

ارائه راه کار جهت بهبود امنیت و حریم خصوصی در سامانه سلامت همراه با استفاده از سیم کارت

مریم میایی جفال^۱، محمدعلی دوستاری^{۲*}

۱- کارشناسی ارشد، دانشگاه شاهد، ۲- استادیار، دانشگاه شاهد

(دریافت: ۹۶/۰۳/۲۲، پذیرش: ۹۷/۰۳/۲۱)

چکیده

امروزه استفاده از تلفن همراه در حوزه ارائه خدمات سلامت الکترونیک گسترش یافته است. امنیت و حریم خصوصی کاربران در سلامت الکترونیک از چالش‌های مهم محسوب می‌شود. با توجه به ماهیت دسترس‌پذیری تلفن همراه، قابلیت‌های متعدد ارتباطی و توسعه بدافزارها، امنیت در این حوزه با چالش مهمی روبروست. در این مقاله راه‌کاری جهت بهبود امنیت و حریم خصوصی در سلامت الکترونیک بر روی گوشی‌های هوشمند ارائه شده است. به این منظور ابتدا سازوکاری جهت نحوه دریافت سیم کارت سلامت توسط متقاضیان بیان شده است. در ادامه پروتکل‌های ارتباطی لازم در شرایط مختلف درمانی جهت افزایش امنیت تراکنش‌های بین ارائه‌دهندگان خدمات درمانی و بیماران که از تلفن همراه استفاده می‌کنند، ارائه شده است. با توجه به اهمیت کاهش سربار محاسباتی در پروتکل‌های پیشنهادی از رمزنگاری خم بیضوی استفاده شده است. همچنین علاوه بر امنیت، گمنامی و حریم خصوصی بیماران نیز مورد توجه قرار گرفته است. از سوی دیگر، راه‌کاری جهت ذخیره‌سازی امن اطلاعات نیز ارائه شده است. در نهایت، به مقایسه طرح پیشنهادی با سایر پژوهش‌ها پرداخته شده و سربار محاسباتی پروتکل‌ها مورد ارزیابی قرار گرفته و امنیت پروتکل‌های مطرح‌شده با استفاده از ابزار آویسپا اثبات شده است.

کلیدواژه‌ها: سلامت همراه، امنیت، حریم خصوصی، سیم کارت، احراز هویت

۱- مقدمه

دستگاه‌های قابل حمل نظیر تلفن‌های همراه، دستگاه‌های نظارت بیمار، دستیاران دیجیتال شخصی^۵ (PDAها) و سایر دستگاه‌های بی‌سیم پشتیبانی می‌کند [۳].

سرویس‌های مبتنی بر سلامت همراه، به بیماران و متخصصان حوزه سلامت اجازه می‌دهد تا به‌آسانی در هر زمان و هر مکانی به داده‌های پزشکی دسترسی یابند. همچنین بیماران به راحتی می‌توانند نیازمندی‌های سلامت خود را در خانه مدیریت کنند. در نتیجه تعداد مراجعین به بیمارستان‌ها و هزینه‌های درمانی کاهش می‌یابد. علاوه بر این پزشکان می‌توانند از راه دور بر سلامتی بیماران خود نظارت داشته باشند و بدون نیاز به ملاقات فیزیکی به آن‌ها مشاوره دهند [۴].

امروزه به سلامت همراه بیش‌ازپیش توجه می‌شود و به دلایل زیر روند رو به رشدی را در پیش گرفته است [۵]:

- ارزان است، در واقع امکانات ارتباطی گسترده‌ای را با هزینه کمتر و کارایی بالاتر ارائه می‌دهد.
- مقبولیت عمومی زیادی دارد و حس اطمینان در استفاده از کامپیوتر و فناوری ارتباطات را به همراه دارد.
- از استانداردهای جهانی رو به رشد در ارتباطات استفاده می‌کند نظیر ویدئو کنفرانس.

سازمان بهداشت جهانی^۱ سلامت الکترونیک را "استفاده ایمن و مقرون به صرفه از اطلاعات و فناوری‌های ارتباطی برای پشتیبانی از حوزه‌های سلامت و حوزه‌های مرتبط با آن، همچون خدمات مراقبت‌های بهداشتی، پیش‌سلامت، مطالعات بهداشت و درمان، آموزش پزشکی، دانش و تحقیقات سلامت" تعریف می‌کند [۱].

پرونده سلامت الکترونیک^۲ (EHR) شامل ابزارهایی جهت مدیریت اطلاعات سلامت است. مدیریت این اطلاعات به منظور ارتباط با منابع درمانی و تحلیل داده‌های جمع‌آوری شده صورت می‌پذیرد. داده‌های جمع‌آوری شده در تحقیقات و ارائه خدمات درمانی کاربرد دارد. EHR امکان سازمان‌دهی و تفسیر داده‌ها و واکنش به آن‌ها را فراهم می‌کند [۲].

سلامت همراه^۳ زیرمجموعه‌ای از سلامت الکترونیک می‌باشد. رصد جهانی سلامت الکترونیک^۴ سلامت همراه را به‌عنوان یک راه‌کار ارائه خدمات عمومی درمانی معرفی نموده است؛ که از

*ایانامه نویسنده پاسخگو: doostari@shahed.ac.ir

1- World Health Organization (WHO)
2- Electronic Health Record (EHR)
3- Mobile Health
4- Global Observatory for eHealth(GOe)

احراز هویت قوی کاربر می‌باشد. طرح‌های احراز هویت به‌طور کلی به سه دسته تقسیم می‌شوند، احراز هویت یک، دو و سه عامل. احراز هویت مبتنی بر رمز عبور احراز هویت یک عاملی گفته می‌شود. در صورتی که از کارت هوشمند نیز استفاده شود احراز هویت مبتنی بر دو عامل خواهد بود. در نهایت با افزودن یک لایه امنیتی بیشتر و استفاده از بیومتریک کاربر احراز هویت، سه عاملی است [۹].

سیم‌کارت نوعی کارت هوشمند است و از چارچوب جاوا کارت پشتیبانی می‌کند. سیم‌کارت محیط سخت‌افزاری و نرم‌افزاری چند کاربردی است. این مسئله به سایر برنامه‌ها، علاوه بر برنامه استاندارد سیم‌کارت، اجازه می‌دهد تا بر روی همان تراشه، مستقر و اجرا شوند [۱۰]. به همین منظور در این طرح از سیم‌کارت به‌عنوان کارت هوشمند سلامت استفاده شده است. که علاوه بر سایر قابلیت‌هایش، به ذخیره‌سازی و پردازش بخشی از اطلاعات سلامت می‌پردازد. همچنین امکان استفاده از المان امن^۳ موجود در سیم‌کارت جهت بهبود امنیت سخت‌افزاری طرح در نظر گرفته شده است.

در مقاله حاضر یک طرح سلامت همراه ارائه شده است که با بهره‌گیری از سیم‌کارت سلامت به بهبود امنیت و حریم خصوصی کاربران می‌پردازد. در طرح پیشنهادی ابتدا به ارائه روندی جهت توزیع ایمن سیم‌کارت سلامت با در نظر گرفتن گمنامی کاربران پرداخته شده است. سپس پروتکل‌های مراحل ثبت‌نام، احراز هویت، بازیابی و بارگذاری اطلاعات ارائه شده‌اند. در این طرح با توجه این‌که رمزنگاری خم بیضوی از نظر امنیت مشابه رمزنگاری RSA می‌باشد ولی طول کلید کوتاه‌تری دارد در نتیجه در پروتکل‌های پیشنهادی از این رمزنگاری استفاده شده است تا تطابق بیشتری با سامانه سلامت همراه داشته باشد.

در بخش ۲ به معرفی مختصر رمزنگاری خم بیضوی پرداخته می‌شود. بخش ۳ برخی راه‌کارهای سلامت الکترونیک مرور شده‌اند. در بخش ۴ کلیات طرح پیشنهادی تشریح شده است. بخش ۵ جنبه‌های امنیتی و حملات طرح پیشنهادی ارزیابی و با سایر طرح‌ها مقایسه شده است. همچنین نتایج ارزیابی با نرم‌افزار Avispa ارائه شده است. مقاله با نتیجه‌گیری در بخش ۶ به پایان می‌رسد.

۲- رمزنگاری خم بیضوی

رمزنگاری خم بیضوی^۴ (ECC) در سال ۱۹۸۵ توسط نیل کوبلیتز^۵ و ویکتور میلر^۱ کشف شد. این طرح قابلیت‌هایی همچون

- جهت پیشگیری از افزایش هزینه‌های درمانی بهداشت ضروری است.
- خدمات درمانی باکیفیت بالا در ۲۴ ساعت روز در ۷ روز هفته برای تمام شهروندان بدون در نظر گرفتن موقعیت فیزیکی فراهم می‌آورد.

در همین راستا گوشی‌های هوشمند زیرساخت^۱ قابل توجه‌ای برای مراقبت‌های بهداشتی و درمانی به‌حساب می‌آیند، به‌طوری‌که، تخمین زده شده تا پایان سال ۲۰۱۷، مجموع درآمد بازار سلامت همراه با ۶۱ درصد رشد، به ۲۶ میلیارد دلار برسد. با توجه به این‌که، دستگاه‌های سلامت همراه قابلیت جمع‌آوری اطلاعات را در بازه‌های زمانی و به‌طور پیوسته دارند، سلامت همراه امکان جمع‌آوری داده‌های پزشکی بیشتری در خصوص بیمار فراهم می‌کند. علاوه بر این، گردآوری اطلاعات در سلامت همراه صرفاً به اطلاعات پزشکی محدود نمی‌شود، بلکه بازه وسیع‌تری از اطلاعات را شامل می‌شود. به‌طور مثال، برنامه‌های سلامت همراه متعدد، اطلاعاتی در مورد سبک زندگی و فعالیت‌های بیمار را جمع‌آوری می‌کند [۶]. به همین دلیل از چالش‌های اساسی در سلامت همراه حفظ امنیت و حریم خصوصی کاربران می‌باشد.

