فصلنامه علمی - پژوهشی فرماندهی و کنترل، سال دوم، شماره ۲، تابستان ۱۳۹۷

ارایه چارچوب حفظ حریم‌خصوصی در سلامت الکترونیک

محمد بهشتی آتشگاه[۱]، محمدرضا عارف[۲]، مجید بیات[۳]، مرتضی براری[٤]

تاریخ دریافت: ۱۳۹۷/۰۳/۰۲ **تاریخ پذیرش: ۱۳۹۷/۰۷/۲۱**

چکیده

مفهوم اینترنت اشیاء جهان دیجیتال واقعی را می‌سازد که در آن تمامی اشیاء به یکدیگر متصل می‌باشند. این مفهوم تقریباً تمامی حوزه‌های کاربردی موجود را دچار تغییرات اساسی کرده است. حوزه سلامت هوشمند یکی از پرکاربردترین زیرحوزه‌های اینترنت اشیاء محسوب می‌گردد که امکانات و سرویس‌های پزشکی و سلامت الکترونیک جدیدی را به ارمغان آورده است. در کنار افزایش کاربرد اینترنت اشیاء و زیرحوزه‌های مختلف آن، نگرانی‌ها و مشکلات امنیتی و حریم‌خصوصی نیز به شدت افزایش یافته و تبدیل به معضل اول پیاده‌سازی مفهوم نهایی اینترنت اشیاء شده است. هر چند که تاکنون کارهای زیادی برای حفظ امنیت و حریم‌خصوصی اینترنت اشیاء و زیرحوزه‌های آن شده است اما هنوز یک چهارچوب امنیتی کامل و کارآمد که بتواند ویژگی‌های امنیتی مختلف را برآورده نماید ارایه نشده است. در این مقاله سعی داریم تا در ابتدا یک چهارچوب امنیتی و حفظ حریم‌خصوصی برای حوزه سلامت الکترونیک را که اخیراً ارایه شده است مورد بررسی قرار داده و چهارچوب کامل‌تری را ارایه نماییم که اولاً حریم‌خصوصی شناسه بیمار و محتوای پرونده او را حفظ نموده و ثانیاً ویژگی‌های امنیتی بیشتری را پوشش دهد. همچنین یک طرح احرازاصالت با ویژگی حفظ حریم‌خصوصی بیمار ارایه می‌نماییم. طرح ارایه‌شده کارآمد و سبک‌وزن بوده و تمامی ویژگی‌های امنیتی مربوطه را برآورده می‌نماید.

کلمات کلیدی: اینترنت اشیاء، سلامت هوشمند، حریم‌خصوصی، احرازاصالت، شناسه، رایانش ابری.*

[۱] دانشجوی دکتری، دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی مالک اشتر، **m_beheshti_a@mut.ac.ir**

[۲] استاد تمام، دانشکده مهندسی برق، دانشگاه صنعتی شریف، نویسنده مسئول **aref@sharif.edu**

[۳] استادیار، دانشکده مهندسی کامپیوتر؛ دانشگاه شاهد، **mbayat@shahed.ac.ir**

[٤] دانشیار، مجتمع دانشگاهی برق و کامپیوتر؛ دانشگاه صنعتی مالک اشتر، **m.barari@mut.ac.ir**

* نسخه اولیه این مقاله در کنفرانس دهمین کنفرانس ملی فرماندهی و کنترل ارایه شده است.

[Downloaded from ic4i-journal.ir on 2026-11-18]

۱. مقدمه

در این بخش، برخی از مفاهیم موردنیاز مقاله را معرفی و مرور می‌نماییم.

۱-۱. اینترنت اشیاء

مفهوم اینترنت اشیاء (IoT) به شبکه‌ای متصل و یکپارچه مبتنی بر اینترنت جهانی اشاره می‌کند که امکان تبادل اطلاعات متنوع را در حجم وسیع میان اشیای هوشمند مختلف تسهیل می‌نماید[1]. این مفهوم گسترده زیرحوزه‌های کاربردی مهم و اساسی همچون شهر هوشمند، خانه/ساختمان هوشمند، شبکه هوشمند انرژی، سلامت هوشمند و غیره دارد. برای نمونه، برخی از مثال‌های کاربردی IoT عبارتند از: مراقبت و کنترل از راه دور سلامت بیماران، کنترل مصرف انرژی، کنترل ترافیک، سیستم پاک‌کردن هوشمند، مدیریت موجودی (کالا)، زنجیره محصول، شخصی‌سازی خرید در سوپر مارکت، حفاظت مدنی. برای همه آن‌ها، کاربران نیاز به محافظت از اطلاعات شخصیشان که مربوط به جابجائی‌هایشان، عادت‌های رفتاری و تعامل با دیگران می‌شود، دارند[2]. در حقیقت با توجه به این مطلب که ارتقای سطح کیفی زندگی بشر یکی از اهداف اصلی اینترنت اشیاء به شمار می‌رود، با توسعه مفهوم اینترنت اشیاء در حوزه‌های مهمی چون سلامت هوشمند و مراقبت‌های بهداشتی شاهد بروز سرویس‌ها و خدمات هوشمند جدید به بیماران خواهیم بود. برای نمونه می‌توانیم به تجهیزات هوشمند پوشیدنی اشاره نماییم که هر کدام وظیفه سنجش و مراقبت از وضعیت قسمتهای حیاتی بدن انسان همانند قلب را برعهده دارند و به محض وقوع علائم خطرناک سلامت شخص قادرند تا به مراجع مربوطه اعلام خطر نموده و وضعیت را گزارش دهند[3].

انتظار می‌رود که در آینده‌ای بسیار نزدیک، شبکه جهانی نامتجانس IoT به لحاظ تعداد دستگاه‌های متصل به طور چشمگیری رشد داشته باشد. پیش‌بینی‌های مختلف تخمین می‌زنند که تعداد دستگاه‌های IoT به رقمی فراتر از ۱۰۰ میلیارد برسد. در واقع، IoT جهش بزرگ بعدی در دنیای فناوری خواهد بود که در آن تقریباً هر چیزی می‌تواند متصل شود[4]. در[5] و [6]، IoT به صورت "یک الگوی جدید تعریف می‌شود که اشیاء را در دنیای واقعی به دنیای مجازی پیوند می‌دهد، بنابراین امکان اتصال و ارتباط در هر زمان و برای هر چیزی و نه فقط یک نفر فراهم می‌نماید. در واقع، IoT به دنیایی اشاره می‌کند که اشیاء فیزیکی و موجودات در آن در یک فضا و زمان یکسان با هم تعامل و تراکنش دارند". هدف این مفهوم، توانمندسازی امکان ارتباط، اتصال و تبادل اطلاعات کارآمد میان مجموعه‌های بزرگی از اشیاء و موجودات نامتجانس است تا با همکاری هم سرویس‌های مفیدی را فراهم آوردند. به هر حال، IoT نگرانی‌های امنیتی و حریم‌خصوصی را با خود آورده که نیاز است تا راه‌حل‌های مناسب و در خور برای آن‌ها ارائه گردد[7].

۱-۲. حوزه سلامت الکترونیک

سازمان بهداشت جهانی[5] سلامت الکترونیک را "استفاده ایمن و مقرون‌به‌صرفه از اطلاعات و فناوری‌های ارتباطی برای پشتیبانی از حوزه‌های سلامت و حوزه‌های مرتبط با آن، همچون خدمات مراقبت‌های بهداشتی، پایش سلامت، مطالعات بهداشت و درمان، آموزش پزشکی، دانش و تحقیقات سلامت" تعریف می‌کند[8].

PHR یک داده پزشکی است که توسط خود بیمار نگهداری و مدیریت می‌گردد[9]. یک PHR خوب شامل یک پرونده کوتاه و جزئی از داده تاریخچه پزشکی بیمار

[5] *World Health Organization (WHO)*

[Downloaded from ic4i-journal.ir on 2026-11-18]

است که از منابع مختلف جمع‌آوری شده‌اند (همانند EHRs). این داده‌ها به آسانی توسط هر کسی که دسترسی مجاز به PHR داشته باشد قابل دسترسی خواهد بود.

پرونده سلامت الکترونیک[6] (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 جمع‌آوری‌شده در تحقیقات و ارائه خدمات درمانی کاربرد دارد. EHR امکان سازماندهی و تفسیر داده‌ها و واکنش به آن‌ها را فراهم می‌کند[10].

سلامت همراه[7] زیر مجموعه‌ای از سلامت الکترونیک می‌باشد. رصد جهانی سلامت الکترونیک[8] سلامت همراه را به‌عنوان یک راهکار ارائه خدمات عمومی درمانی معرفی نموده است؛ که از دستگاه‌های قابل حمل نظیر گوشی‌های موبایل، دستگاه‌های نظارت بیمار، دستیاران دیجیتال شخصی[9] (PDAها) و سایر دستگاه‌های بی‌سیم پشتیبانی می‌کند[11].

سرویس‌های مبتنی بر سلامت همراه، به بیماران و متخصصان حوزه سلامت اجازه می‌دهد تا به آسانی 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[12].

امروزه به سلامت همراه بیش از پیش توجه می‌شود و به دلایل زیر روند رو به رشدی را در پیش گرفته است[13]:

- ارزان است، در واقع امکانات ارتباطی گسترده‌ای را با هزینه کمتر و کارآیی بالاتر ارائه می‌دهد.
- مقبولیت عمومی زیادی دارد و حس اطمینان در استفاده از کامپیوتر و تکنولوژی ارتباطات را به همراه دارد.
- از استانداردهای جهانی رو به رشد در ارتباطات استفاده می‌کند نظیر ویدئو کنفرانس.
- جهت پیشگیری از افزایش هزینه‌های درمانی بهداشت ضروری است.
- خدمات درمانی با کیفیت 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 پلتفرم[10] (بستر) قابل توجه‌ای برای مراقبت‌های بهداشتی و درمانی به حساب می‌آیند، به طوری که، 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 موبایلی قابلیت جمع‌آوری اطلاعات را در بازه‌های زمانی و به طور 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. به طور مثال، برنامه‌های سلامت موبایل متعدد، اطلاعاتی در مورد سبک زندگی و فعالیت‌های بیمار را جمع‌آوری می‌کند[14]. به همین دلیل از چالش‌های اساسی در سلامت همراه حفظ امنیت و حریم خصوصی کاربران می‌باشد.

