نشریه علمی «پدافند الکترونیکی و سایبری»
سال هشتم، شماره ۱، بهار ۱۳۹۹؛ ص ۱۲۴-۱۰۱

یک طرح جدید و امن برای اشتراک‌گذاری داده‌های پزشکی مبتنی‌بر فناوری زنجیره‌بلوکی و رمزنگاری مبتنی‌بر ویژگی

سید مرتضی پورنقی[۱]، مجید بیات[۲]، یعقوب فرجامی*[۳]

۱- دانشجوی دکترای فناوری اطلاعات- امنیت، دانشگاه قم، ایران، ۲- استادیار گروه کامپیوتر، دانشگاه شاهد، تهران، ایران
۳- استادیار گروه کامپیوتر، دانشگاه قم، ایران

(دریافت: ۹۷/۱۲/۲۱، پذیرش: ۹۸/۰۷/۱۰)

چکیده

با توسعه فناوری اطلاعات الکترونیک، استفاده از پرونده سلامت الکترونیک (EMR) یک رویکرد رایج برای ثبت اطلاعات پزشکی بیماران محسوب می‌شود. این اطلاعات در پایگاه‌های اطلاعاتی بیمارستان‌ها و نهادهای پزشکی مختلف به‌صورت مجزا ثبت و ذخیره می‌شود و بیماران هیچ‌گونه کنترلی نسبت به اطلاعات پزشکی خود ندارند، با توجه به این‌که اطلاعات پزشکی از دارایی‌های مهم افراد و نظام سلامت محسوب می‌شود، بنابراین، نگرانی‌هایی جدی در خصوص امنیت و حفظ حریم خصوصی داده‌های پزشکی و چگونگی دسترسی به این اطلاعات وجود دارد. یکی از چالش‌های مهم حوزه سلامت الکترونیک نحوه ذخیره‌سازی و دسترسی کنترل‌شده به اطلاعات پزشکی می‌باشد. ما در این مقاله یک طرح جدید، امن و کارآمد به نام SBA-PHR مبتنی‌بر فناوری زنجیره‌بلوکی و رمزنگاری مبتنی‌بر ویژگی را برای ثبت و ذخیره‌سازی داده‌های پزشکی ارائه کرده‌ایم به گونه‌ای که در این طرح حریم خصوصی کاربران حفظ شده و اجازه کنترل دسترسی دقیق و دانه‌ای به اطلاعات پزشکی بیماران در آن وجود دارد. در طرح SBA-PHR با استفاده از زنجیره‌بلوک‌های خصوصی توانسته‌ایم حق ابطال دسترسی آنی که از چالش‌های رمزنگاری مبتنی‌بر ویژگی است را بهبود بخشیم. ما امنیت طرح پیشنهادی خود را در مدل فرمال و درستی عملکرد آن را مبتنی‌بر منطق BAN به اثبات می‌رسانیم و نشان می‌دهیم که طرح پیشنهادی ما محرمانگی داده‌های کاربر، گمنامی بیماران و حریم خصوصی آن‌ها را به خوبی برآورده می‌کند، همچنین پیچیدگی محاسباتی و ذخیره‌سازی طرح پیشنهادی ما بیانگر کارا بودن طرح SBA-PHR و مقیاس‌پذیر بدون آن می‌باشد.

کلیدواژه‌ها: *سلامت الکترونیک، فناوری زنجیره‌بلوک، رمزنگاری مبتنی‌بر ویژگی، امنیت، منطق* BAN

۱. مقدمه

ارائه خدمات بهداشتی با استفاده از فناوری دیجیتال به‌عنوان "سلامت الکترونیک[۱]" نامگذاری می‌شود. یکی از اهداف سلامت الکترونیک افزایش اثربخشی مراقب‌های بهداشتی و پیامد آن کاهش هزینه‌ها است. به این منظور با تقویت ارتباطات بین مؤسسات مراقبت‌های بهداشتی نیازی به انجام آزمایش‌های غیرضروری، تشخیص‌ها و درمان‌های تکراری نمی‌باشد و در نتیجه هزینه‌ها کاهش پیدا می‌کند. همچنین سلامت الکترونیک با افزایش اثر و امکان تبادل اطلاعات بین مراکز بهداشتی و تصمیم‌گیری مشترک برای درمان، منجر به افزایش کیفیت مراقبت‌های بهداشتی می‌شود. سامانه مراقبت بهداشتی اطلاعات جامع فیزیولوژیکی و سوابق پزشکی بیماران را جمع‌آوری و ذخیره می‌کند، لذا این امر اهمیت داده‌های پزشکی را مهم‌تر از همیشه برجسته می‌سازد. با استفاده از این پایگاه داده جامع، می‌توان ابزارهای تجزیه و تحلیل را برای کشف اطلاعات مفید و شناسایی عوامل محیطی جهت اختلالات نادر و درمان‌های پزشکی انجام داد [۱].

پرونده الکترونیکی سلامت (EMR)[۲] [۳-۲] یک پرونده پزشکی الکترونیکی شامل تمام اطلاعات مرتبط با سلامت شخص در طول حیات او می‌باشد. پرونده الکترونیکی سلامت با در بر داشتن ساختار و استانداردهای مناسب و حفظ اصول محرمانگی، یک پرونده دائم از سابقه بهداشتی درمانی فرد و مراقبت از وی در نظام سلامت را فراهم می‌کند. پرونده الکترونیک سلامت شامل یادداشت‌های بهداشتی درمانی دوران عمر یک فرد مانند تصاویر پزشکی، درمان‌های پزشکی انجام‌شده، داروها، گزارش‌های تجربی، سابقه خانوادگی بیماری ژنتیکی و غیره است که در داخل سامانه بهداشتی درمانی ایجاد و به‌صورت خصوصی و محرمانه نگهداری می‌شود. این پرونده به‌صورت الکترونیکی برای

رایانامه نویسنده پاسخگو: farjami@qom.ac.ir

1- E-Health

2- Electronic Medical Record (EMR)

ارائه‌کنندگان مجاز خدمات در هر مکان و زمان به‌منظور حمایت و پشتیبانی از ارتقا کیفیت خدمات وی باید در دسترس باشد.

به اشتراک‌گذاری امن و مقیاس‌پذیر پرونده الکترونیکی سلامت برای مدیریت موثرتر درمان، همکاری نهادهای درمانی، تسریع در فرایند درمان و مراقبت از بیماران ضروری است. افراد در طول زندگی خود بارها به بیمارستان‌ها و دفاتر خدمات درمانی متعددی مراجعه می‌کنند و در هر بار مراجعه اطلاعات پزشکی خاص و متنوعی را در اختیار این نهادها قرار می‌دهند. مراکز خدمات درمانی برای این‌که بتوانند خدمات درمانی موثر، دقیق، سریع و مقرون به صرفه‌ای را در اختیار بیماران قرار دهند باید بتوانند اطلاعات پزشکی بیماران را به‌صورت محرمانه و سریع به‌روزرسانی کرده و با سایر نهادهای مجاز به اشتراک گذارند.