حریم خصوصی به‌عنوان توانایی فرد یا گروه بر آشکارسازی گزینشی اطلاعات خود بر اساس تغییر شرایط معرفی نمود. محرمانگی، فرد را قادر می‌سازد تا انتشار اطلاعات سلامت خود را نزد ارائه‌دهندگان خدمات کنترل نماید. برای این منظور راه‌کارهای متعددی جهت حفظ حریم خصوصی ارائه شده است. روش‌های گمنام‌سازی، کنترل دسترسی و رمزنگاری از جمله این راه‌کارها می‌باشد [۷].

راه‌کارهای متعددی برای پیاده‌سازی و بهبود امنیت و حریم خصوصی ساختار سلامت همراه ارائه شده است. برخی از این راه‌کارها به ارائه برنامه‌های کاربردی سلامت الکترونیک بر روی پلتفرم تلفن همراه تکیه دارند. این برنامه‌ها برای ارتباط با سایر اجزای سامانه سلامت الکترونیک از امکانات و بسترهای تلفن همراه استفاده می‌کند. همچنین تلفن همراه از قابلیت‌های متعددی جهت برقراری ارتباط با سایر دستگاه‌ها از جمله NFC^۲ را دارا می‌باشد. علاوه بر این تلفن‌های همراه جدید از سخت‌افزارهای امنیتی همچون محیط اجرای قابل‌اعتماد بهره برده‌اند [۸]، که انطباق راه‌کارهای پیشنهادی با آن سبب بهبود امنیت در سطح سامانه می‌گردد.

یکی از مسائل مهم در حفظ امنیت و حریم خصوصی کاربران

3- Secure Element (SE)
4- Elliptic curve cryptography
5- Neal Koblitz

1- Platform
2- Near-field communication

را به عنوان مرکز صدور گواهی تعریف شده است. اطلاعات بیمار به طور متمرکز بر روی MCS ذخیره می شود. در این طرح پروتکل هایی جهت احراز هویت، بارگذاری و بازیابی اطلاعات درمانی از سرور مرکزی پزشکی نیز ارائه شده است. علاوه بر این که این طرح مبتنی بر کارت هوشمند می باشد به گمنامی بیمار نیز توجه نشده است.

ری و بیسواز [۱۵] راه کار دیگری را برای سلامت همراه ارائه کردند که برای ارائه خدمات از ارسال پیامک از طریق درگاه دسترسی امن جهت ارتباط با سامانه هوشمند پزشکی بهره می گیرد. این راه کار با وجود این که امکان ارائه خدمات درمانی راه دور را فراهم می آورد اما به دلیل ذخیره اطلاعات به صورت پیامک، امکان افشا و جعل هویت کاربر در صورت سرقت گوشی وجود دارد.

دوستاری و همکاران [۱۶] نیز به جهت بهبود طرح های ارائه شده توسط ری و بیسواز به ارائه راه کاری جهت برقراری نیازمندی های حریم خصوصی و امنیتی HIPAA که به گمنامی کاربران توجه دارد پرداختند. به این منظور از امضای کور عادلانه و زیرساخت کلید عمومی استفاده نمودند. با این وجود، در این طرح، احراز هویت مستقل وجود نداشت در نتیجه امکان حمله تکرار و قابلیت ردیابی بیمار فراهم است.

چادهری و همکارانش [۱۷] پروتکل احراز هویت برای سامانه اطلاعات پزشکی راه دور ارائه کرد. این طرح بهبود یافته طرح [۱۸] می باشد. در این پروتکل از رمزنگاری خم بیضوی استفاده شده است و بیومتریک بیمار جهت احراز هویت مورد استفاده قرار گرفته است. این طرح به برقراری ارتباط امن بین بیمار و پزشک با استفاده از یک سرور پزشکی مرکزی قابل اعتماد می پردازد. با این وجود احراز هویت سرور پزشکان توسط سرور مرکزی انجام نمی پذیرد.

۴- طرح پیشنهادی

اولین گام در ارائه طرحی جهت حفظ امنیت و حریم خصوصی کاربران در سلامت همراه شناخت موجودیت ها و روابط آنها با یکدیگر است. بر اساس این روابط، روال دریافت و فعال سازی سیم کارت سلامت برای کاربران تعریف می شود. گام دوم استفاده از شناسه و کلیدهای کاربر برای احراز اصالت مؤثر وی در سامانه سلامت جهت ارائه خدمات می باشد. علاوه تضمین امنیت و یکپارچگی اطلاعات در طول انتقال، جهت حفظ حریم خصوصی کاربر بایستی سازوکاری برای نگهداری ایمن اطلاعات در سرور سلامت و گوشی کاربر تعریف گردد. همچنین لازم است،

طرح RSA ارائه می کند. در یک سطح امنیتی مورد نظر طول کلید دستگاه های خم بیضوی بسیار کوچک تر از RSA می باشد. به طور مثال از نظر امنیت، امنیتی که کلید ۱۶۰-بیتی رمز مبتنی بر خم بیضوی برقرار می نماید معادل امنیتی است که کلید ۱۰۲۴-بیتی RSA ایجاد می کند [۱۱]. از این منظر ECC به عنوان یک رمزنگاری کلید عمومی کارآمد برای دستگاه های همراه شناخته شده است [۴].

فرض کنید p عدد اول و \mathbb{F}_q میدان به پیمان p باشد. یک خم بیضوی E بر بروی \mathbb{F}_q با معادله (۱) تعریف می شود [۱۱]:

$$y^2 = x^3 + ax + b \quad (1)$$

که $a, b \in \mathbb{F}_p$ در معادله (۲) صدق می کند:

$$4a^3 + 27b^2 \equiv 0 \pmod{p} \quad (2)$$

یک جفت (y, x) که $x, y \in \mathbb{F}_p$ یک نقطه روی منحنی است اگر (y, x) است در معادله صدق کند.

۳- پژوهش های پیشین

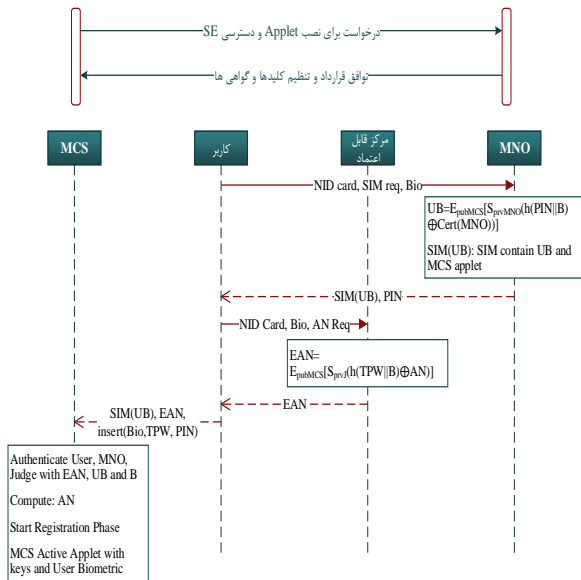
در این بخش برخی طرح های ارائه شده در سامانه سلامت الکترونیک به اختصار مرور شده است. همچنین نقاط قوت و ضعف این طرح ها بیان شده است. نقاط قوت هر یک از طرح های پیشین در طرح پیشنهادی در نظر گرفته شده است.

ستیا و همکارانش [۱۲] به ارائه معماری برای سلامت الکترونیک با کمک فناوری های NFC و المان امن پرداختند. در این معماری سه حالت استفاده از برچسب NFC، همتا با همتا NFC و شبیه ساز کارت NFC در نظر گرفته شده است. این طرح برای افزایش امنیت ذخیره سازی اطلاعات از المان امن بهره برده است. با این وجود امکان ارتباط راه دور بین کاربران فراهم نمی باشد.

لطفی و دوستاری [۱۳] پروتکلی در حوزه پرداخت سیار که مبتنی بر سناریوی ارتباطی فروشنده محور ارائه کردند. در این پروتکل از طرح کلید عمومی خودگواهی مبتنی بر رمزنگاری خم بیضوی استفاده شده است. همچنین در این طرح گمنامی مشتری و انجام تراکنش منصفانه لحاظ شده است. طرح ارائه شده در حوزه پرداخت همراه می باشد.

ری و بیسواز [۱۴] سامانه سلامت الکترونیک منطبق با نیازمندی های استاندارد HIPAA ارائه کردند. در این طرح از زیرساخت کلید عمومی استفاده شده است سرور مرکزی پزشکی^۲

کاربر برای دریافت سیم‌کارت به‌طور حضوری به MNO مراجعه می‌نماید. سیم‌کارت کاربر پس از بررسی هویت بیمار صادر می‌شود. اپراتور بیومتریک و PIN متقاضی را امضا کرده به همراه گواهی خود با کلید عمومی MCS رمز می‌کند. در واقع با این مقدار رمز شده (UB) برنامه‌ک را برای کاربر شخصی‌سازی می‌کند. جزئیات این روند در شکل (۲) نمایش داده شده است.