[6] *Electronic Health Record (EHR)*
[7] *Mobile Health*
[8] *Global Observatory for eHealth (GOe)*
[9] *Personal Digital Assistant (PDA)*
[10] *Platform*

[Downloaded from ic4i-journal.ir on 2026-11-18]

۳-۱. رایانش ابری در حوزه سلامت

هرچند که رایانش ابری به تنهایی با حوزه اینترنت اشیاء و زیرحوزه‌های آن متفاوت می‌باشد؛ اما باید توجه نمود که IoT بدون آمیخته‌شدن با دو فناوری رایانش ابری و داده‌بزرگ به مفهوم نهایی خود نخواهد رسید. البته در این میان باید توجه نمود که نیاز است تا جایگاه رایانش ابری برای زیرحوزه‌های مختلف IoT از جمله حوزه سلامت الکترونیک محرز و به نوعی شخصی‌سازی شود چرا که به عنوان مثال، در حالت کلی تفاوتی میان استفاده از رایانش ابری در خانمه هوشمند و استفاده از رایانش ابری در سلامت الکترونیکی وجود ندارد و نیاز است که این کاربرد در هر زیرحوزه IoT شخصی‌سازی و منحصر به فرد گردد.

فناوری رایانش ابری[11] (CC) امکان دسترسی آسان و ساده به شبکه‌ای از یک گروه مشترک از منابع پردازشی را فراهم می‌کند که در آن‌ها، نصب و حفظ داده‌ها و نرم‌افزارها با حداقل زحمت صورت می‌پذیرد. امروزه این فناوری تبدیل به یک فناوری مهم شده و بسیاری از اندیشمندان و محققان ادعا می‌کنند که رایانش ابری فرآیندهای پردازشی و بازار IT را دچار تغییرات اساسی نموده است. زمانی که دسترسی به وسیله رایانش ابری صورت می‌پذیرد، کاربران می‌توانند مجموعه‌های جامع از ابزارها برای ارزیابی کاربردهای مختلف و امکان ذخیره‌سازی داده خود بر روی سرورهای توزیع‌شده ابری را در اختیار داشته باشند و پلتفرم‌های مربوطه را از طریق فضای اینترنت مورد بهره‌برداری قرار دهند[15].

موسسه ملی استانداردها و فناوری[12] (NIST) ایالات متحده اظهار می‌کند که CC یک مُدل برای استفاده از منابع رایانه‌ای و دیگر عاملیت‌های فناورانه مُدرن در دنیای فناوری اطلاعات به منظور فراهم‌نمودن سرویس‌هایی همانند ذخیره‌سازی و کاربردهای مختلف می‌باشند[16]. کاربران می‌توانند به سرویس‌های رایانش ابری دسترسی داشته و از آن استفاده نمایند بدون آن که نیاز به کسب دانش، تجربه یا حتی مدیریت زیرساخت‌هایی را داشته باشند که این سرویس‌ها را پشتیبانی می‌نمایند. به طور کلی، سه نوع سرویس اصلی توسط ابرها پیشنهاد می‌شود[17]: نرم‌افزار به عنوان یک سرویس[13] (SaaS)، پاتفرم به عنوان یک سرویس[14] (PaaS) و زیرساخت به عنوان یک سرویس[15] (IaaS) [18]. به علاوه، چهار مُدل پیاده‌سازی برای راه‌حل‌های معماری ابری پیشنهاد شده است: ابر محرمانه[16]، ابر ارتباطی[17]، ابر عمومی[18] و ابر ترکیبی[19] [20,19]. به دلیل آن که رایانش ابری منابع توزیع شده‌ای در اینترنت و در میان چندین اینترانت قرار می‌دهد پس مبحث امنیت مسأله مهمی به شمار می‌رود.

۲. کارهای مربوطه

حریم خصوصی به‌عنوان توانایی فرد یا گروه بر آشکارسازی گزینشی اطلاعات خود براساس 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[21].

راهکارهای متعددی برای پیاده سازی و بهبود امنیت و حریم خصوصی ساختار سلامت همراه ارائه شده است.

[11] *Cloud Computing*
[12] *National Institute of Standards and Technology*
[13] *Software as a Service*
[14] *Platform as a Service*
[15] *Infrastructure as a Service*
[16] *Private cloud*
[17] *Community cloud*
[18] *Public cloud*
[19] *Hybrid cloud*

[Downloaded from ic4i-journal.ir on 2026-11-18]

برخی از این راهکارهای به ارائه برنامه‌های کاربردی سلامت الکترونیک بر روی پلتفرم تلفن همراه تکیه دارند. این برنامه‌ها برای ارتباط با سایر اجزای سیستم سلامت الکترونیک از امکانات و بسترهای موبایل استفاده می‌کند. یکی از مسائل مهم در حفظ امنیت و حریم خصوصی کاربران احرازهویت قوی کاربر می‌باشد. طرح‌های احرازهویت/احرازاصالت به طور کلی به سه دسته تقسیم می‌شوند، احرازهویت یک، دو و سه فاکتور. احرازهویت مبتنی بر رمزعبور احرازهویت یک فاکتوری گفته می‌شود. در صورتی که از کارت هوشمند نیز استفاده شود احرازهویت مبتنی بر دو فاکتور خواهد بود. در نهایت با افزودن یک لایه امنیتی بیشتر و استفاده از بیومتریک کاربر احراز هویت، سه فاکتوری است[22]. در [23]، Jiang و همکارانش یک طرح احرازاصالت سه-عاملی ارایه می‌نمایند که در حوزه سلامت هوشمند ارایه شده است. این طرح از حریم‌خصوصی شناسه کاربر محافظت می‌نماید. Irshad و همکارانش [24] به طرح Jiang و همکارانش حمله نموده و سپس یک طرح بهبویافته مبتنی بر طرح آن‌ها ارائه نمودند. در سال ۲۰۱۶، Liu و Chung [25] یک طرح احرازصالت کاربر برای شبکه‌های حسگر بی‌س‌ی‌م سلامت هوشمند ارای‌ه نمودند که در توسط Li و همکارانش در [26] مورد ارزیابی امنیتی قرار گرفته و بهبود داده شد؛ البته آن‌ها هیچ اثبات امنیتی رسمی با ابزار استاندارد ارایه نکرده‌اند.

Nordgren نیز در [27] براساس ایده حریم‌خصوصی در طراحی[20] که توسط Cavoukian و همکارانش [28] به حوزه حریم‌خصوصی در طراحی و ابعاد مختلف آن پرداخته است اما در عمل هیچ طرح، پروتکل یا چهارچوب مشخصی برای محافظت از حریم‌خصوصی ارایه نکرده است. به طور مشابه، Chen و همکارانش در [29] یک چهارچوب برای حظ حریم‌خصوصی در حوزه سلامت الکترونیک ارایه نموده‌اند اما هیچ طرح یا پروتکل کاربردی در آن معرفی نشده است. در [15]، Sahi و همکارانش یک چهارچوب برای حفظ امنیت و حریم‌خصوصی ارایه نمودند که بحث رمزگذاری پرونده شخصی الکترونیک بیمار و ذخیره‌سازی آن در ابر را با استفاده از پروتکل توافق کلید 3PAKE[21] [30] و سیستم رمزگذاری AES انجام می‌دهد. در اکثر ورش‌ها و رویکردهای ارایه‌شده مبتنی بر دانش رمزنگاری، اولیه‌ها و پروتکل‌های آن می‌باشند اما به هر حال رویکردهای غیررمزنگاری نیز ارایه شده‌اند. برای نمونه، Anjum و همکارانش در [31]، مکانیزمی برای حفظ حریم‌خصوصی در سلامت هوشمند براساس روش k-گمنامی ارایه شده است که این روش نیز هیچ اثبات امنیتی نداشته و تنها در قالب یک مدل ارایه شده است. همچنین اخیراً رویکرد دیگری توسط GabyDager و همکارانش مبتنی بر فناوری زنجیره بلوکی ارایه شده است[32]. در این مقاله، مولفین یک چهارچوبی به نام Ancile ارایه نموده‌اند که از قراردادهای هوشمند مبتنی بر زنجیره‌های بلوکی براساس رمزارز اِتریوم بهره می‌برد. هرچند که زنجیره بلوکی فناوری جدیدی است که اعتماد و امنیت را با خود به ارمغان می‌آورد اما این فناوری با محدودیت‌هایی نظیر کارآمدی، مصرف بالای انرژی، هزینه نگهداری بالا، وضعیت رگولاتوری نامشخص، نگرانی پیرامون امنیت و حریم‌خصوصی و غیره روبرو است که مانع پذیرش کاربردی این فناوری در تمامی حوزه‌ها می‌شود.

