ارائه یک معماری جامع سیستم سلامت الکترونیک برای دسترسی امن به پرونده‌های سلامت شخصی (PHR) با استفاده از فناوری موبایل

سلیمه یساری زارع[1*]، دکتر محمدعلی دوستاری[2]، سمیرا طارمی[3]

۱- دانشجوی کارشناسی ارشد فناوری اطلاعات، دانشگاه شاهد، تهران

۲- استادیار، دانشگاه شاهد، تهران

۳- دانشجوی کارشناسی ارشد فناوری اطلاعات، دانشگاه شاهد، تهران

خلاصه

در عصر حاضر، استفاده از فناوری‌های دیجیتال در حوزه سلامت این امکان را فراهم می‌کند که تبادل اطلاعات و اسناد پزشکی میان مؤسسات بهداشتی و درمانی به‌راحتی امکان‌پذیر باشد. با کمک این فناوری‌ها هر بیمار می‌تواند در هر مکانی از کشور خود و یا کشورهای دیگر، با ارائه پرونده سلامت شخصی آنلاین خود، از خدمات سلامت مراکز درمانی آنجا بهره‌مند شود، و این یعنی سوابق درمانی یک فرد تنها با همراه داشتن یک تلفن هوشمند در همه‌جا به‌صورت مجازی در دسترس خواهد بود. اما مهم‌ترین مسئله در تبادل این اطلاعات حساس در بین مراکز درمانی و حمل آن بر روی تلفن هوشمند بیمار، حفظ امنیت و حریم خصوصی آنهاست که تا زمانی که تأمین نشود، استفاده از فناوری‌های نو در این راستا نه تنها مفید نخواهد بود، بلکه بستر مناسبی برای سرقت و سوءاستفاده از این اطلاعات محرمانه فراهم خواهد کرد. در این پژوهش، معماری جامعی برای سیستم سلامت الکترونیکِ یک کشور ارائه شده است که علاوه بر به‌کارگیری فناوری‌های ارتباطی جدید، راهکارهایی همچون به‌کارگیری زیرساخت کلید عمومی و پروتکل‌های ارتباطی امن نیز برای حفظ امنیت و حریم خصوصی پرونده‌های سلامت شخصی بیماران پیشنهاد شده است. هدف از ارائه این معماری، ایجاد امکان دسترس به پرونده سلامت شخصی بیمار، در هر مکان و هرزمانی، توسط افراد مجاز، و با اعمال کنترل‌های دسترسی تعیین‌شده توسط خود بیمار است. هدف دیگر که بیمار محور بودن پرونده‌های سلامت الکترونیک است، در راستای سیاست توانمندسازی عموم مردم در برنامه‌های ارتقا سلامت شکل‌گرفته است؛ و هدف دیگر، کاهش هزینه‌های دولتی جهت ایجاد زیرساخت‌های لازم برای پیاده‌سازی یک سیستم جامع سلامت الکترونیک در کشور است. در این مقاله، اهداف بیان‌شده، با توجه به معماری جامع سه سطحی پیشنهادی، و پایگاه داده توزیع‌شده‌ای که در آن بکار رفته است، به‌خوبی تأمین‌شده‌اند.

کلمات کلیدی: معماری سیستم سلامت الکترونیک، پرونده سلامت شخصی (PHR)، معماری پایگاه داده توزیع‌شده، معماری جامع سلامت الکترونیک، PKI، NFC، سلامت الکترونیک موبایلی (m-health)، معماری بیمار- محور

* S.yasari@shahed.ac.ir

۱. مقدمه

سلامت الکترونیکی، الگوهای جدیدی از ارتباط میان پزشک و بیمار؛ و پزشک و پزشک است که درمان‌های آنلاین، محرمانه ماندن اطلاعات بیماران، محرمانه نگه‌داشتن مهارت‌های تخصصی پزشکان و نیز رضایت پزشک و بیمار در درمان از جمله کارکردهای آن است. استفاده از امکانات دیجیتال در حوزه سلامت این امکان را فراهم می‌کند که تبادل اطلاعات و اسناد پزشکی میان مؤسسات بهداشتی و درمانی فراهم شود به‌نحوی‌که همواره از آخرین تغییرات دارویی، نسخه‌های درمانی، آموزش‌های پرستاری و مراقبتی و دیگر اطلاعات موردنیاز بتوان آگاه شد، همچنین با به‌روز کردن بانک‌های اطلاعاتی در این حوزه می‌توان آخرین تجربیات خود را در اختیار همگان قرار داد [۱].

در کشورمان بند الف ماده ۳۵ قانون برنامه پنجم توسعه وزارت بهداشت، درمان و آموزش پزشکی را موظف کرده تا به‌منظور ارائه خدمات الکترونیکی سلامت، نسبت به استقرار سامانه پرونده الکترونیکی سلامت ایرانیان و سامانه‌های اطلاعاتی مراکز سلامت در هماهنگی با پایگاه ملی مرکز آمار ایران و سازمان ثبت‌احوال اقدام کند. آخرین اقدامات وزارت بهداشت در این زمینه نشان می‌دهد که در حال حاضر حدود ۵۷ هزار نقطه بهداشتی و درمانی در سطح کشور وجود دارد که بر اساس برنامه پنجم توسعه، حدود ۲۷ هزار نقطه باید به شمس (شبکه ملی سلامت) مجهز شوند اما آخرین اقدامات این وزارتخانه در این حوزه نشان می‌دهد تشکیل ۴/۵ میلیون پرونده الکترونیک سلامت، مهم‌ترین اقدام وزارت بهداشت، درمان و آموزش پزشکی در حوزه فناوری اطلاعات در سال گذشته بوده است.

اما راه‌اندازی مرکزی، برای تبادل اطلاعات بین دیگر سازمان‌های مرتبط با وزارت بهداشت نیازمند راه‌اندازی پروژه‌ای با نام «پرونده ملی سلامت» است که به دلیل آماده نبودن زیرساخت‌های لازم این پروژه به راه‌اندازی شمس (شبکه ملی سلامت) تبدیل شده است تا پس از آماده شدن زیرساخت‌های لازم سامانه پرونده الکترونیک سلامت به‌طور کامل بر آن قرار گیرد. با راه‌اندازی زیرساخت شبکه ارتباطی و مرکز ملی داده‌های سلامت، تاکنون اتصال ۱۲۰۰ مرکز بهداشتی درمانی جدید به این شبکه تحقق یافته است [۱].

هدف از ارائه این مقاله، پیشنهاد یک معماری سه سطحی کاربردی برای دسترسی امن به پرونده‌های الکترونیکی سلامت بیمار (PHR) است، که در آن کلیه ارتباطات از سطح کشوری تا سطح تلفن هوشمند بیمار در نظر گرفته شده و پروتکل‌های لازم برای این ارتباطات طراحی شده است. در این معماری سه سطح (با توجه به پایگاه داده مستقر در آن سطح) شامل سطح ملی، سطح استانی و سطح بیمار در نظر گرفته شده که توضیحات مرتبط با هر سطح در بخش ۳ ارائه‌شده است. در طراحی این معماری، کلیه معماری‌های موجود که در قالب مقالات ارائه‌شده بودند موردمطالعه و بررسی قرار گرفته و برای رفع کمبودها و مشکلات آنها در معماری حاضر راه‌حل‌هایی ارائه‌شده است.