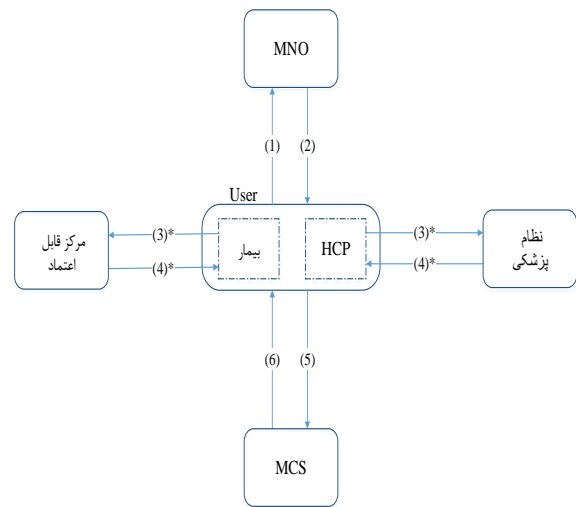
شکل (۲): روند دریافت و فعال‌سازی سیم‌کارت سلامت

از طرف دیگر بیمار برای دریافت نام مستعار خود به مرکز قابل اعتماد (Judge) مراجعه می‌نماید. مرکز پس از تأیید هویت کاربر چکیده رمز عبور موقتی و بیومتریک بیمار را به همراه نام مستعار وی امضا می‌کند و با کلید عمومی MCS رمز می‌نماید. مقدار رمز شده نام مستعار به همراه بیومتریک (EAN) تأیید مرکز بر روی نام مستعار بیمار می‌باشد. کادر درمانی نیز با ارائه مستندات تحصیلی و هویتی خود به نظام پزشکی پس از تأیید آن مقدار رمز شده و امضا شده هویت و بیومتریک خود (EHC) را دریافت می‌کنند. حال کاربر با مراجعه به MCS و ارائه (SIM(UB) و EAN برای بیماران و EHC برای کادر درمانی تقاضای ثبت‌نام در سامانه سلامت الکترونیک را می‌نمایند. MCS با ارزیابی امضاها و تأیید بیومتریک و رمز عبور ورودی کاربر، هویت کاربر را تأیید می‌کند و پس از آن مرحله ثبت‌نام در MCS آغاز می‌شود. نمادهای استفاده‌شده در طرح پیشنهادی در جدول (۱) آورده شده است.

پروتکل‌هایی جهت ارائه خدمات درمانی که با ساختار حاضر سازگاری دارد، ارائه شود.

۴-۱- روند دریافت و فعال‌سازی سیم‌کارت سلامت

کاربر بایستی جهت دریافت خدمات بهداشتی و درمانی دارای سیم‌کارت سلامت باشد. در گام اول، کاربر سیم‌کارت را از MNO دریافت می‌کند. با توجه به این‌که کاربران به‌طور کلی به دو دسته بیماران و کادر درمانی تقسیم می‌شوند، در گام دوم کادر درمانی با مراجعه به نظام پزشکی تأیید صلاحیت خود را دریافت می‌نمایند. مرکز قابل اعتمادی همچون ثبت‌احوال برای بیماران نام مستعار در نظر می‌گیرد و بیمار نام مستعار تأیید شده خود را دریافت می‌کند. این نام مستعار به جهت افزایش حریم خصوصی بیماران می‌باشد. در صورت وجود مشکل قانونی فقط مرکز قابل اعتمادی می‌تواند هویت بیمار را آشکار نماید. در گام آخر بیمار برای ثبت‌نام و عقد قرارداد به MCS مراجعه می‌نماید. این روند در شکل (۱) نمایش داده شده است.



شکل (۱): ساختار ارتباط موجودیت‌ها برای ثبت‌نام در سامانه سلامت

برای استقرار این سامانه، MCS درخواست نصب برنامه‌ک^۲ و دسترسی به SE سیم‌کارت‌ها را برای MNO ارسال می‌کند. پس از آن‌که دو طرف بر عقد قرارداد توافق نمودند، MNO کلید و گواهی لازم برای دسترسی MCS به برنامه‌ک خود بر روی SE را در اختیار وی قرار می‌دهد. بارگذاری برنامه‌ک و فعال نمودن آن توسط MCS را می‌توان از طریق پروتکل‌های OTA بر روی سیم‌کارت‌ها اجرا کرد.

3- Encrypted Anonymous Name (EAN)

4- Encrypted of Healthcare Provider Certificate(EHC)

1-Mobile Network Operator (MNO)

2-Applet

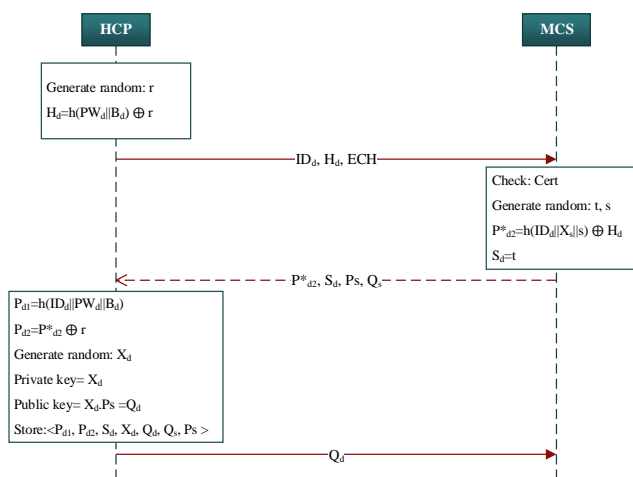
جدول (۱): نمادهای مورداستفاده در پروتکل های پیشنهادی

نماد	توضیحات
P	بیمار
D	ارائه دهنده خدمات درمانی (پزشک و ...)
S	سرور MCS
B	بیومتریک
PW	رمز عبور
AN	نام مستعار
ID	شناسه موجودیت
Tr	برچسب زمانی
Ckeys	کلید کلاس های پرونده سلامت
(X,Q)	(کلید عمومی، کلید خصوصی)
SK	کلید نشست
D/E	رمزگذاری و رمزگشایی متقارن
.	ضرب نقطه ای ECC
Ps	نقطه اولیه ECC
h()	تابع چکیده ساز یک طرفه
\oplus	عملگر XOR
	عملگر الحاق

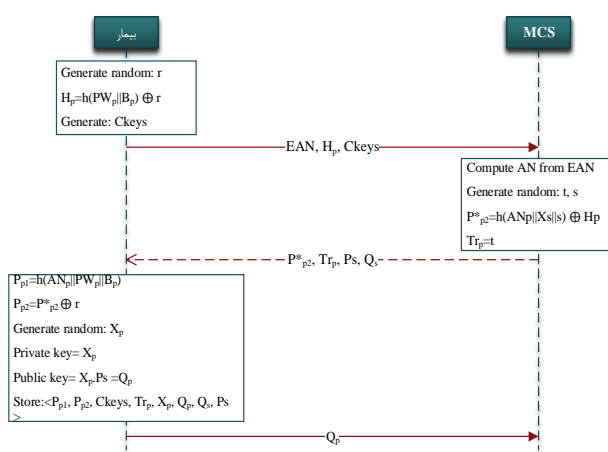
۴-۲- مرحله ثبت نام کاربر در MCS

مرحله ثبت نام پس از تأیید EAN و ECH آغاز می گردد. مرحله ثبت نام از طریق یک کانال امن و یا به صورت حضوری انجام می گردد. ابتدا بیمار مقدار H_p که ترکیبی از رمز عبور و بیومتریک بیمار می باشد را محاسبه می نماید. همچنین هسته مرکزی برنامه مجموعه کلیدهای کلاس های پرونده سلامت را تولید می کند. کاربرد این مجموعه کلید در بخش ۴-۴ تشریح خواهد شد. این مقادیر را به MCS می دهد.

MCS مقدار Tr جهت جلوگیری از حمله تکرار و P_{p2}^* که ترکیبی از مؤلفه های خصوصی سرور و بیمار می باشد، را تولید می نماید. این مقادیر را به همراه مؤلفه های رمزنگاری خم بیضوی و کلید عمومی MCS برای بیمار ارسال می گردد. بیمار پس از محاسبه P_{p1} و P_{p2} به تولید کلید خصوصی و عمومی خود می پردازد. در نتیجه مقادیر محاسبه شده را به همراه، کلید کلاس ها، مقدار Tr و زوج کلید خود در SE ذخیره می نماید به نحوی که دسترسی به این مقادیر صرفاً توسط برنامه مجاز صورت پذیرد. مرحله ثبت نام بیمار در شکل (۳) نشان داده شده است. ثبت نام ارائه دهندگان خدمات درمانی نیز تقریباً مشابه بیمار می باشد. مقدار مشترک مخفی تصادفی S_d توسط MCS برای HCP^1 ارسال می شود. مراحل ثبت نام HCP در MCS در شکل (۴) نمایش داده شده است.



شکل (۴): پروتکل مرحله ثبت نام HCP در MCS



شکل (۳): پروتکل مرحله ثبت نام بیمار در MCS

۴-۳- مرحله احراز اصالت بیمار و کادر درمانی

یکی از اصلی ترین مؤلفه ها در تضمین امنیت و حریم خصوصی کاربران، خصوصاً بیماران، احراز اصالت موجودیت هاست.

