چهره است. این روش این اجزا پس از تغییر اندازه با یکدیگر ترکیب شده و پس از آن با اعمال الگوریتم SVM به صورت «یکی در مقابل سایرین» مدلی برای تشخیص چهره از بین یک پایگاه داده آموزش داده شده است.



شکل ۳-۵ (a) تمامی ۱۴ جزء صورت که مکان‌یابی می‌شوند
(b) اجزا مورد استفاده در الگوریتم شناسایی هویت این روش (۱۰ جزء)

«روش‌های کلی» برای تشخیص چهره از زاویه‌ی روبه‌رو به خوبی عمل می‌کنند اما مقاومت این روش‌ها در مقابل تغییرات زاویه مناسب نیست، به این علت که ویژگی‌های ظاهری با تغییرات زاویه بسیار تغییر پذیر هستند. با هم‌تراز (Alignment) کردن تصاویر چهره با یک تصویر مرجع، پیش از اعمال طبقه‌بند می‌توان تا حدی این مشکل را بهبود داد. در طول هم‌تراز کردن تصویر، نقاط خاصی از تصویر (مانند نقطه‌ی وسط دو چشم و نقاط دو طرف دهان) در نظر گرفته می‌شود و به مختصات مشخصی منتقل می‌شوند. از جمله روش‌های کلاسیک و مهم این زمینه الگوریتم eigenface [9] می‌باشد. این روش که در ابتدای دهه‌ی ۱۹۹۱ میلادی ارائه شد، یکی از زمینه‌های رشد زمینه‌ی تشخیص چهره به شمار می‌رود. الگوریتم‌های بر پایه‌ی تطابق گراف‌ها (Graph matching)، مدل مخفی مارکف (Hidden Markov model)، تطابق ویژگی هندسی (Geometrical feature matching)، تطابق نمونه‌ها (Template matching)، نقشه‌ی خطوط لبه (LEM: Line edge map) و همچنین SVM نیز از دیگر روش‌هایی هستند که در مسئله‌ی تشخیص هویت به کمک چهره به کار رفته‌اند [10] .

یک دسته‌بندی دقیق‌تر از الگوریتم‌های تشخیص چهره و سیر پیشرفت آن‌ها را می توان در شکل ۳-۶ مشاهده کرد [11] .



شکل ۳-۶ سیر تحول الگوریتم‌های تشخیص چهره و دقت هریک در محک LFW (Benchmark) از دهه‌ی ۱۹۹۰ تا به امروز [11]

از یک منظر، الگوریتم‌های تشخیص چهره را می‌توان در این چهار دسته قرار داد:

- یادگیری کلی: در این روش‌ها که بیشتر در دهه‌ی ۱۹۹۰ و اوایل دهه‌ی ۲۰۰۰ میلادی مورد توجه قرار گرفتند، تلاش بر این بود که به کمک یک پراکندگی فرضی، یک بازنمایی با تعداد ابعاد محدود برای هر چهره ارائه شود. اولین و بارزترین نمونه‌ی روش، eigenface است. در سال‌های ۱۹۸۷ و ۱۹۹۰ میلادی در مقالات مختلفی با استفاده از تحلیل مولفه‌های اصلی (PCA: Principal component analysis)، یک بازنمایی بهینه از تصویر چهره به کمک برداری از اعداد ارائه شد و نشان داده شد تصویر هر چهره را می‌توان با همراه داشتن یک مجموعه تصویر استاندارد و یک بردار از ضرایب نمایش داد. پس از آن در سال ۱۹۹۱ میلادی، با الهام از پژوهش‌های قبلی روشی با عنوان eigenface برای طبقه‌بندی تصاویر چهره ارائه شد [9] . این روش‌ها تحت شرایط محیطی مختلف معمولا با مشکل مواجه می‌شوند.
- ویژگی‌های محلی: در دهه‌ی ۲۰۰۰ میلادی، روش‌هایی بر پایه‌ی ویژگی‌های محلی (مانند نتایج فیلترهای گابور) ارائه شد. این روش‌ها تا حدودی نسبت به شرایط محیطی مختلف مقاومت نشان می‌دادند اما فشردگی کافی را نداشتند و همچنین قابلیت ایجاد تمایز در آن‌ها کافی نبود. پژوهش [17] که بر پایه‌ی فیلترهای گابور ارائه شد، به عنوان یک روش بارز در این بخش شناخته می‌شود.

- یادگیری کم‌عمق: در اوایل دهه‌ی ۲۰۱۰ میلادی روش‌هایی ارائه شدند که در آن‌ها توصیف‌گرهای محلی بر پایه‌ی یادگیری معرفی شدند. در واقع در این روش‌ها با توجه به پایگاه داده، فیلترهایی آموزش داده می‌شوند که بیشترین ایجاد تمایز را ایجاد می‌کنند. اما هنوز این روش‌ها مقاومت کافی در برابر تبدیل‌های غیر خطی و پیچیده‌ی چهره را نداشتند. پژوهش [18] نمونه روش ارائه شده در این زمینه است.
- یادگیری عمیق: در سال ۲۰۱۴ میلادی با ارائه‌ی الگوریتم DeepFace توسط تیم تحقیقاتی شرکت Facebook [12] سری دیگری از روش‌های تشخیص چهره بر پایه‌ی یادگیری عمیق کلید خورد. در این روش‌ها بر خلاف روش‌های یادگیری کم‌عمق، تعداد لایه‌های زیادی به صورت متوالی به منظور استخراج ویژگی و تبدیل آن‌ها در نظر گرفته شده و بدین ترتیب در سطوح ویژگی‌های مختلفی با سطوح پیچیدگی مختلف شناسایی می‌شوند و این ویژگی‌ها نسبت به حالت چهره و شرایط محیطی نیز مقاوم هستند. لازم به ذکر است DeepFace برای اولین بار دقت الگوریتم‌های تشخیص چهره را به دقت تشخیص چهره توسط انسان (حدود ۹۷ درصد) رسانید. پس از ارائه‌ی DeepFace الگوریتم‌های دیگری نیز بر پایه‌ی یادگیری عمیق تشخیص چهره کردند از جمله‌ی این روش‌ها می‌توان به FaceID، VGGFace، VGGFace2 و FaceNet اشاره کرد. الگوریتم FaceNet در سال ۲۰۱۵ توسط تیم تحقیقاتی شرکت Google ارائه شد [13] . این روش از یادگیری عمیق برای تشخیص چهره استفاده کرده و بر خلاف روش DeepFace که یک مدل سه بعدی از چهره ساخته و برای هم‌ترازی و شناسایی از آن بهره می‌گیرد، FaceNet روش ساده‌تری برای تشخیص چهره ارائه کرده و با افزایش تعداد پارامترها و لایه‌های شبکه، بار پردازشی بیشتری را بر روی آن قرار داده است.

۳-۱-۲) تشخیص زنده بودن

در فناوری زیست‌سنجی تشخیص زنده بودن فرد یک توانایی کامپیوتری است تا مطمئن شود که سیستم با یک وجود فیزیکی از یک انسان رو به رو است نه یک مصنوع برای کلاهبرداری از سیستم. اگرچه تشخیص چهره یک روش زیست‌سنجی ایده‌آل برای برنامه‌های کاربردی تلفن همراه است، اما هم‌چنان در مقابل تهدیدها آسیب‌پذیر است در این امر ممکن است یک فرد کلاهبردار از یک عکس، فیلم یا ماسک چاپی یا دیجیتالی برای جعل هویت یک قربانی هدفمند یا برای اثبات هویت کاذب استفاده کند. روش‌های تشخیص زنده بودن برای

مقابله با این مشکل طراحی شده‌اند. الگوریتم‌های تشخیص زنده بودن را می‌توان به طور کلی به سه دسته تقسیم نمود [19] :

- تشخیص زنده بودن فعال: این روش مستلزم ایجاد یک چالش و پاسخ است. ممکن است از کاربر خواسته شود در هنگام ضبط چهره عملی را انجام دهد مانند چشمک زدن، لبخند زدن یا جا به جا کردن یک وسیله.
- تشخیص زنده بودن غیرفعال: این روش در پس زمینه برنامه اتفاق می‌افتد و به الگوریتم‌هایی متکی است که می‌توانند آن آثار را در تصویر شناسایی و ارزیابی کنند از جمله ماسک‌ها، بریدگی‌ها، پوست، بافت و سایر شاخص‌های نشان دهنده چهره.
- ترکیبی: یک روش ترکیبی نیازی به تعامل با کاربر ندارد اما با این وجود توسط یک کلاهبردار قابل مشاهده است و باعث می‌شود که از یک رویکرد صرفاً منفعل آسیب‌پذیرتر شود.

از یک منظر دیگر، بر اساس نوع داده ورودی، روش‌های تشخیص زنده بودن را می‌توان به دو دسته تشخیص زنده بودن دوبعدی و تشخیص زنده بودن سه بعدی تقسیم کرد. در دسته تشخیص زنده بودن دوبعدی، از تصاویر دوبعدی برای تحلیل و تشخیص زنده بودن استفاده می‌شود که در صورت عدم استفاده از تشخیص فعال، تصاویر و فیلم‌های دو بعدی امکان گول خوردن را دارند. به طور مثال اگر ویدیوی نمایش داده شده از یک صفحه نمایش 4k در مقابل یک دوربین قرار بگیرد، می‌تواند سیستم را فریب دهد. روش‌های تشخیص زنده بودن دوبعدی رایج شامل چشمک زدن، لبخند زدن، چرخاندن سر، چراغ چشمک‌زن، حالت‌های تصادفی چهره، صحبت کردن و گفتن اعداد تصادفی است. در تشخیص زنده بودن سه بعدی، از احراز هویت سه بعدی استفاده می‌شود که در آن داده‌های مورد نیاز برای این کار نگاشت سه بعدی چهره نامیده می‌شود و نمی‌توان از عکس‌های صورت، فیلم‌ها یا حتی اسکن‌های سه بعدی از چهره استخراج کرد.

در مجموع، روش‌های تشخیص زنده بودن را می‌توان در چهار گروه شکل ۳-۷ دسته‌بندی کرد [14] .