هدف دیگر این مقاله، حذف نیاز به کارت هوشمند برای احراز هویت و نگهداری از اطلاعات حساس و بخشی از اطلاعات پرونده سلامت بیمار (که در اکثر معماری‌ها مطرح شده‌اند)، و یا نیاز به حافظه جانبی به‌منظور ذخیره‌سازی اطلاعات پرونده سلامت بیمار است.

یکی از محدودیت‌های اصلی برای پیاده‌سازی یک سیستم مدیریت داده‌های کلینیکی بیماران در یک مقیاس کامل، نیاز به ایجاد یک زیرساخت فیزیکی برای ایجاد اتصال بین دفاتر مرکزی مختلف سیستم‌های سلامت دولتی و خصوصی است، که بتواند نیازمندی‌های نقل‌وانتقال داده‌ها و همگام‌سازی اطلاعات را برآورده سازد. [۲]

در این پژوهش تلاش شده است که با ارائه یک معماری پیشنهادی، با استفاده از روش ارائه‌شده در [۲] بر محدودیت‌هایی که توسط سیستم‌های سنتی مدیریت داده‌های متمرکز تحمیل شده‌اند غلبه کنیم. هدف دیگر این پژوهش، پیشنهاد یک راه‌حل نو است که بتواند به طرز قابل‌توجهی هزینه‌های سرمایه گذاری برای زیرساخت را برای مدیریت دولتی

کاهش دهد. ما در این مقاله، به‌منظور کاهش هزینه‌های دولتی برای ارائه زیرساخت‌های لازم جهت ذخیره‌سازی حجم انبوهی از اطلاعات بیماران در یک استان، از سیستم‌های توزیع‌شده در این سطح استفاده کرده‌ایم، و در نتیجه نیاز به وجود سرورهای گران‌قیمت و فضاهای امنیتی لازم برای نگهداری از این سرورها، در معماری پیشنهادی این پژوهش حذف شده است. این در حالی است که در معماری مشابهی که در [۳] ارائه‌شده، در سطح استانی نیز زیرساخت‌های جداگانه‌ای برای ذخیره‌سازی EHRها در نظر گرفته شده و علاوه بر وجود افزونگی‌های غیرضروری در آن معماری، لایه‌های ارتباطی افزایش یافته و هزینه‌های سنگینی به بخش دولتی یک کشور تحمیل خواهد شد.

این مقاله از ۶ بخش تشکیل‌شده است. در بخش ۲ مقالاتی که کارهای مشابه با این مقاله انجام داده‌اند معرفی، و به‌طور مختصر با معماری مقاله ما مقایسه شده‌اند. در بخش ۳ در مورد معماری پیشنهادی، مؤلفه‌های آن و امنیت ارتباطات آن توضیحاتی ارائه‌شده است. در بخش ۴ معماری پایگاه داده توزیع‌شده‌ای که در قسمت S_D_PHRC از معماری ما استفاده شده، توصیف شده است. همچنین در بخش ۵، معماری‌مان را جهت درک بهتر، با توصیف یک سناریو نشان داده‌ایم. و در بخش ۶ به بیان نتیجه‌گیری و کارهای آینده‌مان جهت تکمیل ساختار سطح بیمار در معماری پیشنهادی پرداخته‌ایم.

۲. کارهای مرتبط

در مقاله [۴] یک طرح محافظت از محتوای کاربر محور برای استفاده در ترکیب با سیستم‌های مدیریت سلامت موجود معرفی شده است. این مقاله با در نظر گرفتن نیازمندی‌های اکید برای حفظ حریم خصوصی بیمار، محرمانگی و ارتباطات متقابل در EHR، یک رویکرد نو برای ذخیره‌سازی EHR روی رسانه ذخیره‌سازی، یک دسترسی دوگانه مبتنی بر قاعده با استفاده از توکن کارت هوشمند بیمار، و یک عامل کارت هوشمند مجازی را پیشنهاد داده است. یک نوع دستگاه جدید با قابلیت‌های توسعه‌یافته در مکان ترمینال کارت هوشمند معرفی شده است که دسترسی آنلاین و آفلاین به پرونده‌های الکترونیک سلامت رمز شده را ممکن ساخته است. در این معماری، با استفاده از دستگاه طراحی‌شده اختصاصی‌ای به نام «رسانه ذخیره‌سازی شخصی»* دسترسی و ارتباطات متقابل خوبی در سیستم محافظت از محتوای EHR، به وجود آمده است. اما بزرگ‌ترین عیب این معماری وجود یک کارت هوشمند و یک حافظه قابل‌حمل مستقل از آن برای نگهداری پرونده‌های الکترونیک سلامت است که احتمال گم‌شدن، دزدیده شدن و سوءاستفاده از آن بسیار زیاد بوده و حمل‌ونقل و همراه داشتن آن برای بیمار کار مشکلی خواهد بود. در معماری پیشنهادی این پژوهش این مشکل با در نظر گرفتن کلیه مسائل امنیتی، با استفاده از حافظه و امکانات تلفن‌های هوشمند برطرف گردیده و هر دو مورد فوق در داخل این دستگاه تعبیه‌شده‌اند.

در مقاله [۵] یک راه‌حل برای سیستم PHR ارائه‌شده که اجازه تبادل داده‌های بیماران را در مراکز درمانی، با استفاده از دستگاه موبایلِ بیمار می‌دهد. این سیستم به بیمار اجازه می‌دهد همزمان هم به سیستم‌های PHR آنلاین که در آنها ثبت‌نام کرده دسترسی داشته باشد و هم به PHR موجود بر روی موبایلش برای اینکه بتواند دسترسی مستقیم به داده‌هایش را به پزشک بدهد. یکی از مشکلات این معماری که در معماری پیشنهادی برطرف شده است، این است که علاوه بر وجود موبایل بیمار که نرم‌افزار m-PHR بر روی آن نصب‌شده است، نیاز به یک کارت هوشمند مستقل نیز به‌منظور تأمین بخشی از فرایند شناسایی و احراز هویت بیمار موردنیاز است.

* Personalized Media Recorder (PMR)

Healthpass [۶و۷] یک سیستم PHR مبتنی بر موبایل را معرفی کرده که قادر به تبادل داده‌های PHR با یک پزشک در یک مرکز مراقبتی است. یک مشکلی که در Healthpass وجود دارد این است که این سیستم برای اجرای کنترل دسترسی به کل EHR، به موبایل بیمار اعتماد می‌کند، بنابراین پیاده‌سازی یک بخش روی دستگاه موبایل که بتواند فقط توسط یک پزشک مورد دسترسی قرار گیرد را تضمین نمی‌کند. همچنین در مورد امنیت و حریم خصوصی در شرایطی که مثلاً موبایل بیمار گم شود نیز بحثی نکرده است. این سیستم مجوزهای دسترسی به بخش‌های مختلف PHR را می‌تواند فراهم کند، اما در مورد اینکه این کار چگونه انجام و پیاده‌سازی می‌شود بحثی نکرده است. و مشکل دیگر این معماری نیز این است که مشخص نکرده چطور یک PHR موبایل با PHR آنلاین ارتباط برقرار می‌کند.