هنگامی که بیمار^۱ بخواهد خدماتی دریافت نماید، برای ایجاد نشست ایمن، احراز اصالت بین بیمار و ارائه دهنده خدمات با واسطه MCS انجام می شود. در مرحله احراز اصالت، علاوه بر

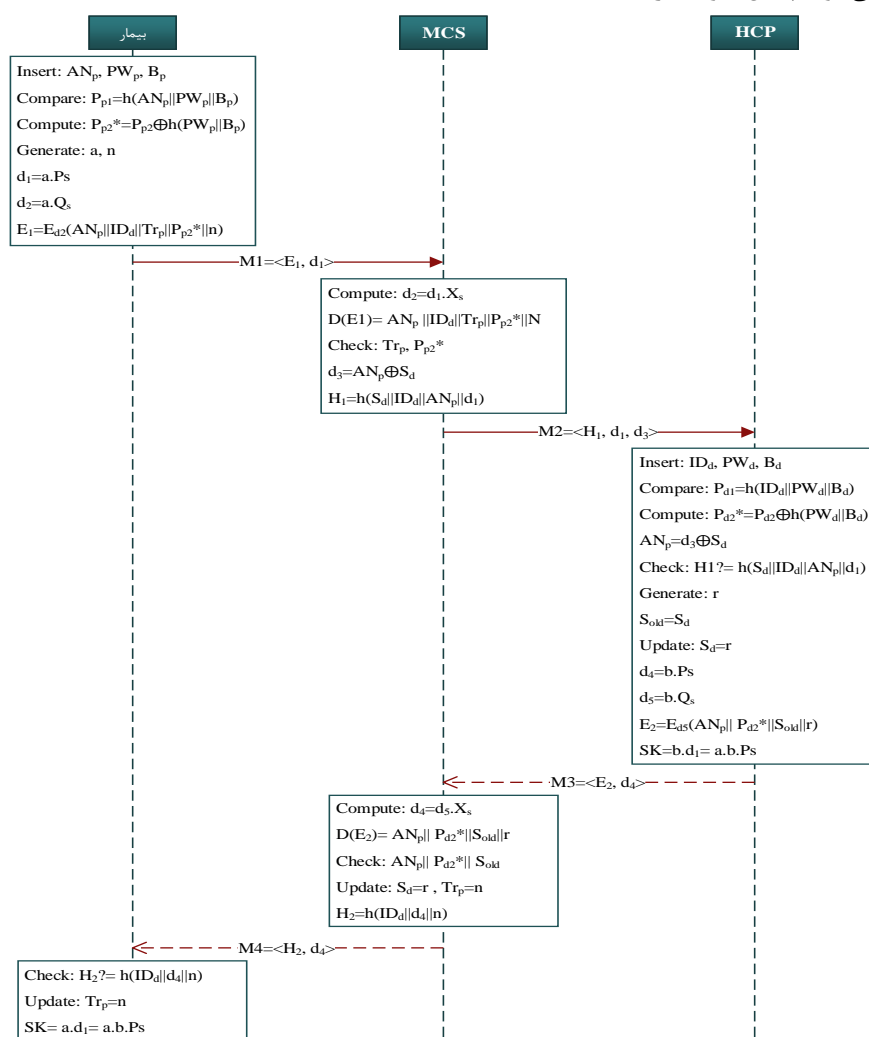
1- Health Care Provider (HCP)

MCS محاسبه می‌شود. در نهایت مقادیر E_1 و d_1 برای MCS ارسال می‌گردد.

گام ۲: MCS مقدار کلید d_2 را با ضرب نقطه‌ای کلید خصوصی خود در d_1 محاسبه می‌کند و با آن تابع E_1 را رمزگشایی می‌نماید. بر اساس AN_p مقادیر Tr و Pp_2 را ارزیابی می‌نماید. پس از احراز اصالت بیمار نزد MCS، مقادیر H_1 ، d_1 و d_3 برای HCP ارسال می‌شود

تائید هویت موجودیت‌ها برای یکدیگر، گمنامی و قابلیت عدم ردیابی بیمار نیز در نظر گرفته شده است. پروتکل احراز اصالت در شکل (۵) نمایش داده شده است. جزئیات این پروتکل در ادامه تشریح می‌شود.

گام ۱: بیمار نام مستعار، رمز عبور و بیومتریک خود را وارد می‌کند، مقدار P_{p1} محاسبه می‌شود و با مقداری که در SE محافظت می‌شود، مقایسه می‌شود. در صورت صحت، دو عدد تصادفی a و n تولید می‌شود. چالش n و مقدار d_2 با کمک مسئله



شکل (۵): پروتکل احراز اصالت بیمار و ارائه‌دهنده خدمات درمانی

مسئله ECDLP، مقدار E_2 را به محاسبه می‌نماید. همچنین مقدار تصادفی r را به‌عنوان مقدار S_d جدید برای MCS ارسال می‌نماید. در نهایت مقدار کلید نشست SK را محاسبه می‌نماید. امنیت این کلید بر اساس ECDHP می‌باشد.

گام ۴: MCS همچون گام ۲ مقدار E_2 را رمزگشایی می‌نماید. بر اساس محتوای رمزگشایی‌شده، هویت HCP را ارزیابی می‌نماید. سپس مقادیر S_d و Tr را به ترتیب بر اساس r و n به‌روز

گام ۳: HCP پس از دریافت پیام، رمز عبور و بیومتریک خود را وارد می‌کند و همچون بیمار، هویتش در سیستم کارت تائید می‌شود. سپس نام مستعار بیمار را محاسبه نموده و یکپارچگی مقدار H_1 را ارزیابی می‌کند. به دلیل آن‌که مقدار S_d مخفی مشترک متغیر در هر ارتباط بین HCP و MCS می‌باشد، بر اساس آن HCP هویت MCS را احراز می‌نماید و از عدم تکراری بودن پیام اطمینان می‌یابد. HCP با تولید عدد تصادفی b و

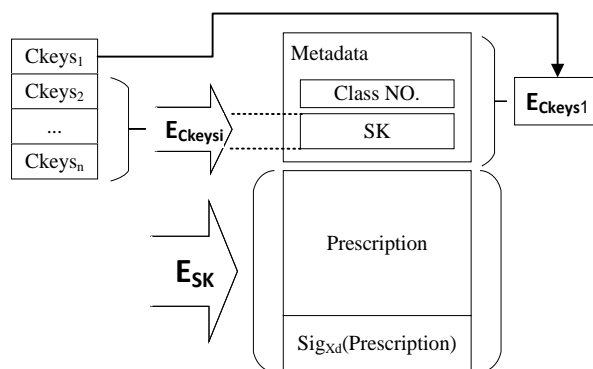
می‌نماید و مقادیر H2 و d4 را برای بیمار ارسال می‌نماید.

گام ۵: بیمار با دریافت پاسخ، مقدار H2 را ارزیابی می‌کند. به دلیل اینکه مقدار n را خود به‌عنوان چالش برای MCS ارسال نموده بود، حال هویت MCS را تأیید می‌نماید. سپس مقدار Tr خود را بر اساس n به‌روز می‌نماید. در نهایت مقدار کلید نشست SK را تقریباً مشابه HCP محاسبه می‌نماید.

۴-۴- راه کار ذخیره سازی امن

در فاز ثبت نام مجموعه کلید Ckeys تولید و به‌طور محرمانه بین سیم کارت بیمار و MCS به اشتراک گذاشته شد. این مجموعه جهت رمز کردن اجزای مختلف پرونده بیمار استفاده می‌شود. در واقع پرونده بیمار به زیرمجموعه‌های تقسیم شده و هر یک از این کلیدها متعلق به یک زیرمجموعه می‌باشد. پرونده را می‌توان بر اساس نوع داده و یا محتوای آن تقسیم‌بندی نمود. نحوه رمزگذاری و کلیدهای اختصاص داده شده برای هر نسخه در شکل ۶ نشان داده شده است.

هر نسخه بیمار با کلید نشستی که بین پزشک و بیمار توافق شده، رمز می‌شود. با توجه به اینکه کلید نشست در انتهای ارتباط از بین می‌رود و برای کاهش سرباز رمزگشایی و رمزگذاری مجدد، از کلید نشست به‌عنوان کلید رمزگذاری نسخه استفاده می‌شود. این کلید سپس با کلید کلاس مربوطه رمز شده و در فراداده^۱ نسخه به همراه شماره کلاس ذخیره می‌شود. کل فراداده نیز با کلید $Ckeys_1$ رمز می‌شود. برای رمزگذاری متادیتا تخصیص داده شده است. این ایده با الهام از ایده شرکت اپل در ذخیره سازی فایل‌ها بروی گوشی [۱۹] ارائه شده است.



شکل (۶): کلیدها و رمزگذاری نسخه بیمار

۴-۵- پروتکل‌های ارائه خدمات درمانی

برای ارائه خدمات به بیماران لازم است مراحل بارگذاری و بازیابی اطلاعات درمانی بیمار بررسی شود. همچنین بررسی راه کاری

جهت افزایش حریم خصوصی و ارائه اطلاعات به پزشکان و واحد اورژانس معتبر در شرایط اضطراری اهمیت دارد. با توجه به تأکید بر تغییر رمز عبور و بیومتریک به ارائه پروتکل سازگار با مرحله ثبت نام و احراز اصالت ضروری است. در این بخش به ارائه پروتکل‌هایی خدمات درمانی پرداخته شده است.

تمامی پروتکل‌های ارائه شده با فرض حضور فعال بیمار در هر تراکنش می‌باشد. در صورتی که نیاز به ارائه خدمات در یک بازه زمانی مشخص و توسط پزشکان و یا مراکز درمانی معین باشد، بیمار با MCS قراردادی توافق می‌نماید که به‌موجب آن در تمامی این پروتکل‌ها نقش بیمار را MCS ایفا می‌کند.

۴-۵-۱- مرحله بارگذاری اطلاعات در MCS و تلفن

هوشمند بیمار

در این مرحله بیمار یا حضوراً نزد پزشک می‌باشد و یا علائم و نتایج جمع‌آوری شده توسط حسگرهای تلفن همراه را با کلید نشست رمز کرده و برای پزشک ارسال می‌نماید. پزشک پس از تشخیص، نسخه را امضا نموده و با کلید نشست رمز می‌نماید. با تولید عدد تصادفی a، مقدار مخفی d2 محاسبه می‌شود. سپس درخواست بارگذاری به همراه شناسه پزشک و بیمار و کلید نشست با d2 رمز شده (L4) و برای MCS به همراه نسخه رمز شده ارسال می‌کند. مراحل این پروتکل در شکل (۷) نمایش داده شده است.