شکل ۳-۷- روش‌های تشخیص زنده بودن چهره

۳-۲) توجیهات امنیتی و راهبردی

از نظر راهبردی و امنیتی، توجیهات ذیل قابل ذکر هستند:

- ارتقاء شأن و منزلت شهروندان و احترام به حقوق آنها با تسهیل و تسریع فرایندها و افزایش کیفیت خدمات از راه دور
- توسعه پلیس دانش‌بنیان و پلیس هوشمند فناور با سامانه‌ها، ابزارها و تجهیزات مدرن که منجر به افزایش توان عملیاتی و اشراف اطلاعاتی می‌گردد.
- لزوم تقویت امنیت ملی با توجه به وجود تهدیدات موجود در منطقه و رویکرد دشمنان برای ضربه زدن به کشور و نظام
- توسعه دولت الکترونیک با بهره‌گیری از ظرفیت‌های موجود و یکپارچه‌سازی سامانه‌ها و بانک‌های اطلاعاتی مختلف

۳-۳) تحلیل بهره‌وری

بهره‌وری طرح از جنبه‌های مختلف، در ادامه تحلیل شده است:

- از نظر افزایش کارآیی سازمان
  - افزایش سرعت ارائه خدمات پلیسی
  - افزایش توان عملیاتی پلیس برای کنترل دسترسی و بهبود امنیت در جرائم مرتبط نظیر جعل هویت، دسترسی غیرمجاز و موارد مشابه
  - یکپارچه‌سازی و تعامل سامانه‌های اطلاعاتی مختلف و ایجاد اشراف اطلاعاتی
  - ایجاد تدریجی بانک اطلاعات بیومتریک
  - امکان ارائه خدمات ۲۴*۷
  - افزایش دقت‌عمل و کاهش خطاها و اشتباه‌های انسانی
  - امکان خدمت‌رسانی به سایر سازمان‌ها و شرکت‌های مرتبط داخل کشور در راستای ارتقای امنیت ملی

- از نظر اقتصادی
  - کاهش هزینه ارائه خدمات پلیسی
  - کاهش تردد داخل شهری
  - کاهش هزینه دریافت خدمات برای شهروندان

- از نظر سلامتی و زیست محیطی
  - کاهش تماس مستقیم شهروندان و عدم تجمع در محیط‌های سربسته (به ویژه در شرایطی مانند بحران کرونا)
  - کاهش تردد داخل شهری و در نتیجه کاهش ترافیک و آلودگی

- از نظر تولید دانش
  - ایجاد و ارتقای دانش فنی در حوزه‌های مختلف در داخل سازمان شامل:
    - کنترل دسترسی مبتنی بر بیومتریک
    - امنیت اسناد الکترونیکی
    - پردازش تصویر

- هوش مصنوعی

- از نظر کسب مهارت و فنآوری
  - کسب مهارت جهت مدیریت بهینه و مکانیزه کنترل دسترسی
  - فناوری تشخیص چهره
  - فناوری تطبیق بیومتریک
  - فناوری تشخیص زنده بودن چهره

۳-۴) بررسی توجیهی هزینه و زمان لازم

از آنجا که این نسخه اول پیشنهاد مجری به کارفرما است، تحلیل هزینه لازم برای اجرای این طرح بعد از دریافت فیدبک از کارفرما از ابعاد فنی و تعهدات مجری در پیشنهاد فعلی ارائه می‌شود چرا که این فیدبک می‌تواند مبتنی بر انجام اصلاحات و تغییرات در تعهدات شود و در هزینه تاثیر بگذارد.

۱-۴-۳) منابع انسانی

مبالغ هزینه‌های نیروی انسانی برای دوره ۱۲ ماه پروژه و به میلیون تومان آورده شده است.

تحصیلات	دکتری		فوق لیسانس		لیسانس		فوق دیپلم		دیپلم		جمع (میلیون تومان)	
عضویت	تعداد	هزینه	تعداد	هزینه	تعداد	هزینه	تعداد	هزینه	تعداد	هزینه	تعداد	هزینه
رسمی	۱	۱۱۷									۱	۱۱۷
قراردادی تمام وقت			۱	۲۱۶	۲	۴۰۸					۳	۶۲۴
قراردادی ساعتی			۲	۳۶۰							۲	۳۶۰
دانشجو	۱	۱۴۴	۱	۹۰							۲	۲۳۴
جمع کل (میلیون تومان)		۲۶۱		۶۶۶		۴۰۸						۱.۳۳۵

۲-۴-۳) اقلام سرمایه‌ای

با توجه به آماده بودن موتورهای تشخیص چهره و تشخیص زنده بودن، از آنها در این پروژه استفاده می‌شود. با توجه به نیاز این موتورها به اختصاصی‌سازی در این پروژه، هزینه لیسانس‌های این دو موتور نرم‌افزاری با ۸۰٪ تخفیف آورده شده است.

ردیف	نام دستگاه	شرکت سازنده یا فروشنده	تعداد یا مقدار لازم	قیمت واحد (میلیون تومان)	کل هزینه (میلیون تومان)
۱	لیسانس موتور تشخیص چهره	شرکت سپیدسیستم	۱	۵۰	۵۰
۲	لیسانس موتور تشخیص زنده بودن	شرکت سپیدسیستم	۱	۶۵	۶۵
جمع (میلیون تومان)					۱۱۵

۳-۴-۳) هزینه‌های مصرفی

ردیف	نام مواد و لوازم مصرفی	شرکت سازنده یا فروشنده	تعداد یا مقدار لازم	قیمت واحد (میلیون تومان)	کل هزینه (میلیون تومان)
۱	ایاب و ذهاب	-	۱۲ ماه	۱	۱۲
۲	چاپ و تکثیر و پذیرایی	-	۱۲ ماه	۱	۱۲
۳	نصب و استقرار و پشتیبانی		۱	۴۵	۴۵
جمع (میلیون تومان)					۶۹

۴-۴-۳) خلاصه هزینه‌های اجرای طرح

ردیف	شرح هزینه	مبلغ کل (میلیون تومان)
۱	هزینه‌های منابع انسانی	۱.۳۳۵
۲	هزینه اقلام سرمایه‌ای	۱۱۵
۳	هزینه اقلام مصرفی	۶۹
جمع کل (میلیون تومان)		**۱.۵۱۹**

یادآور می‌شود که کلیه هزینه‌های مربوط به تامین هرگونه تجهیزات و سخت‌افزار لازم بر عهده کارفرما است.

۳-۵) توجیه و تحلیل اقتصادی و بازگشت سرمایه

اجرای طرح eKYC به دلایل متعدد برای سازمان توجیه اقتصادی داشته و سرمایه صرف شده قابل بازگشت خواهد بود. در ذیل دلایل این ادعا ارائه می‌شود:

- امکان دریافت هزینه از مشتری در ازای ارائه خدمات احراز هویت شده از راه دور فراهم می‌شود که در صورت تعیین نوع خدماتی که از سرویس eKYC استفاده می‌کنند، می‌توان برآورد دقیق‌تری از میزان درخواست و مبلغ هزینه و در نتیجه بازگشت سرمایه داشت.
- امکان مقیاس‌پذیری (Scalability) پروژه و توسعه بهره برداری از سرویس eKYC با افزودن خدمات قابل ارائه از راه دور در فازهای بعدی این پروژه به آسانی و بدون افزایش چشمگیر هزینه فراهم می‌شود که به نوبه خود مشابه تحلیل بیان شده در بند قبلی، امکان بازگشت سرمایه را فراهم می‌کند.
- کاهش نقش مستقیم نیروی انسانی و فراهم شدن امکان بکارگیری آنها در سایر مأموریت‌های سازمانی
- کاهش هزینه‌های سربار ناشی از بکارگیری روش‌های سنتی احراز هویت حضوری (نیاز به فضای فیزیکی و ...)
- فراهم شدن بستر برای کسب درآمد به واسطه ارائه خدمات این سرویس به سایر سازمان‌ها از طریق استعلام آنها از ناجا

۴) فصل چهارم: معماری سیستم

۴-۱) تحلیل نیازها

نیازهای مورد توجه در این طرح برای رسیدن به هدف آن (احراز هویت غیرحضوری) به شرح زیر است:

- ارائه یک سرویس مستقل برای بررسی هویت فرد به منظور احراز هویت او و امکان تولید پاسخ تایید یا رد به صورت درصدی یا بله و خیر
- امکان انجام تطبیق چهره و تشخیص زنده بودن به صورت جدا و ارائه پاسخ به ازای هر کدام از آنها
- ارائه سرویس به صورت API جهت تولید پاسخ به سامانه‌های استفاده کننده از آن
- فراهم کردن دقت مطلوب در احراز هویت
- امکان ارائه با سرعت مطلوب
- در نظر گرفتن ملاحظات امنیتی و مدیریت دسترسی

۴-۲) ارایه راه حل فنی (نقشه‌ی مفهومی سیستم/محصول با شرح)

ساختار روش پیشنهادی و مراحل و ماژول‌های سرویس eKYC این طرح به صورت نشان داده شده در شکل ۴-۱ است. در این پروژه فرض بر آن است که بخش کلاینت توسط سامانه‌ای که از سرویس eKYC استفاده می‌کند، ارائه می‌شود و جزو تعهدات این پروژه نیست و سرویس eKYC روی سرور ارائه می‌شود.

همان‌گونه که در شکل ۴-۱ آمده است، مراحل انجام کار به صورت زیر است:

۱- کلاینت (اپ کارفرما): مشتری بعد از دریافت اپ تلفن همراه پلیس (و یا در صورت صلاحدید ناجا، با مراجعه به وب سایت مربوطه) به بخش ثبت‌نام مراجعه می‌کند و با شروع ثبت‌نام، شماره تلفن همراه خود را که به اسم خودش هست، به همراه کد ملی خود، وارد کرده و ثبت نام را شروع می‌کند.

۲- سرور: صحت شماره تلفن اعلامی مشتری از سامانه شاهکار استعلام گرفته شده و یک کد صورت گذرواژه یکبار مصرف (OTP) تولید و به شماره او پیامک می‌شود.

۳- کلاینت: شماره پیامک شده را در اپ وارد می‌کند تا به سرور بر گردانده شود.

۴- سرور: با تایید دریافت پاسخ رمز یکبارمصرف، درخواست دریافت تصویر و اطلاعات هویتی فرد از طریق استریم کردن ویدئویی که در آن یکی از اسناد هویتی فرد (کارت ملی و گواهی‌نامه) نمایش داده می‌شود، ارسال می‌شود. استفاده از کارت ملی به دلیل امکان استعلام از ثبت احوال در نظر گرفته شده

است. در صورتی که امکان استعلام از سامانه‌های ناجا (گواهی‌نامه، گذرنامه یا کارت پایان خدمت) فراهم باشد، پیشنهاد می‌شود از یکی از آنها (مثلا گواهینامه) در این پروژه استفاده شود.

۵- کلاینت: از دوربین گوشی (یا لپ‌تاپ در صورت استفاده از نسخه وب) ویدئوی مشتری به صورت زنده به سمت سرور استریم می‌شود. مشتری با گرفتن قسمت رو و پشت سند هویتی (کارت ملی، گواهی‌نامه) خود، تصویر سند هویتی خود را (از طریق ویدئو) ارسال می‌کند و سمت سرور با پردازش ویدئو آن را دریافت می‌کند. برای مدیریت پیچیدگی‌ها و خطاهای ناشی از سرویس نویسه خوان نوری (OCR)، در این پروژه فرض می‌شود فیلدهای اطلاعاتی لازم روی اسناد هویتی که برای استعلام گرفتن از ثبت احوال یا پایگاه داده ناجا ضروری است (مانند نام و نام خانوادگی، کد ملی و سریال کارت) به صورت دستی وارد شود و ویدئوی استریم شده فقط با هدف نظارت دریافت می‌شود.

