چهارمین کنفرانس بین المللی پژوهش های کاربردی در
مهندسی کامپیوتر و پردازش سیگنال
۲۰ آبان ماه ۹۵، تهران، ایران

ارائه پروتکل حفظ حریم خصوصی و گمنامی در سلامت الکترونیک با استفاده از زیرساخت کلید عمومی

محمدعلی دوستاری [*۱]، مریم میابی جغال [۲]، مسعود مومنی تزنگی [۳].

۱- استادیار، گروه مهندسی کامپیوتر و فناوری اطلاعات، دانشکده فنی و مهندسی، دانشگاه شاهد تهران.

۲- دانشجوی کارشناسی ارشد فناوری اطلاعات، گروه مهندسی کامپیوتر و فناوری اطلاعات، دانشکده فنی و مهندسی، دانشگاه شاهد تهران

۳- کارشناسی ارشد فناوری اطلاعات، گروه مهندسی کامپیوتر و فناوری اطلاعات، دانشکده فنی و مهندسی، دانشگاه شاهد تهران

خلاصه

با توجه به توسعه سلامت الکترونیک، حفظ امنیت و حریم خصوصی بیماران اهمیت ویژه‌ای دارد. به همین منظور در این مقاله راهکارهای موجود جهت حفظ امنیت و حریم خصوصی بیماران بررسی شده‌اند. در این راستا از زیرساخت کلید عمومی و امضای دیجیتال برای افزایش امنیت بیماران استفاده شده است. با توجه به اینکه در اکثر پژوهش‌های قبلی گمنامی بیمار لحاظ نشده بود، در این طرح از امضای کور عادلانه برای این منظور بهره گرفته شده است. همچنین جهت احرازهویت علاوه بر رمزعبور، بیومتریک بیمار نیز مورد استفاده قرار گرفته است. با استفاده از پروتکل پیشنهادی، بیمار در کشور خارجی نیز می‌تواند از خدمات سلامت بهره‌مند شود. پروتکل پیشنهادی با نیازمندی‌های امنیتی و حریم خصوصی استاندارد HIPPA تطابق دارد. در نهایت، ویژگی‌های امنیتی طرح پیشنهادی با سایر روش‌های موجود مورد ارزیابی و مقایسه قرار گرفته است.

کلمات کلیدی: حریم خصوصی، زیرساخت کلید عمومی، سلامت الکترونیک، گمنامی

۱. مقدمه

از دهه ۱۹۶۰ میلادی، سیستم‌های اطلاعاتی کامپیوتری در سیستم سلامت رواج یافت. بیشتر تمرکز سیستم اطلاعات سلامت در سال‌های ۱۹۶۰ تا ۱۹۹۰ میلادی محدود به استفاده از نرم‌افزارهای کاربردی، کتابخانه‌ای و مدیریتی بود. در طول دهه ۱۹۹۰، تحقیقات و نرم‌افزارهای تجاری به سمت پردازش اطلاعات بیمار و یکپارچه‌سازی اطلاعات سلامت حرکت کردند. در حال حاضر توسعه سیستم‌های امن با اهداف ثبت الکترونیکی اطلاعات سلامت، انتقال اطلاعات سلامت بین ارائه دهندگان خدمات سلامت و همچنین تولید و گسترش دانش پزشکی براساس اطلاعات سلامت مورد توجه قرار گرفته است[۱].

* **Email:** doostari@shahed.ac.ir

حفظ اطلاعات بیماران و کنترل دسترسی به این اطلاعات محرمانه، از جمله مسائلی است که امروزه نگرانی‌هایی را به وجود آورده است[۲]. به همین منظور در سال ۱۹۹۶ استاندارد HIPPA* در صنعت سلامت الکترونیک آمریکا بعنوان قانون فدرال ایالات متحده تنظیم شد. براساس این استاندارد، حریم خصوصی بیمار بایستی در تمامی سیستم‌های سلامت لحاظ گردد، با این وجود تعریف دقیقی مبنی بر چگونگی اعمال حریم خصوصی و امنیت در این استاندارد بیان نشده است[۵-۳]. نیازمندی‌های امنیتی و حریم خصوصی مطرح شده در این استاندارد به صورت زیر بیان می‌شود:

- آگاهی بیمار: بیمار بایستی از نحوه استفاده و نگهداری اطلاعات سلامتش آگاهی یابد.
- محرمانگی: حفاظت از داده‌ها در طول ذخیره‌سازی و انتقال ضروری است.
- کنترل بیمار: بیمار می‌تواند دستیابی به اطلاعات سلامت خود را از طریق مدیریت کلیدهای رمزگذاری کنترل کند.
- تمامیت: اطلاعات سلامت بیمار باید بدون حذف، تحریف و تخریب محافظت شود.
- شرایط اورژانس: در شرایط اضطراری و نجات زندگی بیمار، دسترسی به اطلاعات سلامت بیمار بدون اجازه وی ممکن باشد.