در مقاله[۸] یک راه‌حل مبتنی بر تلفن همراه برای ارائه خدمات به بیماران راه دور، ارائه‌شده است. هدف نویسندگان از طرح این معماری رفع مشکل معماری‌های مشابه که نیاز به اینترنت داشتند (درحالی‌که اینترنت، همه‌جا در دسترس نیست) بوده است، و بر این اساس سیستم سلامتی پیشنهاد داده‌اند که بر پایه شبکه GSM و پیام کوتاه کار می‌کند. در این معماری، اطلاعات سلامت محافظت‌شده* (PHI) بیماران، اطلاعات شناسایی درمانگران و بیماران، و شماره همراه درمانگران و بیماران، همگی بر روی سرورهای یک مرکز با نام MCS† قرارگرفته‌اند که این باعث ایجاد نیاز به یک درگاه دسترسی امن‡ برای ورود به سرورهای این مرکز شده است. درحالی‌که در معماری پیشنهادی مقاله‌ی ما یک سرور جداگانه برای نگهداری از اطلاعات شناسایی درمانگران مجاز و بیماران در هر استان وجود دارد (که مدیریت، مانیتورینگ و پشتیبانی این سرورها بر عهده یک سرور مرکزی ملی است)، که این سرورها درگاه ورودی به سرورهای پایگاه داده توزیع‌شده پرونده‌های سلامت شخصی بیماران هستند. علاوه بر این، در این معماری، بیمار تنها می‌تواند بخش بسیار کوچکی از PHI خود را بر روی تلفن همراهش به‌صورت پیامک داشته باشد و مالکیت و کنترلی بر روی پرونده سلامت خود ندارد.

با توجه به اینکه عدم دسترسی به اطلاعات پزشکی کافی از بیمار می‌تواند منجر به آسیب‌ها و تلفات زیادی شود، در مقاله [۳]، معماری جامعی با استفاده از فناوری‌های نوظهوری همچون: سیم‌کارت‌های جاوا (JSC)، تلفن‌های هوشمند، شبکه‌های نسل بعد (NGN)،ارتباطات میدان نزدیک (NFC)، زیرساخت کلید عمومی (PKI) و تشخیص هویت بیومتریک، یک چارچوب امن برای دسترسی همه‌جا حاضر به پرونده‌های پزشکی بیماران ارائه‌شده است. در این معماری به دلیل وجود محدودیت در حافظه سیم‌کارت، تنها بخشی از پرونده الکترونیک سلامت بیمار در آن ذخیره می‌شود، درحالی‌که در معماری ما، کل پرونده سلامت بیمار به‌صورت رمزشده در حافظه داخلی دستگاه بیمار قرارگرفته، و کلیدها با استفاده از تکنیک‌های امنیت سخت‌افزاری، در مخزن امن§، ذخیره‌سازی شده‌اند.

در معماری مقاله [۳] یک (مرکز پرونده‌های الکترونیک سلامت استانی) وجود دارد که یک کپی از EHRهای بیمارانی است که در یک استان مشخص مقیم هستند. درحالی‌که در معماری پیشنهادی ما این مرکز حذف شده و یک سرور گران، حجیم وجود ندارد که در مکانی فیزیکی به صورت امن نگهداری شود، بلکه از مفهوم سیستم‌های توزیع‌شده (که سرور پایگاه داده موجود در هر مرکز درمانی بخشی از این سیستم توزیع‌شده است) استفاده‌شده است که علاوه بر افزایش امنیت و توزیع بار در مکان‌های فیزیکی متعدد، هزینه‌های دولتی را به طرز قابل‌توجهی کاهش خواهد داد.

در معماری مطرح‌شده در مقاله [۳] ارتباط بین سطح استانی و سطح بیمار از طریق اینترنت (شبکه NGN) صورت می‌گیرد درحالی‌که در معماری ما به دلیل حذف سرویس‌دهنده‌های اضافی در سطح استانی، ارتباط مستقیم کاربر با شبکه محلی مراکز درمانی (و در نتیجه شبکه درمانی توزیع‌شده استانی) میسر شده و نیاز به اینترنت، تدابیر امنیتی و اقتصادی

* Protected Health Information
† Medical Centre Servers
‡ Secure Access Gateway (SAG)
§ Secure Storage

لازم برای دسترسی به این شبکه جهانی و ایجاد زیرساخت‌های لازم، در این سطح برطرف گردیده، و بدون وجود شبکه جهانی اینترنت نیز می‌توان ارتباطات را به صورت محلی بین بیمار و پزشک با پایگاه داده توزیع‌شده آن استان، برقرار کرد.

در معماری مقاله [۳] از مفهوم پرونده الکترونیک سلامت (EHR) برای نگهداری از اطلاعات بیماران استفاده‌شده درحالی‌که معماری ما بیمار محور بوده و با توجه به سیاست توانمندسازی عموم مردم در برنامه‌های ارتقا سلامت (که بر مبنای آن باید هر فرد مسئولیت سلامت خود را به عهده گیرد و پرونده سلامت، کاربر محور باشد) [۵و۹]، در این معماری از مفهوم پرونده سلامت شخصی (PHR)* استفاده شده است تا به بیمار اجازه داده شود که کنترل کند چه کسانی به پرونده سلامت او، چه نوع دسترسی‌ای داشته باشند.

در مقاله [۲]، نتایج پروژه CCE ارائه‌شده که یک معماری توزیع‌شده برای داده‌های پزشکی ارائه می‌کند که در آن بیمار نقطه مرکزی فرآیندها در نظر گرفته شده است. در واقع بیمار مالک و نگهدارنده† واقعی داده‌هایش است؛ چراکه بیمار بیمار کارت هوشمندی به همراه یک حافظه جانبی دارد که حاوی همه گزارشات پزشکی، نسخه‌ها، عکس‌های پزشکی و ... است. این مقاله یک معماری برای ذخیره‌سازی، تبادل و استفاده از داده‌های سلامت برای مقاصد همه‌گیرشناسی و مدیریتی (بدون اینکه به حریم خصوصی بیماران خدشه‌ای وارد شود) ارائه کرده است به‌نحوی‌که بیماران می‌توانند در یک شرایط امن و آسان، داده‌هایشان را برای اهداف تحقیقاتی قابل‌استفاده سازند. در این پژوهش، از طرح پیشنهادی این مقاله برای طراحی سیستم‌های توزیع‌شده (تشکیل‌شده از سرویس‌دهنده‌های پایگاه داده مراکز درمانی) در سطح استانی استفاده شده است.