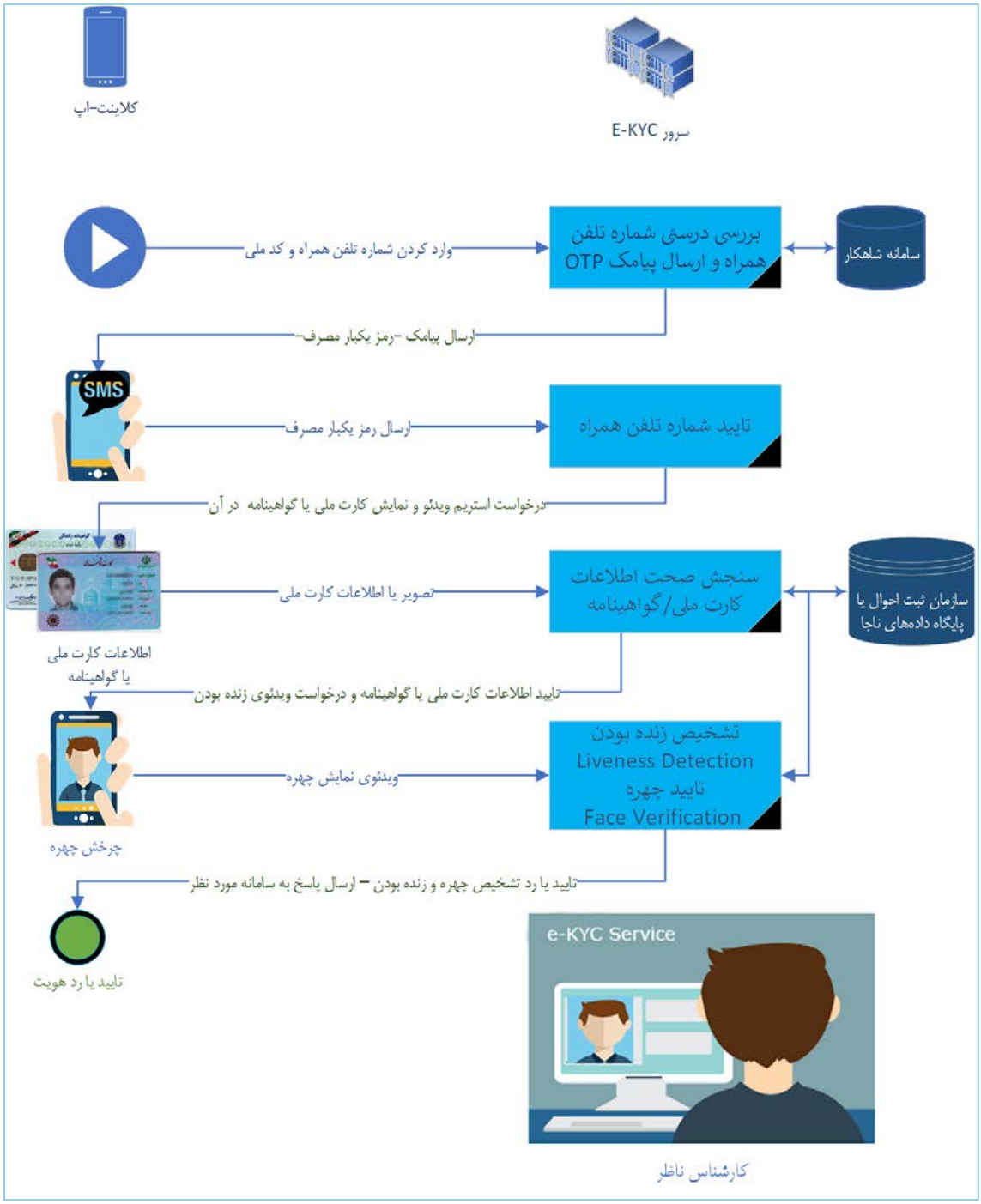
۶- سرور: با دریافت اطلاعات هویتی کارت ملی/گواهینامه مشتری در سمت سرور، از ثبت احوال/ناجا در مورد فعال بودن این کارت و دریافت اطلاعات آن استعلام می‌شود (کد ملی فرد در زمان ثبت نام دریافت شده است). اطلاعات دریافتی از استعلام، به عنوان اطلاعات هویتی مرجع جهت مقایسه (به ویژه تصویر چهره) استفاده می‌شود.

۷- کلاینت: بعد از تایید اطلاعات هویتی کارت ملی، به منظور تشخیص چهره (Face Recognition) و تشخیص زنده بودن تصویر (Liveness Detection) از مشتری خواسته می‌شود که سر خود را به طرف راست و چپ بچرخاند و یا به صورت تعیین شده پلک بزند.

۸- سرور: ابتدا با استفاده از مقایسه تصویر دریافتی مشتری (که یک یا چند مورد از آن به صورت تصادفی از ویدئوی استریم شده استخراج می‌شود) و عکس او در سامانه ثبت احوال/ناجا (عکس داخل کارت ملی/گواهینامه) به تایید چهره (Face Verification) پرداخته می‌شود و سپس واحد تشخیص زنده بودن (Liveness Detection) به بررسی تصویر ارسالی از نظر شاخص‌های واقعی بودن تصویر با پردازش ویدئوی ارسالی و تحلیل حرکات فریم‌های متوالی تصویر از نظر شاخص‌های مرتبط مانند بافت، تغییرات حالت چهره، جابجایی محل اندام‌های روی صورت و ... می‌پردازد. بعد از تایید هویتی فرد، این موضوع به سامانه بهره‌بردار از سرویس eKYC اعلام می‌شود تا مراحل بعدی کار توسط آن سامانه دنبال شود.

نکات تکمیلی راهکار پیشنهادی موارد زیر هستند:

- ناظر انسانی: به عنوان یک قابلیت اصلی، همواره یک نفر «ناظر انسانی» شاهد ویدئوی ارسالی به سرور و نظارت بر آن است و در صورت لزوم می‌تواند با مشتری نیز صحبت کند. با توجه به حساسیت روی موارد امنیتی در برخی خدمات، پیشنهاد می‌شود یک نفر ناظر انسانی از همان ابتدا مشابه مکالمه دوطرفه با مشتری همراه باشد تا بر صحت انجام کارها نظارت کند.
- ارتباط با سرویس‌های ناجا: در صورت لزوم به ارتباط با سایر سرویس‌های موردنظر ناجا در فرایند احراز هویت (مانند کنترل‌های ضروری دیگر مثل استعلام‌ها و بررسی لیست‌های سیاه و ...)، راهکار پیشنهادی در قالب فراخوانی API مربوطه، امکان برقراری ارتباط‌های لازم را در سمت سرور دارد.



شکل ۴-۱ مراحل سرویس eKYC پیشنهادی

۴-۳) تشریح اجزای سیستم

همانگونه که تشریح شد، در راهکار پیشنهادی از تکنولوژی‌های مختلفی استفاده می‌شود که از مهم‌ترین بخش‌های آن ماژول‌های هوشمند آن است که با بهره‌گیری از الگوریتم‌های یادگیری ماشین و هوش مصنوعی ما در رسیدن به هدف اصلی یاری می‌کنند. واحدهای اصلی مورد استفاده در این بخش و مشخصات آنها عبارتنداز:

- مکان یابی چهره (Face Detection): در این ماژول با بهره‌برداری از یک روش مبتنی بر شبکه عصبی عمیق، مکان چهره‌ها در یک تصویر استخراج می‌شود. در این ماژول با دریافت یک یا چند تصویر، تمامی چهره‌های موجود در هریک از تصاویر را تشخیص داده و مکان آن‌ها را به عنوان خروجی بازمی‌گرداند.
- تشخیص چهره (Face Recognition): ماژول تشخیص چهره مورد استفاده با الهام از روش‌های یادگیری عمیق، یکی از کاراترین الگوریتم‌های تشخیص چهره است که با دریافت چهره از ویدئو در حال پخش، بعد از تشخیص محل چهره (Face Detection)، نرمال کردن تصویر و حذف نویز، کار تطبیق چهره را با عکس مرجع (در این راهکار، عکس مورد استفاده در کارت ملی هوشمند) انجام می‌دهد. خطای تشخیص این الگوریتم روی دادگان مرجع LFW کمتر از ۰.۶٪ است.
- تشخیص زنده بودن (Liveness Detection): آسیب‌پذیری سیستم‌های تشخیص چهره در برابر حملات نمایش چهره غیر زنده (که به عنوان حملات مستقیم یا حملات کلاهبرداری شناخته می‌شود) یکی از نگرانی‌های اصلی استفاده از این روش زیست‌سنجی است. هدف حمله نمایش (Presentation Attack)، دور زدن سیستم تشخیص چهره با استفاده از نمایش چهره مصنوعی است. استفاده‌های رایج از چهره غیر واقعی شامل عکس چاپ شده، نمایش الکترونیکی یک عکس صورت، پخش ویدیو با استفاده از یک نمایشگر الکترونیکی و ماسک‌های صورت سه‌بعدی می‌باشد. با این حال برای مقابله با این ریسک، الگوریتم حملات تشخیص چهره زیادی ارائه شده است که با شناسایی آنها حملات احتمالی و هدفمند را می‌توان کاهش داد. در راهکار پیشنهادی، یک روش دو مرحله‌ای برای این موضوع در نظر گرفته شده است که شامل تشخیص زنده بودن در تصاویر ویدئویی با تحلیل بافت تصویر چهره است و همچنین تشخیص حرکات داخل تصویر (چرخاندن سر یا پلک زدن) و استخراج اطلاعات لازم از آن است. برای کاهش خطاهای این ماژول، می‌توان از سایر روش‌های توسعه داده شده توسط پیشنهاد دهنده (شامل روش‌های خواندن لب (Lip Reading) و تشخیص گفتار (Speech

Recognition)) نیز استفاده کرد اما برای مدیریت مقیاس و پیچیدگی پروژه، به همراه کاهش سربار محاسباتی، استفاده از این دو در این مرحله از پروژه پیشنهاد نمی‌شود و توصیه می‌شود در فاز توسعه پیاده‌سازی شوند. هرچند در صورت تاکید کارفرما، می‌توان این ماژول‌ها را در همین فاز هم به سرویس افزود.

سایر اجزای سامانه پیشنهادی عبارتنداز:

- مدیریت درخواست‌ها: وظیفه این زیرسیستم دریافت درخواست‌ها از سامانه‌های استفاده‌کننده از سرویس eKYC، مدیریت ارتباط آنها با سایر زیرسیستم‌های سرویس eKYC و تولید پاسخ به سامانه سرویس‌گیرنده می‌باشد.
- استعلام: ظیفه این ماژول دریافت استعلام از سامانه‌های بیرونی مانند سامانه شاهکار، سامانه ثبت احوال و سامانه‌های ناجا می‌باشد.
- گزارش‌گیری: این زیرسیستم کار ارائه گزارش‌های مختلف از عملکرد و فعالیت‌های سرویس eKYC را فراهم می‌کند.
- مدیریت کاربران و کنترل دسترسی: وظیفه این زیرسیستم، مدیریت کاربران استفاده‌کننده از سرویس eKYC و کنترل دسترسی‌های آنها به سایر زیرسیستم‌های سرویس می‌باشد.

۴-۴) جداول مشخصات فنی سیستم (و اجزای آن)

مشخصات فنی سیستم و اجزای آن به شرح بیان شده در جدول ۴-۱ است.

جدول ۴-۱ مشخصات فنی سیستم و اجزای آن

سیستم/اجزا	شاخص	توضیح
سیستم	قالب ارتباط با سرویس	به صورت API است
	سرعت پاسخگویی	متناسب با حجم درخواست همزمان و پیکره‌بندی سرور ارائه شده توسط کارفرما تعیین می‌شود.
	دسترسی پذیری	بر اساس دسترسی‌پذیری سرور ارائه شده توسط کارفرما و سیاست‌های کارفرما تعیین می‌شود.