در سال‌های اخیر مؤسسات پزشکی بسیاری شروع به جمع‌آوری اطلاعات EMR بیماران با ساز و کارهای مختلف و مخصوص به خود را کرده‌اند، اما این رویکرد به اشتراک‌گذاری داده‌های پزشکی را به همراه ندارد. به همین منظور برای استفاده بهتر از داده‌های EMR و اشتراک‌گذاری بهتر آن‌ها و همچنین راحتی بیماران و مراکز درمانی برخی از مراکز جمع‌آوری داده‌های EMR به‌صورت متمرکز ایجاد شده است. این رویکرد، نیازمند صرف هزینه‌های بسیار زیاد و پشتیبانی فنی پیچیده‌ای است. بنابراین، سامانه‌های ذخیره‌سازی مبتنی‌بر ابر می‌توانند یک راه‌کار مناسب تلقی شوند. استفاده از فناوری ذخیره‌سازی مبتنی‌بر ابر دارای مزایای انتقال سریع اطلاعات، به اشتراک‌گذاری خوب داده‌ها، ظرفیت ذخیره‌سازی بالا، هزینه کم، دسترسی آسان به اطلاعات و ارتباط پویا را شامل می‌شود [۴].

با این حال، هنگامی که کاربران اطلاعات EMR را در سرورهای ابری ذخیره می‌کنند، با انواع تهدیدات امنیتی مانند نقض حریم خصوصی بیماران، یکپارچگی داده‌ها و احراز هویت آن‌ها مواجه می‌شوند. بنابراین، خطرات بسیار زیادی متوجه مدیریت متمرکز داده‌های پزشکی است. داده‌های پزشکی می‌تواند به راحتی سرقت، دستکاری و یا حتی به‌طور کامل حذف شوند. در این موارد نمی‌توان داده‌های پزشکی را به‌صورت قابل اعتماد ضبط یا بازیابی کرد، که موجب تاخیر در فرآیند درمان و یا حتی به خطر انداختن زندگی بیمار خواهد شد. امروزه تخمین زده می‌شود اطلاعات پزشکی افراد ۱۰ برابر با ارزش‌تر از رمز کارت اعتباری آن‌ها است. در سامانه‌های متمرکز اگر سامانه به‌طور مخرب مورد حمله قرار گیرد، تمام گره‌های دیگر از بین می‌روند و قادر به ذخیره و استفاده از داده‌ها نیستند. با این حال، اگر از فناوری معماری توزیع‌شده زنجیره‌بلوکی استفاده کنیم، حتی اگر برخی از گره‌ها به‌صورت مخرب مورد حمله قرار گیرند، گره‌های دیگر تحت تاثیر قرار نمی‌گیرند و شبکه به حیات خود ادامه می‌دهد. متخصصین و محققان حوزه امنیت نگاه تردیدآمیزی به ذخیره‌سازی اطلاعات مهم پزشکی در پایگاه داده متمرکز دارند، همچنین بیشتر مردم هنوز نگران امنیت و حریم خصوصی این پایگاه‌های داده هستند. یکی از نگرانی‌های جدی در این حوزه چگونگی اعمال سیاست‌های کنترل حق دسترسی به اطلاعات پزشکی است. در این معماری نهاد مرکزی این امکان را دارد تا برخی از سیاست‌های دسترسی به داده‌ها را نادیده بگیرد و بر خلاف رویه مورد انتظار شبکه عمل کند [۵].

به تازگی یک فناوری امیدوارکننده با نام زنجیره‌بلوکی در مطالعات مورد بحث قرار گرفته است. این فناوری به اهداف غیرمتمرکزسازی و قراردادهای هوشمند می‌پردازد. در عمل برای اشتراک‌گذاری داده‌های پزشکی بسیاری از موانع در زیرساخت‌های فنی شبکه IT[1] سلامت وجود دارد که مانع دسترسی امن و مقیاس‌پذیر به داده‌های پزشکی در سرتاسر شبکه می‌شود. این نگرانی‌ها شامل حفظ حریم خصوصی بیماران، عدم اعتماد بین نهادهای بهداشتی، مقیاس‌پذیری و کنترل حق دسترسی دقیق به اطلاعات می‌شود [۶-۷].

۱-۱. نوآوری مقاله

در این مقاله یک معماری جدید برای اشتراک‌گذاری امن و مقیاس‌پذیر داده‌های پزشکی که بتواند حریم خصوصی کاربران را نیز به خوبی حفظ کند، به همراه جزئیات پیاده‌سازی این معماری ارائه شده است. ما در طرح پیشنهادی خود برای حل مشکلات امنیتی اشتراک‌گذاری موثر اطلاعات پزشکی و ایجاد یک فرآیند کنترل حق دسترسی دقیق و دانه‌ای[2] به اطلاعات پزشکی که حریم خصوصی کاربران را نیز به خوبی حفظ کند، یک روش امن و کارآمد کنترل سطح دسترسی برای ثبت و ذخیره داده‌های پزشکی با تلفیق رمزنگاری مبتنی‌بر ویژگی، پروتکل‌های مبتنی‌بر زنجیره‌بلوکی و سامانه‌های ذخیره‌ساز ابری ارائه می‌دهیم.

در طرح پیشنهادی ما به‌منظور کنترل سطح دسترسی دقیق و دانه‌ای بر روی داده‌های پزشکی و حفظ حریم خصوصی بیمار از رمزنگاری مبتنی‌بر ویژگی استفاده شده است، همچنین جهت اطمینان از صحت داده‌های پزشکی، عدم تغییر آن‌ها و بهبود فرآیندهای ابطال و وکالت حق دسترسی به داده‌های پزشکی که از چالش‌های اساسی رمزنگاری مبتنی‌بر ویژگی است از فرآیندهای مبتنی‌بر زنجیره‌بلوکی و قراردادهای هوشمند بهره گرفته‌ایم. ما در طرح پیشنهادی خود از دو نوع زنجیره‌بلوکی خصوصی permission و permissionless استفاده کرده‌ایم. با

1- Health IT Systems
2- Fine Grain

توجه به حجم بالای داده‌های پزشکی به‌منظور افزایش کارایی سامانه، این داده‌ها در سامانه‌های ذخیره‌ساز ابری نگهداری می‌شوند و به علت ناکارآمدی روش‌های رمزنگاری کلید عمومی جهت رمزنگاری داده‌های با حجم بالا، از رمزنگاری متقارن جهت حفظ محرمانگی داده‌های پزشکی استفاده می‌کنیم و کلید آن توسط الگوریتم‌های رمزنگاری مبتنی‌بر ویژگی رمزنگاری می‌شود.

ما صحت عملکرد طرح پیشنهادی خود را بر اساس منطق BAN مورد بررسی قرار داده و اثبات می‌کنیم که پروتکل پیشنهادی می‌تواند نیازمندی‌های امنیتی به اشتراک‌گذاری داده‌های پزشکی را برآورده کند. همچنین ما امنیت پروتکل‌های رمزنگاری مبتنی‌بر ویژگی به‌کار رفته در این معماری را به‌صورت فرمال و در مدل اوراکل تصادفی اثبات می‌کنیم و پیچیدگی محاسباتی و فضای ذخیره‌سازی طرح پیشنهادی خود را مورد بررسی قرار می‌دهیم.