گمنام‌سازی یکی از راهکارهای ممکن جهت اعمال حریم خصوصی در سیستم‌های سلامت الکترونیک می‌باشد. گمنامی تضمین می‌کند که کاربر می‌تواند از خدمات و سرویس‌ها بدون افشای هویت خود استفاده نماید[۶]. استفاده از امضای کور و امضای کور عادلانه یکی از روش‌ها برای گمنام‌سازی می باشد[۷].

موضوع امنیت اطلاعات پزشکی بیماران به هنگام برقراری ارتباط با پزشک و سرور مرکزی بهداشت از جمله مسائل و مشکلات موجود در سلامت الکترونیک است. یکی از راه‌حل‌های اساسی برای حل این مشکل، استفاده از زیرساخت کلید عمومی است که تبادل اطلاعات سلامت را به صورت امن از طریق اینترنت فراهم می‌سازد[۸]. زیرساخت کلید عمومی ترکیبی از تکنولوژی، سیاست و فرایندهای اجرایی است که ذخیره اطلاعات حساس را در محیط ناامن از طریق رمزنگاری کلید عمومی فراهم می‌کند[۹].

هدف اصلی این مقاله ارائه سیستم سلامت الکترونیکی شامل ویژگی‌های حریم خصوصی در استاندارد HIPAA به همراه تضمین گمنامی می‌باشد. در واقع می‌خواهیم پروتکلی ارائه دهیم که حریم خصوصی بیماران را حفظ کرده و همچنین گمنامی بیماران را به منظور اطمینان از امن بودن و حفظ محرمانگی اطلاعات تضمین نماید. در این پروتکل جهت حفظ حریم خصوصی از زیرساخت کلید عمومی و برای تضمین گمنامی بیماران از امضای کور عادلانه استفاده شده است.

در بخش دوم برخی از کارهای تحقیقاتی انجام شده مورد تحلیل قرار گرفته‌اند. در بخش سوم، به معرفی امضای کور عادلانه به عنوان پیشنیاز پروتکل می‌پردازیم. در بخش چهارم علاوه بر ارائه معماری مورد نظر، پروتکل پیشنهادی در چهار فاز به طور کامل تشریح می‌شود. در بخش پنجم به ارزیابی و مقایسه پروتکل پیشنهادی با سایر پروتکل‌ها و همچنین تطابق پروتکل با نیازمندی‌های امنیتی و حریم خصوصی HIPPA می‌پردازد. در نهایت مقاله را در بخش ششم جمع‌بندی و نتیجه‌گیری می‌شود.

۲. کارهای انجام شده

*Health Insurance Portability and Accountability Act

لی و همکارانش در سال ۲۰۰۸ یک طرح رمزنگاری مدیریت کلید با استفاده از کارت هوشمند برای برقراری نیازمندی‌های امنیتی و حریم خصوصی ارائه داده‌اند. در این طرح بیمار در سرور قابل اعتماد اداره بهداشت و درمان ثبت نام نموده و کارت هوشمند خود را دریافت می‌نماید. سپس با ارائه کارت خود به سرور ارائه دهنده خدمات درمانی، از خدمات آن بهره‌مند می‌گردد. محدودیت‌های این طرح شامل عدم توجه به گمنامی بیمار، نیاز به ارائه کارت هوشمند و حضور بیمار در هر دسترسی به PHI، عدم توانایی در تعویض رمز کارت هوشمند توسط بیمار و عدم دسترسی چندگانه به PHI توسط افراد مختلف در موقعیت‌های مکانی متفاوت می‌باشد[۵]. در سال ۲۰۱۱ هوانگ و لیو با استفاده از رمزنگاری خم بیضوی سربار محاسباتی طرح لی و همکارانش را بهبود بخشیدند. این طرح شامل تمام محدودیت‌های طرح لی و همکارانش می‌باشد با این تفاوت که قابلیت تعویض رمزعبور کارت هوشمند، توسط بیمار در این طرح لحاظ شده است[۱۰].

در سال ۲۰۱۰ هو و همکارانش یک راه‌حل مبتنی بر زیر ساخت کلیدعمومی ترکیبی برای قوانین حریم خصوصی و امنیت ارائه کردند. این طرح مبتنی بر قرارداد بوده و مدیریت اعتماد و امنیت در طول قرارداد بر عهده ارائه دهنده خدمات درمانی می‌باشد. در این روش مرکز صدور کارت هوشمند، مسئول صدور کارت هوشمند برای همه‌ی بیماران است و حق دسترسی به اطلاعات بیماران توسط سرور مرکزی پزشکی* در طول قرارداد کنترل می‌گردد. ضعف‌های این روش عبارتند از عدم گمنامی بیمار، عدم وجود روندی مشخص برای شرایط اورژانس, عدم دسترسی به پرونده سلامت الکترونیک† در کشور خارجی، عدم کنترل دسترسی بیمار و حذف PHI پس از پایان قرارداد[۱۱].