	پهنای باند	متناسب با تعداد درخواست‌های همزمان و نحوه استفاده از سرویس (چند ثانیه ویدئو و چند بار فراخوانی به ازای هر درخواست) تعیین می‌شود.
مدیریت درخواست‌ها	–	این ماژول توان مدیریت همه درخواست‌ها و تولید پاسخ مناسب برای آنها را دارد.
استعلام	–	این ماژول از همه منابع بیرونی متناسب با نوع نیاز استعلام می‌گیرد. سرعت و دسترسی پذیری این زیرسیستم وابسته به سرعت و دسترسی پذیری منابع استعلامی است.
گزارش‌گیری	–	امکان گزارش‌گیری از جزئیات درخواست‌ها و فعالیت‌های هر سامانه بهره‌بردار از سرویس با فیلترهای مختلف فراهم می‌شود.
مدیریت کاربران	امنیت	تامین امنیت و کنترل مدیریت دسترسی‌ها برای کاربران مجاز تعریف شده در سرویس eKYC در این زیرسیستم انجام می‌شود.
مکان‌یابی چهره	سرعت و دقت	سرعت این ماژول وابسته به پیکره‌بندی سرور است ولی می‌تواند روی سرور مناسب زیر دو ثانیه انجام شود. دقت تشخیص برای تصاویر گرفته شده از روبرو و در شرایط نوری مناسب ۹۹.۹٪ است.
تایید هویت چهره	سرعت و دقت	سرعت این ماژول وابسته به پیکره‌بندی سرور است ولی می‌تواند روی سرور مناسب زیر دو ثانیه انجام شود. دقت تشخیص روی دادگان LFW حدود ۹۹.۴٪ است.
تشخیص زنده بودن	سرعت و دقت	سرعت این ماژول وابسته به پیکره‌بندی سرور و نوع تحلیل (فقط ویدئو، پلک زنی و ...) است و می‌تواند از ۳ تا ۱۰ ثانیه (بسته به نوع تحلیل) انجام شود.

۵) فصل پنجم: امکان‌سنجی

۵-۱) بررسی سوابق طرح (مقایسه با محصولات مشابه از نظر فناوری و ساخت)

برای احراز هویت انسان‌ها، از قدیم روش‌های مختلفی پیشنهاد شده است که خلاصه آنها را می‌توان در سه دسته نشان داده شده در شکل ۵-۱ بیان کرد. از میان این روش‌ها، اگرچه هر سه دسته را می‌توان برای احراز هویت راه دور استفاده کرد، اما استفاده از روش‌های مبتنی بر زیست‌سنجی به دلیل سادگی و هزینه کمتر آنها مطلوب‌تر بوده است، هرچند در این فرایند معمولا از آنچه که افراد دارند (مانند کارت شناسایی) نیز بهره گرفته می‌شود.

شکل ۵-۱ انواع رویکردهای احراز هویت

از آنجا که دیجیتالی شدن در اغلب حوزه‌ها همچنان به رشد جهانی خود ادامه می‌دهد، انتظارات مشتریان از تجربیات کاملاً دیجیتالی در قلمرو خدمات مالی، بیمه، مخابراتی، پلیسی و ... گسترش یافته است. برای منعکس کردن این تغییر، طی چند سال گذشته وضع‌کنندگان به آرامی دستورالعمل‌های جدید eKYC را ارائه می‌دهند تا به موسسات مختلف اجازه دهد بررسی‌های KYC را انجام دهند و برنامه‌های مشتری را به صورت الکترونیکی تصویب کنند. در این زمینه، موسسات مالی پیش‌روتر از سایرین بوده‌اند.

با همه‌گیر شدن کوید ۱۹، در تاریخ ۱ آوریل، کارگروه ویژه اقدام مالی(FATF) بیانیه رسمی صادر کرد و به استفاده از فناوری، از جمله فین‌تک، رگ‌تک و سوپ‌تک برای ورود به سیستم دیجیتال مشتری، تشویق کرد. ارائه‌دهندگان خدمات مالی وظیفه دارند مشتری‌های خود را شناسایی کرده و خطراتی که ممکن است ایجاد

شوند را قبل از ارائه خدمات درک کنند. با روش‌های نظارت دقیق مشتری، از طرف عرضه، هزینه‌های انطباق برای ارائه‌دهندگان کاهش می‌یابد و ارائه خدمات به مشتریان کم درآمد سودآورتر می‌شوند. از طرف تقاضا، افتتاح حساب تسریع می‌شود، با دسترسی به تلفن همراه انجام معاملات آسان‌تر می‌شوند. برای اینکه سیستم‌های eKYC مؤثر باشند، باید از زیرساخت قوی شناسه‌ی دیجیتال با پوشش گسترده حمایت شود. بانک جهانی شناسه دیجیتال را به عنوان مجموعه‌ای از خصوصیات هویتی ثبت‌شده و ذخیره شده الکترونیکی تعریف می‌کند که یک شخص را در یک بستر مشخص توصیف می‌کند و برای معاملات الکترونیکی مورد استفاده قرار می‌گیرد. در سطح ملی، بسیاری از وضع‌کنندگان پیش از این دستورالعمل‌های تجدید نظر در مورد تأیید مشتری از راه دور صادر کرده‌اند تا به مؤسسات مالی کمک کنند تا از تداوم تجارت و تعهد مشتری در هنگام تعطیلی اطمینان حاصل کنند. به عنوان مثال، نهادهای مالی نیوزلند از نسخه‌های اسکن شده اسناد به جای اصل و از احراز هویت الکترونیکی به جای تماس چهره به چهره با مشتریان، استفاده کرده‌اند.

به همین ترتیب، بورس اوراق بهادار هند اکنون به سرمایه‌گذاران کارهای خارجی اجازه می‌دهد نسخه‌های اسکن شده اسناد مورد نیاز را پس از ثبت‌نام ارائه دهند، در حالی که بانک مرکزی فیلیپین به طور موقت الزام ارائه کارت شناسایی معتبر را در هنگام ورود به سیستم مشتری برداشته است (اما این فقط مربوط به معاملات کوچک است). در اوایل سال ۲۰۲۰، واحد اطلاعات مالی بنگلادش راهنمایی‌های جدیدی را منتشر کرد که به موسسات مالی دستور می‌داد رویکرد مبتنی بر ریسک را برای eKYC دنبال کنند. بسته به ریسک مرتبط با مشتری، مراحل ساده یا معمولی eKYC باید رعایت شود. اگرچه به طور منظم eKYC به مراحل بیشتری برای جمع‌آوری اطلاعات نیاز دارد، هر روشی باید به یکی از دو مدل مبتنی بر زیست‌سنجی، یا استفاده از تطبیق اثر انگشت یا تطبیق چهره، پایبند باشند.

۱-۱-۵) چهار مدل eKYC در دنیا

با نگاهی به مشترکات و تفاوت‌های موجود بین طرح‌های eKYC موجود در سرتاسر جهان، می‌توان بسیاری از آن‌ها را به تعداد محدودی از مدل‌ها دسته‌بندی کرد که چهار گروه زیر می‌تواند یک دسته‌بندی مناسب باشد [20].

احراز هویت و تطابق هویت: مدل هنگ‌کنگ

مقررات اولیه eKYC رویکردی مبهم در الزامات خود دارند. نهادها بجای الزام به فناوری‌ها یا فرآیندهای خاص، راهنمایی‌های کلی را ارائه دادند و برای تجزیه و تحلیل و تصویب/رد مراحل خاص توسط موسسات مالی به طور دقیق، فرایندهای خاص ارائه نشده است.

این مدل که از سال ۲۰۱۱ با قانون مبارزه با پولشویی در هنگ کنگ شروع شده و در فوریه سال ۲۰۱۹ مؤسسه پولی هنگ کنگ، بخشنامه‌ای به روز شده درمورد "ورود و ثبت از راه دور از مشتری‌های حقیقی" را منتشر کرد. راهنمایی جدید یک لیست خاص از اقدامات مورد نیاز را ارائه نمی‌دهد، اما می‌گوید که فناوری اتخاذ شده برای مقاصد از راه دور باید تأیید هویت و تطابق هویت را انجام دهد (به عنوان مثال تشخیص چهره، تشخیص زنده بودن فرد).

انواع دیگر این مدل هنگ‌کنگ، شامل مالزی و کلیت اتحادیه اروپا است. در دسامبر سال ۲۰۱۹، بانک نگارا مالزی، پیش‌نویس الزامات مربوط به مؤسسات مالی را که به دنبال اجرای eKYC هستند، از جمله استفاده از فناوری زیست‌سنجی، کشف تقلب و تشخیص زنده بودن فرد را صادر کرد.

روند مثبت این مدل انعطاف پذیر این است که به اسناد هویتی و همچنین تشخیص زنده بودن متکی است – این است که منجر به اکوسیستم گسترده‌ای از راه حل‌ها می‌شود که مستعد حمله نیستند و می‌توانند در کل سیستم مالی کار کنند. یکی از عدم قطعیت‌ها دراین روش می‌تواند این باشد که الزامات نسبتاً مبهم باعث ایجاد تیم‌های مسئول جدید برای هرگونه فناوری‌های نوآورانه جدید می‌شوند که می‌خواهند آن‌ها را تطبیق دهند.

تأیید ویدیو: مدل آلمانی

راه دیگر – به نوعی سنتی‌تر – برای جلوگیری از جعل هویت جعلی در فرآیند eKYC، جایگزینی جلسات حضوری با تماس‌های ویدیویی دو طرفه است. آلمان یکی از اولین حوزه‌های قضایی بود که رویکرد احراز هویت ویدیویی (تصویری) را اتخاذ کرد. وضع‌کننده‌ی قوانین در آلمان در بخشنامه ۲۰۱۴ که در سال ۲۰۱۷ به روز شد، برای اولین بار، شناسایی و تأیید مشتری را از طریق یک لینک ویدیویی دو طرفه مستقیم با یک متخصص امکان‌پذیر کرد.

نمونه‌های قابل توجه دیگر بانک مرکزی هند است، که در ژانویه سال ۲۰۲۰ اعلام کرد که KYC ویدیویی به عنوان گزینه‌ای برای احراز هویت مشتری باشد. در هند، صنعت مالی مدت‌هاست که به دنبال مجوز برای اجرای KYC ویدیویی برای جلوگیری از پرداخت هزینه‌های بالای دسترسی فیزیکی

به مشتریان در مناطق دور افتاده است. به همین ترتیب، در سال ۲۰۱۸، مؤسسه پولی سنگاپور صریحاً پیشنهاد کرد که کنفرانس ویدئویی در زمان واقعی برای تأیید هویت باید "ارتباط چهره به چهره قابل مقایسه" باشد. احراز هویت ویدیویی مزیت جلوگیری از سرقت تصویری هویت را دارد اما این کار، مسئولیت زیادی را برای تیم مدیریت ایجاد می‌کند. سیل تماس‌های ویدیویی دریافتی بسیار زیاد خواهد بود و در مقیاس‌پذیری در مقایسه با روش‌های حضوری هیچ مزیتی نخواهد داشت.

رویه‌ی شناسه دیجیتالی: مدل‌های سوئدی و هندی

یکی از رویکردهای بنیادین eKYC، ایجاد شناسه‌های دیجیتال فدرالیک یا برنامه‌های متمرکزکننده KYCاست. این مدل یک منبع رسمی معتبر از اطلاعات – که همیشه دولتی نیست – را موظف می‌کند که موسسات مالی می‌توانند هنگام بررسی هویت مشتری به آن مراجعه کنند. هند با سیستم EKYC Aadhaarخود یکی از پیشگامان این مدل بود. Aadhaar در سال ۲۰۰۹ راه‌اندازی شد و به عنوان آرکیپید جهانی eID شناخته می‌شود، اکنون بیش از ۱.۲۱ میلیارد کاربر را به خود اختصاص می‌دهد. به بیان ساده‌تر، Aadhaar یک شماره شناسایی شخصی است که توسط سازمان شناسایی منحصر به فرد هند[1] (UIDAI) به منظور ایجاد هویت منحصر به فرد برای هر مشترک صادر شده است. متأسفانه ، یک طرح متمرکز، مستعد خطرات بزرگی از حملات هکری یا مشکلات اجرای آن است. Aadhaar دقیقاً چنین اتفاقی را در ژانویه سال ۲۰۱۹ مشاهده کرده است، هنگامی که دولت هند اعلام کرد که میلیون‌ها پرونده زیست‌سنجی کامل از کاربران Aadhaar به بیرون درز کرده است و باعث متوقف شدن موقت هرگونه استفاده غیردولتی از سیستم شد.