۱-۲. سازمان‌دهی مقاله

در بخش ۲ مروری بر کارهای گذشته در حوزه به اشتراک‌گذاری داده‌های پزشکی داریم و در بخش ۳ ملزومات و پیش‌نیازهای طرح پیشنهادی خود را بیان می‌کنیم. سپس در بخش ۴ معماری طرح پیشنهادی خود را به همراه جزئیات پروتکل‌ها ارائه می‌کنیم. در بخش ۵ امنیت طرح پیشنهادی خود و در بخش ۶ کارایی آن را مورد بررسی قرار می‌دهیم. در پایان در بخش ۷ جمع‌بندی و کارهای آینده را ارائه می‌دهیم.

۲. کارهای گذشته

سامانه‌های ذخیره‌سازی مبتنی‌بر ابر جهت ذخیره‌سازی داده‌های پزشکی در سامانه‌های سلامت الکترونیکی ورود پیدا کرده است. این روش‌ها راه‌حل‌های امیدوارکننده‌ای را برای به اشتراک گذاشتن داده‌های PHI در میان مؤسسات پزشکی در سامانه‌های e-Health ارائه می‌دهند، جایی که امنیت و حفظ حریم خصوصی از نگرانی‌های حیاتی هستند. اگر چه تمام کارهای فوق جهت به‌دست آوردن ویژگی‌های امنیتی در محیط‌های ابری تمرکز دارد، اما یک چالش همواره در این روش‌ها وجود دارد؛ در تمام این روش‌ها انتظار می‌رود که ابر یک مرکز قابل اطمینان برای ذخیره و مدیریت داده‌های حساس پزشکی باشد. بنابراین، همواره نگرانی‌هایی جهت سوءاستفاده از داده‌ای پزشکی، از دست رفتن اطلاعات PHI، نشت و یا سرقت آن‌ها وجود دارد. اقدامات زیادی با استفاده از روش‌های رمزنگاری و یا سایر روش‌ها پیشنهاد شده است، اما متاسفانه این تهدیدات با توجه به ویژگی‌های متمرکز بودن محیط‌های ابری همواره باقی مانده است [۸].

یو[1] و همکاران [۹] یک برنامه کاربردی را برای به اشتراک گذاشتن داده‌های مراقبت‌های بهداشتی ارائه داده‌اند، که در آن بیماران کنترل و ارسال داده‌های خود را به‌راحتی در آن انجام می‌دهند. در این طرح یک سامانه سه لایه شامل لایه داده کاربر، لایه مدیریت داده و لایه ذخیره‌سازی داده پیشنهاد شده است. تفاوت این طرح با سایر طرح‌ها در این است که در آن پیشنهاد شده است که از زنجیره‌بلوکی خصوصی به‌عنوان ابر استفاده شود.

کیو[2] و همکاران [۱۰] سامانه MeDShare را پیشنهاد داده‌اند که در آن، مشکل اشتراک داده‌های پزشکی در میان سرورهای داده‌های بزرگ پزشکی در یک محیط بی اعتماد مورد بررسی قرار گرفته است. در این سامانه بر مبنای یک زنجیره‌بلوکی permissioned تنها اجازه دسترسی به کاربران دعوت‌شده و تأییدشده به زنجیره‌بلوکی داده می‌شود.

اکبلا[3] و همکاران [۴] سامانه MedRec را پیشنهاد داده‌اند که یک سامانه مدیریت رکورد غیرمتمرکز مبتنی‌بر زنجیره‌بلوکی برای رفع سوابق سلامت الکترونیک است. در این چارچوب برای مدیریت احراز هویت و اشتراک‌گذاری داده‌ها از زنجیره‌بلوکی permissioned استفاده شده است که فقط کاربران مجاز می‌توانند به آن دسترسی داشته باشند. در این سامانه گره‌های استخراج‌کننده[4] توسط دست‌یابی به ابر داده‌های پزشکی تشویق می‌شوند که در فرآیند استخراج مشارکت کنند.

پیترسون[5] و همکارانش [۱۱] یک سامانه مراقبت‌های بهداشتی مبتنی‌بر زنجیره‌بلوکی ارائه داده‌اند که ملاحظات استاندارد FHIR[6] در آن ادغام شده است. آن‌ها یک سامانه درخت مرکل[7] مبتنی‌بر زنجیره‌بلوکی را پیشنهاد داده‌اند که فرآیند اجماع آن برای استخراج بلوک‌ها بر اساس اثبات قابلیت همکاری[8] انجام می‌شود. در این طرح اثبات قابلیت همکاری بر اساس سازگاری با پروتکل FHIR است، به این معنی که استخراج‌کننده‌ها باید پیام‌های پزشکی ارسال‌شده به بلوک‌های خود را برای اطمینان از سازگاری با استانداردهای ساختاری و معنایی شناخته‌شده تایید کنند.

دوبو ویفساکا[9] و همکارانش [۱۲] یک چارچوب مبتنی‌بر

1- Yue
2- Qi
3- Ekblaw
4- Miner
5- Peterson
6- Fast Healthcare Interoperability Resources
7- Merkle-Tree
8- Proof of Interoperability
9- Dubovitskaya

زنجیره‌بلوکی permissioned برای مدیریت و اشتراک‌گذاری مدارک پزشکی برای مراقبت از بیماران سرطانی ارائه داده‌اند. در طرح آن‌ها با استفاده از یک نام کاربری / رمز عبور، احراز هویت و تایید ثبت‌نام سرویس عضویت کاربران انجام می‌شود. هویت بیمار از طریق ترکیبی از اطلاعات شناسایی شخصی (شامل شماره امنیت اجتماعی، تاریخ تولد، نام، و کد پستی) تولید و برای امنیت رمزگذاری‌شده است. فایل‌های داده پزشکی به یک سرور ابری بارگذاری شده و دسترسی به آن‌ها توسط منطق زنجیره‌بلوکی مدیریت می‌شود.

در تمامی این تحقیقات فقط از زنجیره‌بلوکی به‌عنوان یک ابزار ذخیره‌سازی استفاده شده است. بنابراین، امکان اشتراک‌گذاری همکارانه داده‌های پزشکی با کنترل سطح دسترسی دقیق و دانه‌ای توسط نهاد تولیدکننده آن در این طرح‌ها به خوبی تبیین نشده است [۱۳]. علاوه‌بر این در این کارها یک راه‌حل دقیق به همراه جزئیات پروتکل‌های مورد نیاز آن ارائه نگردیده است. لذا ما در این مقاله یک روش کنترل سطح دسترسی دقیق و دانه‌ای مبتنی‌بر رمزنگاری ABE و زنجیره‌بلوکی را جهت دسترسی و ذخیره داده‌های پزشکی به همراه جزئیات این طرح ارائه می‌دهیم.