برخی از طرح‌های ارایه‌شده مبتنی بر سیم‌کارت مخابراتی شبکه سلولی می‌باشند. سیم‌کارت نوعی کارت هوشمند است و از چهارچوب جاوا کارت پشتیبانی می‌کند. سیم‌کارت محیط سخت‌افزاری و نرم‌افزاری چند

[20] *Privacy by design*

[21] *Three-Party Key Exchange Protocol*

[Downloaded from ic4i-journal.ir on 2026-11-18]

کاربردی است. این مسأله به سایر برنامه‌ها، علاوه بر برنامه استاندارد سیم‌کارت، اجازه می‌دهد تا بر روی همان تراشه، مستقر و اجرا شوند[22]. به همین منظور در بسیاری از طرح‌های ارائه‌شده در این حوزه از سیم کارت به عنوان کارت هوشمند سلامت استفاده شده است که علاوه بر سایر قابلیت‌هایش، به ذخیره‌سازی و پردازش بخشی از اطلاعات سلامت می‌پردازد. از طرفی، در طرح تحول سلامت کشور که در چند سال اخیر مطرح شده و در حال توسعه می‌باشد رویکرد استفاده از کارت هوشمند سلامت در نظر گرفته شده است. بنابراین در این مقاله، ما نیز چهارچوبی ارائه می‌نماییم که مبتنی بر کارت هوشمند سلامت بیمار بوده و حریم‌خصوصی شناسه بیمار را محافظت می‌نماید. ایده کلیات چهارچوب جدید ارایه‌شده مبتنی بر طرح Sahi و همکارانش [15] می‌باشد اما آن‌ها در طرحشان تنها از حریم‌خصوصی محتوای پرونده سلامت و آن هم با استفاده از رمزگذاری از محتوای پرونده سلامت شخصی بیمار محافظت می‌کنند. در حقیقت منظور Sahi و همکارنش از حفظ حریم‌خصوصی، محافظت از حریم‌خصوصی محتوای پرونده پرونده شخصی بیمار بوده است و آن‌ها هیچ توجهی به حریم‌خصوصی شناسه بیمار نداشته‌اند.

ادامه این مقاله بدین صورت سازماندهی شده است: در بخش بعد، کلیات چهارچوب حفظ حریم‌خصوصی ارایه‌شده مورد معرفی و بحث قرار می‌گیرد. در بخش۳، پروتکل احرازاصالت پیشنهادی با ویژگی محافظت از حریم‌خصوصی بیمار را با جزییات ارایه می‌نماییم. ویژگی‌های امنیتی مربوط به طرح احرازاصالت پیشنهادی در بخش۵ مورد بررسی و تحلیل قرار گرفته و نهایتاً با نتیجه‌گیری در بخش٦ به کار خود پایان می‌دهیم.

۳. مروری بر کلیات چارچوب ارایه‌شده

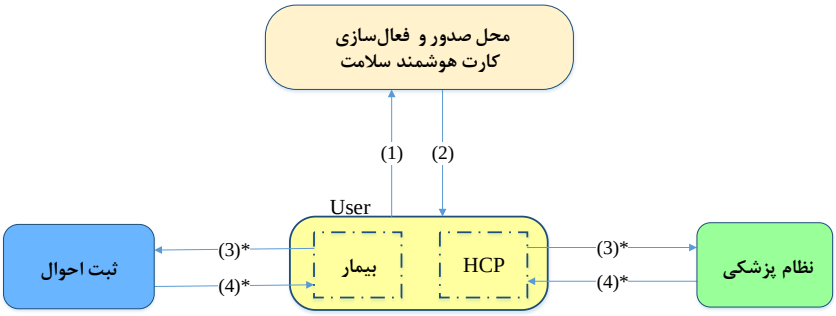
در این بخش قصد داریم تا کلیات چهارچوب حفظ حریم‌خصوصی پیشنهادی خود را ارایه نماییم. این چهارچوب پیشنهادی شامل گام‌های زیر می‌باشد:

گام ۱) اولین گام در ارائه طرحی جهت حفظ حریم خصوصی کاربران در سلامت همراه شناخت موجودیت‌ها و روابط آن‌ها با یک دیگر است. براساس این روابط، روال دریافت و فعال‌سازی کارت هوشمند سلامت برای کاربران تعریف می‌شود. در حقیقت، گام اول تعریف و فعال‌سازی کارت هوشمند سلامت بیمار می‌باشد. این کارت حاوی اطلاعات پزشکی و شخصی بیمار نظیر کلمه‌های عبور لازمه می‌باشد. همچنین می‌توان برای حفظ امنیت بیشتر کارت سلامت بیمار، چند عامل برای احراز مجوز لازم دسترسی به آن تعریف نمود که اثرانگشت بیمار می‌تواند یک‌ی از آن‌ها باشد.

گام ۲) در این گام، بیمار برای خود یک وکیل انتخاب می‌کند که می‌تواند از اعضای خانواده، آشنایان و یا دوستان او باشد. بدین منظور، ما استفاده از یک طرح امضای وکالتی دو بخشی را پیشنهاد می‌نماییم. در حقیقت، در چنین طرحی صاحب امضا (بیمار) وکالت خود را به دو بخش یعنی وکیل و میانجی امنیتی[۲۲] (SEM) اعطا می‌کند. هر زمان که وکیل بخواهد به نمایندگی از صاحب امضا، امضایی صورت داده و یا در روند احرازاصالت شرکت نماید مجبور است با SEM همکاری نماید.

[۲۲] *SEcurity Mediator*

[Downloaded from ic4i-journal.ir on 2026-11-18]



شکل ۱. صدور و فعال‌سازی کارت هوشمند سلامت بیمار.

بدین منظور، ما استفاده از یک طرح امضای وکالتی دو بخشی را پیشنهاد می‌نماییم. در حقیقت، در چنین طرحی صاحب امضا (بیمار) وکالت خود را به دو بخش یعنی وکیل و میانجی امنیتی[۲۳] (SEM) اعطا می‌کند. هر زمان که وکیل بخواهد به نمایندگی از صاحب امضا، امضایی صورت داده و یا در روند احرازاصالت شرکت نماید مجبور است با SEM همکاری نماید.

گام ۳) در این گام، بیمار به همراه وکیل خود از یک نهاد قانونی همانند ثبت‌احوال، شناسه مستعار دریافت می‌کنند. متعاقباً، آن‌ها باید براساس شناسه جدید خود کلیدهای مستعاری نیز داشته باشند. پزشکان نیز می‌توانند چنین فرآیندی را دنبال نمایند. با استفاده از شناسه‌های مستعار، شناسه واقعی بیمار و در نهایت حریم‌خصوصی شناسه بیمار مورد محافظت قرار می‌گیرند.

گام ٤) این گام شامل احرازاصالت دو طرف اصلی یعنی بیمار (به عنوان طرف اول) و پزشکان و پرستاران و به عبارت صحیح‌تر، کلیه ارائه‌دهندگان سرویس‌های پزشکی و سلامتی (به عنوان طرف دوم) می‌باشد. برای این منظور، ما یک طرح احرازاصالت پیشنهاد خواهیم نمود که از یک دروازه[۲۴] به عنوان میانجی امنیتی استفاده می‌کند. نقش دروازه را می‌تواند همان کنترل‌کننده ایفا نماید. در طی این گام، طرفین احرازاصالت، یک کلید نشست میان خود به اشتراک خواهند گذاشت که به منظور تأمین امنیت نشست مورداستفاده قرار خواهد گرفت.

گام ۵) پس از انجام موفقیت‌آمیز فرآیند احرازاصالت توسط طرفین ارتباط، مجوز دسترسی HCP ها یا همان ارائه‌دهندگان سرویس‌های سلامت به پرونده‌های PHR ذخیره‌شده در ابر صادر شده و امکان دسترسی به اطلاعات پزشکی بیمار برای HCP ها وجود خواهد داشت.

شمای کلی چهارچوب پیشنهادی در قالب شکل۲ نشان داده شده است. رویکرد ارائه‌شده برای محافظت از حریم‌خصوصی شامل موجودیت‌های زیر می‌شوند:

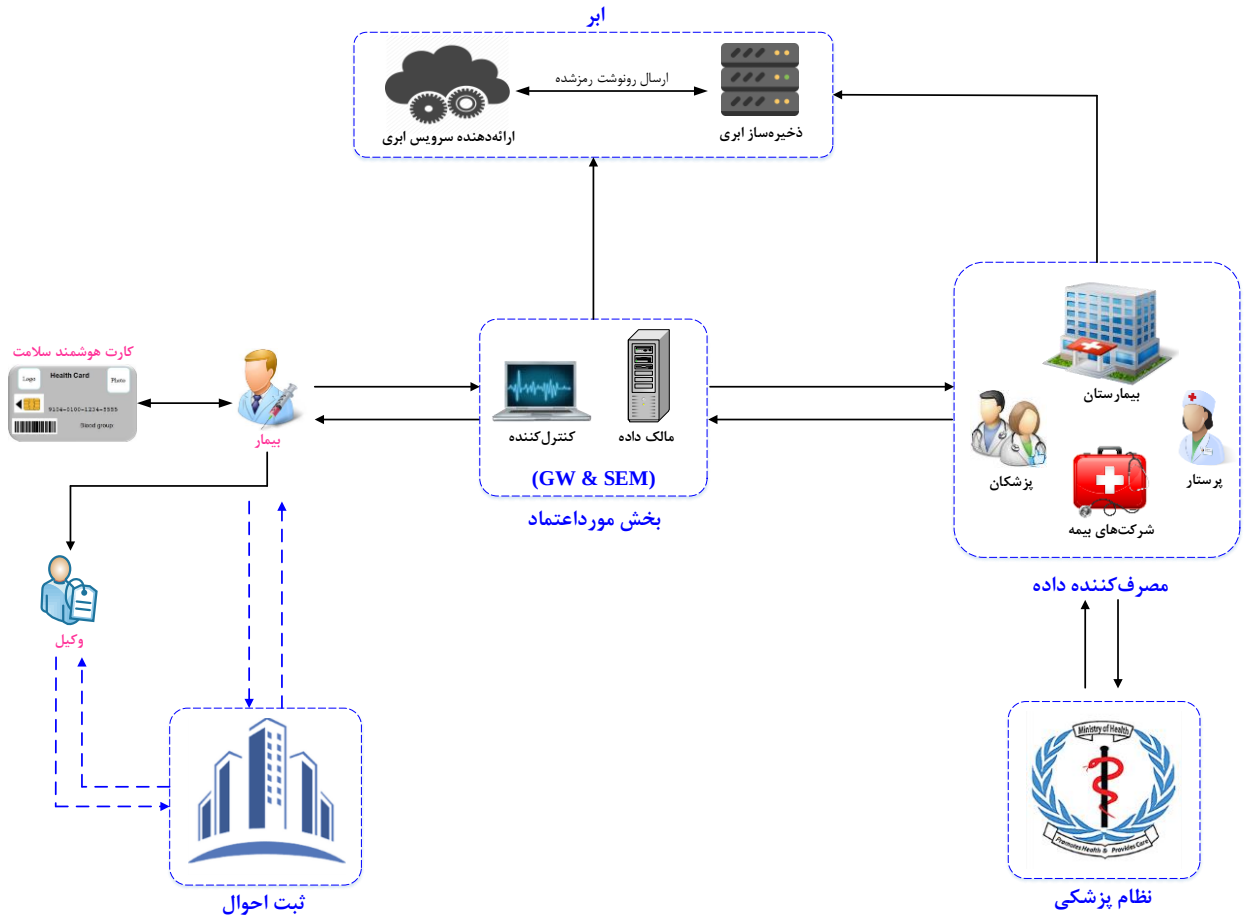
- **مصرف‌کننده داده:** افراد یا شرکت‌هایی هستند که علاقه‌مند به استفاده از داده PHR یا EHR می‌باشند. به بیان دیگر، مصرف‌کننده داده ارائه‌دهنده‌های مراقبت‌های بهداشتی همچون پزشکان و پرستاران می‌باشند.
- **کنترل‌کننده:** مسئول مذاکره و برقراری و تولید کلید نشست برای بخش‌های مربوطه می‌باشد.
- **صاحب داده:** تنها بخشی است که دسترسی کامل به داده EHR دارد.
- **بخش مورداعتماد:** دو موجودیت کنترل‌کننده و مالک‌داده توسط تمامی بخش‌ها مورد اعتماد هستند.