سوئد نمونه جالب دیگری از انواع دیگر طرح‌های شناسایی دیجیتال را ارائه می‌دهد: یک طرح شناسایی دیجیتالی فدرال شده که ابتدا توسط بانک‌ها معرفی شد، اما شناسه‌های الکترونیکی که به این ترتیب ایجاد شده‌اند اکنون به عنوان شکلی از شناسایی توسط مقامات دولتی نیز پذیرفته شده‌اند. گروهی از بانک‌های بزرگ سوئدی – از جمله بانک دانسکه سیستم BankID را در سال ۲۰۰۳ معرفی کردند. تخمین زده می‌شود که ۸۰٪ از جمعیت سوئد اکنون به طور مداوم از آن استفاده می‌کنند. اطلاعات هویتی در این طرح در بانک کاربر قرار دارد، نه در مکان متمرکز و بنابراین کمتر مستعد حمله هک هستند.

[1] Unique Identification Authority of India (UIDAI)

در سنگاپور ، دولت در ماه مه ۲۰۱۶ پلتفرم داده‌های شخصی با نام MyInfo را معرفی کرد تا تأیید هویت را در معاملات آنلاین ساده کند. با طراحی یک سیستم بسیار ایمن که بدون توزیع داده‌های گفته شده در مکان‌های مختلف کار می‌کند، در حفاظت از داده‌های کاربر موفق‌تر عمل کرده است.

ارزیابی جدی در مقابل ارزیابی ساده: مدل انگلستان

در حالی که اکثر برنامه‌های KYC و الزامات AML رویکردی مبتنی بر ریسک (توصیه به سطوح مختلف نظارت بر اساس ریسک بالقوه مرتبط با مشتری) دارند، سازمان رفتار مالی در انگلیس مسائل را به سطح دیگری برده است. در این رویکرد، مشتریان کم‌ریسک واجد شرایط می‌توانند شامل ارزیابی ساده (در مقابل ارزیابی جدی) باشند و موسسات مالی می‌توانند با جمع‌آوری نام، تاریخ تولد و اطلاعات آدرس مسکونی و تأیید اطلاعات ارائه شده توسط منابع رسمی (به عنوان مثال ثبت‌نام در انتخابات، احکام دادگاه، اطلاعات موجود در مؤسسات اعتباری) هویت مشتریان را تأیید کنند.

طبق قوانین، معیارهای تأیید اعتبار ۲ + ۲ نامیده می‌شود زیرا به مؤسسات مالی اجازه می‌دهد تا با تطبیق ۲ مورد از اقلام اطلاعاتی داده شده توسط مشتری با ۲ قلم داده ارائه شده توسط یک منبع داده قابل اعتماد، مشتری را تایید کنند. به عنوان مثال، نام شخص به علاوه تاریخ تولد آن‌ها یا نام به علاوه آدرس آن‌ها. آشنایی با کارکردهایی مانند مقایسه چهره، تأیید هویت مبتنی بر هوش مصنوعی و تشخیص زندگی افزایش یافته است و در نتیجه، اشاراتی به چنین نوآوری‌ها به صراحت در مقررات در سراسر جهان گنجانده شده است.

از بین تمام مدل‌های مورد بررسی، آنهایی که محبوب‌ترین استانداردها را نشان می‌دهند، مواردی هستند که در هنگ کنگ (تأیید هویت/ تطبیق هویت) و سنگاپور (شناسه دیجیتالی) اتخاذ شده‌اند. وضع‌کننده هنگ‌کنگ با پذیرش راه‌حل های مهم و برجسته در عمل، تعهد خود را به نوآوری نشان داد بدون آنکه محدودیت‌های بیش از حد محدودکننده‌ای را برای استفاده از نرم‌افزارها یا روش‌های دقیق پیروی از آن اعمال کند.

در عین حال، شناسه دیجیتالی طرح‌های فوق‌العاده مفید برای استانداردسازی شناسایی مشتری برای موسسات مالی، کاهش هزینه‌ها و ساده کردن فرایندهای داخلی تا حد بالایی را نشان داده‌اند. اگرچه معرفی طرح‌های دیجیتالی که از فناوری‌های جدید به عنوان مثال بلاکچین استفاده می‌شوند، ممکن است هنوز مدتی طول بکشد.

۵-۱-۲) هند پیش‌رو در احراز هویت الکترونیکی

برای احراز هویت غیرحضوری جهان از هند یاد می‌گیرد! زیرا برنامه Aadhaar هند با موفقیت، دیجیتالی‌سازی شناسه را برای بیش از ۹۰٪ از جمعیت هند ممکن ساخته است. اکثر بانک ها در هند توانسته‌اند روند شناسایی از مشتری را با استفاده از KYC دیجیتالی سرعت بخشند. تعداد فزاینده‌ای از کشورهای در حال توسعه eKYC را اجرا می‌کنند یا قوانینی برای حمایت استفاده از آن در کشورهایی مانند بنگلادش، کنیا، پاکستان، تانزانیا و فیلیپین در دست تهیه هستند. اما هند از نظر مقیاس برنامه eKYC خود، که در سال ۲۰۱۲ آغاز شد، متمایز است. تجربه این کشور تا به امروز نشانگر تعادل دشوار سیاست‌گذاران در هنگام استفاده از سیستم‌های شناسه دیجیتال در برابر نگرانی‌های مربوط به امنیت داده‌ها است.

احرازهویت منحصر به فرد هند یا برنامه Aadhaar توجه جهانیان را به دلیل ابتکار، رشد سریع و مقیاس به طور کامل جلب کرده است. این برنامه به هر یک از ثبت‌کنندگان یک شماره شناسایی ۱۲رقمی منحصر به فرد مرتبط با حداقل اطلاعات شخصی (شامل نام، جنسیت، تاریخ تولد، و یک عکس دیجیتالی) و اطلاعات زیست‌سنجی (اثر انگشت و اسکن عنبیه) اختصاص می‌دهد که می‌تواند برای تأیید اعتبار استفاده شود. از آن‌جا که سازمان شناسایی منحصر به فرد هند (UIDAI) اولین شناسه Aadhaar را در سال ۲۰۱۰ صادر کرد، بیش از ۱.۲ میلیارد نفر (نزدیک به ۹۰ درصد از جمعیت هند) در این برنامه ثبت‌نام کرده‌اند. هدف اصلی بیان شده Aadhaar کاهش کلاهبرداری در برنامه یارانه گسترده دولت با از بین بردن کپی‌های تکراری بود. با این حال، استفاده از شناسه به سرعت در مناطق دیگر از جمله تشکیل اظهارنامه مالیات بر درآمد، تأیید اعتبار پرداخت و اسناد امضای دیجیتالی گسترش یافت. دولت در تلاش است تا با همکاری با کارشناسان فناوری، کارایی سیستم را گسترش دهد و از آن‌ها برای توسعه برنامه‌هایی که به پایگاه داده شناسه‌ها وصل می‌شوند، استفاده کنند.

eKYC مستقر در Aadhaar به مشتریان اجازه می‌دهد تا به صورت الکترونیکی اطلاعات جمعیتی و شخصی خود را از جمله اثبات هویت، اثبات آدرس، تاریخ تولد و جنسیت را به ارائه‌دهندگان مالی که می‌توانند آن را در زمان واقعی تأیید کنند، ارائه دهند. اما استفاده از Aadhaar برای KYC نگرانی‌های مربوط به حریم خصوصی را نیز برانگیخته است. در حالی که سیستم Aadhaar در ابتدا برای ارسال پاسخ‌های "بله/خیر" به سؤالات طرفین خارج طراحی شده بود که نشان می‌دهد آیا ویژگی‌های مشتری با آن‌هایی که در پایگاه داده UIDAI ذخیره شده‌اند مطابقت دارد یا خیر، در ادامه احراز هویت KYC با استفاده از Aadhaar اطلاعات اضافی در مورد مشتریان خود به موسسات مالی را نیز ارائه می‌دهد. کارشناسان حفظ حریم خصوصی معتقدند که این یک تغییر اساسی است که مصرف‌کنندگان را در معرض خطر قرار می‌دهد.

نحوه‌ی کار سیستم Aadhaar

این سیستم یک سیستم کاملا از راه دور تلقی نمی‌شود و برای جمع‌آوری اطلاعات و ضبط داده‌های زیست‌سنجی آن‌ها نیاز به حضور افراد در نمایندگی‌های مورد اطمینان نهاد UIDAI است. بعد از ثبت افراد در سیستم‌های اطلاعاتی، امکان دریافت داده‌ها توسط سایر نهادها مانند بانک وجود دارد و از این طریق دیگر نیاز به اسناد کاغذی و حضور اقراد در موسسات برای افتتاح حساب یا امور بانکی و مالی نمی‌باشد [21].

بسته به کاربرد و سطح اطمینان، سه نوع eKYC مبتنی بر Aadhaar وجود دارد:

- زیست‌سنجی: تأیید اثر انگشت و عنبیه
- دموگرافیک: تأیید اطلاعات آماری
- رمز یکبار مصرف (OTP): این رمز توسط تلفن همراه افراد دریافت می‌شود.

جدول ۵-۱ اطلاعات انواع روش‌های احراز هویت Aadhaar

نوع احراز هویت	داده‌های لازم برای احراز هویت	نوع تایید	درجه اطمینان
زیست‌سنجی	اثر انگشت/عنبیه	فرد چه کسی است؟	زیاد
دموگرافیک	نام، جنسیت، تاریخ تولد، آدرس	فرد چه می‌داند؟	کم
OTP	یک بار رمز عبور	فرد چه چیزی دارد؟	متوسط

۵-۱-۳) سیستم‌های احراز هویت الکترونیکی در ایران

در سال گذشته با شیوع بیماری کرونا، بسیاری از شرکت‌ها و موسسه‌های مالی و هم‌چنین بانک‌ها برای ایجاد راه‌های جدید برای ارائه‌ی خدمات الکترونیکی به مشتری‌ها و هم‌چنین ارتقای خدمات موجود اقدامات مختلفی را انجام دادند. با این وجود در سال جاری این فناوری در ایران بیشتر مورد توجه قرار گرفت و اکثر فعالیت‌ها و خدمات در این زمینه مربوط به این دوران بیماری می‌باشد.