۲-۱. رمزنگاری مبتنی‌بر ویژگی

رمزنگاری مبتنی‌بر ویژگی یک نوع خاصی از رمزنگاری کلید عمومی است که در آن ویژگی‌های کاربر می‌تواند به‌عنوان کلید عمومی او مورد استفاده قرار گیرد. از آنجا که اطلاعات شناسه کاربر را می‌توان به‌عنوان یک ویژگی خاص در نظر گرفت، رمزنگاری مبتنی‌بر ویژگی به‌طور ضمنی شامل رمزنگاری مبتنی‌بر شناسه نیز است. مفهوم رمزنگاری مبتنی‌بر شناسه اولین بار توسط شامیر در سال ۱۹۸۴ پیشنهاد شد [۱۴]. سپس در سال ۲۰۰۱ بونه و فرانکلین [۱۵] اولین طرح رمزنگاری مبتنی‌بر شناسه (IBE[1]) را با استفاده از زوج‌سازی‌های دوخطی معرفی کردند. در سال ۲۰۰۵، ساهای و واترز مفهوم رمزنگاری مبتنی‌بر شناسه فازی را پیشنهاد دادند [۱۶]، که می‌تواند به شکل اولیه رمزنگاری مبتنی‌بر ویژگی (ABE[2]) در نظر گرفته شود. سپس، گویال و همکاران. [۱۷] تعریف رسمی ABE را در سال ۲۰۰۶ ارائه کردند. دو نوع متفاوت از رمزنگاری مبتنی‌بر ویژگی وجود دارد، یکی بر پایه سیاست کلید (KP-ABE[3]) و دیگر بر پایه سیاست متن رمزی (CP-ABE[4]).

۲-۱-۱. KP-ABE

در رمزنگاری KP_ABE متن رمز به مجموعه‌ای از ویژگی‌ها وابسته است و کلید کاربر وابسته به یک ساختار دسترسی می‌باشد. در این روش کاربر تنها زمانی می‌تواند عمل رمزگشایی را انجام دهد که مجموعه ویژگی‌های متن رمز در ساختار دسترسی کلید صدق کند. بنابراین، در KP_ABE کلید خصوصی کاربر با ساختار دسترسی در ارتباط است که کنترل می‌کند یک کاربر چه متن‌های رمزی را می‌تواند رمزگشایی کند.

۲-۱-۲. CP-ABE

در رمزنگاری CP_ABE برخلاف KP_ABE، کلید خصوصی کاربران به تعداد دلخواهی از ویژگی‌ها وابسته است و یک پیام به‌وسیله سیاست دسترسی مشخصی که به‌وسیله رمزکننده اتخاذ می‌گردد، رمز می‌شود. در این روش یک کاربر زمانی می‌تواند یک متن رمزی را رمزگشایی کند اگر و تنها اگر ویژگی‌های کاربر، سیاست تعیین‌شده توسط متن رمز را برآورده کند. بنابراین، در CP_ABE متن رمزی با ساختار دسترسی در ارتباط است که کنترل می‌کند کدام کاربر می‌تواند متن رمزی را رمزگشایی کند.

۲-۲. زنجیره‌بلوکی

زنجیره‌بلوکی معمولاً به‌عنوان مجموعه‌ای از فنون مورد استفاده در شبکه‌های غیرمتمرکز برای حفظ پایگاه داده‌ای سازگار در میان تمام اعضا به شمار می‌رود. این روش ابتدا توسط ساتوشی ناکاماتو[5] برای ایجاد روش‌هایی جهت تولید یک پول دیجیتال یا رمز ارز مانند بیت‌کوین معرفی شد [۱۸]. تفاوت ساختار زنجیره‌بلوکی با ساختار شبکه سنتی متمرکز در این است که هیچ گره مرکزی ثابتی در این شبکه‌ها وجود ندارد و همه اعضا در شبکه موقعیت نسبتاً یکسانی دارند و همه یک کپی از اطلاعات زنجیره‌بلوکی را ذخیره می‌کنند. در واقع زنجیره‌بلوکی یک دفتر حساب غیرقابل تغییر از بلوک‌ها بر مبنای زمان است که برای اشتراک گذاشتن و ذخیره داده‌ها به‌صورت توزیع‌شده استفاده می‌شود.

زنجیره‌بلوکی یک پایگاه داده توزیع‌شده است که فهرستی مرتب از اطلاعات ذخیره‌شده و مرتبط با هم را از طریق یک زنجیره در بلوک‌ها ایجاد می‌کند. یک بلوک معمولاً شامل مقدار چکیده از بلوک قبلی، محتوای اطلاعات، امضای شرکت‌کننده و مهر زمانی است. مقدار چکیده بلوک قبلی باعث تغییرناپذیری زنجیره‌بلوکی می‌شود. امضای مشارکت‌کننده و مهر زمانی نشانگر تولیدکننده تراکنش و زمان تولید آن است.

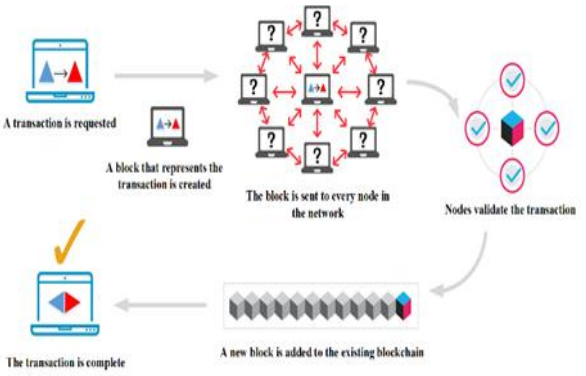
فناوری زنجیره‌بلوکی را می‌تواند به‌عنوان یک مدل توزیع‌شده که اجازه هر نوع ارتباطی را از طریق سامانه همکار به همکار[6] را فراهم می‌کند معرفی کرد، که در آن جزئیات هر تراکنش در هر

1- Identity Based Encryption
2- Attribute Based Encryption
3- Key Policy Attribut Based Encryption
4- Cipher Policy Attribut Based Encryption
5- Satoshi Nakamoto
6- Peer-to-Peer

گره ذخیره می‌شود، و دلیل اصلی این‌که زنجیره‌بلوکی برای ذخیره هر تراکنش نیاز به پایگاه داده متمرکز ندارد همین است. زنجیره‌بلوکی امکان اضافه کردن داده‌های جدید در تراکنش را فراهم می‌کند اما امکان تغییر در آن‌ها را نمی‌دهد. در زنجیره‌بلوکی تراکنش‌ها به‌منظور اطمینان از احراز هویت منبع داده و عدم انکار آن، توسط کلید خصوصی هر کاربر امضا می‌شود. سپس فرآیند چکیده‌سازی برای تایید یکپارچگی تراکنش و اطمینان از عدم تغییر آن اضافه می‌شود. تراکنش‌ها در قالب بلوک‌های مشخصی قرار گرفته و در اختیار تمام گره‌های شبکه قرار می‌گیرد تا دید یکسانی از تعاملات شبکه برای تمام اعضای شبکه ایجاد شود. در زنجیره‌بلوکی، کاربران می‌توانند تعداد دلخواهی از کلیدهای عمومی تولید کنند که به‌طور موثر مانع از ردیابی آن‌ها می‌شود و این امر حریم خصوصی کاربران را تضمین می‌کند [۱۹].