در سال ۲۰۱۴ ری و بیسواز سیستمی مبتنی بر الگوریتم رمزنگاری RSA و زیرساخت کلید عمومی ارائه دادند. در این طرح تمامی موجودیت‌ها دارای گواهی کلید عمومی بوده و به کمک آن یکدیگر را احرازهویت می‌نمایند. اطلاعات بیمار بطور متمرکز بر روی MCS قرار داشته و کنترل دسترسی آن توسط بیمار صورت می‌پذیرد. کادر درمانی و بیمار می‌توانند به MCS از طریق اینترنت دسترسی یابند در نتیجه دسترسی به PHI بیمار محدودیت جغرافیایی نداشته و از کشور خارجی نیز قابل دسترسی است. این طرح بسیاری از محدودیت‌های کارهای قبل را پوشش داده با این وجود به گمنامی بیمار اشاره‌ای نشده است[۱۲, ۱۳].

در کار قبلی ما، پروتکلی جهت حفظ حریم خصوصی و امنیت در سیستم سلامت الکترونیک ارائه شده است. این پروتکل با نیازمندی های حریم خصوصی و امنیتی HIPPA تطابق دارد. در این پروتکل به منظور کاهش گذرهای پروتکل و بهبود سرعت از مهر زمان استفاده شده است. با اینوجود در این طرح نیر به گمنامی بیمار توجه نشده است[۱۴].

در هیچکدام از این کارها بحثی از گمنامی بیماران به میان نیامده است و تقریبا علیرغم اهمیت بسیار این موضوع، این پارامتر مهم امنیتی نادیده گرفته شده است. علاوه بر این، به اهمیت استفاده از بیومتریک در احرازهویت نیز توجه کافی نشده است. تمامی کارهای انجام شده‌ی مذکور برای اثبات امنیت مدل معماری پیشنهادی خود از روش تحلیل امنیتی پروتکل استفاده کرده‌اند وکارایی مدل‌ها و پروتکل‌ها را با فاکتورهای امنیتی از جمله امن بودن در برابر حمله‌ی تکرار، برقراری محرمانگی، قابلیت عدم انکار و ... مورد بررسی و ارزیابی قرار داده‌اند.

۳. امضای کور عادلانه

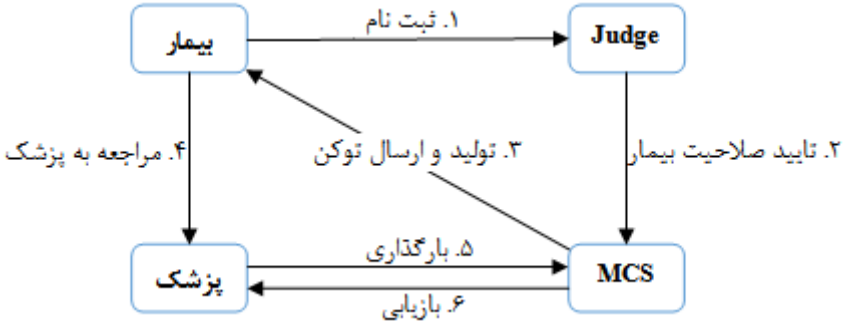
* Medical Center Server (MCS)
† Personal Health Record (PHI)

طرح امضای کور شامل دو عامل فرستنده و امضاکننده می‌باشد. طرح این امکان را به فرستنده می‌دهد تا پیام مورد نظرش را به امضای امضاکننده برساند بدون آنکه امضاکننده اطلاعی در خصوص محتوای پیام و یا هویت فرستنده داشته باشد. این طرح برای گمنام ماندن یکی از طرفین در پروتکل‌هایی همچون رای‌گیری الکترونیک و سیستم پرداخت کاربرد دارد[۷].

متاسفانه در طرح امضای کور به علت گمنامی فرستنده، فرستنده می‌تواند مرتکب تخلف شود و هیچ مرجعی از این تخلف و عامل آن مطلع نمی‌شود. به همین علت طرح امضای کور عادلانه پیشنهاد شده است. طرح امضای کور عادلانه شامل سه عامل فرستنده ، امضا کننده و طرف قابل اعتماد می‌باشد. همچنین این طرح از دو پروتکل امضا و بازیابی ارتباط تشکیل شده است. پروتکل امضا همچون امضای کور بین فرستنده و امضاکننده رخ می‌دهد و پروتکل بازیابی ارتباط بین امضاکننده و طرف قابل اعتماد برقرار است. براساس این طرح طرف قابل اعتماد می‌تواند امضا را به فرستنده پیام مرتبط سازد. در نتیجه علاوه بر حفظ گمنامی فرستنده، در صورت ضرورت و تخلف فقط طرف قابل اعتماد می‌تواند به هویت طرفین پی ببرد[۷].