۳- شرح معماری پیشنهادی

این معماری، که در شکل (۱) نشان داده شده است، دارای سه سطح است که هر سطح پایگاه داده مخصوص به خود را دارد:

- سطح بیمار (پایگاه داده m-PHR)

در پایین‌ترین سطح که سطح بیمار است، پایگاه داده کوچکی حاوی PHR بیمار وجود دارد، که از طریق یک نرم‌افزار موبایلی امن در دسترس بیمار و فرد درمانگر مجاز قرار می‌گیرد. این نرم‌افزار امن از دو قسمت Trusted Application‡ و Normal Application§ تشکیل‌شده است که توسط یک «شخص ثالث مورد اعتماد**» با مجوز یک ارگان دولتی (مثل (مثل وزارت بهداشت) توسعه داده‌شده و در بخش‌های مربوطه در موبایل بیمار قرار گرفته است. (در مورد این نرم‌افزار موبایلی، تأمین امنیت، احراز هویت و ذخیره‌سازی و راه‌اندازی امن آن در موبایل بیمار در مقالات آتی راه‌حل‌هایی ارائه خواهیم کرد). در این مقاله به مجموعه این نرم‌افزار موبایلی و پایگاه داده مرتبط، که PHR بیمار را تشکیل می‌دهند، m-PHR می‌گوییم.

- سطح استانی (پایگاه داده S-PHR)

---

* personal health record

† holder

‡ نرم افزار/بخشی از نرم افزار، که امنیت آن ا ز نظر فیزیکی تامین شده است. (تیم ما در حال ادامه مطالعه و بررسی روی این بخش از نرم افزار موبایلی m-PHR است. ما در مقالات آتی نتایج این کارها را ارائه خواهیم کرد.)

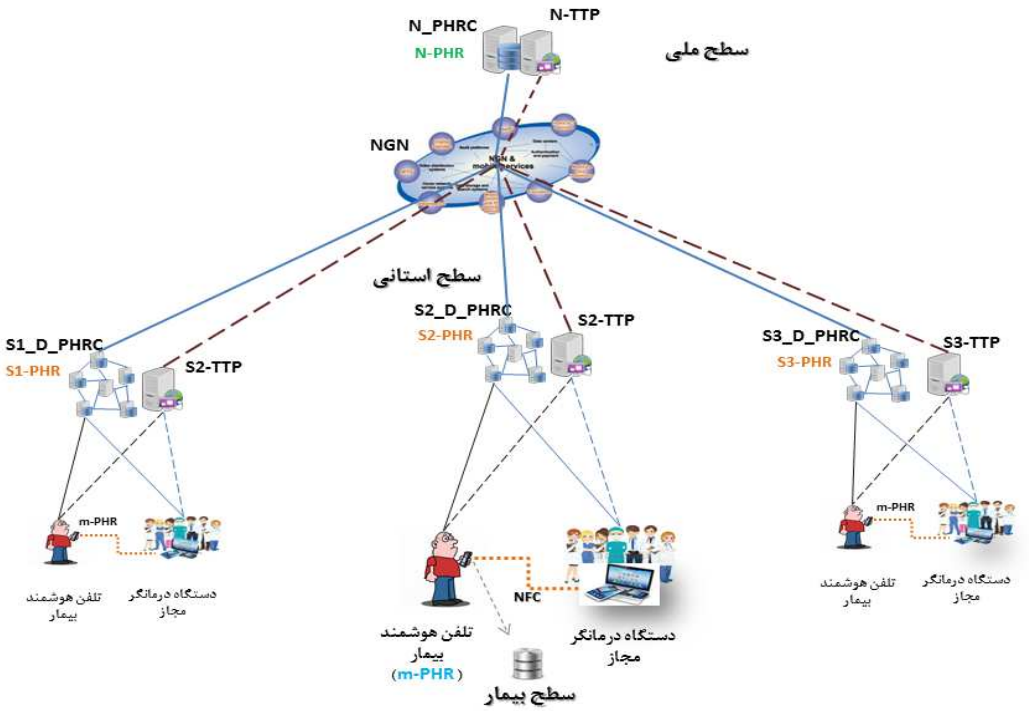
§ بخش ناامن از نرم افزار موبایلی که بر روی سیستم عامل معمولی دستگاه نصب شده و امکان حمله به آن نیز وجود دارد.

** Trusted Third Party (TTP)

ارتباطات بین سرورهای پایگاه داده‌ی مراکز درمانی تشکیل‌دهنده‌ی سیستم توزیع‌شده، با استفاده از پروتکل SSL/TLS و از طریق شبکه VPN محلی استانی صورت می‌گیرد. همچنین سیستم توزیع‌شده‌ی S_D_PHRC، بیمار و درمانگر مجاز، از طریق شبکه اینترنت (NGN) با S-TTP ارتباط برقرار می‌کنند که امنیت این ارتباطات هم از طریق پروتکل SSL/TLS تأمین خواهد شد. این ارتباط مستقیم، باعث می‌شود که احراز هویت دوطرفه بیمار و درمانگر مجاز درجایی خارج از مراکز درمانی تشکیل‌دهنده سیستم توزیع‌شده (مثلاً مطب یک پزشک که اطلاعات او در S-TTP ثبت شده است) ، امکان‌پذیر شود. لازم به ذکر است که در چنین شرایطی (که با درمانگری مجاز و/یا مرکز درمانی‌ای خارج از سیستم توزیع‌شده مواجه هستیم)، از پایگاه داده m-PHR به‌صورت آفلاین استفاده می‌شود و ازآنجایی‌که اطلاعات قبلی بیمار به‌طور کامل در حافظه تلفن هوشمند او ذخیره‌شده است نیازی به اتصال به پایگاه داده S_D_PHRC برای تکمیل اطلاعات PHR بیمار وجود نخواهد داشت.

- سطح کشوری (پایگاه داده N-PHR)

N_PHRC یک کپی از PHRهای کل بیماران یک کشور را به‌عنوان پشتیبان نگه می‌دارد. کاربرد دیگر وجود این مرکز ملی نگهداری از PHRها، زمانی است که فرد ساکنِ یک استان در حین سفر به استانی دیگر نیازمند پزشک شده و به یکی از مراکز درمانی آن استان مراجعه می‌کند. در چنین شرایطی با توجه به عدم وجود PHR آن بیمار در S_D_PHRC آن استان، یک نسخه از PHR کامل او از این پایگاه داده ملی (که حاوی کلیه PHRهای مردم آن کشور است)، در پایگاه داده استانی S_D_PHRC کپی شده و مراحل درمان بدون هیچ مانعی انجام خواهند شد. درصورتی‌که درمانگران استان مقصد، اطلاعاتی را به PHR بیمار اضافه کنند، این اطلاعات در PHR اصلی موجود در N_PHRC بازنویسی می‌شود.



شکل (۱): شمای کلی از معماری سیستم سلامت الکترونیک پیشنهادی، در یک کشور

۳-۱- مؤلفه‌های معماری پیشنهادی

معماری شکل (۱) از ۳ مجموعه مؤلفه‌ی اصلی تشکیل‌شده است که عبارت‌اند از:

۱- **PHR** (**personal Health Record**) که در اینجا به ۳ صورت N-PHR (National personal Health Record)، S-PHR (State personal Health Record) و m-PHR (mobile personal Health Record) به‌کاررفته است.
۲- **PHRC** (**personal Health Record Center**) که در اینجا در دو سطح N-PHRC (National personal Health Record Center) و S_D_PHRC (State Distributed personal Health Record Center) به‌کاررفته است.
۳- **TTP** (**Trusted Third Party**) که در اینجا به‌صورت N-TTP (National Trusted Third Party) و S-TTP (State Trusted Third Party)به‌کاررفته است.