رئیس کمیته احراز هویت بانکداری دیجیتال در کارگروه بانکداری در رابطه با ایجاد سیستم‌های احراز هویت الکترونیکی در بانک‌ها گفته است که یکی از موضوعات اصلی در ارائه خدمات بانکداری الکترونیک و بانکداری نوین بحث احراز هویت دیجیتال است. در بانک مرکزی از کمیته‌ای هم در این خصوص با عنوان کمیته بانکداری دیجیتال تشکیل شده و کارگروه‌هایی هم ذیل این کمیته فعال شده‌اند که یکی از آن‌ها با نام

کارگروه احراز هویت دیجیتال است. در این کارگروه سعی شده از حضور و تجربیات متخصصان و صاحب‌نظران این حوزه از جمله مدیران و متخصص بانکی، فعالان کسب‌وکارهای اینترنتی، فین‌تک‌ها، بوم‌ها و مرکز کاشف و بخش‌های حقوقی و ضدپولشویی بانک مرکزی جمهوری اسلامی ایران و غیره استفاده شود. مراحل دقیقی برای مستندسازی این فرایند دارد طی می‌شود که هم مشتری بتواند کاملاً اطمینان داشته باشد به امنیت و پایداری سرویس و هم بانک‌ها با موانع قانونی و اجرایی و فنی مواجه نشوند و هم اینکه از موجودیت‌ها و زیرساخت‌های خوب حاضر کشور نیز استفاده شود که لازمه آن این است که همه ابعاد حقوقی و اجرایی و تکنیکال آن بررسی شود. در این راه حتماً استفاده از فناوری‌های جدیدی مانند faceId و VideoID ترویج خواهد شد واین امر باعث رشد و نمو و همه گیر شدن وتسهیل کارکرد آن‌ها خواهد شد.

بانک ملی اعلام کرده است که به راه‌اندازی فرایند احراز هویت دیجیتالی برای عقد قراردادها و اسناد تجاری و پرداخت حقوق و عوارض دولتی اقدام کرده است. طبق اعلام بانک ملی این بانک در پروژه اعطای تسهیلات کرونا و همچنین برای اعطای اعتبار خرید تسهیلات از محل وثیقه‌گذاری سهام عدالت از احراز هویت دیجیتالی و امضای الکترونیکی استفاده خواهد کرد. بانک مرکزی چندی پیش اعلام کرد که شبکه بانکی برای اعطای کارت اعتباری می‌توانند از سهام عدالت را به عنوان وثیقه از مشتریانشان دریافت کنند. این اقدام بانک ملی با توجه به شیوع ویروس کرونا وهمچنین تاکید دولت به احراز هویت دیجیتال و به‌کارگیری امضای الکترونیکی اجرایی شده است. این بانک برای صدور امضای الکترونیکی از مرکز ریشه مرکز توسعه تجارت الکترونیکی استفاده خواهد کرد وشعب بانک ملی به عنوان مراکز RA یا مراکز صدور امضای الکترونیکی اقدام به صدور امضا برای کاربران و مشتریان خود خواهند کرد. بانک ملی اعلام کرده است برای احراز هویت کاربرانش از سرویس امضای الکترونیکی بهره خواهد برد و با توجه به اینکه کاربرد عمده هویت دیجیتالی بربستر موبایل صورت می‌گیرد تولید و نگهداری زوج کلید به صورت نرم‌افزاری خواهد بود. همچنین این بانک برای احراز هویت دیجیتالی کاربران خود از مولفه‌های زیست‌سنجی نیز بهره می‌برد. احراز هویت دیجیتالی این بانک از طریق فناوری خاص تشخیص چهره به صورت دو فاکتوره خواهد بود یعنی علاوه براینکه احراز هویت مشتمل بر تشخیص زنده افراد یا تشخیص زنده بودن فرد خواهد بود بلکه نیازمند ورود رمز اختصاصی ۶ رقمی خواهد بود.

در ایران نیز در سال جدید، سازمان بورس تصمیم گرفت تا احراز هویت به شکل غیرحضوری انجام شود. هنگامی که این تصمیم اتخاذ شد، به نظر می‌رسید زیرساخت آن چندان فراهم نبود و تازه مسئولان امر به فکر ایجاد سازوکاری برای این اقدام افتادند. در اواسط اردیبهشت‌ماه بود که صحبت از انجام احراز هویت

غیرحضوری شد. مشاور فناوری و نوآوری شرکت سپرده‌گذاری مرکزی درباره احراز هویت غیرحضوری سجام گفت: «احراز هویت غیرحضوری سجام با همکاری معاونت علمی و فناوری و تیم‌های دانش‌بنیان با استفاده از فناوری هوش مصنوعی انجام خواهد شد».

احراز هویت غیرحضوری سجام

در حال حاضر در برخی اپلیکیشن‌ها مانند سیگنال، و برخی کارگزاری‌ها مانند سهم آشنا، بانک مهر ایران و کارگزاری کارآمد احراز هویت غیرحضوری سجام به صورت آنلاین انجام می‌دهند. در راستای احراز هویت غیرحضوری کارگزاری‌ها، تعدادی از کارگزاری‌ها نیز احراز هویت خود را به صورت غیرحضوری انجام می‌دهند. اینکه چرا تمام کارگزاری‌ها فرایند احراز هویت غیرحضوری را راه‌اندازی نمی‌کنند و چه موانعی برای این کار وجود دارد، سوالی است که به طور خلاصه به آن پاسخ داده می‌شود.

احراز هویت غیرحضوری کارگزاری‌ها پشتوانه قانونی ندارد: کارگزاری‌ها بر این عقیده هستند که در خصوص احراز هویت غیرحضوری مشکل نرم‌افزاری وجود ندارد، بلکه برای این موضوع هنوز قوانینی وضع نشده تا کارگزاری‌ها بتوانند با استناد به آن احراز هویت غیرحضوری انجام دهند.

نبود امضای دیجیتال، مشکل اصلی است: مساله احراز هویت غیرحضوری سجام ارتباطی با مساله ثبت‌نام کارگزاری‌ها ندارد، چراکه کارگزاری‌ها در یک مرحله از ثبت‌نام احراز هویت را انجام می‌دهند که مشتری را بشناسد، اما مرحله دیگر این است که باید با مشتری قرارداد امضا کنند. اکنون مشتری برای افتتاح حساب بورسی در کارگزاری قراردادهایی را مانند قرارداد اعتباری امضا می‌کند که نمی‌توان این مورد را غیرحضوری انجام داد. چون امضای دیجیتال از نظر قانونی پذیرفته شده نیست.

احراز هویت برای دریافت سیم‌کارت در اپراتور ایرانسل

معاون عملیات ایرانسل در حاشیه مراسم اتصال بیش از ۱۰۳۴ روستا به شبکه ملی اطلاعات توسط ایرانسل در خردادماه ۱۳۹۹، پیشنهادی در رابطه با احراز هویت دیجیتالی مشترکین جدید این اپراتور ارائه داد، طرحی برای احراز هویت دیجیتالی مشترکین جدید تدوین کرده‌اند که به واسطه آن می‌توانند فروش سیم کارت را بدون لزوم حضور فیزیکی افراد پیاده سازی کنند. بر اساس این طرح، صفر تا صد فروش سیم‌کارت‌های جدید می‌تواند روندی اینترنتی و غیرحضوری داشته باشد.

در مرحله اول انتخاب سیم کارت در فروشگاه اینترنتی ایرانسل توسط مشترک را انجام خواهد شد و پس از آن به مرحله گرفتن عکس از کارت ملی و ارسال آن از سوی مشترک می‌رسد. برای احراز هویت فرد نیازمند عکس از چهره فرد مذکور خواهیم بود. پس از آن یک ویدیو کوتاه از فرد که خودش آن را ضبط کند و یک متن تصادفی که توسط سیستم به او ارائه شده را خوانده می‌شود. در نهایت مشترک جدید می‌تواند با امضا کردن روی کاغذ و گرفتن عکس از این امضا و ارسال آن، منتظر تاییدیه اطلاعات ارسالی بماند و با پرداخت هزینه، فرایند احراز هویت انجام شود و سیم‌کارت برای کاربر پست شود.

۵-۲) ارزیابی عملیاتی طرح (مقایسه با نیازهای اولیه)

ارزیابی عملیاتی طرح، پس از اجرا و توسط تیم نظارتی کارفرما قابل انجام خواهد بود.

۵-۳) مدیریت ریسک (تعیین گلوگاههای احتمالی در اجرای طرح و راه حل جبرانی)

هنگام استفاده از قناوری احراز هویت غیرحضوری لازم است که ملاحظات مرتبط با آن مانند مسائل قانونی راه‌حل(های) e-KYC به کار رفته، امنیت داده‌های مشتری، حفظ حریم خصوصی و محافظت از داده‌ها در دوره انتقال از اسناد فیزیکی به راه حل‌های شناسه االکترونیکی و میزان و مدت اعتبار آن‌ها را در نظر گرفت. در ادامه این موارد مرور شده و راهکارهای مدیریت آنها پیشنهاد می‌شود.

الزامات قانونی: در مرحله‌ی اول، عمل به الزامات قانونی بسیار اهمیت دارد، بالاخص اگر نیاز به دسترسی به سیستم‌های اطلاعاتی مختلف در نهادهای مختلف باشد. این فرایند به چارچوب‌های قانونی روشن و تفویض مسئولیت‌ها به مقام‌ها یا سازمان‌های مشارکت‌کننده که بخشی از یا همه بانک‌های اطلاعاتی مؤلفه را کنترل می‌کند نیاز دارد. خوشبختانه این موضوع در کشور پذیرفته شده است و همانطور که برخی از نمونه‌های آن بیان شد، هم اکنون این راهکار عملیاتی شده است.

هزینه‌های سرمایه‌ای و عملیاتی: ایجاد سیستم‌های e-KYC به صورت متمرکز و در مقیاس ملی با رویکر شناسه الکترونیکی ملی (مانند مدل هند) می‌تواند پرهزینه باشد. سیستم Aadhaar هند از زمان تأسیس در سال ۲۰۰۹ حدود ۱.۵ میلیارد دلار تا سپتامبر ۲۰۱۸ هزینه داشته است (با هزینه‌های سالانه – عملیاتی و سرمایه – که حدود ۴۲ میلیون دلار در سال است). این در حالی است که هزینه‌های مشتری هم برای استفاده و افتتاح

حساب نباید زیاد باشد زیرا ممکن است او را از این کار منصرف و تعداد مشتری‌ها را کاهش دهد. علاوه بر نیروی کار مورد نیاز و ناظرها، به سیستم‌های اطلاعاتی قوی و غیرقابل نفوذ و همین‌طور ایمن نیاز است. علاوه بر این سیستم‌های کامپیوتری مورد نیاز برای پردازش داده‌ها و زیرساخت‌های اینترنتی لازم از جمله مواردی است که هزینه‌ی قابل توجهی را به خود اختصاص می‌دهد. در این طرح، رویکرد ارائه سرویس eKYC ایجاد شناسه ملی نیست و رویکرد مبتنی بر تطبیق چهره و تشخیص زنده بودن در مقیاس درون سازمانی ناجاست که هزینه آن به مراتب کمتر است و با هزینه مدل شناسه ملی قابل مقایسه نیست.

دوام سیستم: هسته اصلی یک فرآیند e-KYC قادر به احراز هوبت در زمان واقعی از یک پایگاه داده مرکزی برای یک شخص است. این امر مستلزم اتصال مداوم به سرور مرکزی نهاد تأییدکننده است، خواه یک مقام ملی شناسایی یا یک بانک مرکزی باشد و نباید مواردی مانند قطع اتصالات و همین‌طور اینترنت ضعیف وجود داشته باشد. این موضوع نیز با توجه به بستر استعلام گیری سازمان ثبت احوال که سالهاست در اختیار نهادهایی مانند بانک‌هاست که به صورت لحظه‌ای از آن استفاده می‌کنند، مشکلی نخواهد داشت.