[۲۳] *SEcurity Mediator*

[24] *Gateway*

[Downloaded from ic4i-journal.ir on 2026-11-18]

- **بیماران:** بیمار مالک PHR خود بوده و کنترل کاملی بر حریم‌خصوصی اطلاعات PHR خود دارد. او می‌تواند نقش خود را به بخش‌های دیگر همانند یکی از اعضای خانواده و یا دوست تفویض (وکالت) یا واگذار نماید تا در مواقع ضروری به PHR خودش دسترسی داشته باشد.
- **ابر:** شامل ارائه‌دهنده سرویس ابری و ذخیره‌سازی ابری است. ارائه‌دهنده سرویس ابری به درخواست‌ها از سوی مصرف‌کننده داده پاسخ داده و سرویس متناظر آن درخواست را ارائه می‌نماید. ذخیره‌ساز ابری برای ذخیره و تسهیم داده رمزشده از مالک داده مورد استفاده قرار می‌گیرد.



شکل۲. کلیات چهارچوب پیشنهادی برای محافظت از حریم‌خصوصی.

٤. جزئیات پروتکل احرازاصالت پیشنهادی

طرح ارایه‌شده پنج فاز دارد: اخذ شناسه مستعار، آغازین، ثبت‌نام (صدور کارت)، ورود و احرازاصالت، تغییر کلمه عبور.

٤-١. فاز اخذ شناسه مستعار

به منظور حفظ حریم‌خصوصی شناسه کاربر (بیمار)، استفاده از شناسه‌های مستعار را در چهارچوب خود پیشنهاد می‌نماییم. بدین منظور در این فاز، بیمار برای اخذ شناسه مستعار اقدام می‌نماید. او چنین شناسه‌ای را می‌تواند از یک نهاد حاکمیتی همانند ثبت‌احوال درخواست نماید. همچنین برای مواقع ضروری همانند بروز انواع سکته که سطح هوشیاری خود بیمار در حد قابل قبولی نمی‌باشد، نیاز است تا یک نفر به نمایندگی از بیمار کارهای پزشکی و سلامت او را انجام دهد. لذا

[Downloaded from ic4i-journal.ir on 2026-11-18]

بیمار می‌تواند یکی از دوستان یا آشنایان خود را به عنوان وکیل معرفی نماید تا در موارد لازم بتواند کارهای پزشکی او را انجام دهد. بیمار برای موکل خود نیز شناسه مستعار درخواست می‌نماید.

٤-٢. فاز آغازین

میانجی امنیتی SEM یک گروه جمعی G با مرتبه اول بزرگ q بر روی خم $E(F_q)$ تولید می‌کند. P مولد گروه G بوده و ID_{SEM} شناسه میانجی امنیتی SEM می‌باشد. SEM همچنین کلید محرمانه خود یعنی x و دو تابع چکیده‌ساز $H(\cdot)$ و $H_1(\cdot)$ را انتخاب می‌کند.

جدول۱. شیوه نوشتاری مورداستفاده در طرح پیشنهادی

نمادها	توصیف
p, q	اعداد اول بزرگ
$E(F_q)$	خم‌بیضوی E بر روی میدان متناهی F_q
G	زیرگروه F_q با مرتبه اول q
P	مولد گروه G
SEM, x_{SEM}	میانجی امنیتی و کلید محرمانه متناظر آن
p_i, ID_i, PW_{p_i}	بیمار i–اُم، شناسه و کلمه عبور او
d_j, ID_j	پزشک j–اُم و شناسه آن
pr_i, ID_{pr_i}	وکیل بیمار i–اُم و شناسه آن
ID_i', ID_{pr_i}'	شناسه مستعار بیمار و وکیل او
sk_p, sk_d	کلید نشست محاسبه‌شده توسط بیمار و پزشک
$H(\cdot), H_1(\cdot)$	توابع چکیده‌ساز یکطرفه
T_i	مُهر زمانی بیمار p_i
$\mathcal{A}$	مهاجم (حمله‌کننده)
l	پارامتر امنیتی سیستم
$E_k(\cdot)/D_k(\cdot)$	توابع رمزگذاری/رمزگشایی متقارن با کلید k
$a \oplus b, a \parallel b$	عملیات الحاق و جمع پیمانه‌ای رشته‌های a و b
$a \stackrel{?}{=} b$	بررسی این که آیا a و b با هم برابرند؟

٤-٣. فاز ثبت‌نام

این فاز شامل فرآیند ثبت‌نام بیمار p_i و پزشک d_j می‌باشد.

برای p_i:

- کاربر p_i عدد تصادفی r_0 و کلمه‌عبور PW_i را انتخاب می‌کند. پس از آن، او عبارت $MP_i = h(r_0 \parallel PW_i)$ را محاسبه نموده و $\{MP_i, ID_i', ID_i, ID_{pr_i}, ID_{pr_i}'\}$ را از طریق یک کانال امن به SEM ارسال می‌کند.

$$MP_i = h(r_0 \parallel PW_i) \quad (۱)$$

- SEM عبارت $e_i = h(ID_{SEM} \parallel x \parallel ID_i') \oplus MP_i$ و $f_i = h(ID_i' \parallel x) \oplus ID_i'$ را محاسبه نموده و (e_i, f_i, P, p, q) را در داخل کارت هوشمند تزریق کرده و شناسه ID_i و ID_i' را در پایگاه داده ذخیره نموده و کارت هوشمند سلامت را از طریق یک کانال امن به بیمار p_i ارسال می‌کند.

$$e_i = h(ID_{SEM} \parallel x \parallel ID_i') \oplus MP_i \quad (۲)$$

$$f_i = h(ID_i' \parallel x) \oplus ID_i' \quad (۳)$$

- p_i عبارت $d_i = h(ID_i \parallel PW_i) \oplus r_0$ را در داخل کارت هوشمند ذخیره می‌کند.

$$d_i = h(ID_i' \parallel PW_i) \oplus r_0 \quad (٤)$$

برای d_j:

- d_j شناسه خود یعنی ID_j را از طریق یک کانال امن در میانجی امنیتی SEM ثبت می‌کند.
- SEM عبارت $c_j = h(ID_j \parallel x)$ را محاسبه نموده و سپس آن را از طریق یک کانال امن به d_j ارسال می‌کند. d_j همچنین ID_j و c_j را ذخیره می‌کند.

[Downloaded from ic4i-journal.ir on 2026-11-18]

٤-٤. فاز ورود و احرازاصالت

- p_i کارت هوشمند خود را در داخل کارتخوان قرار داده، ID_i' و PW_i را وارد می‌نماید. کارت هوشمند عبارت‌های $r_1 = d_i \oplus h(ID_i' \| PW_i)$ و $MP_i = h(r_1 \| PW_i)$ را محاسبه می‌کند.

$$r_1 = d_i \oplus h(ID_i' \| PW_i) \quad (٥)$$

$$MP_i = h(r_1 \| PW_i) \quad (٦)$$

- p_i اعداد تصادفی $\alpha \in [1, q-1]$، r_2 و r_3 را به همراه پزشک موردنظر خود یعنی d_j انتخاب نموده، همچنین یک مُهر زمانی T_i را به دست آورده و سپس $MI_i^{new} = h(r_2 \| ID_i')$، $B_1 = e_i \oplus MP_i \oplus r_3$، $B_2 = \alpha P$، $B_3 = f_i \oplus ID_i' \oplus MI_i^{new} \oplus h(r_3 \| ID_i')$، $B_4 = h(ID_i \| h(r_3 \| MI_i^{new} \| ID_j) \oplus ID_i'$ و $B_5 = h(ID_i' \| MI_i^{new} \| ID_j)$ را محاسبه می‌نماید.

$$MI_i^{new} = h(r_2 \| ID_i') \quad (٧)$$

$$B_1 = e_i \oplus MP_i \oplus r_3 \quad (٨)$$

$$B_2 = \alpha P \quad (٩)$$

$$B_3 = f_i \oplus ID_i' \oplus MI_i^{new} \oplus h(r_3 \| ID_i') \quad (١٠)$$

$$B_4 = h(r_3 \| MI_i^{new} \| B_2) \oplus ID_i' \quad (١١)$$

$$B_5 = h(ID_i \| ID_i' \| MI_i^{new} \| ID_j \| T_i) \quad (١٢)$$

سپس او پیام M_1 را به میانجی امنیتی SEM ارسال می‌کند.