در ادامه MCS پس از محاسبه d2 به کمک کلید خصوصی خود، L4 را رمزگشایی می‌نماید. اعتبار کلید نشست بین پزشک و بیمار ارزیابی می‌کند. سپس نسخه بیمار را با استفاده از کلید نشست رمزگشایی می‌کند. صحت امضای پزشک بر روی نسخه را نیز بررسی می‌نماید. در نهایت بر اساس نحوه ذخیره پرونده‌ها، کلید نشست با کلید کلاس مربوطه رمز شده و نتیجه نهایی در MCS و در صورت درخواست کاربر در گوشی وی ذخیره می‌شود.

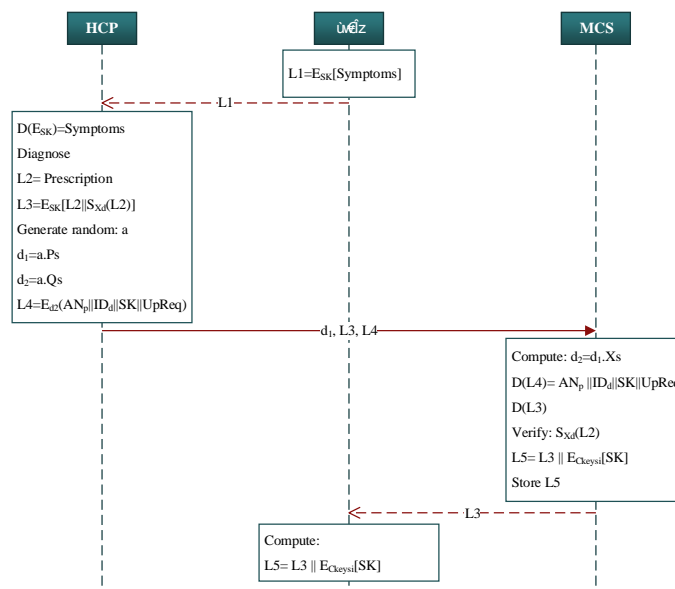
۴-۵-۲- مرحله بازیابی اطلاعات از MCS و تلفن هوشمند بیمار

بیمار

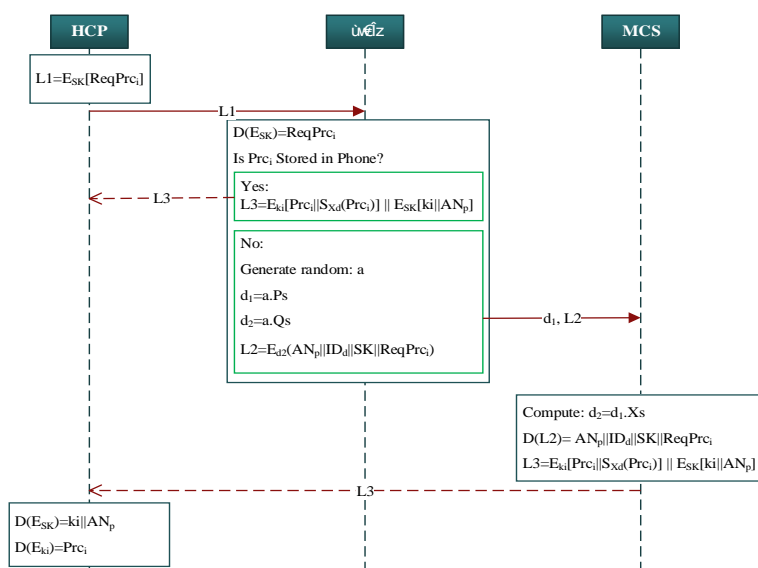
در این مرحله HCP درخواست دریافت نسخه بیمار را با کلید نشست رمز کرده، برای بیمار می‌فرستد. بیمار پس از رمزگشایی بررسی می‌نماید که آیا این نسخه در تلفن همراه وجود دارد یا خیر. در صورت وجود بیمار مقدار کلید نسخه k_i را با رمزگشایی آن توسط Ckeys محاسبه می‌نماید. سپس مقدار L3 را با ترکیب نسخه رمز شده به همراه رمزگذاری k_i با کلید نشست محاسبه می‌نماید. در نتیجه مقدار L3 را برای پزشک ارسال می‌کند. مراحل پروتکل بازیابی در شکل (۸) نشان داده شده است.

MCS پس از رمزگشایی و ارزیابی SK مقدار L3 را همانند بیمار محاسبه نموده و آن را برای HCP ارسال می‌کند.

در صورتی که نسخه در تلفن همراه ذخیره نشده باشد، بیمار مقدار رمز شده L2 را برای MCS ارسال می‌نماید. L2 شامل شناسه HCP و بیمار، کلید نشست و درخواست نسخه می‌باشد.



شکل (۷). پروتکل بازگذاری اطلاعات به پرونده بیمار



شکل (۸): پروتکل بازبایی اطلاعات از پرونده بیمار

شرایط اورژانس را در برنامه بیمار اعلام می‌نماید. پزشک پس از درخواست شناسه توسط برنامه آن را وارد می‌کند. در این زمان دو عملیات هم‌زمان انجام می‌شود.

۱. در برنامه بیمار مقدار تصادفی a محاسبه شده و با کمک ضرب نقطه‌ای مقادیر $d1$ و $d2$ محاسبه می‌شوند. سپس شناسه پزشک، نام مستعار بیمار و اعلام وضعیت اورژانس با کمک $d2$ رمز شده و به همراه $d1$ برای MCS ارسال می‌گردد.

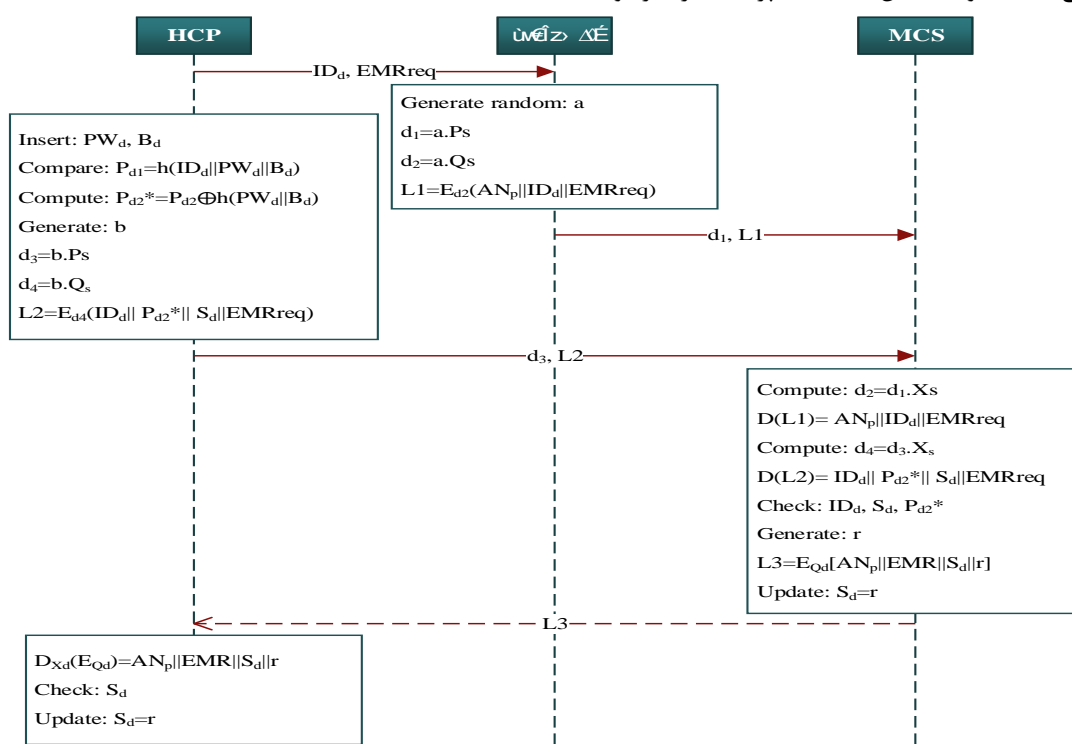
۴-۵-۳- وضعیت اورژانس

در این شرایط فرض بر این است که بخشی از اطلاعات ضروری و مهم بیمار با عنوان EMR بر روی سرور MCS ذخیره شده است. به دلیل آنکه امکان از بین رفتن تلفن همراه در شرایط اورژانس وجود دارد، اجرای این مرحله با فعال کردن سیم‌کارت بر روی دستگاه مرکز اورژانس ممکن است. با توجه به این‌که در شرایط اضطراری بیمار توانایی ورود اطلاعات را به سامانه ندارد، پزشک

پیام یکسان است، MCS به احراز اصالت HCP می پردازد. در صورتی که احراز اصالت موفقیت آمیز باشد، MCS نام گمنام بیمار به همراه پرونده EMR و عدد تصادفی r را با کلید عمومی HCP رمز می نماید. نتیجه حاصل را برای HCP ارسال می کند. مقدار r به عنوان مقدار جدید S_d در نظر گرفته می شود. HCP با رمزگشایی توسط کلید خصوصی خود به پرونده EMR بیمار دسترسی دارد. مراحل این پروتکل در شکل (۹) تشریح شده است.

۲. HCP همچون فاز احراز اصالت پس از ورود رمز عبور و بیومتریک خود، مقادیر ورودی را با مقادیر ذخیره شده مقایسه می نماید؛ سپس مقادیر مخفی خود را به همراه اعلام شرایط اورژانس (L2) رمز می کند. کلید رمزگذاری بر اساس ضرب نقطه ای ECC محاسبه می شود. HCP مقادیر محاسبه شده را برای MCS ارسال می نماید.