زیرمجموعه های این سه مولفه به شرح زیر هستند:

N-PHR: پرونده سلامت شخصی بیمار که بر روی پایگاه داده ملیN-PHRC ذخیره می‌شود.

N-PHRC: پایگاه داده مرکزی شامل همه N-PHRهای بیماران در مقیاس ملی. این سرور نقش یک پشتیبان برای PHR کلیه بیماران یک کشور را، جهت دسترسی در تمامی نقاط کشور و تأمین اهداف جامعیت و دسترس‌پذیری این اطلاعات، ایفا می‌کند. بیماران و کارکنان پزشکی مرتبط در سرتاسر کشور، از طریق اینترنت و با اجازه قبلی بیمار (البته به‌غیراز موقعیت‌های اورژانسی)، به N-PHRC دسترسی پیدا می‌کنند. جهت ارائه درمان در کشورهای خارجی، فراهم‌کنندگان سرویس‌های پزشکی خارجی می‌توانند به PHR بیمار از طریق اینترنت (برای موارد پزشکی از راه دور) و یا توسط تلفن هوشمند بیمار دسترسی داشته باشند.[۱۰]

S-PHR: نسخه اصلی از PHR بیمار، که در اولین مرکز درمانی که بیمار مراجعه کرده است، برای او تشکیل و در سیستم پایگاه داده توزیع‌شده‌ی آن استان ذخیره‌شده است. این S-PHR که یک کپی به‌روز از آن بر روی N-PHRC قرار دارد، در کل آن استان به‌صورت مستقیم قابل‌دسترسی است، اما برای دسترسی از استان‌های دیگر نیاز به دریافت یک کپی از آن از پایگاه داده مرکزی N-PHRC است.

S_D_PHRC: یک پایگاه داده توزیع‌شده شامل همه S-PHRهای بیماران در مقیاس استانی. اجزای تشکیل‌دهنده این پایگاه داده توزیع‌شده، سرورهای پایگاه داده کلیه مراکز درمانی مجاز آن استان است. ساختار پیشنهادی برای این پایگاه داده توزیع‌شده در بخش ۴ شرح داده‌شده است.

N-TTP: برای مدیریت (شامل مجوزدهی، به‌روزرسانی، مانیتورینگ، فعال/غیرفعال کردن یک S-TTP)کلیه S-TTPهای آن کشور. N-TTP پایگاه‌های داده‌ای دارد که اطلاعات شناسایی کلیه بیماران (که بدون اجازه بیمار قابل‌دسترسی نیست) و درمانگران مجاز یک کشور و کلید عمومی و خصوصی آن‌ها در آن ذخیره شده است.

S-TTP: هر S-TTP مسئول مدیریت همه وظایف مرتبط با عملیات، ارتباطات و نگهداری از تلفن هوشمند بیمار، دستگاه درمانگر مجاز و S-PHRC در داخل آن استان است، همچنین برای ایجاد ارتباطات داخلی متقابل بین سیستم‌های اطلاعاتی پزشکی مختلف که به‌طور عادی (به دلیل تفاوت در فرمت داده‌هایشان) نمی‌توانند باهم ارتباط برقرار کنند. علاوه بر این S-TTP نگهدارنده اطلاعات شناسایی بیمار و درمانگر و کلید عمومی اوست. ازآنجایی‌که هر بیمار و درمانگر مجاز باید بتواند در کل کشور شناسایی شود ولیکن اطلاعات شناسایی این افراد تنها در S_TTP یک استان ثبت و ذخیره‌سازی شده است، بنابراین S-TTPی همه استان‌ها باهم به‌صورت نظیر به نظیر شبکه شده‌اند. و N_TTP به‌عنوان ناظر ارتباطات این شبکه و پشتیبان آنها نیز فعالیت می‌کند.

m-PHR: در پایین‌ترین سطح که سطح بیمار است، پایگاه داده کوچکی حاوی PHR بیمار وجود دارد، که از طریق یک نرم‌افزار موبایلی امن در دسترس بیمار و فرد درمانگر مجاز قرار می‌گیرد. این نرم‌افزار امن از دو قسمت Trusted Application* و Normal Application† تشکیل شده است که در بخش‌های مشخصی از در موبایل بیمار قرارگرفته‌اند. قرارگرفته‌اند. در این مقاله به مجموعه این نرم‌افزار موبایلی و پایگاه داده مرتبط، که PHR بیمار را تشکیل می‌دهند، m-PHR می‌گوییم.

درمانگر مجاز: هر فردی اعم از پزشک، مسئول داروخانه، آزمایشگاه، رادیولوژی و ... که قبلاً از طریق یک مرکز درمانی مجاز اقدام به ثبت‌نام در یک S-TTP کرده و بعد از دریافت اطلاعات شناسایی و تأیید هویت کامل، کلید عمومی و خصوصی دریافت کرده است.

دستگاه درمانگر مجاز: این دستگاه می‌تواند یک کامپیوتر، لپ‌تاپ، تلفن هوشمند و یا تبلت باشد. این دستگاه توسط یک درمانگر مجاز برای برقراری ارتباط با تلفن هوشمند بیمار و S-TTP مورداستفاده قرار می‌گیرد. این دستگاه برای ارتباط با دستگاه بیمار باید دارای NFC (به‌صورت تعبیه‌شده یا برچسب) باشد.

تلفن هوشمند بیمار: هر دستگاهی که قابلیت‌های یک تلفن هوشمند با پردازنده و حافظه لازم را دارا باشد تا بتواند نرم‌افزار و پایگاه داده m-PHR را نصب و مدیریت کند، می‌تواند در این جایگاه قرارگرفته و واسطه‌ای برای احراز هویت بیمار (توسط الگوی اثرانگشت و اطلاعات شناسایی ثبت‌شده بیمار در حافظه‌ی Trusted از این دستگاه و سیم‌کارت او) باشد. همچنین این دستگاه باید بتواند با استفاده از NFC با دستگاه درمانگر مجاز ارتباط برقرار کند.

NGN‡: برقراری ارتباط بی‌سیم مبتنی بر پروتکل اینترنت (IP) بین تلفن هوشمند بیمار (یعنی همان m-PHR موجود بر بر روی دستگاه بیمار) و S-TTP، و دستگاه درمانگر مجاز و S-TTP. ازآنجایی‌که سیم‌کارت‌های تلفن‌های همراه، از طریق شبکه GSM مخابراتی باهم ارتباط برقرار می‌کنند، در این مقاله از شبکه نسل جدید مبتنی بر IP به‌جای شبکه GSM استفاده شده چراکه برای نقل و انتقالات داده‌های PHRها به شبکه‌ای با قابلیت‌های بیشتر از GSM نیازمندیم. (در این مقاله از سیم‌کارت به‌عنوان یکی از مؤلفه‌های لازم جهت شناسایی مالک یک m-PHR، و یا صحت هویت درمانگر مجاز استفاده‌شده است. در مقاله آتی ساختارهای مرتبط با این بخش ارائه خواهند شد.)

---

* نرم افزار/بخشی از نرم افزار، که امنیت آن ا ز نظر فیزیکی تامین شده است. (تیم ما در حال ادامه مطالعه و بررسی روی این بخش از نرم افزار موبایلی m-PHR است. ما در مقالات آتی نتایج این کارها را ارائه خواهیم کرد.)