$$M_1 = \{MI_i, ID_j, B_1, B_2, B_3, B_4, B_5, T_i\} \quad (١٣)$$

- SEM اعتبار $|T - T_i| < \Delta$ را بررسی می‌کند که در آن، T نشان‌دهنده زمان حاضر و Δ یک تأخیر از پیش تعریف‌شده می‌باشد. اگر $|T - T_i| > \Delta$ باشد، میانجی امنیتی نشست را لغو می‌کند. اگر T_i پذیرفته گردد، SEM عبارت‌های $r_3 = B_1 \oplus h(ID_{SEM} \| x \| ID_i')$، $MI_i^{new} = B_3 \oplus h(ID_i' \| x) \oplus h(r_3 \| ID_i')$، $B_3 = f_i \oplus ID_i' \oplus MI_i^{new} \oplus h(r_3 \| ID_i')$ را محاسبه می‌کند.

$$r_3 = B_1 \oplus h(ID_{SEM} \| x \| ID_i') \quad (١٤)$$

$$MI_i^{new} = B_3 \oplus h(ID_i' \| x) \oplus h(r_3 \| ID_i') \quad (١٥)$$

$$ID_i' = B_4 \oplus h(r_3 \| MI_i^{new} \| B_2) \quad (١٦)$$

سپس، SEM بررسی می‌کند که آیا ID_i' در پایگاه داده وجود دارد و اگر وجود داشت مقدار واقعی آن یعنی ID_i زا برداشته و $B_5 = h(ID_i \| ID_i' \| MI_i^{new} \| ID_j)$ را محاسبه نموده و بررسی می‌کند که آیا این رابطه برقرار است یا نه. اگر نباشد نشست رد می‌شود. در غیر این صورت، SEM عدد تصادفی $\lambda \in [1, q-1]$ و یک مُهر زمانی T_G را انتخاب و عبارت‌های زیر را محاسبه می‌کند:

$$C_0 = \lambda P \quad (١٧)$$

$$c_j = h(ID_j \| x) \quad (١٨)$$

$$D_1 = h(ID_i' \| ID_j \| c_j C_0 \| B_2 \| T_G) \quad (١٩)$$

سپس، پیام $M_2 = \{ID_i', ID_j, B_2, D_1, C_0, T_G\}$ به پزشک d_j فرستاده می‌شود.

$$M_2 = \{ID_i', ID_j, B_2, D_1, C_0, T_G\} \quad (٢٠)$$

- d_j صحت پارامترهای ID_j، $|T - T_G| > \Delta$ و $D_1 = h(ID_i' \| ID_j \| c_j C_0 \| B_2 \| T_G)$ را بررسی می‌نماید. اگر این بررسی حاکی از نادرست‌بودن هر کدام از این دو پارامتر باشد، d_j نشست را متوقف خواهد کرد. در غیر این صورت، d_j عدد تصادفی $\beta \in [1, q-1]$ را انتخاب نموده و سپس پارامترهای $C_1 = \beta P$، $C_2 = \beta B_2$، $sk_d = h_1(B_2 \| C_1 \| C_2)$، $C_3 = h(ID_i' \| ID_j \| sk_d)$ و $C_4 = h(c_j C_0 \| ID_i' \| ID_j)$ را محاسبه می‌کند.

$$C_1 = \beta P \quad (٢١)$$

$$C_2 = \beta B_2 \quad (٢٢)$$

[Downloaded from ic4i-journal.ir on 2026-11-18]

$$sk_d = h_1(B_2 \| C_1 \| C_2) \quad (۲۳)$$

$$C_3 = h(ID_i' \| ID_j \| sk_d) \quad (۲٤)$$

$$C_4 = h(c_j C_0 \| ID_i' \| ID_j) \quad (۲۵)$$

در ادامه، d_j پیام $M_3 = \{C_1, C_3, C_4\}$ را به SEM ارسال می‌کند.

$$M_3 = \{C_1, C_3, C_4\} \quad (۲٦)$$

- در ابتدا، SEM صحت عبارت $C_4 = h(c_j C_0 \| ID_i' \| ID_j)$ را بررسی می‌کند. اگر درست بود، آن‌گاه $D_2 = h(ID_{SEM} \| x \|$ $MI_i^{new})\oplus h(MI_i^{new} \| r_3)$، $D_3 =$ و $D_4 = h(MI_i^{new} \| x)\oplus h(ID_i' \| r_3)$ $h(ID_i \| ID_i' \| MI_i^{new} \| ID_j \| D_2 \| D_3 \| r_3)$ را محاسبه می‌کند.

$$D_2 = h(ID_{SEM} \| x \| MI_i^{new})\oplus h(MI_i^{new} \| r_3) \quad (۲۷)$$

$$D_3 = h(MI_i^{new} \| x)\oplus h(ID_i' \| r_3) \quad (۲۸)$$

$$D_4 = h(ID_i \| ID_i' \| MI_i^{new} \| ID_j \| D_2 \| D_3 \| r_3) \quad (۲۹)$$

در نهایت، SEM پیام $M_4 = \{C_1, C_3, D_2, D_3, D_4\}$ را به p_i ارسال می‌کند.

$$M_4 = \{C_1, C_3, D_2, D_3, D_4\} \quad (۳۰)$$

- p_i صحت عبارت $D_4 = h(ID_i \| ID_i' \| MI_i^{new} \| ID_j \| D_2 \| D_3 \| r_3)$ را بررسی می‌کند. اگر درست نبود، مقدار $B_6 = \alpha C_1$ و $sk_p = h_1(B_2 \| C_1 \| B_6)$ را محاسبه می‌کند.

$$B_6 = \alpha C_1 \quad (۳۱)$$

$$sk_p = h_1(B_2 \| C_1 \| B_6) \quad (۳۲)$$

- پس از آن، p_i صحت عبارت $C_4 = h(c_j \| ID_i' \| ID_j)$ را بررسی می‌کند. اگر درست بود، کارت هوشمند داده جدید $d_i^{new} = r_2\oplus h(ID_i' \| PW_i)$، $e_i^{new} =$ $D_2\oplus h(MI_i^{new} \| r_3)\oplus h(r_2 \| PW_i)$ و $f_i^{new} = D_3\oplus MI_i^{new}\oplus h(ID_i' \| r_3)\oplus h(r_2 \| PW_i)$ را محاسبه می‌نماید.

$$d_i^{new} = r_2\oplus h(ID_i' \| PW_i) \quad (۳۳)$$

$$e_i^{new} = D_2\oplus h(MI_i^{new} \| r_3)\oplus h(r_2 \| PW_i) \quad (۳٤)$$

$$f_i^{new} = D_3\oplus MI_i^{new}\oplus h(ID_i' \| r_3)\oplus h(r_2 \| PW_i) \quad (۳۵)$$

در نهایت، کاربر عبارت (d_i, e_i, f_i) را با $(d_i^{new}, e_i^{new}, f_i^{new})$ جایگزین می‌کند.

٤-۵. فاز تغییر کلمه عبور

- این گام دقیقاً با گام ۱ از فاز ورود و احرازاصالت یکسان است.
- p_i اعداد تصادفی r_4 و r_5 را انتخاب نموده و سپس عبارت $MI_i^{new} = h(r_4 \| ID_i')$، $B_7 =$ $e_i\oplus MP_i\oplus r_5$، $B_8 =$ $f_i\oplus ID_i'\oplus MI_i^{new}\oplus h(r_5 \| ID_i')$، $B_9 =$ و $B_{10} = ID_i'\oplus h(r_5 \| MI_i^{new} \| B_2)$ $h(ID_i \| ID_i' \| MI_i^{new} \| r_5)$ را محاسبه نماید.

$$MI_i^{new} = h(r_4 \| ID_i) \quad (۳٦)$$

$$B_7 = e_i\oplus MP_i\oplus r_5 \quad (۳۷)$$

$$B_8 = f_i\oplus ID_i'\oplus MI_i^{new}\oplus h(r_5 \| ID_i') \quad (۳۸)$$

$$B_9 = ID_i'\oplus h(r_5 \| MI_i^{new} \| B_2) \quad (۳۹)$$

$$B_{10} = h(ID_i \| ID_i' \| MI_i^{new} \| r_5) \quad (٤۰)$$

p_i پیام $M_5 = \{M_i, B_7, B_8, B_9, B_{10}\}$ را به همراه درخواست تغییر کلمه‌عبور به میانجی امنیتی SEM ارسال می‌کند.