۴. طرح پیشنهادی

در این طرح فرض برای این است بیمار و پزشک از مرجع صدور گواهی، گواهی خود را دریافت نموده‌اند. همچنین، زوج کلیدشان بر روی کارت هوشمند ذخیره شده است. در این پروتکل موجودیت قابل اعتمادی همچون Judge مسئول ثبت‌نام بیماران و تایید نام گمنام آنها می‌باشد. بیمار با نام گمنام خود به سرور خدمات درمانی مراجعه می‌کند تا جهت دریافت خدمات درمانی از هویت واقعی خود استفاده ننماید. پروتکل پیشنهادی دارای چهار فاز مجزا، شامل مرحله‌ی ثبت نام بیمار، آپلود داده‌های بیمار بر روی MCS، بازیابی اطلاعات سلامت بیمار* توسط پزشک معالج از MCS و فاز اورژانس می‌باشد. علاوه بر این، در این طرح بیمار می‌تواند از امکانات درمانی در یک کشور خارجی استفاده نماید. در شکل ۱ شمایی کلی پروتکل نشان داده شده است:



شکل ۱ – طرح کلی پروتکل پیشنهادی

۴-۱. فاز ثبت نام بیمار

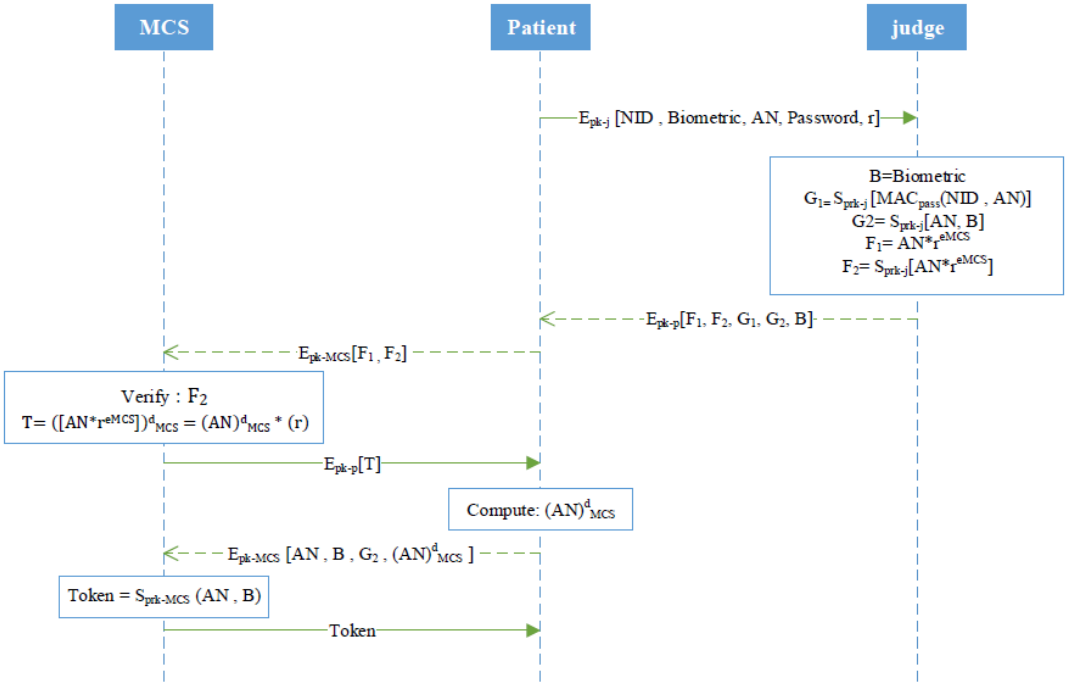
*Patient

در این مرحله هر شهروند برای واجد شرایط شناخته شدن با کارت هوشمند خود به وب‌سایت ثبت‌نام‌کننده*، مراجعه می‌کند. برای این منظور، شهروند اطلاعات هویتی که می‌تواند شامل کد ملی†، پسورد، بیومتریک و فاکتور گمنامی او باشد را به واحد ثبت‌نام‌کننده می‌دهد. هم چنین در این مرحله لازم است که شهروند یک اسم مستعار‡ انتخاب کند.