○ عملکرد زنجیره‌بلوکی

برای استفاده از زنجیره‌بلوکی، ابتدا لازم است یک شبکه نظیر به نظیر با تمام گره‌هایی که علاقه‌مند به استفاده از زنجیره‌بلوکی هستند، ایجاد کنید. هر گره از شبکه دو کلید ایجاد می‌کند؛ یک کلید عمومی که توسط سایر کاربران برای ارسال پیام‌ها به آن گره استفاده می‌شود و یک کلید خصوصی که برای امضاء پیام‌های ارسالی توسط گره استفاده می‌شود. هنگامی که یک گره یک تراکنش را انجام می‌دهد، آن را امضا می‌کند و سپس آن را به همتایان خود در شبکه پخش می‌کند. گره همکار قبل از انتشار تراکنش دریافت‌شده آن را اعتبارسنجی می‌کند و در صورت تأیید آن را در شبکه بازپخش می‌کند. لذا این رویکرد به پخش پیام‌های صحیح در شبکه کمک می‌کند. تراکنش‌های منتشرشده که در شبکه اعتبارسنجی شده‌اند توسط گره‌های مخصوصی به نام miner مرتب شده و در بلوک‌هایی بر اساس زمان انتشار دسته‌بندی می‌شوند. انتخاب minerها و داده‌های موجود در یک بلوک به الگوریتم اجماع استفاده‌شده در زنجیره‌بلوکی بستگی دارد. بلوک‌های دسته‌بندی‌شده توسط minerها مجدد در شبکه بازپخش می‌شود. سپس گره‌های شبکه زنجیره‌بلوکی، اعتبار بلوک منتشرشده را بررسی می‌کنند، این بررسی شامل اعتبارسنجی تمام تراکنش‌های موجود در بلوک و ارجاع صحیح این بلوک به چکیده بلوک قبلی منتشرشده در شبکه می‌باشد. اگر چنین شرایطی برآورده نشود، بلوک حذف می‌شود. با این حال، اگر هر دو شرط با موفقیت تایید شوند، گره‌ها بلوک را به زنجیره خود اضافه و زنجیره‌بلوکی خود را به‌روزرسانی می‌کنند (شکل (۱)).



شکل (۱): ساختار زنجیره‌بلوکی

الگوریتم اجماع قلب یک زنجیره‌بلوکی محسوب می‌شود و بسته به کاربرد زنجیره‌بلوکی در حوزه‌های مختلف می‌تواند روش‌های متفاوتی داشته باشد. به‌طور کلی الگوریتم‌های اجماع در زنجیره‌بلوکی را می‌توان بر اساس حق دسترسی به اطلاعات زنجیره‌بلوکی (مانند زنجیره‌بلوک‌های permissionless و permissioned) و بر اساس حق استخراج بلوک در آن‌ها (مانند زنجیره‌بلوکی عمومی و خصوصی) دسته‌بندی کرد. در زنجیره‌بلوک‌های عمومی هر گره‌ای می‌تواند بدون نیاز به تأیید نهاد سوم به زنجیره‌بلوکی ملحق شود و به‌عنوان یک گره ساده و یا گره miner/valdator در شبکه فعالیت کند.

در زنجیره‌بلوکی‌های خصوصی، گروهی از گره‌ها بر اساس یک مبنای مشخص حق مالکیت دسترسی به شبکه را تعیین کرده و یا محدود می‌کنند. در بسیاری از زنجیره‌بلوکی‌های خصوصی کنترل می‌شود که کدام کاربر اجازه انجام تراکنش‌ها را دارد، کدام گره‌ها می‌توانند قرارداد هوشمند را اجرا کنند و یا به‌عنوان miner فعالیت کنند. نمونه‌هایی از زنجیره‌بلوکی‌های permissioned آن‌هایی هستند که توسط HyperledgerFabric [۲۰] و یا Ripple [۲۱] استفاده می‌شود.

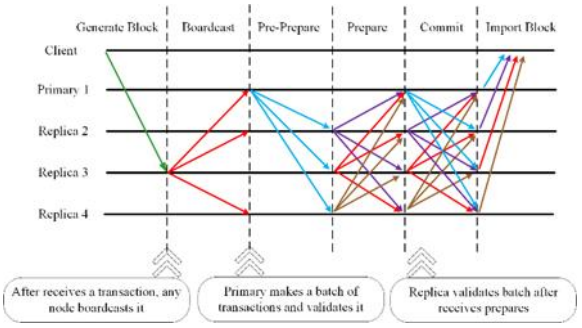
در طرح پیشنهادی ما از دو زنجیره‌بلوکی خصوصی permissionless و permissioned استفاده شده است. استفاده از زنجیره‌بلوکی‌های خصوصی کنترل بیشتر بر حریم خصوصی کاربران را به همراه دارد و این ویژگی مهمی است که در ثبت اطلاعات پزشکی به آن نیاز داریم و بیماران همواره نسبت به آن نگرانی دارند.

○ روش اجماع مبتنی‌بر BPFT

الگوریتم PBFT [۲۲] بر مبنای مسئله ژنرال بیزانسی[1] [۲۳] بنا شده است و سعی دارد با فرض وجود خطا در سامانه با استفاده از تکرار لایه‌های رأی‌گیری به یک توافق سراسری در شبکه دست

1- Byzantine Generals Problem

یابد. پیاس[1] و همکارانش [۲۴] احتمال دست‌یابی به این توافق را با فرض وجود خطا مورد بررسی قرار دادند، آن‌ها اثبات کردند که رسیدن به توافق مورد انتظار با وجود گره‌های خطاکار بیش از ۱/۳ غیرممکن است. روش اجماع BPFT در صورتی می‌تواند در مقابل خطای بیزانسی مقاوم باشد که حداقل ۲/۳ از گره‌های شبکه درست‌کار باشند. بنابراین، اگر فرض کنیم کل گره‌های اجماع n و کل گره‌های تسخیرشده و مخرب f باشد آن‌گاه در صورتی اجماع موفقیت‌آمیز است که $n \geq 3f + 1$ باشد. در این بخش به‌صورت خلاصه روش اجماع PBFT که در سامانه SBA-PHR از آن استفاده می‌کنیم را تشریح می‌کنیم. روش اجماع PBFT در SBA-PHR دارای ۵ مرحله است: (شکل (۲)).



شکل (۲): روش اجماع PBFT

Generate Block: یک leader مسئول ایجاد یک بلوک نامزد جدید است. در سامانه ما گره‌های اجماع به نوبت بلوک نامزد جدید را تولید می‌کنند. یعنی هر گره اجماع به نوبت leader می‌شود.