- به محض دریافت پیام M_5 و درخواست تغییر کلمه‌عبور، SEM عبارت $r_5 =$ $MI_i^{new} =$ $B_7\oplus h(ID_{SEM} \| x \| ID_i')$، $ID_i' =$ $B_8\oplus h(ID_i' \| x)\oplus h(r_3 \| ID_i')$، $B_9\oplus h(r_5 \| MI_i^{new} \| B_2)$ را محاسبه می‌کند.

$$r_5 = B_7\oplus h(ID_{SEM} \| x \| ID_i') \quad (٤۱)$$

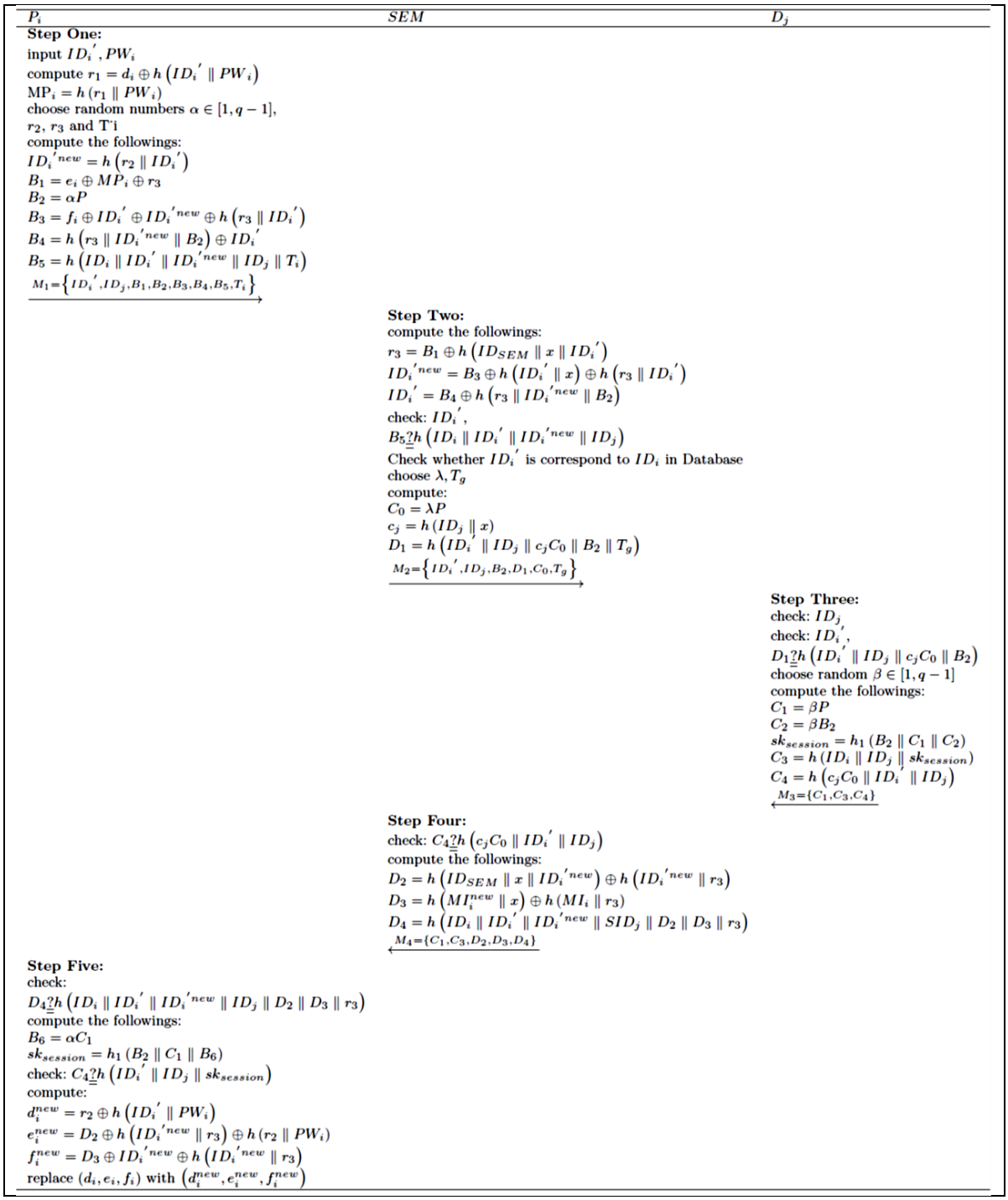
$$MI_i^{new} = B_8\oplus h(ID_i' \| x)\oplus h(r_3 \| ID_i') \quad (٤۲)$$

$$ID_i' = B_9\oplus h(r_5 \| MI_i^{new} \| B_2) \quad (٤۳)$$

[Downloaded from ic4i-journal.ir on 2026-11-18]

و اعتبار ID_i و همچنین $B_{10} = h(ID_i \parallel MI_i \parallel MI_i^{new} \parallel r_5)$ را بررسی می‌نماید.

$$B_{10} = h(ID_i \parallel ID_i' \parallel MI_i^{new} \parallel r_5) \quad (٤٤)$$



شکل۳. شمای مربوط به فازهای ورود و احرازاصالت طرح پیشنهادی.

اگر هر کدام از این پارامترها نامعتبر باشند، درخواست احرازاصالت رد می‌شود.

- در غیر این صورت، SEM عبارت‌های $D_5 = h(ID_{SEM} \parallel x \parallel MI_i^{new}) \oplus h(MI_i^{new} \parallel r_5)$، $D_6 = h(MI_i^{new} \parallel x) \oplus h(ID_i' \parallel r_5)$ و $D_7 = h(ID_i \parallel r_5 \parallel ID_i' \parallel MI_i^{new} \parallel D_5 \parallel D_6)$ را محاسبه می‌نماید. SEM پیام $M_6 = \{D_5, D_6, D_7\}$ را به کاربر p_i ارسال می‌کند.

[Downloaded from ic4i-journal.ir on 2026-11-18]

$$D_5 = h(ID_{SEM} \parallel x \parallel MI_i^{new}) \oplus h(MI_i^{new} \parallel r_5) \quad (٤٥)$$

$$D_6 = h(MI_i^{new} \parallel x) \oplus h(ID_i' \parallel r_5) \quad (٤٦)$$

$$D_7 = h(ID_i \parallel r_5 \parallel ID_i' \parallel MI_i^{new} \parallel D_5 \parallel D_6) \quad (٤٧)$$

SEM پیام $M_6 = \{D_5, D_6, D_7\}$ را به کاربر p_i ارسال می‌کند.

$$M_6 = \{D_5, D_6, D_7\} \quad (٤٨)$$

- ابتدا p_i اعتبار $D_7 = h(ID_i \parallel r_5 \parallel ID_i' \parallel MI_i^{new} \parallel D_5 \parallel D_6)$ را بررسی می‌کند. اگر این معادله اشتباه بود، p_i نشست را لغو می‌نماید. در غیر این صورت، p_i درخواست ورود یک کلمه‌عبور PW_i^{new} می‌نماید.

سپس، کارت هوشمند عبارت‌های مربوطه یعنی $MP_i^{new} = (r_4 \parallel PW_i^{new})$، $e_i^{new2} = D_5 \oplus h(MI_i^{new} \parallel r_5) \oplus MP_i^{new}$، $f_i^{new2} = D_6 \oplus h(ID_i' \parallel r_5) \oplus MI_i^{new}$ و $d_i^{new2} = r_4 \oplus h(ID_i' \parallel PW_i^{new})$ را محاسبه می‌نماید.

$$MP_i^{new} = (r_4 \parallel PW_i^{new}) \quad (٤٩)$$

$$e_i^{new2} = D_5 \oplus h(MI_i^{new} \parallel r_5) \oplus MP_i^{new} \quad (٥٠)$$

$$f_i^{new2} = D_6 \oplus h(ID_i' \parallel r_5) \oplus MI_i^{new} \quad (٥١)$$

$$d_i^{new2} = r_4 \oplus h(ID_i' \parallel PW_i^{new}) \quad (٥٢)$$

نهایتاً (d_i, e_i, f_i) را با $(d_i^{new2}, e_i^{new2}, f_i^{new2})$ به‌روزرسانی می‌کند.

۵. تحلیل رسمی امنیت با ProVerif

برای بررسی و ارزیابی امنیت طرح ارایه‌شده، ابتدا باید آن را به زبان مورد فهم برای ابزار ProVerif تبدیل نماییم. بدین منظور ابتدا تعاریف کُد ProVerif و مقدمات کلی را به صورت زیر تعریف می کنیم :

تعریف کُد ProVerif

```
(* Channels and shared keys are listed below *)
    free ch1: channel. (* the public channel between the user and the sensor *)
    free ch2: channel. (* the public channel between the sensor and SEM *)
    free sch1: channel [private]. (* the secret channel between the user and SEM *)
    free sch2: channel [private]. (* the secret channel between the sensor and SEM *)
    free sks: bitstring [private]. (* the session key between Patient and Doctor *)
(* Constants are listed below *)
    free x:bitstring [private]. (* the private key of SEM *)
    free IDi:bitstring [private]. (* pi's identity *)
    free ID'i:bitstring [private]. (* pi's alias identity *)
    free IDpr_i:bitstring [private]. (* pi proxy's identity *)
    free ID'pr_i:bitstring [private]. (* pi proxy's alias identity *)
    free PWi:bitstring [private]. (* pi's password *)
    free Ti:bitstring [private]. (* TimeStamp of Patient *)
    free Tg:bitstring [private]. (* TimeStamp Of SEM *)
    const IDSEM:bitstring. (* SEM's identity *)
    const P:bitstring. (* the generator P *)
    const IDj:bitstring. (* dj's identity *)
    table d(bitstring). (* database in SEM *)
(* Functions and equations are listed below: *)
    fun h(bitstring):bitstring. (* hash function *)
    fun h1(bitstring):bitstring. (* hash function *)
    fun mul(bitstring,bitstring):bitstring. (* scalar multiplication function *)
    fun xor(bitstring,bitstring):bitstring. (* X-OR function *)
    fun con(bitstring,bitstring):bitstring. (* string concatenation *)
    equation forall m:bitstring,n:bitstring; xor(xor(m,n),n)=m.(* X-OR computation *)
    equation forall m:bitstring,n:bitstring; mul(mul(P,m),n)= mul(mul(P,n),m).(* scalar multiplication
    *)
```


[Downloaded from ic4i-journal.ir on 2026-11-18]

رویدادها و پرسش و پاسخ‌های مربوط به کُد ProVerif نیز به صورت زیر است:

رویدادها و پرسش و پاسخ‌های کُد ProVerif

```
(*Events*)
    event PatientStart(bitstring).
    event PatientAuth(bitstring).
    event DoctorStart(bitstring).
    event DoctorAuth(bitstring).
(*Queries*)
    query attacker(sks).
    query attacker(sks).
    query id:bitstring;
    inj-event(PatientAuth(id)) ==>  inj-event(PatientStart(id)).
    query sid:bitstring;
    inj-event(DoctorAuth(sid)) ==> inj-event(DoctorStart(sid)).
```

کُد ProVerif مربوط به نقش‌های موجودیت‌های شرکت‌کننده یعنی بیمار، پزشک و میانجی امنیتی (SEM) باید به تفکیک تعریف شوند. به دلیل وجود محدودیت در تعداد صفحات مقاله، در اینجا تنها به آوردن کُد ProVerif بیمار اکتفا کرده و از آوردن کُدهای پزشک و میانجی امنیتی خودداری نموده‌ایم.