سپس judge پارامتر F_1 که نام مستعار کور شده به کمک فاکتور گمنامی و پارامتر F_2 که امضا شده‌ی پارامتر F_1 می‌باشد را محاسبه می‌نماید. حال این دو فاکتور را برای بیمار ارسال می‌کند. علاوه بر این، پارامتر G_1 که شامل امضای judge بر روی مک NID و AN و پارامتر G_2 که شامل امضای judge بر روی بیومتریک و نام مستعار بیمار می‌باشد، به بیمار تحویل داده می‌شود.

حال، بیمار پارامترهای F_2 , F_1 را که با کلید عمومی MCS رمز کرده است به MCS می‌فرستد. MCS نیز پس از ارزیابی F_2 عبارت T را محاسبه کرده و آن را برای بیمار بصورت رمز شده می‌فرستد. سپس، بیمار پس از رمزگشایی T آن را به r تقسیم کرده و به $(AN)^d_{MCS}$ دست پیدا می‌کند که این عبارت همان امضای MCS بر روی اسم مستعار بیمار است. سپس بیمار اسم مستعار، اسم مستعار امضا شده، G_2 و بیومتریک را با کلید عمومی MCS رمز کرده و به MCS می‌فرستد.

در نهایت MCS بر روی اسم مستعار و بیومتریک بیمار امضا کرده و آن را به عنوان توکن بیمار در کارت هوشمنداش ذخیره می‌کند. کلیه این مراحل در شکل ۲ با جزئیات نمایش داده شده است.



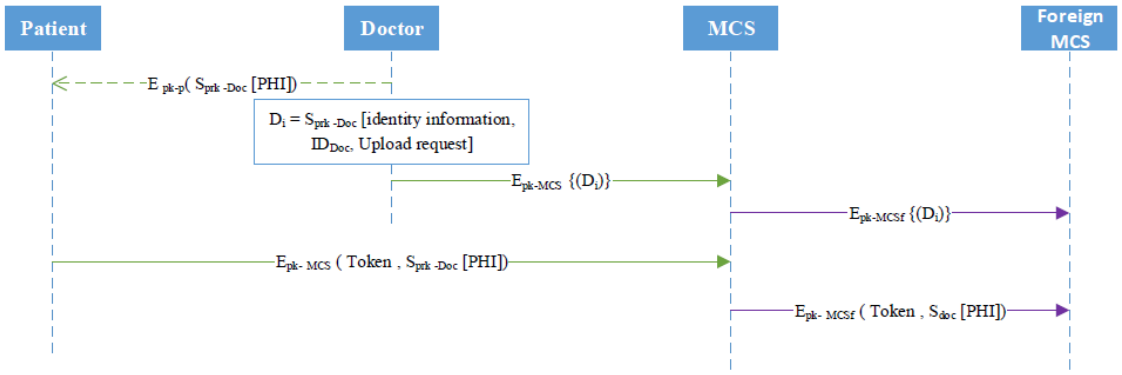
شکل ۲ – فاز ثبت‌نام

*judge
†National ID (NID)
‡Anonymous name

۴-۲. فاز نوشتن داده درMCS

پزشک در این مرحله PHI را امضا کرده و به کارت بیمار می‌فرستد. در این مرحله، هر بار که پزشک می‌خواهد اطلاعات پزشکی بیمار را در پایگاه داده MCS بنویسد باید احرازهویت شود. بدین منظور پزشک اطلاعات هویتی خود را بهراه ID پزشکی خود بعد از امضا توسط کلید خصوصی خود و رمز کردن توسط کلید عمومی MCS، به MCS می‌فرستد و توسط MCS احرازهویت صورت می‌پذیرد. اگر بیمار فردی با ملیتی خارجی باشد، اطلاعات دکتر توسط MCS به MCS_f فرستاده می‌شود تا احرازهویت صورت پذیرد.

نرم افزار ترمینال پزشک، ارتباط بین MCS و کارت هوشمند بیمار را مستقیما برقرار می‌کند. سپس بیمار توسط کارت خود اطلاعات مورد نیاز را به MCS می‌فرستد. اگر بیمار مربوط به کشور خارجی باشد اطلاعات PHI جدید تولید شده‌ی بیمار توسط MCS داخلی به MCS خارجی فرستاده می‌شود. مراحل این فاز در شکل ۳ نمایش داده شده است.