Pre-prepare (Block Data): گره leader بلوک نامزد را به سایر گره‌های اجماع پخش عمومی می‌کند.

Prepare (Block Hash): هر گره‌ای که بلوک را دریافت کند آن را صحت‌سنجی می‌کند و prepare message را به همراه چکیده بلوک پخش عمومی می‌کند.

Commit (Block Hash): بعد از دریافت تعداد کافی prepare messages (به‌عنوان مثال تعداد کل پیام‌ها بیشتر از ۲/۳ کل گره‌ها شود) برای هر پیام commit message محاسبه و به همه گره‌ها پخش عمومی می‌شود.

Import Block: گره‌ها در مورد بلوک پیشنهادی به یک اجماع می‌رسند. اگر تعداد پیام‌های commit messages کمتر از ۲/۳ از تعداد کل گره‌های شبکه نباشد یعنی بلوک می‌تواند به زنجیره بلوک زنجیره‌بلوکی اضافه شود.

1 -Pease

○ قراردادهای هوشمند

قرارداد هوشمند اولین بار توسط نیک سزابو[2] در سال ۱۹۹۴ معرفی شد [۲۵] و در آن قرارداد هوشمند به‌عنوان یک پروتکل که شرایط قرارداد یک تراکنش کامپیوتری را اجرا می‌کند معرفی شد. هنگامی که یک قرارداد هوشمند با زنجیره‌بلوکی ترکیب می‌شود برای همیشه در آن باقی می‌ماند. هر قرارداد هوشمند می‌تواند بخشی از یک پایگاه داده با یک آدرس منحصربه‌فرد باشد، که انتشار یک تراکنش به آدرس آن می‌تواند توابع آن را برای مدیریت آن بخش از پایگاه داده فعال کند.

مفهوم قرارداد هوشمند به مجموعه‌ای از کدهای نرم‌افزاری اشاره دارد که شرایط اجرای پیش‌تعیین‌شده در آن را مشخص می‌کنند. قراردادهای هوشمند اغلب به فرم شرطی "if … then …" سازماندهی می‌شوند. هنگامی که شرایط اجرای قرارداد به‌درستی برآورده شود، اجرای قرارداد به‌طور خودکار و بدون دخالت انسانی و نظارت شخص ثالث اتفاق خواهد افتاد.

سازنده قرارداد هوشمند آن را در زنجیره‌بلوکی قرار می‌دهد. سپس کاربران با ارسال پارامترهای مورد نیاز به آدرس آن قرارداد هوشمند آن را فعال می‌کنند. در طرح SBA-PHR قرارداد هوشمند یک تراکنش ثبت‌شده در زنجیره‌بلوکی را به‌عنوان ورودی دریافت کرده و پس از بررسی شرایط قرارداد در خروجی تراکنشی متناسب با آن را که شامل کلید رمزگذاری داده و مکان ذخیره‌سازی آن در ابر است را باز می‌گرداند.

۳. طرح پیشنهادی

در این بخش ابتدا به توضیح کلیات طرح پیشنهادی SBA-PHR برای ذخیره‌سازی و اشتراک‌گذاری داده‌های پزشکی PHI می‌پردازیم. سپس جزئیات پیاده‌سازی هر یک از مراحل اجرای طرح را تشریح می‌کنیم. شکل‌های (۵-۳) فرآیند اجرای طرح پیشنهادی SBA-PHR را توصیف می‌کند. طرح SBA-PHR را می‌توان به سه لایه تولید محتوای پزشکی، ذخیره‌سازی اطلاعات PHI و استفاده از اطلاعات PHI تقسیم‌بندی کرد.

در این سامانه از دو نوع زنجیره‌بلوکی خصوصی استفاده کرده‌ایم؛ یکی زنجیره‌بلوکی خصوصی premissined که برای ذخیره‌سازی اطلاعات کلید رمزگذاری داده‌های PHI و مسیر ذخیره‌سازی آن‌ها در ابر استفاده می‌شود و نهادهای استفاده‌کننده از داده‌های پزشکی به آن دسترسی دارند. دیگری زنجیره‌بلوکی خصوصی permissionless است که برای ذخیره‌سازی شرح مختصری از اطلاعات PHI و کلید واژه‌های

2- Nick Szabo

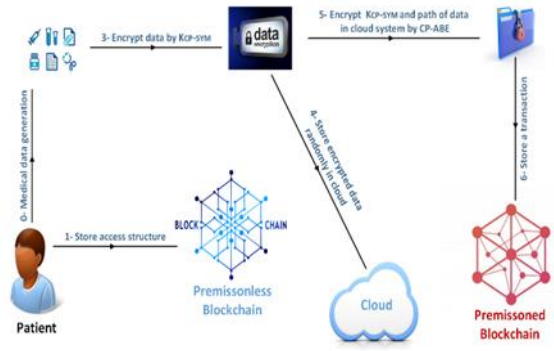
مرتبط با داده‌های ذخیره شده در زنجیره‌بلوکی خصوصی premissined استفاده می‌شود و دسترسی به آن برای تمام نهادهای پزشکی و بیمارستان‌ها آزاد است. ماهیت و عملکرد این دو زنجیره‌بلوکی متفاوت است اما گره‌های برپاکننده آن‌ها می‌توانند به‌صورت مشترک توسط رایانه‌های بیمارستان‌ها و یا بیماران به اجرا در بیایند. بنابراین، در طرح پیشنهادی ما یک زیرساخت شبکه‌ای زنجیره‌بلوکی وجود دارد اما دو عملکرد متفاوت را ارائه می‌دهند.

برای افزایش کارایی سامانه و به علت حجم زیاد داده‌های پزشکی، اطلاعات PHR بیماران به‌صورت رمزگذاری‌شده و تصادفی در سامانه‌های ابری ذخیره‌سازی می‌شود. با توجه به این‌که رمزگذاری کلید عمومی برای رمزگذاری داده‌های با حجم بالا دارای پیچیدگی زمانی و محاسباتی زیادی است، لذا اطلاعات PHR توسط الگوریتم رمزنگاری متقارن AES توسط نهاد تولیدکننده داده و به‌وسیله کلید تصادفی k_{sym} رمزگذاری می‌شود و سپس کلید k_{sym} توسط رمزگذاری مبتنی‌بر ویژگی و بر اساس ساختار دسترسی مورد نظر نهاد تولیدکننده داده رمز می‌شود. برای آن که نهادهای استفاده‌کننده از داده بتوانند به اطلاعات پزشکی مورد نیاز دسترسی داشته باشند و از صحت آن‌ها نیز مطمئن باشند، نهاد تولیدکننده محتوای پزشکی کلید رمزگذاری اطلاعات PHR را بر اساس سیاست دسترسی مورد نظر توسط رمزنگاری مبتنی‌بر ویژگی رمز کرده و به همراه مسیر ذخیره‌سازی داده رمزشده در ابر، چکیده محتوای PHR و ساختار دسترسی مجاز به اطلاعات PHR به‌صورت گمنام در یک تراکنش متناسب با ساختار زنجیره‌بلوکی قرار داده و سپس این تراکنش را امضا می‌کند و برای ثبت در یک زنجیره‌بلوکی خصوصی premissioned انتشار می‌دهد، همچنین تراکنش دیگری شامل توضیحی از داده رمزشده و ساختار دسترسی مجاز به آن ایجاد کرده و به‌صورت گمنام در یک زنجیره‌بلوکی خصوصی premissioness منتشر می‌کند تا در اختیار تمامی نهادهای استفاده‌کننده از داده‌های پزشکی قرار گیرد. گره‌های بررسی‌کننده صحت تراکنش‌ها در زنجیره‌بلوکی، هر تراکنش منتشرشده را مورد بررسی قرار داده و تراکنش‌هایی که بتوانند تعداد مشخصی از آرای گره‌های معتمد زنجیره‌بلوکی را کسب کنند سپس توسط گره leader که در فرآیند اجماع تعیین شده است، در زنجیره بلوک زنجیره‌بلوکی خصوصی ثبت می‌شوند.