کُد مربوط به بیمار

```
(*% Code for the Patient: The Patient's process:*)
    let Patient=
    new r0:bitstring;
    let MPi=h(con(r0,PWi)) in
    out(sch1,(MPi,ID'i,IDi,IDpr_i,ID'pr_i));
    in(sch1,(xei:bitstring,xfi:bitstring));
    let ei = xei in
    let fi = xfi in
    let di = xor(h(con(IDi,PWi)),r0) in
    !
    (
    event PatientStart(ID'i);
    let r1 = xor(di,h(con(ID'i,PWi))) in
    let MPi' = h(con(r1,PWi)) in
    new alpha:bitstring;
    new r2:bitstring;
    new r3:bitstring;
    new Ti' :bitstring;
    let ID'inew = h(con(r2,IDi)) in
    let B1= xor(xor(ei,MPi'),r3) in
    let B2 = mul(P,alpha) in
    let B3 = xor(xor(xor(fi,ID'i),ID'inew),h(con(r3,ID'i))) in
    let B4 = xor(ID'i,h(con(con(r3,ID'inew),B2))) in
    let B5 = h(con(con(con(con(IDi,ID'i),ID'inew),IDj),Ti)) in
    let M1 =(ID'i,IDj,B1,B2,B3,B4,B5) in
    out(ch1,M1);
    in (ch1,(xC1:bitstring,xC3:bitstring,xD2:bitstring,xD3:bitstring,
    xD4:bitstring));
    if xD4 = h(con(con(con(con(con(con(IDi,ID'i),ID'inew),IDj),
    xD2),xD3),r3)) then
    let B6 = mul(xC1,alpha) in
```


[Downloaded from ic4i-journal.ir on 2026-11-18]

```
let sku' = h1(con(con(B2,xC1),B6)) in
if xC3 = h(con(con(ID'i,IDj),sks)) then
let dinew = xor(r2,h(con(IDi,PWi))) in
let einew = xor(xor(xD2,h(con(ID'inew,r3))), h(con(r2,PWi))) in
let finew = xor(xor(xD3,ID'inew),h(con(ID'i,r3))) in
let di' = dinew in
let ei' = einew in
let fi' = finew in
0
).
```

در نهایت کُد فوق را با دستور زیر اجرا می‌نماییم:

process !Patient|!SEMReg2|!Doctor!

خروجی اجرای نرم‌افزار به صورت نشان‌داده شده در شکل٤ می‌باشد.

```
-- Query inj-event(DoctorAuth(sid)) ==> inj-event(DoctorStart(sid))
nounif mess(sch2[],yIDj_5387)/-5000
Completing...
Starting query inj-event(DoctorAuth(sid)) ==> inj-event(DoctorStart(sid))
RESULT inj-event(DoctorAuth(sid)) ==> inj-event(DoctorStart(sid)) is true.
-- Query inj-event(PatientAuth(id)) ==> inj-event(PatientStart(id))
nounif mess(sch2[],yIDj_12018)/-5000
Completing...
Starting query inj-event(PatientAuth(id)) ==> inj-event(PatientStart(id))
RESULT inj-event(PatientAuth(id)) ==> inj-event(PatientStart(id)) is true.
-- Query not attacker(sks[])
nounif mess(sch2[],yIDj_18364)/-5000
Completing...
Starting query not attacker(sks[])
RESULT not attacker(sks[]) is true.
-- Query not attacker(sks[])
nounif mess(sch2[],yIDj_24508)/-5000
Completing...
Starting query not attacker(sks[])
RESULT not attacker(sks[]) is true.
```

شکل٤. نمایش خروجی نرم‌افزار ProVerif.

۵. تحلیل ویژگی‌های امنیتی

در این بخش، مقاومت طرح ارایه‌شده را در مواجهه با حملات و تهدیدات مختلف بررسی می‌نماییم.

- **مقاومت در برابر حمله داخلی:** در خلال فاز ثبت‌نام، p_i عبارت $MP_i = h(r_0 \| PW_i)$ را به میانجی امنیتی SEM ارسال می‌کند. به دلیل آن که مهاجم عدد تصادفی r_0 را ندارد، قادر نیست تا کلمه‌عبور PW_i را حدس بزند. بنابراین یک میانجی امنیتی بداندیش نمی‌تواند کلمه‌عبور بیماران را به دست آورد.
- **مقاومت در برابر حمله حدس کلمه‌عبور آفلاین:** فرض کنید یک مهاجم همانند $\mathcal{A}$ کانال ارتباطی میان کاربر p_i و SEM را با هدف به دست آوردن کلمه‌عبور PW_i شنود نماید. مهاجم پیام M_1 را ضبط نموده و سعی می‌کند تا کلمه‌عبور را بیابد. به دلیل آن که کلمه‌عبور در پیام M_1 وجو ندارد، مهاجم قادر به یافتن PW_i نیست. به علاوه، در نظر بگیرید که مهاجم کارت هوشمند سلامت بیمار را دزدیده و پارامترهای e_i، f_i و d_i را به دست آورد. به دلیل آن که مهاجم عدد تصادفی r_0 و پارامتر محرمانه x را ندارد، نمی‌تواند کلمه‌عبور را از روی

[Downloaded from ic4i-journal.ir on 2026-11-18]

e_i و d_i بیابد. بنابراین، طرح ارایه‌شده در مقابل حمله حدس کلمه‌عبور آفلاین ایمن می‌باشد.

- **مقاومت در برابر حمله جعل کاربر:** به منظور جعل p_i، مهاجم $\mathcal{A}$ باید یک پیام معتبر M_1 را تولید نماید. به دلیل این که $\mathcal{A}$ مقدار x را نمی‌داند، محاسبه مقادیر $B_1 = h(ID_{SEM} \| x \| ID_i')\oplus r_3$ و $B_3 = h(ID_i' \| x)\oplus MI_i^{new}\oplus h(r_3 \| ID_i')$ ممکن نیست. به علاوه، به خاطر وجود مُهرزمانی، مهاجم نمی‌تواند یک پیام قدیمی M_1 را به منظور جعل p_i مورد استفاده قرار دهد. بنابراین، پروتکل ارایه‌شده در برابر حمله جعل کاربر امن است.
- **مقاومت در برابر حمله جعل میانجی امنیتی:** اگر مهاجم $\mathcal{A}$ بخواهد میانجی امنیتی SEM را جعل نماید، باید به ترتیب مقادیر D_1، D_2، D_3 و r_3 را محاسبه نماید. به خاطر آن که $\mathcal{A}$ مقدار محرمانه x را ندارد، محاسبه مقادیر موردنظر مربوطه ممکن نمی‌باشد. بنابراین، $\mathcal{A}$ قادر نیست تا SEM را در طرح ارایه‌شده جعل نماید.
- **مقاومت در برابر حمله غیرهمزمان‌سازی:** حمله غیرهمزمان‌سازی به این معنی است که میانجی امنیتی، ورود و احرازاصالت کاربران مجاز را رد می‌کند. در طرح ارایه‌شده، کلمه‌عبور قبل از تغییر در نشست با میانجی امنیتی بررسی می‌شود. در حقیقت، کلمه‌عبور اشتباه وارد می‌شود. همچنین، ممکن است داده ناسازگار مابین میانجی امنیتی و بیمار منجر به این حمله گردد. میانجی امنیتی هیچ اطلاعاتی در مورد کاربران واقعی ندارد مگر جز شناسه آن‌ها. داده مبادله‌شده همواره تنها در طرف بیمار رخ می‌دهد. غیرممکن است که داده ناسازگار میان بیمار و میانجی امنیتی ظاهر می‌شود. بنابراین، طرح ارایه‌شده از وقوع حمله غیرهمزمان‌سازی جلوگیری می‌کند.
- **مقاومت در برابر حمله تکرار:** به دلیل وجود اعداد تصادفی مورداستفاده توسط بیمار، میانجی امنیتی و پزشک و همچنین استفاده از مُهرزمانی، طرح ارایه‌شده در مقابل حمله تکرار امن می‌باشد.
- **مقاومت در برابر حمله کلید مشخص:** در طرح ارایه‌شده، کلید نشست $sk_p = h_1(B_2 \| C_1 \| C_2)$ است که در آن $C_2 = \beta B_2 = \alpha C_1$ می‌باشد. به دلیل آن که β و α در هر نشست به طور تصادفی انتخاب می‌شوند، کلیدهای نشست کاملاً به طور مستقل ایجاد می‌شوند. بنابراین، اگر مهاجم $\mathcal{A}$ می‌تواند یک کلید نشست را به دست آورد، نمی‌تواند کلیدهای نشست بعدی را محاسبه نماید.
- **گمنامی کاربر:** در طرح ارایه‌شده، به جای استفاده از شناسه واقعی بیمار (ID_i)، از شناسه مستعار (ID_i') استفاده می‌شود. علاوه بر آن، حتی همین شناسه مستعار هم در طرح ارایه‌شده بر روی کانال ارتباطی به صورت فاش ارسال نمی‌گردد. بنابراین طرح ارایه‌شده ویژگی گمنامی را برای کاربر (بیمار) p_i برآورده می‌کند.
- **امنیت پیشرو قوی:** فرض کنید که مهاجم یعنی کسی که جریان‌های نشست‌های قبلی را ضبط می‌کند، تمامی اطلاعات محرمانه p_i، d_j و SEM را به دست می‌آورد. با فرض غیرقابل حل بودن مسأله دیفی–هِلمن مبتنی بر خم‌بیضوی (ECCDLP)، او نمی‌تواند مقادیر تصادفی α، β و کلید نشست مربوط به نشست‌های قبلی را محاسبه نماید. بنابراین، طرح ارایه‌شده ویژگی امنیت پیشرو قوی را برآورده می‌کند.