ابتدا MCS مقادیر دریافتی از برنامه ک بیمار و HCP را رمزگشایی می نماید. با توجه به این که شناسه پزشک در هر دو



شکل (۹): پروتکل شرایط اورژانس

۵- ارزیابی و نتایج

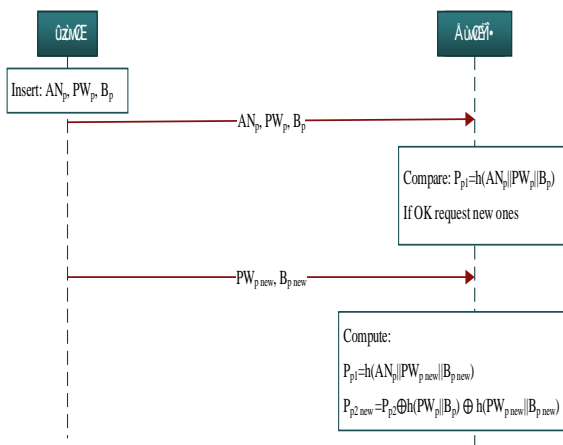
در این بخش ابتدا به معرفی و ارزیابی حملات بر روی پروتکل احراز اصالت پیشنهادی می پردازیم. سپس ویژگی های این پروتکل را مطرح نموده و تحلیل می نماییم. در نهایت به مقایسه پروتکل پیشنهادی با سایر طرح ها می پردازیم.

۵-۱- ارزیابی حملات

حمله حدس رمز عبور: این حمله، زمانی ممکن است که مهاجم یک کپی رمز شده از کلمه عبور را در کانال های ارتباطی و یا کارت های هوشمند به دست آورد. در این حمله، مهاجم با استفاده از لغت نامه رمز عبور \mathcal{P} و یا حدس هزاران رمز در ثانیه به

۴-۵-۴- تغییر رمز عبور و بیومتریک

این مرحله به دلیل اهمیت تغییر رمز عبور و بیومتریک، برای راحتی کاربر، به کمک برنامه کاربردی سلامت و برنامه صورت می پذیرد. در نتیجه نیازی به مراجعه به مرکزی جهت تغییر رمز نمی باشد. به این منظور ابتدا کاربر نام مستعار، رمز عبور و بیومتریک خود را وارد می نماید. با محاسبه مقدار $P_{p1}=h(AN_p||PW_p||B_p)$ و مقایسه آن با مقدار ذخیره شده احراز اصالت کاربر نزد سیم کارت انجام می شود. سپس از وی تقاضای ورود رمز عبور و بیومتریک جدید را می نماید. پس از ورود با محاسبه مقادیر $(P_{p1new}=P_{p2new} \oplus h(PW_p||B_p) \oplus h(PW_{p.new}||B_{p.new}))$ جدید جایگزین مقادیر قبلی می گردد.



شکل (۱۰): پروتکل تعویض رمز عبور و بیومتریک

حمله انکار سرویس^۳: در این حمله، مهاجم حجم بالایی

پیام‌های تکراری و یا نادرست را به سرور می‌فرستد تا سرور را مشغول نگه دارد و از ارائه خدمات به کاربران قانونی جلوگیری نماید [۹]. با توجه به این که پروتکل پیشنهادی نسبت به حمله تکرار مقاوم است، در صورت ارسال پیام تکراری سرور بلافاصله متوجه شده و منابع سرور صرف محاسبات اضافی نمی‌شود. از طرفی در صورت ارسال پیام نادرست نیز در اولین ارزیابی سرور به ارتباط خاتمه می‌دهد.

حمله جعل هویت^۴: در این حمله، مهاجم هویت یکی از

موجودیت‌های قانونی را برای دسترسی به سامانه سرقت می‌کند [۹]. در حمله جعل هویت کاربر، مهاجم بایستی بتواند مقدار E_1 و d_1 قانونی را تولید نماید. برای تولید E_1 باید مقدار صحیح P_{p2}^* را محاسبه نماید. محاسبه مقدار صحیح P_{p2}^* منحصر به دانستن کلید خصوصی سرور و یا هر سه عامل احراز اصالت می‌باشد. در نتیجه پروتکل در برابر حمل کاربر (بیمار و HCP) مقاوم است.

زمانی که مهاجم بخواهد هویت سرور را برای HCP جعل نماید، بایستی مقدار قانونی H_1 را برای HCP ارسال نماید. محاسبه مقدار قانونی H_1 منحصر به دانستن مخفی S_h می‌باشد. از طرف دیگر مهاجم فقط با ارسال مقدار قانونی H_2 می‌تواند هویت سرور را برای بیمار جعل نماید. با توجه به اینکه عدد تصادفی n موجود در H_2 قبلاً توسط بیمار با مقدار d_2 رمز شده است، مهاجم فقط با دانستن کلید خصوصی سرور می‌تواند مقدار n را محاسبه نماید؛ بنابراین پروتکل در برابر این حمله مقاوم است.

جستجو می‌پردازد تا انطباق آن‌ها با کلمه عبور رمز شده موفقیت‌آمیز باشد. در حدس رمز عبور آنلاین پس از تعداد محدودی حدس اشتباه، فعالیت مهاجم مسدود می‌شود. در حالی که مهاجم در حدس رمز عبور آنلاین با چنین محدودیتی مواجه نیست [۹].

فرض می‌کنیم مهاجم مقادیر P_{p2} ، P و Tr_p را به همراه بیومتریک سرقت می‌نماید. مهاجم با حدس PW_p' به محاسبه قبلی مقدار E_1 را ضبط نموده است. برای تأیید حدس رمز عبور، رمزگشایی E_1 لازم است. $E_1 = E_{d2}(AN || Tr_{pold} || P_{p2} || Tr_p)$ شامل Tr_{pold} که مقدار تصادفی حذف شده می‌باشد. مهاجم برای رمزگشایی E_1 نیاز به محاسبه d_2 بر اساس d_1 دارد که این محاسبه با توجه به مسئله ECDH بسیار دشوار است. این تحلیل به همین ترتیب برای نیز HCP نیز صادق است

حمله تکرار^۱: در حمله تکرار، دشمن کانال ارتباطی را شنود کرده و پیام‌های تأیید هویت را به دست می‌آورد. پیام‌های را مجدداً برای دسترسی و سوءاستفاده از موجودیت‌ها مورد استفاده قرار می‌دهد. حملات تکرار همچنین می‌توانند بر روی در دسترس بودن سامانه تأثیر بگذارند، به این صورتی که مهاجم پیام‌های تکراری را ارسال و سامانه به پردازش آن‌ها پردازد، حمله تکرار رخ می‌دهد [۹].

مهاجم ابتدا به ضبط پیام‌های مبادله شده می‌پردازد. در ارتباط جدید در صورت ارسال تکراری پیام M_1 سرور با مقایسه Tr_p با مقداری که در جدول خود دارد، متوجه تکراری بودن پیام می‌گردد. در صورتی که مهاجم بخواهد پیام M_2 و یا M_3 را تکرار کند، HCP و MCS بر اساس S_h به تکراری بودن پیام پی می‌برند. تکراری بودن پیام M_4 نیز با ارزیابی H_2 و مقدار n مشخص می‌شود. در نتیجه پروتکل پیشنهادی نسبت به حمله تکرار مقاوم است.

حمله داخلی ممتاز^۲: این حمله توسط یک فرد با دسترسی

مجاز به سامانه صورت می‌گیرد. فرد می‌تواند اطلاعات حساس کاربر را از سامانه سرقت نماید، از این رو حریم خصوصی، عدم ردیابی و ناشناس ماندن کاربر به راحتی توسط مهاجم به خطر می‌افتد [۹].

در مرحله ثبت نام، رمز عبور و بیومتریک با یک مقدار تصادفی ادغام شده، برای سرور ارسال می‌شود، در نتیجه کاربر ممتاز در سمت سرور به مقادیر دقیق رمز عبور و بیومتریک دسترسی ندارد. به همین دلیل پروتکل‌های ارائه شده، در برابر حمله داخلی ممتاز مقاوم است.

HCP مقادیر P_{d2} و X_d و برای سرور X_s می باشد. در صورت افشاء این اطلاعات محرمانه، مهاجم نمی تواند کلیدهای نشست قبلی را استخراج نماید. کلید نشست ترکیبی از مقادیر تصادفی موقتی می باشد که بر اساس ECDHP محافظت می شود.

توافق کلید نشست^۴: یک کلید نشست کلید متقارنی است که برای حفظ ارتباط بین دو طرف و پس از احراز اصالت موفق توافق می گردد [۹]. در پایان مرحله احراز اصالت پروتکل پیشنهادی، کلید نشست SK که ترکیبی از مقادیر تصادفی تولیدشده توسط پزشک و بیمار می باشد، محاسبه می شود. به همین منظور توافق کلید نشست در این پروتکل عادلانه است.

تغییر کارآمد رمز عبور و بیومتریک^۵: در یک پروتکل ارتباطی کارآمد جهت تعویض رمز عبور و بیومتریک نیاز به رمز عبور قبلی و مطابقت آن می باشد. رمز عبور به طور رمز نشده بر روی کانال های ارتباطی انتقال نمی یابد. همچنین قبل از ارتباط با سرور سمت کاربر ارزیابی می گردد [۹]. با توجه به اینکه سرور مقادیر رمز عبور و بیومتریک را ذخیره نمی کند، در مرحله تعویض رمز عبور و بیومتریک کاربر می تواند بدون مراجعه به سرور، تغییر را به طور امنی اعمال نماید.

۵-۳- مقایسه پروتکل پیشنهادی

در این بخش به مقایسه پروتکل های پیشنهادی با سایر پروتکل های ارائه شده می پردازیم. مقایسه کلی پروتکل های پیشنهادی در جدول (۲) آورده شده است. طرح پیشنهادی از تلفن همراه و زیرساخت های قابل اعتماد بهره می گیرد. در حالی که در طرح هایی که پروتکل های بازیابی و بارگذاری اطلاعات سلامت و ارتباط پزشک و بیمار را مطرح می کنند به این مسئله توجه ای نشده است. سر بار محاسباتی طرح پیشنهادی نسبت به طرح های قبلی به دلیل استفاده از رمزنگاری خم بیضوی کاهش یافته است.