در این سامانه دو نوع اطلاعات پزشکی داریم، یکی اطلاعات EHR که توسط دستگاه‌ها و حسگرهای مرتبط با بیمار روزانه توسط بیمار تولید می‌شود و دیگری اطلاعات پزشکی است که توسط بیمارستان، آزمایشگاه و یا پزشک معالج تولید می‌شود اما وابسته به یک بیمار مشخص است مانند عکس‌های رادیولوژی، نسخه پزشک، صورت حساب بیمه و غیره. اطلاعات EHR توسط خود بیمار رمزگذاری می‌شود و در ابر ذخیره می‌شود اما داده‌های پزشکی تولیدشده توسط بیمارستان رمزگذاری می‌شود اما کلید رمزگذاری آن بر اساس ساختار دسترسی مورد نظر بیمار رمزگذاری‌شده و به همراه چکیده داده و مسیر ذخیره‌سازی داده در ابر، در زنجیره‌بلوکی خصوصی ذخیره می‌شود. بنابراین، در سامانه SBA-PHR دو موجودیت، قابلیت رمزگذاری داده را دارند، یکی بیمارستان که داده‌های پزشکی مرتبط به بیمار را رمزگذاری می‌کند و دیگری خود بیمار است که داده‌های ثبت‌شده EHR و آن بخشی از داده‌های پزشکی مربوط به خود را که تمایل دارد در اختیار نهادهای دیگر و یا والدین و دوستان خود قرار دهد، رمزگذاری می‌کند.

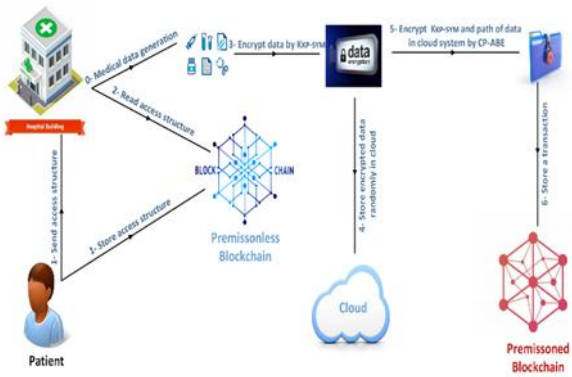
داده‌های رمزشده توسط بیمارستان توسط سامانه رمزگذاری KP-ABE رمزگذاری می‌شود. بنابراین، ساختار دسترسی مجاز برای رمزگشایی داده‌ها در کلید خصوصی تولیدشده توسط نهاد KGC قرار داده شده است و بر اساس این ساختار دسترسی نهادهای مشخصی مجاز به‌دسترسی به این داده‌ها خواهند بود، بیمار اطلاعی از این نهادها ندارد. اما بیمار ویژگی‌های لازم برای نهادی که تمایل به رمزگشایی این داده‌ها را دارد را در یک تراکنش معتبر در زنجیره‌بلوکی ثبت می‌کند و بیمارستان موظف به رعایت این سیاست دسترسی برای رمزگذاری این داده‌ها است، بیمارستان این داده‌ها را با کلید تصادفی k_{kp-sym} رمزگذاری کرده و سپس این کلید را بر اساس ویژگی‌های مشخص‌شده توسط بیمار به کمک رمزنگاری KP-ABE رمزگذاری می‌کند.

سیاست دسترسی مورد نظر بیمار برای رمزگذاری داده با سیاست دسترسی اعمال‌شده توسط بیمارستان بر روی کلید k_{kp-sym} توسط گره‌های زنجیره‌بلوکی مورد بررسی قرار می‌گیرد و در صورت یکسان بودن آن‌ها، مسیر ذخیره‌سازی داده در ابر و چکیده این داده‌ها در زنجیره‌بلوکی خصوصی برای استفاده نهادهای مورد نظر ثبت می‌شود و همزمان یک تراکنش که فقط شامل شرح مختصری از داده و ساختار دسترسی مجاز به آن است در زنجیره‌بلوکی عمومی منتشر می‌شود. فرآیند رمزگذاری داده‌های پزشکی تولیدشده توسط بیمارستان و داده‌های با حجم بالا به‌منظور سهولت و افزایش کارایی سامانه به بیمارستان محول شده است (شکل (۳)).



شکل (۳): نحوه ثبت اطلاعات پزشکی توسط بیمارستان

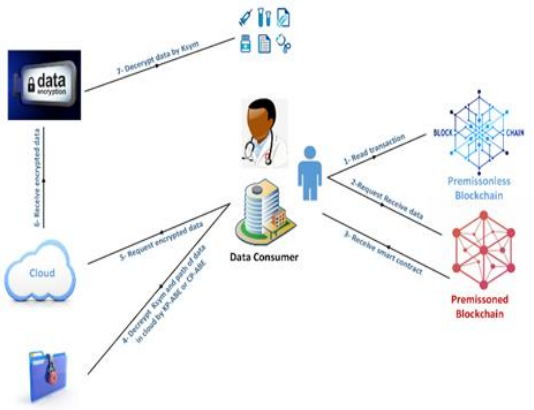
داده‌های EHR و آن بخشی از اطلاعات که بیمار تمایل دارد آن را در اختیار نهادهای خاص، دوستان و یا پزشک مشاور قرار دهد، به‌وسیله رمزنگاری CP-ABE بر اساس ساختار دسترسی مورد نظر خود بیمار به‌صورت دقیق مشخص می‌شود. در این بخش کلیدهای خصوصی توسط خود بیمار تولید شده و در اختیار این افراد و یا نهادها قرار می‌گیرد و سپس هر بخش از اطلاعات توسط کلید تصادفی k_{cp-sym} رمزگذاری‌شده و این کلید بر اساس ساختار دسترسی مورد نظر بیمار رمزگذاری‌شده و به همراه ساختار دسترسی مجاز و چکیده داده‌ها در زنجیره‌بلوکی برای استفاده از نهادهای مجاز ثبت و ذخیره می‌شود (شکل (۴)).