امنیت سیستم‌ها و داده‌های کاربر: با توجه به اندازه و ارزش اطلاعات موجود در این سیستم‌ها اهمیت این موضوع دو چندان می‌شود، سیستم مشهور Aadhaar در هند مورد حمله‌ی اینترنتی قرار گرفت که منجر به نشت جزئیات مربوط به چندین ثبت‌نام، ایجاد تعدادی شماره جعلیAadhaar، و همچنین غیرفعال کردن ویژگی امنیتی GPS نرم افزار ثبت‌نام شد. یکی از دلایل این اتفاق‌ها، اجازه دادن به آژانس‌های خصوصی برای ثبت نام کاربران با استفاده از نرم‌افزار رسمی ثبت‌نام با پلتفرم چندگانه بود. در این پروژه، این مشکل به دو دلیل زیر نگرانی بالایی ندارد: ۱- داده‌های حساس مشتریان در پایگاه داده‌های دیگری مانند ثبت احوال نگهداری و محافظت می‌شود که تاکنون مورد دسترسی غیرمجاز نبوده است و ۲- دسترسی به سرویس احراز هویت غیرحضوری توسط سیستم‌های داخلی ناجا خواهد بود که امکان تامین امنیت بالا در ارتباط بین آنها فراهم است.

حفظ حریم خصوصی و محافظت از داده‌ها: تضمین محافظت از داده‌ها و حفظ حریم خصوصی هنگام برخورد با حجم زیادی از داده‌های شناسه ملی و e-KYC موضوعی مهم است که در بسیاری از حوزه‌های قضایی مورد بحث قرار می‌گیرد. بسیاری از کشورها، به ویژه کشورهای در حال توسعه، قوانین جامع حمایت از

داده ها را ندارند. فناوری های جدید مانند DLTs / blockchain امکان رمزگذاری، ذخیره‌سازی ، انتقال و تأیید صحت داده‌های شناسایی ملی را فراهم می‌آورد اما مقررات نظارتی برای محافظت از داده‌ها و حفظ حریم خصوصی نیز برای محافظت از کاربران و رفع نگرانی از حریم خصوصی و امنیت داده‌ها برای e-KYC ضروری است. در سامانه پیشنهادی داده‌های مرجع از مراکز استعلامی دریافت می‌شود که امنیت آنها تامین شده است و سایر داده‌های کاربران رمز می‌شود.

کارایی و تقلب: یک سرویس احراز هویت خودکار ممکن است به دلیل تصمیم اشتباه در احراز هویت یا تشخیص زنده بودن، اجازه دسترسی غیرمجاز را به یک سامانه فراهم کند. برای جلوگیری از این موضوع در این پروژه، پارامترهای تعیین آستانه تصمیم‌گیری می‌تواند کاملا سخت‌گیرانه تعیین شود (مثلا در صورت اطمینان بالای ۹۵٪ اجازه کار داده شود) و در صورتی که مقدار اطمینان از سطح مطلوب کمتر بود، آن فرد را به عامل انسانی برای تصمیم‌گیری ارجاع دهد و یا به مراجعه حضوری به مراکز موجود هدایت کند.

۵-۴) تعیین روش (متدولوژی) تحقیق

از آنجا که این پروژه علاوه بر ابعاد پژوهشی، دارای گام‌های عملیاتی نیز هست، فرایند کار در انجام آن به صورت زیر است:

- مطالعه و بررسی نیازهای کارفرما برای تعیین دقیق آنها جهت نهایی کردن نحوه ارائه سرویس احراز هویت و تعیین یک سامانه استفاده کننده از آن به همراه تعیین جامعه مخاطبان. با توجه به جدید بودن موضوع در سازمان، پیشنهاد می‌شود جامعه مخاطبان و نوع خدمات قابل ارائه بر اساس این روش، محدود و دارای ریسک امنیتی کم باشد.
- بررسی دانش فنی مرتبط با نیاز پروژه و ارائه گزارش علمی از آن
- پیاده‌سازی یک نسخه از سرویس احراز هویت غیرحضوری متناسب با نیاز کارفرما
- نصب و راه‌اندازی سرویس احراز هویت در محل کارفرما و اتصال سامانه بهره‌بردار به آن
- پایلوت کردن استفاده از سرویس جهت دریافت بازخورد و انجام اصلاحات لازم
- پایدار کردن سرویس و راه‌اندازی عمومی آن
- ارائه آموزش و انتقال دانش فنی لازم به کارفرما
- در صورت تایید کارفرما، شروع فاز دوم کار برای انجام فرایند توسعه

۵-۵) پیشنهاد پتانسیل‌ها/منابع علمی برای اجرای پروژه

نیازمندی‌های علمی-پژوهشی و پیاده‌سازی سرویس احراز هویت توسط مجری تامین می‌شود. برای این کار تجربه اجرایی مجری در این حوزه در انجام پروژه‌های عملیاتی و صنعتی (که حدود ۱۵ سال است) و همچنین دانش علمی (که در حدود ۲۰ سال گذشته در دانشگاه آن را دنبال کرده است) مورد استفاده قرار می‌گیرد. در انجام این پروژه، بهره گیری از دانش روز در حوزه مرتبط با موضوعات پروژه (الگوریتم‌های هوش مصنوعی و امنیتی) که از پژوهش علمی حاصل می‌شود، در کنار توان و تجربه عملیاتی کردن این دانش (روش‌های تحلیل و پیاده‌سازی سامانه‌های نرم افزاری) ضروری است.

۵-۶) روش کنترل کیفیت و تحویل دهی

خروجی این طرح، علاوه بر مستندات علمی مرتبط با موضوع، شامل نسخه پیاده‌سازی شده سرویس نیز خواهد بود. بنابراین، به صورت خلاصه خروجی‌های پروژه عبارتنداز:

- مستندات علمی حاوی دانش فنی موضوع و روش‌های علمی حوزه تایید هویت از روی چهره و تشخیص زنده بودن با روش تحلیل کیفیت تصویر و پلک زدن
- یک نسخه از سرویس پیاده‌سازی شده در سرورهای کارفرما حاوی ماژول‌های بیان شده در فصل ۴
- ارائه مستندات راهنمای فنی استفاده از سرویس

۶) فصل ششم: برنامه اقدام

۶-۱) تعیین سیاست‌های اجرائی و نقشه راه

با توجه به نوع پروژه و پیچیدگی آن تا رسیدن به هدف، سیاست‌های کلی اجرایی برای پوشش مسائل مرتبط شامل موارد ذیل می‌شود:

- در نظر گرفتن قوانین و استانداردهای بالادستی در سطح کشور و ناجا
- در نظرگرفتن ملاحظات و حساسیت‌های امنیتی ملی و سازمانی
- لحاظ کردن مقیاس‌پذیری و توسعه پروژه برای توسعه‌های بعد از این فاز از پروژه
- توجه به تجربیات موفق مرتبط با موضوع در دنیا

۶-۲) فازبندی/زمان‌بندی

فازبندی پروژه شامل ریز فعالیت های هر فاز و زمان‌بندی آنها در ادامه آورده شده است.

۶-۲-۱) فازبندی

این طرح در چهار فاز کلی اجرا خواهد شد که هر فاز مشتمل بر مجموعه‌ای از فعالیت‌ها است که در تعامل تنگاتنگ با کارفرما اجرا و نتایج حاصله با دریافت نقطه نظرات مربوطه اصلاح و دقیق خواهد شد تا از انحراف طرح از اهداف اصلی در طول اجرا جلوگیری شود. فازبندی اجرای طرح در شکل ۶-۱ آورده شده است و ریز فعالیت‌های مربوط به هر فاز در ادامه ارائه شده است.

شکل ۶-۱ فازهای کلان پروژه احراز هویت غیرحضوری

ریز فعالیت‌هایی که در هر فاز انجام می‌شود در جدول ۶-۱ ارائه شده است.

جدول ۶-۱ ریز فعالیت‌های فازهای پروژه

شماره فاز	عنوان فاز	ریز فعالیت‌ها	خروجی
اول	تحلیل نیاز، مطالعه و بررسی روش‌ها	تحلیل نیازمندی‌های فنی و بهره‌برداری سرویس در جلسات مشترک با کارفرما	سند تحلیل نیازهای پروژه
		طراحی سرویس احراز هویت غیرحضوری بر اساس نیازمندی‌های استخراج شده	سند طراحی پروژه
		مرور روش‌های علمی مرتبط با احراز هویت غیرحضوری (تشخیص چهره و تشخیص زنده بودن) همراستا با نیازمندی‌ها	سند مطالعه و بررسی روش‌ها
دوم	پیاده‌سازی اولیه سرویس احراز هویت غیرحضوری	اختصاصی کردن ماژول‌های تشخیص چهره و تشخیص زنده بودن برای پروژه	نصب نسخه اولیه سرویس اختصاصی شده روی سرور کارفرما
		اختصاصی کردن ماژول‌های مدیریت کاربران، مدیریت دسترسی و استعلام برای پروژه	

		نصب اولیه سرویس در سرور کارفرما	
سوم	یکپارچه‌سازی سرویس با سامانه بهره‌بردار و پایلوت	پیاده‌سازی بخش یکپارچه‌سازی سرویس احراز هویت با سامانه بهره‌بردار	سرویس یکپارچه شده با سامانه بهره‌بردار نصب شده روی سرور کارفرما
		تست سامانه و سرویس روی سرور تستی و جامعه بهره‌دار آزمایشی	سند ارزیابی سرویس و سامانه
		دریافت بازخوردها و تحلیل آنها برای پیاده‌سازی	سند تحلیل بازخوردها و تعیین پیاده‌سازی‌های لازم
چهار	نهایی کردن سرویس و تحویل آن	پیاده‌سازی اصلاحات جمع‌آوری شده در ارزیابی و اعمال در سامانه	سرویس یکپارچه شده با سامانه بهره‌بردار حاوی اصلاحات بعد از ارزیابی
		اجرای نسخه نهایی سرویس و سامانه	
		مستندسازی فنی و آموزش	سند راهنمای فنی و بهره‌برداری سامانه با جلسات آموزشی

۶-۲-۲) زمان‌بندی

این طرح در مدت ۱۲ ماه، مطابق جدول زمان‌بندی نشان داده شده در جدول ۶-۲ اجرا می‌شود.

جدول ۶-۱ ریز فعالیت‌های فازهای پروژه

فاز	عنوان فاز	زمان (ماه)											
		۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
اول	تحلیل نیاز، مطالعه و بررسی روش‌ها												
دوم	پیاده‌سازی اولیه سرویس احراز هویت غیرحضوری												
سوم	یکپارچه‌سازی سرویس با سامانه بهره‌بردار و پایلوت												
چهارم	نهایی کردن سرویس و تحویل آن												

۶-۳) پشتیبانی و توسعه

خروجی این طرح با توجه به اینکه یک سرویس عملیاتی است نیاز به پشتیبانی فنی دارد که برای این کار، سرویس تحویل داده شده از زمان انتهای قرارداد این پروژه، به مدت ۱۲ ماه پشتیبانی رایگان دارد. این پشتیبانی شامل نگهداری سرویس و رفع باگ‌های احتمالی آن است.