ذخیره سازی پرونده سلامت الکترونیک در طرح های قبلی بر روی MCS بوده و در برخی از طرح ها با توجه به فضای کم حافظه ذخیره سازی کارت هوشمند چند نسخه آخر بیمار بر روی کارت ذخیره شده است. اما در طرح پیشنهادی علاوه بر ذخیره سازی بر روی MCS بر اساس حافظه ذخیره سازی تلفن همراه، بخش هایی از پرونده بر روی تلفن همراه ذخیره می شود. همان طور که در بخش ۴-۴ آورده شد، در این طرح سازوکاری جهت رمزنگاری پرونده ها ارائه کردیم تا پرونده سلامت را به بخش های مختلف تقسیم نموده و سر بار رمزنگاری مجدد پرونده را کاهش دهیم.

حمله Stolen verifier: در این حمله، مهاجم داده های ارزیابی شده را از سرور در یک نشست احراز اصالت موفق فعلی یا گذشته سرقت می کند. مهاجم با استفاده از اطلاعات به سرقت رفته، پیام های احراز اصالت را تولید کرده و آن را به سرور می فرستد. اگر سرور پیام های احراز اصالت را بپذیرد، مهاجم موفق به جعل هویت یک کاربر قانونی شده است [۹].

در پروتکل پیشنهادی، مهاجم مقادیر AN_p ، s' و Tr_p برای بیمار و مقادیر ID_d ، s و S_d را برای HCP از سرور استخراج می نماید. این اطلاعات شامل رمز عبور و بیومتریک کاربر نمی باشد. در صورتی که کلید خصوصی سرور مخفی باقی بماند، مهاجم نمی تواند با استفاده از اطلاعات استخراج شده، خود را برای سرور احراز اصالت نماید.

۵-۲- ویژگی های حریم خصوصی و امنیتی

احراز اصالت دوطرفه^۱: در پروتکل پیشنهادی، احراز اصالت دوطرفه بین تمامی موجودیت ها برقرار است. MCS با رمزگشایی E_1 و مقایسه P_{p2} بیمار را احراز اصالت می نماید، به همین ترتیب با رمزگشایی E_2 و مقایسه P_{d2} پزشک را احراز اصالت می نماید. بیمار نیز بر اساس پاسخ چالش عدد تصادفی n و مقدار سرور را احراز اصالت نموده و به طور ضمنی بر اساس $h(ID_d || d_h || n)$ پزشک را تأیید صلاحیت می نماید. از طرف دیگر پزشک با ارزیابی $h(S_d || ID_d || AN_p || d_1)$ سرور و بیمار را احراز اصالت می نماید.

گمنامی: این ویژگی به حفاظت از هویت واقعی کاربر و تضمین حریم خصوصی اشاره دارد. گمنامی عدم افشاء هویت واقعی کاربر را در طول انتقال تضمین می کند [۹]. علاوه بر اینکه بیمار از یک نام مستعار استفاده می نماید، مقدار AN در E_1 مخفیانه برای MCS ارسال می گردد. بدون دانستن کلید خصوصی MCS رمزگشایی E_1 و استخراج AN غیرممکن است.

عدم ردیابی^۲: این ویژگی تضمین می کند که مهاجم نمی تواند سلسله ارتباطات کاربر را ردیابی نماید [۹]. در پروتکل احراز اصالت، شناسه کاربر به همراه مقدار تصادفی n که متعلق به همان نشست است، رمزگذاری و ارسال می شود. در نتیجه این مقدار در هر نشست مقداری غیرقابل ردگیری است.

امنیت پیشرو^۳: این ویژگی تضمین می کند که در صورت افشاء کلید و اطلاعات محرمانه طولانی مدت، مهاجم نتواند کلید نشست های قبلی را بیابد و ارتباطات گذشته را ردیابی نماید [۹]. اطلاعات محرمانه طولانی مدت کاربر شامل P_{p2} ، AN_p و X_p برای

4- Session key agreement

5- Efficient password and biometric change

1- Mutual Authentication

2- Untraceability

3- Forward secrecy

جدول (۲): مقایسه پروتکل‌های پیشنهادی با پروتکل‌های موجود

پیشنهادی	[۱۶]	[۱۵]	[۱۴]	ویژگی‌ها	
نامتقارن	نامتقارن	نامتقارن	نامتقارن	نوع کلید	
ECC	RSA	RSA	RSA	روش رمزنگاری	
✓	x	✓	برای پزشک	فاز احراز اصالت مجزا	
✓	✓	✓	✓	کارت	فاکتورهای احراز اصالت
✓	✓	x	x	رمز عبور	
✓	✓	x	x	بیومتریک	
تلفن	کارت	تلفن/SMS	Internet	واسط ارتباط با MCS	
MCS/تلفن	MCS/کارت	MCS	MCS	محل ذخیره پرونده	
✓	x	✓	✓	دسترسی هم‌زمان به پرونده	
✓	✓	x	✓	راهکار جهت وضعیت اورژانس	
✓	✓	✓	x	مقاومت در برابر حمله تکرار	
✓	✓	✓	✓	مقاومت در برابر حمله مردمیانی	
✓	x	x	x	عدم نیاز به رمزنگاری مجدد کل پرونده	
✓	x	x	x	تغییر کارآمد رمز عبور	

جدول (۴): مقایسه ویژگی‌های امنیتی و حریم خصوصی پروتکل احراز اصالت پیشنهادی

پیشنهادی	[۱۷]	[۱۸]	ویژگی‌های امنیتی و حریم خصوصی
✓	✓	✓	احراز اصالت دوطرفه
✓	✓	✓	گمنامی
✓	✓	✓	عدم ردیابی
✓	✓	✓	امنیت پیشرو
✓	✓	✓	توافق عادلانه کلید نشست
✓	✓	x	تغییر کارآمد رمز عبور و بیومتریک
✓	x	x	احراز اصالت مبتنی بر بیومتریک پزشک

در جدول (۵)، سربرار به تفکیک هزینه محاسباتی سمت کاربر و سرور آورده شده است. این تفکیک به دلیل محدودیت محاسباتی بیشتر در سمت کاربر که از دستگاه‌هایی با توان محاسباتی محدودتر نسبت به سرور استفاده می‌کند، انجام شده است. بر اساس محاسبات، سربرار محاسباتی کاربر در پروتکل پیشنهادی بهبود جزئی نسبت به پروتکل [۱۷] و بهبود قابل توجه‌ای نسبت به پروتکل [۱۸] دارد. همچنین هزینه ارتباطی پروتکل‌ها نیز محاسبه شده‌اند. بر اساس نتایج، سربرار ارتباطی پروتکل پیشنهادی نسبت به هر دو پروتکل دیگر کاهش مناسبی داشته است.

در طرح پیشنهادی اکثر ارائه‌دهندگان خدمات درمانی مدنظر بوده و صرفاً به ارتباط پزشک و بیمار پرداخته نشده است. در مرحله اورژانس با توجه به احراز اصالت پزشک بر اساس رمز عبور و بیومتریک و همچنین ارسال شناسه پزشک توسط سیستم کارت و احتمال تخلف کاهش یافته و تخلف قابل پیگیری است.

در این طرح به ارائه مرحله احراز اصالت مجزا پرداخته‌ایم. امنیت در سایر مراحل به احراز اصالت و توافق کلید موفق وابسته است. به همین منظور در ادامه به بررسی پروتکل احراز اصالت پیشنهادی می‌پردازیم. همان‌طور که در جدول‌های (۴-۳) نمایش داده شده است و در بخش قبل تحلیل شد، پروتکل پیشنهادی تمامی این ویژگی‌ها را دارا می‌باشد. از این منظر با پروتکل [۱۷] برابر است. درحالی‌که پروتکل امین نسبت به حمله stolen verifier مقاوم نمی‌باشد.

جدول (۳): مقایسه مقاومت در برابر حملات پروتکل احراز اصالت پیشنهادی

پیشنهادی	[۱۷]	[۱۸]	مقاومت در برابر حملات
✓	✓	✓	حدس رمز عبور
✓	✓	✓	تکرار
✓	✓	✓	داخلی ممتاز
✓	✓	✓	انکار سرویس
✓	✓	✓	جعل هویت
✓	✓	x	Stolen verifier

جدول (۵): ارزیابی سربار محاسباتی و ارتباطی

هزینه ارتباطی	هزینه محاسباتی		پروتکل
	کاربر	سرور	
2048 bits	$8T_{mec} + 11T_{ha} + 4T_{eds}$	$3T_{mec} + 6T_{ha} + 1T_{eds}$	[۱۸]
	17.8517ms	6.6964ms	
1664 bits	$6T_{mec} + 9T_{ha} + 5T_{eds}$	$1T_{mec} + 4T_{ha} + 1T_{eds}$	[۱۷]
	13.3997ms	2.2398ms	
1536 bits	$6T_{mec} + 6T_{ha} + 2T_{eds}$	$2T_{mec} + 4T_{ha} + 2T_{eds}$	پیشنهادی
	13.379ms	4.4704ms	

```
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/span/span/testsuite/results/Authentication.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.22s
visitedNodes: 64 nodes
depth: 6 plies
```

```
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL
PROTOCOL
/home/span/span/testsuite/results/Authentication.if
GOAL
As Specified
BACKEND
CL-AtSe
STATISTICS
Analysed : 6 states
Reachable : 0 states
Translation: 21.50 seconds
Computation: 0.00 seconds
```

شکل (۱۱): خروجی ارزیابی پروتکل احراز اصالت با استفاده از ابزار آویسپا

۶- نتیجه گیری

در این مقاله راه کاری جهت بهبود امنیت و حریم خصوصی در سلامت الکترونیک بر روی گوشی های هوشمند ارائه شده است. در طرح پیشنهادی از سیم کارت به عنوان یک کارت هوشمند

محاسبات انجام شده در جدول (۵) بر اساس [۱۷] می باشد. بر این اساس، زمان محاسباتی برای هر یک از عملیات رمزنگاری را به صورت زیر محاسبه می کنیم: $T_{ha} \approx 0.0023ms$, $T_{eds} \approx 0.0046ms$, $T_{mec} \approx 2.226ms$. که در آن، T_{ha} زمان محاسباتی تابع چکیده ساز، T_{eds} زمان لازم برای عملیات رمزگذاری و رمزنگاری متقارن و T_{mec} زمان محاسبه ضرب نقطه ای ECC می باشد.