† بخش ناامن از نرم افزار موبایلی که بر روی سیستم عامل معمولی دستگاه نصب شده و امکان حمله به آن نیز وجود دارد.

‡ Next Generation Networks

NFC[*] در حالت شبیه‌ساز کارت: تلفن هوشمند بیمار برای ایجاد ارتباط با دستگاه درمانگر مجاز (در حدود ۱۰ سانت فاصله) باید مجهز به NFC API باشد. تلفن هوشمند بیمار با استفاده از NFC قادر به ارسال رضایت بیمار به دستگاه درمانگر مجاز یا S-TTP برای استفاده مجاز از m_PHR نصب‌شده بر روی آن، خواهد بود.

PKI: در سیستم پیشنهادی، هر بیمار و درمانگر مجاز، باید گواهینامه کلید عمومی خودش را داشته باشد. در این مقاله، PKI برای تولید پیام‌های غیرقابل‌انکار توسط تلفن هوشمند بیمار و دستگاه درمانگر مجاز کاربرد دارد.

دلیل استفاده از PHR به‌جای EHR

محتوای EHR را عمدتاً پزشکان و سایر خدمات دهندگان حوزه سلامت، بدون نظارت و اطلاع بیمار، فراهم می‌کنند. اما با توجه به اینکه یکی از تحولات اخیر درزمینه‌ی ارتقاء سلامت توانمندسازی بیماران بوده است، که بر مبنای آن هر فرد مسئولیت سلامت خود را به عهده می‌گیرد، هر بیمار باید قادر باشد تا:

- نسخه‌ای از اطلاعات سلامت که تاکنون برای او ایجاد شده است را داشته باشد.
- حداقل به‌طورکلی با محتوای سابقه طبی خود آشنا باشد.
- از تمام منابع برای یادگیری بیشتر موضوعات سلامت استفاده کند.
- با خدمات دهندگان در ارتقا سلامت خود مشارکت داشته باشد. [۹]

PHR: سیستم‌های پرونده سلامت شخصی به‌عنوان راه‌حلی برای توانمندسازی عموم مردم، با دادن مکانی برای ذخیره‌سازی و دسترسی به داده‌های سلامتشان معرفی‌شده‌اند. همچنین، آنها یک پروفایل آنلاین شخصی برای بیماران فراهم می‌کنند که امکان کنترل حریم خصوصی را به آنها می‌دهد؛ یعنی به بیمار اجازه می‌دهد که کنترل کند چه کسانی به پرونده سلامت آنها چه نوع دسترسی‌ای داشته باشند. [۵] بنابراین در طراحی این معماری از PHR استفاده شده است.

۳-۲- امنیت ارتباطات

جهت تأمین امنیت در ارتباطات معماری پیشنهادی از پروتکل‌های زیر استفاده شده است:

PKI: در این مقاله PKI برای تولید پیام‌های غیرقابل‌انکار توسط تلفن هوشمند بیمار و دستگاه درمانگر مجاز، و S-TTP کاربرد دارد. (همان‌طور که در بالا ذکر شد هر بیمار و درمانگر مجاز باید یک کلید عمومی/خصوصی جهت به رسمیت شناخته شدن و فعالیت در این ساختار، داشته باشد.)

SSL/TLS: برای برقراری یک جلسه امن بین موجودیت‌های این معماری از این نوع ارتباطات امن استفاده شده است. به عبارت دیگر برای پیاده‌سازی جلسات امن بین یک تلفن هوشمند بیمار یا یک دستگاه درمانگر مجاز با یک S-TTP، و بین یک S-TTP و N-TTP استفاده شده است. ارتباطات بین سرورهای پایگاه داده‌ی مراکز درمانی تشکیل‌دهنده‌ی سیستم توزیع‌شده، با استفاده از پروتکل SSL/TLS و از طریق شبکه VPN استانی صورت می‌گیرد. همچنین در سیستم توزیع‌شده‌ی S_D_PHRC، بیمار و درمانگر مجاز، از طریق شبکه اینترنت (NGN) با S-TTP ارتباط برقرار می‌کنند که امنیت این ارتباطات هم از طریق پروتکل SSL/TLS تأمین خواهد شد.

هر بیمار و درمانگر مجاز، می‌توانند به‌طور مستقل از یک مرکز درمانی، توسط S-TTP احراز هویت شوند. این در مواردی کاربرد دارد که یک درمانگر مجاز نیاز دارد که در خارج از محیط مرکز درمانی، هویت خود را برای دستگاه بیمار

[*] Near Field Communications

احراز کند تا بتواند از اطلاعات مجاز m-PHR جهت کمک در درمان بیمار استفاده کند. همچنین با توجه به دوطرفه بودن احراز هویت در این معماری، هویت بیمار نیز توسط S-TTP برای درمانگر مجاز احراز می‌شود.

اما درصورتی‌که بیمار بخواهد در یک مرکز درمانی مجاز اقدام به دریافت خدمات از درمانگران مجاز کند، این احراز هویت دو طرف (بیمار و درمانگر)، به‌واسطه S_D_PHRC و از طریق S-TTP صورت می‌گیرد، که در این صورت از نسخه S-PHR (سطح استانی) برای روند درمان بیمار استفاده خواهد شد و نه m-PHR دستگاه بیمار.

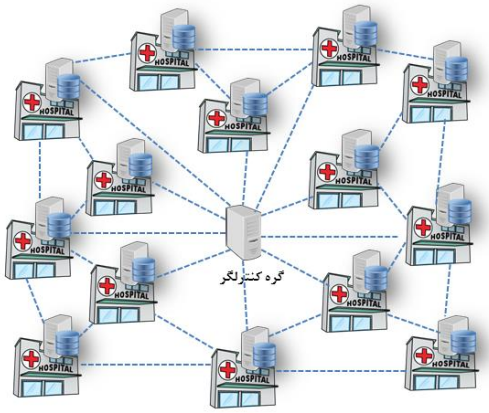
۴- پایگاه داده توزیع‌شده S_D_PHRC

برای ایجاد یک پایگاه داده توزیع‌شده از مراکز درمانی یک استان در (S_D_PHRC) از روش مطرح‌شده در مقاله [۲] استفاده کرده‌ایم.

معماری ارائه‌شده، یک سیستم مدیریت سرویس‌های سلامت یکپارچه‌سازی شده است، که یک اتصال داخلی از سیستم‌های اطلاعات ایجاد می‌کند که مقیاس آن بدون سرمایه گذاری های اضافه برای راه‌اندازی زیرساخت‌های جدید، قابل‌افزایش است.

ازآنجایی‌که چنین سیستمی از مزایای معماری توزیع‌شده بهره می‌گیرد، لازم نیست که هر کلینیکی برای مراکز داده‌ای بزرگ و گران برای خودش سرمایه‌گذاری کند. (در معماری توزیع‌شده پیشنهادی در این پروژه، سرمایه‌گذاری کمی برای زیرساخت‌ها صورت خواهد گرفت).