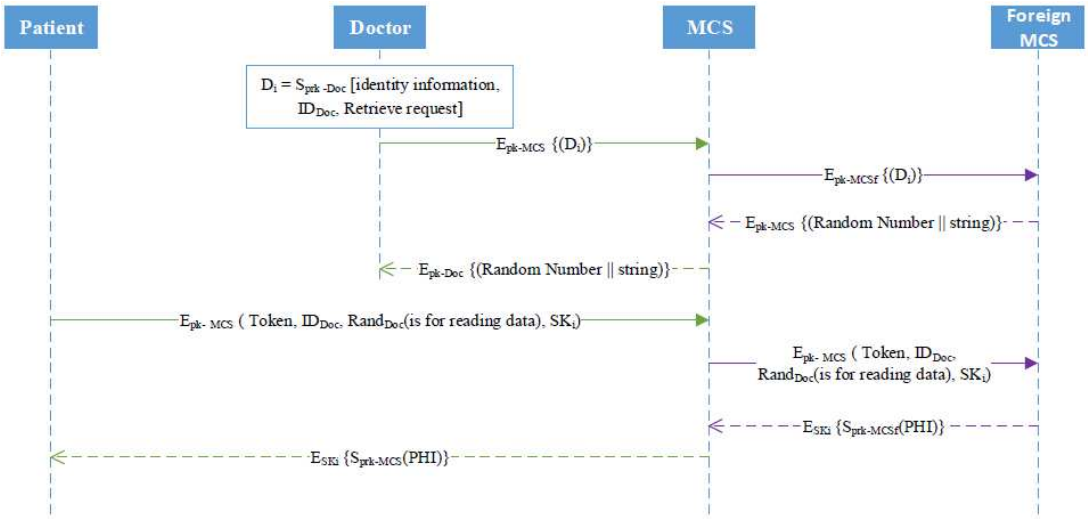


شکل ۳ – فاز نوشتن داده در MCS

۴-۳. فاز بازیابی اطلاعات پزشکی از MCS

هر بار که پزشک می‌خواهد اطلاعات پزشکی بیمار را از پایگاه داده MCS بخواند باید احرازهویت شود. بدین منظور پزشک اطلاعات هویتی خود را به همراه شناسه خود بعد از امضا توسط کلید خصوصی‌اش و رمز کردن توسط کلید عمومی MCS، به MCS می‌فرستد. سپس احرازهویت توسط MCS صورت می‌پذیرد. اگر بیمار فردی با ملیتی خارجی باشد، اطلاعات پزشک توسط MCS به MCS_f فرستاده می‌شود تا احرازهویت صورت پذیرد. سپس، یک عدد تصادفی به همراه یک رشته‌ی تصادفی توسط MCS_f تولید شده و به MCS محلی فرستاده می‌شود. حال، این رشته‌ی تصادفی توسط MCS محلی به پزشک داده می‌شود. در غیر اینصورت فقط یک رشته‌ی تصادفی توسط MCS محلی تولید شده و به پزشک داده می‌شود.

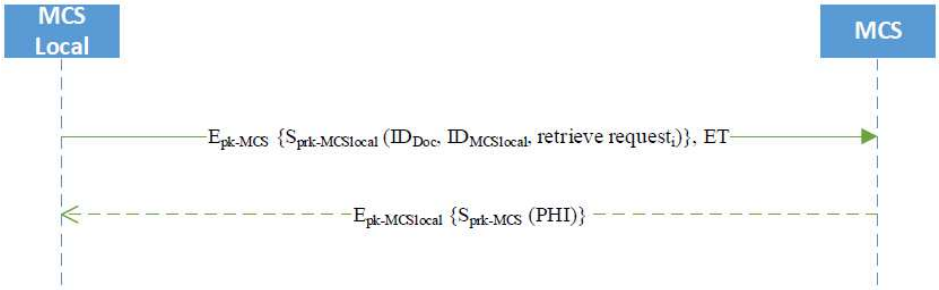
در این مرحله بیمار با استفاده از کارت هوشمند خود، توکن و یک کلید متقارن و پزشک نیز عدد تصادفی و ID خود را برای MCS می‌فرستند. حال MCS اطلاعات PHI را که با کلید خصوصی خودش امضا شده، به کارت هوشمند بیمار می‌فرستد تا جهت بررسی سوابق قبلی بیمار در اختیار پزشک قرارگیرد. اگر بیمار خارجی باشد MCS اطلاعات را به MCS_f می‌فرستد. سپس در MCS_f اطلاعات PHI بیمار را بعد از امضا به MCS داخلی می‌فرستد و در مرحله بعد PHI به کارت بیمار فرستاده می‌شود. مراحل این فاز در شکل ۴ نمایش داده شده است.



شکل ۴ – فاز بازیابی اطلاعات پزشکی از MCS

۴-۴. فاز اورژانس

در این فاز بیمار در حالتی قرار دارد که امکان ارائه هیچگونه اطلاعاتی را به پزشک یا مراکز درمانی ندارد. بنابراین در این فاز باید امکانی فراهم شود تا بتوان بدون اجازه بیمار و برای نجات جان او به اطلاعات پزشکی وی دسترسی داشت. به این منظور پس از وارد کردن کارت بیمار در ترمینال مرکز درمانی، گزینه اورژانس انتخاب می‌شود. در صورت امکان بخش اول احرازهویت با استفاده از اثر انگشت نیز باید انجام شود. در این فاز حضور مرکز درمانی، کلید عمومی وخصوصی آن الزامی می‌باشد. مراحل این فاز در شکل ۵ نمایش داده شده است.