از طرفی با توجه به اینکه سرویس خروجی این پروژه، فاز اول بهره‌برداری از این سرویس است، لازم است بعد از اتمام این پروژه از منظرهای مختلفی توسعه داده شود. برخی از محورهای توسعه پیشنهادی برای فاز(های) بعدی پروژه عبارتنداز:

- توسعه کاربری سرویس با اتصال سامانه‌های بیشتر به سرویس احراز هویت غیرحضوری
- بهبود کارایی سامانه به ویژه در بخش تشخیص زنده بودن با افزودن قابلیت‌هایی مانند لب خوانی و تشخیص گفتار
- توسعه دامنه پوشش سامانه با افزودن قابلیت احراز هویت با کارت‌های هوشمند (مانند کارت ملی و گواهینامه و گذرنامه) و با استفاده از اطلاعات هویتی روی کارت (مانند اثرانگشت یا چهره)
- امکان افزودن امضای الکترونیکی به سرویس برای رمزنگاری و امضای دیجیتال اسناد و اطلاعات رد و بدل شده بین سرویس و کلاینت
- تولید SDK و ابزارهای تعاملی بیشتر برای فراهم کردن امکان بکارگیری سرویس در سامانه‌ها و بسترهای مختلف

۷) فصل هفتم: پیوست‌ها

۷-۱) پیوست الف) اطلاعات مجری طرح

۷-۱-۱) اطلاعات مدیر اجرایی طرح

نام و نام‌خانوادگی	مدرک تحصیلی	رشته تحصیلی	مرتبه علمی	محل خدمت	شماره تلفن
هادی ویسی	دکتری	مهندسی کامپیوتر	استادیار	دانشگاه تهران	۰۹۱۲۶۲۱۴۳۰۳

۷-۱-۲) اطلاعات همکاران طرح

ردیف	نام و نام‌خانوادگی	مدرک تحصیلی	رشته تحصیلی	محل خدمت	درصد مشارکت	شماره تلفن
۱	هادی ویسی	دکتری	م. کامپیوتر	دانشگاه تهران	۴۰	۰۹۱۲۶۲۱۴۳۰۳
۲	وریا فتحی	دانشجوی دکتری	م. کامپیوتر	دانشگاه تهران	۱۰	۰۹۱۸۸۷۳۹۹۱۰
۳	بهنام بخشی	دانشجوی ارشد	م. کامپیوتر	دانشگاه تهران	۱۰	۰۹۱۵۶۶۴۷۹۶۷
۴	منیره یوسفی	دانشجوی ارشد	م. کامپیوتر	دانشگاه تهران	۱۰	۰۹۳۵۱۱۵۲۳۵۶
۵	خسرو حسین زاده	کارشناسی ارشد	م. کامپیوتر	شرکت سپیدسیستم	۱۰	۰۲۱۲۸۱۲۴
۶	علیرضا مختاری	کارشناسی ارشد	م. کامپیوتر	شرکت سپیدسیستم	۱۰	۰۲۱۲۸۱۲۴
۷	امیرحسین قربانی	کارشناسی	م. کامپیوتر	شرکت سپیدسیستم	۱۰	۰۲۱۲۸۱۲۴

۷-۱-۳) سوابق تحقیقاتی مرتبط موفق

ردیف	عنوان طرح	تاریخ شروع	تاریخ خاتمه	میزان موفقیت	مبلغ طرح (میلیون ریال)	محل اجرای طرح
۱	زیست‌سنجی چند وجهی (ترکیب اثر انگشت، چهره، و گفتار) با یادگیری عمیق	۱۳۹۶/۱۰/۰۱	۱۳۹۹/۰۳/۳۰	۱۰۰٪	-	دانشگاه تهران
۲	گنجه: سامانه مدیریت صندوق	تابستان	تابستان ۱۳۹۹	۱۰۰٪	۸۶۰۰	شرکت سپیدسیستم

	امانات و کنترل تردد و دسترسی مبتنی بر بایومتریک (اثر انگشت، چهره)	۱۳۹۷				شریف
۳	سپیداستار: سامانه مدیریت دستگاه‌ها و اطلاعات کنترل تردد و دسترسی مبتنی بر بایومتریک (اثر انگشت، چهره)	تابستان ۱۳۹۵	بهار ۱۳۹۷	۱۰۰٪	۵۵۰۰	شرکت سپیدسیستم شریف
۴	شناسا: سامانه تشخیص هویت و تعیین هویت از روی صدا	تابستان ۱۳۸۸	بهار ۱۳۹۳	۱۰۰٪	۴۲۰۰	شرکت عصر گویش پرداز
۵	سامانه تلفن‌همراه خواندن تصاویر فارسی (تبدیل عکس به گفتار)	۱۳۹۴/۱۱/۳۰	۱۳۹۵/۱۱/۳۰	۱۰۰٪	۸۹۵	دانشگاه تهران با حمایت معاونت علمی ریاست جمهوری

۴-۱-۷) طرح‌های تحقیقاتی در دست اجرا

ردیف	عنوان طرح	تاریخ شروع	تاریخ خاتمه	میزان موفقیت	مبلغ طرح (میلیون ریال)	محل اجرای طرح
۱	طرح استقرار سامانه کنترل خودکار مرز (ABC) در مبادی تردد مرزی کشور	۱۳۹۸/۰۵/۱۹	۱۳۹۹/۰۵/۱۹	۸۵٪	۱۸۰۰	دانشگاه تهران- کارفرما: ناجا
۲	سپیدباکس: سامانه مدیریت هویت دیجیتال (مبتنی بر بیومتریک و رمزنگاری)	تابستان ۱۳۹۷	-	۹۰٪	۷۸۰۰	شرکت سپیدسیستم شریف
۳	امکان سنجی جداسازی سیگنال راداری با یادگیری عمیق	۱۳۹۶/۱۲/۲۸	۱۳۹۷/۰۵/۲۸	در حال انجام	۷۹۱	دانشگاه تهران- کارفرما: صاایران

۲-۷) پیوست ب: تعریف واژه‌ها و اصطلاحات تخصصی

اختصارات، واژه‌ها و اصطلاحات تخصصی بکار رفته در این سند، در جدول ذیل تشریح شده‌اند.

جدول اختصارات، واژه‌ها و اصطلاحات تخصصی بکار رفته در سند			
ردیف	اصطلاح	ریشه	تعریف
۱	eKYC	Electronic Know Your Customer	منظور احراز هویت و شناسایی الکترونیکی مشتری است
۲	OTP	One-Time Password	منظور گذرواژه یکبار مصرف می‌باشد.
۳	FAR	False Acceptance Rate	منظور معیاری است که برای اندازه‌گیری نرخ "پذیرش اشتباه" در الگوریتم‌های شناسایی یا تطبیق بیومتریکی استفاده می‌شود.
۴	EER	Equal Error Rate	منظور نرخ خطا به ازای FRR و FAR برابر است.
۵	PIN	Personal Identification Number	منظور کدی است که برای احراز هویت مالک کارت مورد استفاده قرار می‌گیرد.
۶	API	Application Programming Interface	رابط نرم‌افزاری بین یک کتابخانه/سرویس/سیستم‌عامل و سایر برنامه‌هایی است که از آن تقاضای سرویس می‌کنند.
۷	SDK	Software Development Kit	منظور بسته توسعه نرم‌افزاری که برای استفاده توسط سایر نرم‌افزارها ارائه می‌شود.

۳-۷) پیوست ج: منابع و مراجع

[1] Givens G.H., Beveridge J.R., Phillips P.J., Draper B., Lui Y.M., Bolme D., “Introduction to face recognition and evaluation of algorithm performance,” Computational Statistics and Data Analysis, Vol. 67, 2013.

[2] Hjelmås E., Low B.K., “Face detection: A survey,” Computer Vision and Image Understanding, Vol. 83, No. 3, 2001.

[3] Zhang C., Zhang Z., “A Survey of Recent Advances in Face Detection,” Tech. Report, Microsoft Research, No. June, 2010.

[4] Viola P., Jones M., “Rapid object detection using a boosted cascade of simple features,” in Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. CVPR 2001, 2001, Vol. 1, page I-511-I-518.

[5] Mathias M., Benenson R., Pedersoli M., Van Gool L., “Face detection without bells and whistles with supplementary material,” in Eccv, 2014, pages 720–735.

[6] Waring C.A., Liu X., “Face detection using spectral histograms and SVMs,” IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, Vol. 35, No. 3, 2005.

[7] Farfade S.S., Saberian M., Li L.-J., “Multi-view Face Detection Using Deep Convolutional Neural Networks,” in Proceedings of the 5th ACM on International Conference on Multimedia Retrieval, 2015, pages 643–650.

[8] Krizhevsky A., Hinton G.E., “ImageNet Classification with Deep Convolutional Neural Networks,” in Neural Information Processing Systems, 2012, pages 1–9.

[9] Turk M.A., Pentland A.P., “Face recognition using eigenfaces,” in Proceedings. 1991 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pages 586–591.

[10] Tolba A.S., El-Baz A.H., El-Harby A.A., “Facial Recognition: A literature Review,” International Journal of Signal Processing, Vol. 2, No. 2, 2006.

[11] Sharif M., Naz F., Yasmin M., Shahid M.A., Rehman A., “Face recognition: A survey,” Journal of Engineering Science and Technology Review, Vol. 10, No. 2, 2017.

[12] Yaniv Taigman Ming Yang Marc’Aurelio Ranzato Lior Wolf, Tel, “DeepFace - Closing the Gap to Human-Level Performance in Face Verification,” in A Multi-Center, Randomized, Controlled Evaluation of the Safety and Efficacy of LASIK With Cross-linking Performed With the KXL System and Photrexa ZD[TM] (Riboflavin Ophthalmic Solution) Compared to LASIK Alone for Hyperopia and Hyperopic Astigmatism, 2014, pages 1701–1708.

[13] Bombardelli F., “FaceNet: A Unified Embedding for Face Recognition and Clustering Felipe Bombardelli FaceNet: A Unified Embedding for Face Recognition and Clusteri Introduction Algorithm Results References,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2015, pages 815–823.

[14] Mohanraj, V., S. Sibi Chakkaravarthy, I. Gogul, V. Sathiesh Kumar, Ranajit Kumar, and V. Vaidehi. "Hybrid feature descriptors to detect face spoof attacks." Journal of Intelligent & Fuzzy Systems 34, no. 3 (2018): 1411-1419.

[15] livebank24 website, “potential of eKYC digital account.” https://livebank24.com/the-untapped-potential-of-ekyc-digital-account-opening-journeys/.

[16] B. Heisele, P. Ho, and T. Poggio, “Face recognition with support vector machines: Global versus component-based approach,” in Proceedings of the IEEE International Conference on Computer Vision, 2001, vol. 2, pp. 688–694.
[17] C. Liu and H. Wechsler, “Gabor feature based classification using the enhanced Fisher linear discriminant model for face recognition,” IEEE Trans. Image Process., vol. 11, no. 4, pp. 467–476, 2002.
[18] Z. Cao, Q. Yin, X. Tang, and J. Sun, “Face recognition with learning-based descriptor,” in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2010, vol. 91, no. 6, pp. 2707–2714.
[19] Aware website, “Liveness detection in biometrics.” https://www.aware.com/blog-liveness-detection-mobile-authentication-onboarding.
[20] Regulationasia website, “the four e kyc models around the world.” https://www.regulationasia.com/the-four-e-kyc-models-around-the-world/.
[21] CGDEV website, “‘Know Your Customer’ Hurdle with E-KYC.” https://www.cgdev.org/blog/overcoming-know-your-customer-hurdle-e-kyc.