در این طرح چندین مرکز درمانی از طریق یک VPN محلی به هم وصل می‌شوند و پایگاه داده در میان چندین سرور توزیع خواهد شد. بنابراین از سرمایه‌گذاری‌های بزرگ برای پیاده‌سازی و مدیریت مراکز ذخیره‌سازی بزرگ جلوگیری می‌شود.



شکل (۲): معماری پیشنهادی برای پایگاه داده توزیع‌شده در S_D_PHRC

معماری پیشنهادی شکل (۲) از شبکه نظیر به نظیر استفاده می‌کند و گره‌های آن شامل سرورهای پایگاه داده‌ای می‌شود که حاوی اطلاعات سلامت بیماران مراجعه‌کننده به آن مرکز درمانی هستند. بنابراین یک مؤلفه اصلی برای پیاده‌سازی این شبکه جهت تبادل داده‌ها، سرور مانیتورینگ است که در اینجا به‌عنوان گره کنترل‌گر نشان داده شده است. این سرور یک نقش کلیدی ایفا می‌کند زیرا ابزاری است که از طریق آن داده‌های سرویس‌های سلامت ذخیره شده و برای پشتیبان گیری همگام‌سازی می‌شوند.

این سیستم نظیر به نظیر از طریق N2N [۱۱] محقق می‌شود. این یک شبکه نظیر به نظیر لایه ۲ است که مزیت‌هایی از ویژگی‌های شبکه P2P را به‌جای استفاده از لایه کاربردی به کار می‌گیرد، که کاربران می‌توانند IPی بومی* قابل رویتی بگیرند که می‌تواند از طریق یک آدرس IP محلیِ† تعیین‌شده توسط شبکه رسیده باشد.

سرورهای مستقر در مراکز درمانی متعدد به‌واسطه یک سرور مانیتور از طریق یک VPN محلی به هم متصل شده‌اند (این LAN مجازی توسط یک سرور مانیتور مدیریت می‌شود)، ولی هر یک از آنها مستندات xmlی را درباره گزارشات پزشکی یا نسخه‌های ارائه‌شده توسط آن مرکز را نگهداری می‌کند. همان‌طور که در بخش ۳-۲ بیان شد، ارتباطات در بین این مراکز درمانی از طریق پروتکل SSL/TLS صورت می‌گیرد.

یک کپی از داده‌های بیمار (به‌منظور وجود پشتیبان) روی یک سرور در مرکز داده‌ای مجزا (N-PHRC) باقی می‌ماند تا در صورت گم، سرقت و یا دستکاری شدن این اطلاعات در این پایگاه داده توزیع‌شده، مشکل عدم یکپارچگی ایجاد نشود.

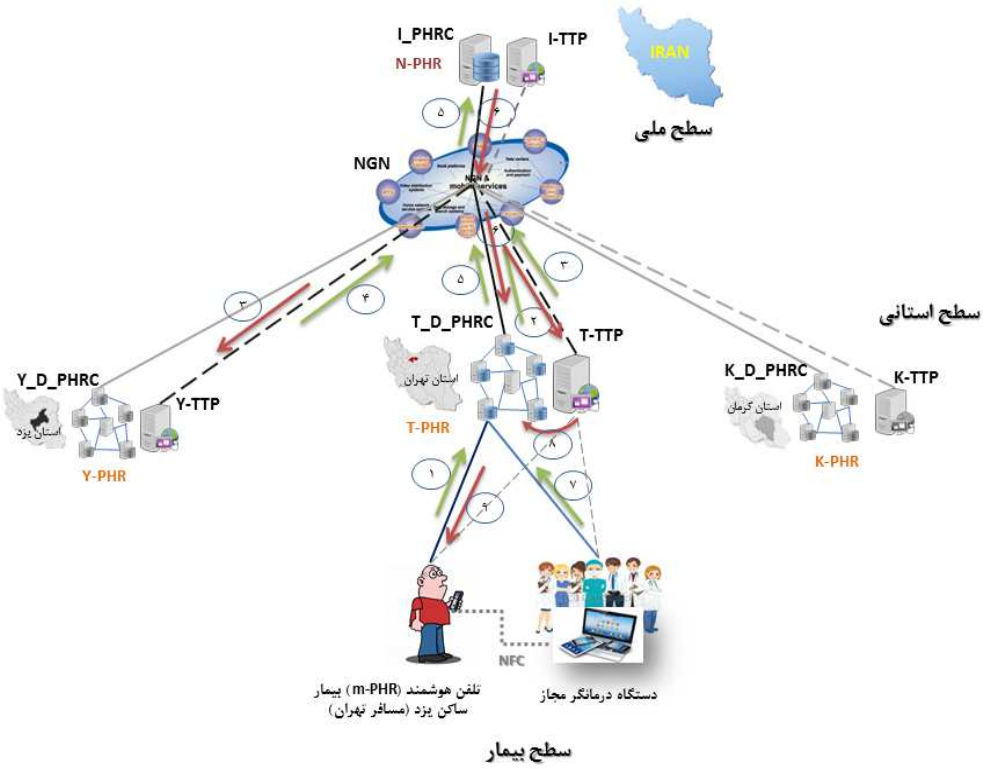
۵- معماری ارتباطی محلی (اجرای پروتکل ارتباطی در یک سناریوی نمونه)

در این بخش به‌منظور درک بهتر معماری پیشنهادی، سناریویی را با توجه به شکل (۳) توضیح داده‌ایم.

مؤلفه‌های این سناریو عبارت‌اند از:

- ✓ **I-TTP (Iran TTP)**، **I-PHRC (Iran PHRC)**: مؤلفه‌های ملی که در بخش ۳ بیان شدند که در اینجا منظور از ملی کشور ایران است.
- ✓ **T-TTP (Tehran TTP)**، **T-D-PHRC (Tehran PHRC)**: TTP استانی و پایگاه داده توزیع‌شده‌ی شامل همه مراکز درمانی مجاز استان تهران. این پایگاه داده توزیع‌شده حاوی تمامی T-PHRهای ساکنین استان تهران است.
- ✓ **Y-TTP (Yazd TTP)**، **Y-D-PHRC (Y PHRC)** و **Y-PHR**: همانند مورد بالا، برای استان یزد.

* Native IP
† Local IP



شکل (۳): شمای یک سناریو از معماری پیشنهادی، در شرایطی که بیمار مسافر استان دیگری است.

مراحل این سناریو به شرح زیر است:

۱- بیماری ساکن شهر یزد، که در حال حاضر به تهران آمده است، به علت بروز علائم یک بیماری به بیمارستانی در شهر تهران مراجعه می‌کند. این بیمار قبلاً در سیستم سلامت الکترونیک کشوری ثبت‌نام کرده و در بیمارستانی در شهر یزد y-PHR تشکیل داده و یک کپی از آن را بر روی تلفن هوشمند خود دارد. او در ابتدای ورود جهت احراز هویت، اطلاعات شناسایی خود را از طریق سامانه متصدی پذیرش به سیستم پایگاه داده توزیع‌شده T_D_PHRC می‌فرستد تا علاوه بر تأییدهویت، RHRش را نیز بازیابی کند.

۲- T_D_PHRC اطلاعات شناسایی بیمار را جهت تأییدهویت به T_TTP می‌فرستد. اما ازآنجایی‌که فرد از ساکنان شهر تهران نیست، اطلاعاتش نیز در این پایگاه داده وجود ندارد.