شکل۵ – فاز اورژانس

۵. مقایسه و ارزیابی امنیتی

۵-۱. تحلیل امنیتی

در این بخش برقراری نیازمندی‌های امنیتی و حریم خصوصی HIPPA در پروتکل پیشنهادی مورد ارزیابی و بررسی قرار می‌گیرد. در انتها نیز مقایسه‌ای بین طرح پیشنهادی و سایر طرح ها صورت می‌پذیرد.

۵-۱-۱. گمنامی

در پروتکل پیشنهادی، گمنامی با استفاده از نام مستعار برای بیمار و امضای کور عادلانه تضمین شده است. در واقع بیمار ابتدا در Judge براساس اطلاعات حقیقی خود ثبت‌نام نموده و سپس با مراجعه به MCS توکنی را دریافت می‌کند

که این توکن براساس امضای MCS بر روی نام مستعار و بیومتریک بیمار ساخته می‌شود. این مورد باعث مخفی ماندن اطلاعات شخصی بیمار می‌گردد. با توجه به اینکه نگاشت بین هویت واقعی و اسم مستعار بیمار فقط در Judge صورت می پذیرد، در نتیجه احتمال افشای هویت واقعی بیمار و نقض گمنامی MCS و پزشک وجود ندارد.

۵-۱-۲. کنترل و آگاهی بیمار

در طرح پیشنهادی به هنگام بارگذاری و بازیابی اطلاعات بیمار، حتما نیاز به حضور خود بیمار می‌باشد و بدون اجازه‌ی بیمار امکان دستیابی به اطلاعات PHI توسط پزشک منتفی است. همچنین به دلیل استفاده از عدد تصادفی تولید شده توسط MCS و ارسال آن برای پزشک، بیمار نیز بدون اجازه‌ی پزشک قادر به بارگذاری اطلاعات نمی‌باشد.

۵-۱-۳. محرمانگی

وجود مکانیزم زیر ساخت کلید عمومی و استفاده از گواهینامه‌ی دیجیتال برای هر موجودیت در پروتکل، این اعتماد را فراهم می‌سازد که تبادل اطلاعات با امنیت بالا صورت می‌پذیرد. همچنین استفاده از کلید متقارن در هنگام بازیابی داده‌ها توسط MCS، این امکان را فراهم می‌کند تا نتوان بدون اجازه بیمار به اطلاعات سلامت وی دسترسی یافت.

۵-۱-۴. تمامیت

به منظور برقراری یکپارچگی و صحت اطلاعات تبادل شده و همچنین قابلیت عدم انکار، در این پروتکل از امضای دیجیتال استفاده شده است. در فاز بارگذاری اطلاعات، نسخه بیمار توسط پزشک امضا می‌شود در نتیجه علاوه براینکه MCS و یا مهاجم قادر به جعل آن نمی‌باشد، پزشک نیز نمی‌تواند تشخیص و درمانی در نظر گرفته برای بیمار را انکار نماید.

۵-۱-۵ . کنترل فاز اورژانس

در پروتکل‌های ارائه شده قبلی، پزشک می‌توانست ادعا کند که در فاز اورژانس است و از MCS اطلاعات بیماران را بصورت رمزنشده درخواست نماید. در نتیجه به اطلاعات بدون اجازه‌ی بیمار دست می‌یافت. در پروتکل پیشنهادی با توجه به اینکه توکن رمزشده با کلید عمومی MCS، در کارت بیمار ذخیره شده است، لذا MCS محلی قادر به جعل آن نمی‌باشد و درخواست دسترسی به اطلاعات رمزنشده بیمار بدون در دسترس بودن کارت بیمار ممکن نیست. علاوه بر این به علت استفاده از بیومتریک در صورت سرقت کارت استفاده از کارت در انحصار بیمار می‌باشد.

۵-۲. مقایسه

مقایسه این پژوهش با سایر طرح‌ها در جدول ۱ آورده شده است. در این پژوهش برای جلوگیری از حمله مردی میانی از کلیدهای جلسه و متقارن استفاده شده است. همچنین این طرح گمنامی بیماران را همانگونه که در بخش‌های قبل توضیح داده شد فراهم می‌سازد. این در حالی است که اکثر طرح‌های قبلی به گمنامی بیمار توجه‌ای نداشته‌اند. علاوه بر این امکان ارائه خدمات به بیماران خارجی از دیگر ویژگی‌های پروتکل ارائه شده می‌باشد. همچنین برای احرازهویت بیمار علاوه بر رمزعبور از بیومتریک نیز استفاده شده است.