همچنین برای محاسبه هزینه ارتباطی طول ضرب نقطه ای ECC و خروجی تابع چکیده ساز را ۱۶۰ بیت و طول تمامی شناسه ها و اعداد تصادفی را ۳۲ بیت در نظر می گیریم. طول توابع رمزگذاری نیز مجموعی از طول ورودی تابع می باشد.

با توجه به جداول، پروتکل پیشنهادی از امنیت قابل قبولی برخوردار است. همچنین سربار ارتباطی و سربار محاسباتی آن در سمت کاربر کاهش یافته است. با این وجود سربار محاسباتی در سمت سرور نسبت به [۱۷] افزایش داشته است. این مسئله به دلیل اهمیت احراز اصالت ارائه دهندگان خدمات درمانی نزد سرور می باشد، این در حالی است که در پروتکل چادهری به این احراز اصالت توجه نشده و صرفاً سرور پزشکی به صورت ضمنی نزد بیمار احراز اصالت می شود. همچنین در پروتکل پیشنهادی ارائه دهندگان خدمات درمانی نیز همچون بیمار بر اساس سه عامل، احراز اصالت می شوند که در پروتکل [۱۷] با فرض سرور پزشکی به جای ارائه دهندگان خدمات درمانی این مسئله لحاظ نشده است.

نتیجه تحلیل امنیت پروتکل احراز اصالت پیشنهادی بر اساس ابزار آویسپا به روش OFMC و CL-AtSe در شکل (۱۱) نشان داده شده است. در این ابزار به بررسی احراز اصالت موجودیت ها و محرمانگی هر یک از اطلاعات حساس همچون رمز عبور، بیومتریک، کلید خصوصی سرور و ... پرداخته شده است. احراز اصالت پزشک و بیمار با واسطه MCS انجام می شود. بر اساس خروجی ابزار، پروتکل احراز اصالت پیشنهادی امن می باشد.

- Maghsoudloo, and M. Mayabi Joghali, "An Innovative Solution for Preventing Relay Attack on Mobile Phones Using TEE," *Journal of Electronical & Cyber Defence*, vol. 6, 2017. (in Persian)
- [9] M. U. Aslam, A. Derhab, K. Saleem, H. Abbas, M. Orgun, W. Iqbal, et al., "A Survey of Authentication Schemes in Telecare Medicine Information Systems," *Journal of medical systems*, vol. 41, p. 14, 2017.
- [10] I. Kounelis, H. Zhao, and S. Muftic, "Secure Middleware for Mobile Phones and UICC Applications," in *International Conference on Mobile Wireless Middleware, Operating Systems, and Applications*, pp. 143-152, 2011.
- [11] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*: Springer Science & Business Media, 2006.
- [12] D. Sethia, D. Gupta, T. Mittal, U. Arora, and H. Saran, "NFC based secure mobile healthcare system," in *Communication Systems and Networks (COMSNETS), 2014 Sixth International Conference on*, pp. 1-6, 2014.
- [13] A. Lotfi and M. A. Doostari, "A New M-Payment protocol Using SignCryption & Elliptic Curve Cryptography," *Journal of Electronical & Cyber Defence*, vol. 1, 2015. (in Persian)
- [14] S. Ray and G. Biswas, "A Certificate Authority (CA)-based cryptographic solution for HIPAA privacy/security regulations," *Journal of King Saud University-Computer and Information Sciences*, vol. 26, pp. 170-180, 2014.
- [15] S. Ray and G. Biswas, "Design of an efficient mobile health system for achieving HIPAA privacy-security regulations," *International Journal of Wireless and Mobile Computing*, vol. 7, pp. 378-387, 2014.
- [16] M. A. Doostari, M. Mayabi Joghali, and M. Momeny Tazangi, "Design of Protocol Providing Privacy and Anonymity in E-Health using Public Key Infrastructure," presented at the 4th International Conference on Applied Research in Computer Engineering & Signal Processing, Tehran, 2016. (in Persian)
- [17] S. A. Chaudhry, M. T. Khan, M. K. Khan, and T. Shon, "A multiserver biometric authentication scheme for TMIS using elliptic curve cryptography," *Journal of medical systems*, vol. 40, p. 230, 2016.
- [18] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, and N. Kumar, "An efficient and practical smart card based anonymity preserving user authentication scheme for TMIS using elliptic curve cryptography," *Journal of medical systems*, vol. 39, p. 180, 2015.
- [19] Apple, "iOS security, ios 8.3 or later," Apple, 2015.

جهت ذخیره‌سازی کلیدها، اجرای عملیات رمزنگاری و احراز اصالت کاربر استفاده شده است. روند ثبت‌نام و دریافت سیم‌کارت سلامت توصیف شد. همچنین امکان استفاده از المان امن و محیط اجرایی قابل اعتماد نیز در آن در نظر گرفته شده است.

بیماران در سامانه سلامت پیشنهادی، با یک نام مستعار ثبت‌نام می‌کنند. سپس در مرحله احراز اصالت، بیمار و پزشک به کمک سرور مرکزی پزشکی برای یکدیگر احراز اصالت شده و توافق کلید بین آن‌ها انجام می‌شود. در این مرحله گمنامی و عدم ردیابی بیمار جهت حفظ حریم خصوصی لحاظ شده است. همچنین پروتکل‌های بازیابی و بارگذاری اطلاعات به همراه راهکاری جهت ارائه اطلاعات حیاتی در زمان اورژانس پیشنهاد شده‌اند. راه‌کار اورژانس، در صورت از بین رفتن گوشی با سیم‌کارت قابل اجراست. در پروتکل‌های ارائه‌شده به‌جای استفاده از RSA، از رمزنگاری خم بیضوی استفاده شده است، چرا که این رمزنگاری جهت استفاده در تلفن همراه مناسب‌تر می‌باشد. برای ارزیابی پروتکل‌های پیشنهادی، ابتدا حملات مختلف و ویژگی‌های امنیتی و حریم خصوصی بیان گردید و پروتکل پیشنهادی بر اساس آن‌ها مورد تحلیل قرار گرفت و مقاومت پروتکل‌های پیشنهادی به‌صورت نظری و با کمک نرم‌افزار Avispa اثبات شد. درنهایت، به محاسبه سربرابر محاسباتی و ارتباطی پروتکل پرداخته شد که نسبت به پژوهش‌های پیشین کاهش داشته است.

۷- منابع

- [1] L. DeNardis, "Standards and eHealth," ITU-T Technology watch report, 2011.
- [2] E. H. Shortliffe and J. J. Cimino, "Biomedical informatics: computer applications in health care and biomedicine," Springer-Verlag London, 2014.
- [3] M. Kay, J. Santos, and M. Takane, "mHealth: New horizons for health through mobile technologies," 2011.
- [4] F. Zubaydi, A. Saleh, F. Aloul, and A. Sagahyoon, "Security of mobile health (mHealth) systems," in *Bioinformatics and Bioengineering (BIBE), 2015 IEEE 15th International Conference on*, pp. 1-5, 2015.
- [5] S. A. Basheer, "QUESTION 14-2/2: Mobile eHealth solutions for Developing Countries," International Telecommunication Union, 2010.
- [6] D. Kotz, S. Avancha, and A. Baxi, "A privacy framework for mobile health and home-care systems," in *Proceedings of the first ACM workshop on Security and privacy in medical and home-care systems*, pp. 1-12, 2009.
- [7] S. Sadki and H. El Bakkali, "Towards controlled-privacy in e-health: A comparative study," in *Multimedia Computing and Systems (ICMCS), 2014 International Conference on*, pp. 674-679, 2014.
- [8] S. Taremi, M. A. Doostari, S. Hajimohseni, M.

A Scheme for Improvement of Security and Privacy in Mobile Health Systems by Using SIM Card

M. Mayabi Joghhal, M. A. Doostari*

*Shahed University

(Received: 12/06/2017, Accepted: 11/06/2018)

ABSTRACT

Nowadays, mobile devices are going to be widely used in the field of e-health services. Therefore, the security and privacy of users in e-health are considered as major challenges. Due to accessibility nature of mobile, multiple communication capabilities and malware expansion, security in this area is facing major challenges. This article provides a solution to improve the security and privacy of mobile health on smartphones. Accordingly, a mechanism is proposed for obtaining a health SIM card by the applicants. Here, some communication protocols necessary in different treatment settings are provided to enhance the security of transactions between healthcare providers and patients who use mobile phones. Considering the importance of reducing the computational overhead, the elliptic curve cryptography is applied in the proposed protocols. In addition to security, attention has also been paid to anonymity and privacy of patients. Furthermore, a solution is provided for secure storage of information. Finally, the proposed plan is compared with other studies, and the computational overhead is evaluated and the security of the protocols is proved by Avispa tools.

Keywords: Mobile Health, Security, Privacy, SIM card, Authentication .