۳- T_TTP از طریق شبکه نظیر به نظیر، اطلاعات شناسایی بیمار را به Y_TTP (که متعلق به محل سکونت این بیمار است) می‌فرستد.

۴- Y_TTP پس از دریافت اطلاعات شناسایی بیمار، هویت او را احراز کرده و نتیجه را برای T_D_PHRC ارسال می‌کند.

۵- T_D_PHRC پس از اطمینان از صحت اطلاعات شناسایی بیمار، به دنبال PHR او در پایگاه داده توزیع‌شده‌ی استان تهران (T_D_PHRC) می‌گردد و چون موفق به یافتن آن نمی‌شود (چون این سطح از PHR بیمار تنها در

استان محل زندگی‌اش (یعنی یزد) وجود دارد)، اطلاعات شناسایی بیمار را برای پایگاه داده کشوری I_PHRC می‌فرستد.

۶- I_PHRC، یک کپی از N_PHR بیمار را برای T_D_PHRC می‌فرستد تا درمانگران مجاز قادر به دیدن و اعمال تغییرات در بخش‌های مجاز از این سند باشند. این پرونده به‌عنوان Y_PHR نیز در سطح استان تهران ذخیره می‌شود (بدین ترتیب هم برای درمانگران این استان در دسترس خواهد بود و هم مشخص می‌شود که محل زندگی این بیمار در شهر یزد است و پرونده او با این مشخصه ذخیره خواهد شد).

۷- بیمار پس از احراز هویت و انتقال پرونده‌اش به بیمارستان مقصد، به ملاقات پزشک مربوطه می‌رود. در این مرحله پزشک نیز باید احراز هویت شود تا علاوه بر شناسایی، سطح دسترسی مجاز او به PHR بیمار نیز تعیین گردد. پزشک از طریق دستگاه خود (کامپیوتر، تبلت، تلفن هوشمند) درخواست شناسایی خود را برای T_D_PHRC می‌فرستد.

۸- T_D_PHRC اطلاعات شناسایی پزشک را برای T_TTP می‌فرستد و T_TTP تأییدیه این احراز هویت را برای T_D_PHRC ارسال می‌کند. این ارتباطات از طریق شبکه NGN صورت می‌گیرد.

۹- پس از اتمام معاینه مریض، لازم است که پزشک اطلاعات جدیدی را در Y_PHR بیمار بازنویسی کند. بعد از اتمام این مرحله، اطلاعات جدید ثبت‌شده در Y_PHRبرای همگام‌سازی بر روی m_PHR و Y_PHR استان یزد (واقع در Y_D_PHRC) بازنویسی می‌شوند.

۱۰- در آخرین مرحله کلیه تغییرات صورت گرفته در Y_PHR بر روی پایگاه داده پشتیبان کشوری (I_PHRC) بازنویسی می‌شود.

۶- نتیجه‌گیری و کارهای آتی

در این پژوهش، یک معماری جامع سیستم سلامت الکترونیک برای یک کشور، با استفاده از فناوری‌های ارتباطی نو (مانند تلفن هوشمند و تبلت) ارائه شده؛ که علاوه بر ایجاد دسترس‌پذیریِ در هر مکان/ هر زمان برای پرونده‌های سلامت شخصی، امنیت اطلاعات این پرونده‌ها و حفظ حریم خصوصی بیماران (در حین تبادل آنها بین مراکز و رایانه‌های مختلف) نیز تأمین شده است. معماری پیشنهادی به دلیل استفاده از پایگاه داده توزیع‌شده بین مراکز درمانی در سطح استانی، هزینه‌های دولتی برای ایجاد زیرساخت‌های لازم را به میزان قابل‌توجهی کاهش داده و درعین‌حال امنیت، جامعیت و دسترس‌پذیری اطلاعات را افزایش داده است. ما بنا داریم که در مقالات آتی، به بیان پروتکل‌های امن ارتباطی، برای لایه‌های مختلف این معماری پرداخته و راهکاری را برای تأمین امنیت در حساس‌ترین نقطه این معماری (m-PHR که بر روی محیط ناامن سیستم عامل تلفن هوشمند بیمار قرار می‌گیرد) ارائه کنیم. به منظور ارائه این راهکار، ما در پژوهش جداگانه ای، از مفهوم محیط اجرایی امن (TEE) و سخت‌افزارهای مورداعتماد (Trusted) تعبیه‌شده در تلفن‌های هوشمند جدید استفاده کرده ایم؛ که بزودی نتایج آن را در قالب مقاله ای ارائه خواهیم کرد.

مراجع

۱. روزنامه دنیای اقتصاد، "۴.۳ میلیون پرونده بیماران، الکترونیکی شد؛ وضعیت سلامت الکترونیکی در ایران"، ۴ تیر ۱۳۹۴

2. Giorgio Mario Grasso , Alfredo Cuzzocrea , Alfredo Cuzzocrea. (2014), "A Patient-Centric Distributed Architecture for Electronic Health Record Systems", International Conference on Network-Based Information Systems.
3. Reza Hassanzadeh, Tony Sahama, Colin Fidge. (2010), "A Secure Framework and Related Protocols for Ubiquitous Access to Electronic Health Records Using Java SIM Cards", IFIP Advances in Information and Communication Technology Volume 335, 2010, pp 102-113.
4. Weider D. Yu, Mark A. Chekhanovskiy. (2007) "An Electronic Health Record Content Protection System Using SmartCard and PMR", e-Health Networking, Application and Services, 2007 9th International Conference on, 19-22 June, Taipei
5. uhammad H. Aboelfotoh, Patrick Martin, Hossam S. Hassanein. (2014), "A mobile-based architecture for integrating personal health record data", IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom).
6. R. Steele and K. Min. (2009), "Role-based access to portable personal health records," in MASS'09. International Conference on Management and Service Science. IEEE, pp. 1–4.
7. R. Steele and K. Min. (2010), "Healthpass: Fine-grained access control to portable personal health records," in 24th IEEE International Conference on Advanced Information Networking and Applications (AINA).IEEE, pp. 1012–1019.
8. Sangram Ray and G.P. Biswas. (2014), " Design of an efficient mobile health system for achieving HIPAA privacy-security regulations ", Int. J. Wireless and Mobile Computing, Vol. 7, No. 4,

۹. دبیرخانه شورای راهبری فناوری اطلاعات و ارتباطات بهداشتی (تکفاب)،"خدمات اطلاعات سلامت، نظام پرونده سلامت الکترونیک، خدمات نسخه الکترونیک، خدمات online"، http://it.behdasht.gov.ir/uploads/101_105_15.pdf

10. Sangram Ray, G. P. Biswas. (2012), " Design of RSA-CA Based E-Health System for Supporting HIPAA Privacy-Security Regulations ", 2nd International Conference on Communication, Computing & Security [ICCCS-2012], 954 – 961
11. L. Deri and R. Andrews, (2008) "N2n: A layer two peer-to-peer vpn," in Proceedings of the 2Nd International Conference on Autonomous Infrastructure, Management and Security: Resilient Networks and Services, ser. AIMS '08. Berlin, Heidelberg: Springer-Verlag, pp. 53–64.