جدول ۱ - مقایسه پروتکل پیشنهادی با پروتکل‌های موجود

	[۵]	[۱۱]	[۱۰]	[۱۲]	[۱۳]	[۱۴]	پروتکل پیشنهادی
حفظ گمنامی بیمار	×	×	×	×	×	×	✓
مصونیت در برابر حمله مردی میانی	×	×	✓	×	×	✓	✓
امکان ارائه خدمات سلامت به بیماران کشور خارجی	×	✓	×	✓	✓	✓	✓
استفاده از بیومتریک در احرازهویت	×	✓	×	×	×	×	✓
نیاز به مجوز بیمار هنگام بارگذاری PHI	×	✓	✓	×	✓	✓	✓

۱۲. نتیجه‌گیری

در این مقاله، پروتکلی جهت امنیت و حریم خصوصی اطلاعات بیمار در سیستم سلامت الکترونیک ارائه شد. سیستم سلامت الکترونیک پیشنهادی مبتنی بر زیرساخت کلید عمومی و امضای دیجیتال است. همچنین جهت گمنامی و عدم انکار از امضای کور عادلانه استفاده شده است. در این طرح، بیمار از نام مستعار برای استفاده از خدمات درمانی بهره می‌گیرد. پرونده سلامت بیمار بر روی سرور مرکزی بهداشت ذخیره می‌شود و فقط با اجازه بیمار قابل دسترسی است. همچنین شرایط اورژانس و حضور بیمار در کشور خارجی نیز مورد توجه قرار گرفته است. این طرح با نیازمندی‌های امنیتی و حریم خصوصی HIPPA تطابق داشته و مزایای این طرح نسبت به سایر طرح‌های قبلی مورد بررسی قرار گرفته است. بررسی راهکارهای موجود برای ارائه این طرح بر روی پلتفرم موبایل از جمله کارهای آتی می‌باشد.

۱۲. مراجع

1. A. Flores, "Secure exchange of information in electronic health records," Doctor of Philosophy, School of Information Systems & Technology, University of Wollongong, 2010.
2. A. Act, "Health insurance portability and accountability act of 1996," in *Public law* vol. 104, ed, 1996, p. 191.
3. B. Blobel and P. Pharow, "Public key infrastructures for health," *Advanced Health Telematics and Telemedicine: The Magdeburg Expert Summit Textbook,* vol. 96, p. 111, 2003.
4. J. Jin, G.-J. Ahn, H. Hu, M. J. Covington, and X. Zhang, "Patient-centric authorization framework for electronic healthcare services," *computers & security,* vol. 30, pp. 116-127, 2011.

5. W.-B. Lee and C.-D. Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," *IEEE Transactions on Information Technology in Biomedicine,* vol. 12, pp. 34-41, 2008.
6. Y. Tsukada, K. Mano, H. Sakurada, and Y. Kawabe, "Anonymity, privacy, onymity, and identity: A modal logic approach," in *Computational Science and Engineering, 2009 .CSE'09. International Conference on*, 2009, pp. 42-51.
7. M. Stadler, J.-M. Piveteau, and J. Camenisch, "Fair blind signatures," in *International Conference on the Theory and Applications of Cryptographic Techniques*, 1995, pp. 209-219.
8. E. Murray ,J. Burns, C. May, T. Finch, C. O'Donnell, P. Wallace*, et al.*, "Why is it difficult to implement e-health initiatives? A qualitative study," *Implementation Science,* vol. 6, p. 1, 2011.
9. S. Boeyen, T. Howes, and P. Richard, "Internet X. 509 public key infrastructure operational protocols-LDAPv2," 2070-1721, 1999.
10. H.-F. Huang and K.-C. Liu, "Efficient key management for preserving HIPAA regulations," *Journal of Systems and Software,* vol. 84, pp. 113-119, 2011.
11. J. Hu, H.-H. Chen, and T.-W. Hou" ,A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations," *Computer Standards & Interfaces,* vol. 32, pp. 274-280, 2010.
12. S. Ray and G. Biswas, "Design of RSA-CA Based E-Health System for Supporting HIPAA Privacy-Security Regulations," *Procedia Technology,* vol. 6, pp. 954-961, 2012.
13. 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.

۱۴. مومنی تزنگی، م. پارسیان، ز. دوستاری، م. (۱۳۹۲)، "روشی جدید مبتنی بر زیر ساخت کلید عمومی برای حفظ حریم خصوصی در سلامت الکترونیک،" اولین همایش منطقه ای بهینه سازی و روشهای محاسبه نرم در مهندسی برق و کامپیوتر.