[Downloaded from ic4i-journal.ir on 2026-11-18]

٦. نتیجه‌گیری

کاربرد IoT در حوزه‌های نظامی جزء جدانشدنی و اضطراری توسعه اطلاعاتی بخش نظامی محسوب می‌گردد. IoT توسعه حوزه نظامی را به طور عمده‌ای پیش خواهد برد و به نظر می‌رسد که به زودی شاهد شبکه‌های اینترنت اشیاء نظامی باشیم که در آن نقش انسان کمرنگ‌تر از قبل شده و دستگاه‌ها و جنگ‌افزارهای هوشمند با تکیه بر ارتباطات گسترده و متعاقباً توانایی تصمیم‌گیری و انجام فعالیت‌های تصمیم‌گیرانه، نقش‌آفرینی قابل ملاحظه‌ای داشته باشند.

همانند تمامی حوزه‌ها و زیرحوزه‌های اینترنت اشیاء، امنیت و حریم‌خصوصی داده از عوامل مهم در حوزه سلامت الکترونیک به شمار می‌رود. به ویژه حریم‌خصوصی به دلیل امکان انتشار موراد و اطلاعات محرمانه و شخصی کاربران بسیار مورد توجه می‌باشد. تاکنون چندین رویکرد به منظور حفظ حریم‌خصوصی کاربران در حوزه سلامت الکترونیک ارائه شده است که چهارچوب پیشنهادی Sahi و همکارانش در سال ابرها و رایانش ابری به شمار می‌روند. در این مقاله، دو رویکرد جدید رائه شده است که یکی با رویکرد تأمین میلادی یکی از جدیدترین آن‌ها به شمار می‌رود. رویکرد آن‌ها تنها به حفظ حریم‌خصوصی محتوای پرونده پزشکی بیمار پرداخته و به حفظ حریم‌خصوصی شناسه بیمار اشاره نکرده است. ضمن آن که در مواقعی که بیمار خودش در وضعیت پزشکی بحرانی قرار داشته باشد، چهارچوب پیشنهادی آن‌ها هیچ راهکاری پیشنهاد نمی‌نماید. در این مقاله، یک چهارچوب کلی جدیدی را به همراه طرح احرازاصالت جدید برای حفظ حریم‌خصوصی در حوزه سلامت الکترونیک ارائه نمودیم که هم حریم‌خصوصی محتوای پرونده بیمار و هم حریم‌خصوصی شناسه بیمار را در ارتباطات موردنظر حفظ می‌نماید. طرح ارایه‌شده از اولیه‌های سبک‌وزن رمزنگاشتی بهره می‌برد و بنابراین سربار پردازشی چندانی ندارد. همچنین تمامی ویژگی‌های امنیتی برای یک طرح احرازاصالت با ویژگی حفظ حریم‌خصوصی شناسه بیمار را برآورده می‌نماید. همچنین علاوه بر تأمین ویژگی‌های امنیتی موردنظر، نشان دادیم که طرح ارایه‌شده به طور رسمی نیز امن می‌باشد. بدین منظور از نرم‌افزار معروف ProVerif استفاده نمودیم که به منظور ارزیابی امنیتی پروتکل‌های امنیتی طراحی و پیاده‌سازی شده است. همان‌طور که خروجی این نرم‌افزار نشان می‌دهد طرح ارایه‌شده امن بوده و مهاجم قادر به یافتن کلید نشست میان پزشک و بیمار نخواهد بود.

سپاس‌گذاری

این مقاله توسط صندوق حمایت از پژوهشگران و فناوران کشور به شماره قرارداد ۵۳۹۷۹/ص/۹٦ مورد حمایت قرار گرفته است.

منابع

[1]. R. H. Weber, “Internet of things: Privacy issues revisited”, Computer Law and Security Review 31, pp. 618-627, 2015.

[2]. S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead”, Computer Networks 76, pp. 146-164, 2015.

[3]. E. Borgia, “The Internet of Things vision: Key features, Applications and open issues,” Computer Communications, pp. 1–31, 2014.

[4]. S. Iraji, P. Mogensen, R. Ratasuk, “Recent Advance in M2M Communications and Internet of Things”, International Journal of Wireless Information Networks 24 (3), pp. 240-242, 2017.

[5]. H. Sundmaeker, P. Guillemin, P. Friess, & S. Woelfflé, “Vision and challenges for realising the Internet of Things”. Cluster of European Research Projects on the Internet of Things, European Commission (CERP-IoT), 2010.

[6]. A. Al-Gburi, A. Al-Hasnawi, L. Lilien, “Differencing Security from Privacy in Internet of Things: A Survey of Selected Threats and Controls”. In: Daimi. K (eds) Computer and Network Security Essentials, Springer, pp. 153-172, 2017.

[Downloaded from ic4i-journal.ir on 2026-11-18]

[7]. C.-P. Pfleeger, S.-L. Pfleeger, & J. Margulies, "Security in computing (5th ed.)". Englewood Cliffs, NJ: Prentice Hall, 2015.

[8]. L. DeNardis, "Standards and eHealth," ITU-T Technology watch report 2011.

[9]. A. Abbas, S.-U. Khan, "A review on the state-of-the-art privacy-preserving approaches in the e-health clouds", IEEE J. Biomed. Health Inform.18, pp. 1431–1441, 2014.

[10]. E. H. Shortliffe and J. J. Cimino, "Biomedical informatics: computer applications in health care and biomedicine", Springer Science & Business Media, 2013.

[11]. M. Kay, J. Santos, and M. Takane, "mHealth: New horizons for health through mobile technologies," 2011.

[12]. F. Zubaydi, A. Saleh, F. Aloul, and A. Sagahyroon, "Security of mobile health (mHealth) systems, " in Bioinformatics and Bioengineering (BIBE), 2015 IEEE 15th International Conference on, pp. 1-5, 2015.

[13]. S. A. Basheer, "QUESTION 14-2/2: Mobile eHealth solutions for Developing Countries" International Telecommunication Union 2010.

[14]. 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.

[15]. A. Sahi, D. Lai, Y. Li, "Security and privacy preserving approaches in the eHealth clouds with disaster recovery plan". Computers in Biology and Medicine, Vol. 78, pp. 1–8, 2016.

[16]. P. Mell, T. Grance, "The NIST Definition of Cloud Computing", 2011.

[17]. M. Sugumaran, B.B. Murugan, D. Kamalraj, "An architecture for data security in cloud computing", in: Proceedings of the 2014 World Congress on Computing and Communication Technologies (WCCCT), pp. 252–255, 2014.

[18]. K.-E. Kushida, J. Murray, J. Zysman, "Cloud Computing: From Scarcity to Abundance", BRIE Working Paper, Springer, 2014.

[19]. D. Zissis, D. Lekkas, "Addressing cloud computing security issues", Future Gener. Comput. Syst. 28, pp. 583–592, 2012.

[20]. I. Hsu, F.-Q. Cheng, "SAaaS: a cloud computing service model using semantic-based agent", Expert Syst. 32, pp. 77–93, 2013.

[21]. 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.

[22]. M. U. Aslam, A. Derhab, K. Saleem, H. Abbas, M. Orgun, W. Iqbal, "A Survey of Authentication Schemes in Telecare Medicine Information Systems," Journal of medical systems, vol. 41, 2017.

[23]. Q. Jiang, M.-K. Khan, X. Lu, J. Ma, D. He, "A privacy preserving three-factor authentication protocol for e-health clouds", Journal of Supercomputing, doi:10.1007/s11227-015-1610-x, 2016.

[24]. A. Irshad, Sh.-A. Chaudhry, "Comments on a privacy-preserving three-factor authentication protocol for e-health clouds", Journal of Supercomputing, doi:10.1007/s11227-016-1837-1, 2016.

[25]. C.-H. Liu, Y.-F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks", Computer Electronic Engineering, 59, pp. 250-261, doi:10.1016/j.compeleceng, 2016.01.002, 2016.

[26]. Ch.-T. Li, T.-Y. Wu, Ch.-L. Chen, Ch.-Ch. Lee, Ch.-M. Chen, "An Efficient User Authentication and User Anonymity Scheme with Provably Security for IoT-Based Medical Care System", Sensors, doi:10.3390/s17071482, 2017.

[27]. A. Nordgren, "Privacy by design in personal health monitoring", Health Care Anal, doi:10.1007/s10728-013-0262-3, 2013.

[28]. A. Cavoukian, A. Fisher, S.Killen & D. Hoffman, "Remote home health care technologies: How to ensure privacy? Build it in: Privacy by design", Identity in the Information Society, 3(2), pp. 363-378, 2010.

[29]. F. Chen, Y. Lou, J. Zhang, Z. Zhang, Ch. Zhao, T. Wang, "An infrastructure framework for privacy protection of community medical internet of things. Transmission Protection, Strong Protection & Access Control", World Wide Web, doi:10.1007/s11280-017-0455-z, 2017.

[30]. A.-S. Khader, D. Lai, "Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol", in: Proceedings of the 22nd International Conference on Telecommunications (ICT), 2015, pp.204–208.

[31]. A. Anjum, S.-R. Malik, K.-K. Chao, A. Haroon, S. Jan, S.-U. Khan, A. Khan, B. Raza, "An efficient privacy mechanism for electronic health records", Computers & Society, doi:10.1016/j.cose.2017.09.014, 2017.

[32]. G. GabyDagher, J. Mohler, M. Milojkovic, P.-B. Marella, "Ancile: privacy-preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology", Sustainable Cities & Society, doi:10.1016/j.scs.2018.02.014, 2018.

[Downloaded from ic4i-journal.ir on 2026-11-18]