شکل (۴): نحوه ثبت اطلاعات پزشکی توسط بیمار

نهادهایی که تمایل به استفاده از داده‌های پزشکی را دارند علاوه‌بر این‌که باید کلید متناسب با ساختار دسترسی مجاز به آن اطلاعات را داشته باشند تا بتوانند k_{cp-sym} و یا k_{kp-sym} را رمزگشایی کرده و محتوای داده را دریافت کنند، باید بتوانند یک تراکنش معتبر ایجاد کنند که در آن به یک تراکنش استفاده‌نشده از سوی تولیدکننده محتوا اشاره شده باشد. این عمل به این معنی است که نهاد تولیدکننده محتوا حق دسترسی به اطلاعات پزشکی خود را با آن ساختار دسترسی مشخص هنوز ابطال نکرده است. این فرآیند به کمک قراردادهای هوشمند انجام می‌شود.

ورودی این قرارداد هوشمند یک تراکنش مصرف‌نشده از تراکنش‌های زنجیره‌بلوکی premissinless با ساختار دسترسی مشخص که توسط یک موجودیت با کلید عمومی PK تولید شده است و تراکنشی که در آن درخواست دسترسی به این تراکنش ثبت شده است می‌باشد. خروجی این قرارداد هوشمند یک تراکنش معتبر در زنجیره‌بلوکی premissioned است که در آن مسیر ذخیره‌سازی داده در ابر و کلید متقارن k_{sym} به‌صورت رمزشده در آن وجود دارد که قبلاً توسط بیمار یا بیمارستان تولید شده است و در زنجیره‌بلوکی ذخیره شده است. لزوم ارائه یک تراکنش مصرف‌نشده از سوی نهادهای استفاده‌کننده از داده برای دریافت اطلاعات کلید و مکان ذخیره‌سازی داده رمزشده باعث افزایش کارایی و سهولت فرآیند ابطال دسترسی به‌صورت آنی در رمزنگاری مبتنی‌بر ویژگی می‌شود (شکل (۵)).



شکل (۵): نحوه درخواست اطلاعات پزشکی

۳-۱. مدل معماری

در سامانه SBA-PHR شش موجودیت مرکز ثبت‌نام KGC، سامانه ذخیره‌ساز ابری، شبکه زنجیره‌بلوکی، نهادهای استفاده‌کننده از داده، و بیماران وجود دارد:

مرکز ثبت‌نام و تولید کلید (KGC): این مرکز پارامترهای عمومی شبکه را تعیین و منتشر می‌کند. تمامی نهادهای استفاده‌کننده از داده‌های پزشکی مانند بیمارستان‌ها، مؤسسات بیمه، مراکز تحقیقات پزشکی و غیره باید در این مرکز ثبت نام کنند. سپس مرکز KGC با توجه به ویژگی‌های هر نهاد و ساختار دسترسی مجاز برای آن نهاد (Γ_{kp}) کلیدهای خصوصی رمزگشایی متناسب با آن ساختار دسترسی را تولید و به‌صورت امن در اختیار آن‌ها قرار می‌دهد. در واقع KGC مشخص می‌کند هر نهاد به چه پیام‌های رمزی می‌تواند دسترسی داشته باشد. همچنین KGC کلیدهای امضای مراکز تولیدکننده داده را تولید و به‌صورت امن در اختیار آن‌ها قرار می‌دهد.

سامانه ذخیره‌ساز ابری (Cloud Storage): با توجه به حجم زیاد داده‌های پزشکی، باید داده‌ها به‌صورت رمزگذاری‌شده در یک یا چند سامانه ابری ذخیره‌سازی شوند. نهادهای ثبت‌کننده اطلاعات PHR و یا بیماران می‌توانند داده‌ها را به‌صورت رمزگذاری‌شده در مکان‌های تصادفی در سامانه‌های ابری ذخیره‌سازی کنند و سپس مکان این ذخیره‌سازی و کلید آن را در اختیار نهادهای استفاده‌کننده از داده مجاز قرار دهند.

زنجیره‌بلوکی: در سامانه SBA-PHR از دو زنجیره‌بلوکی خصوصی یکی به‌صورت permissionless و دیگری به‌صورت permissioned مبتنی‌بر روش‌های اجماع PBFT استفاده شده است. مسیر ذخیره‌سازی داده‌ها در سامانه ابری، کلید رمزگشایی آن‌ها به‌صورت رمزشده به همراه چکیده داده در تراکنش‌های زنجیره‌بلوکی ذخیره می‌شود. گره‌های مشارکت‌کننده در شبکه زنجیره‌بلوکی به دو دسته validation node (vdN) برای بررسی صحت تراکنش‌های ارسالی به شبکه زنجیره‌بلوکی و bookkeeping node (bkN) برای ثبت تراکنش‌های صحیح در زنجیره‌های زنجیره‌بلوکی تقسیم‌بندی می‌شوند. گره‌های vdN که می‌توانند از سامانه‌های کامپیوتری بیمارستان‌ها و یا مؤسسات بیمه و نهادهای بهداشتی باشند، صحت امضا و ساختار دسترسی ارائه‌شده در تمامی تراکنش‌های منتشرشده در شبکه را بررسی کرده و در صورت معتبر بودن یک تراکنش با اجرای پروتکل اجماع PBFT یک گره را به‌عنوان مسئول ثبت آن تراکنش در زنجیره بلوک زنجیره‌بلوکی انتخاب می‌کنند و گره bkN آن تراکنش را در زنجیره‌بلوکی ذخیره می‌کنند و به اطلاع تمام اعضای شبکه می‌رساند. همچنین گره‌های عضو زنجیره‌بلوکی قادر به اجرای قراردادهای هوشمند جهت بررسی اعتبار ساختار دسترسی نهادها و در اختیار قرار دادن مسیر ذخیره‌سازی داده در ابر و کلید رمزنگاری‌شده آن به نهادهای استفاده‌کننده از داده هستند.

نهادهای تولیدکننده داده (Data Producer): مانند بیماران، بیمارستان‌ها، آزمایشگاه‌ها و سایر نهادهای بهداشتی که داده‌های PHR مربوط به بیماران را تولید می‌کنند.

نهادهای استفاده‌کننده از داده (Data Consumer): نهادهای استفاده‌کننده از داده به دو دسته تقسیم‌بندی می‌شوند. یکی نهادهای قانونی استفاده‌کننده از داده‌های پزشکی مانند بیمارستان‌ها، مؤسسات بیمه، مراکز تحقیقات پزشکی که تمایل دارند از داده‌های پزشکی بیماران جهت پیشبرد منافع خود استفاده کنند. دسته دوم شامل تمام نهادهایی می‌شود که بیمار تمایل دارد تا بخشی از اطلاعات پزشکی خود را به‌صورت داوطلبانه در اختیار آن‌ها قرار دهد مانند دوستان، والدین، پزشک مشاور و غیره.

بیماران: افرادی هستند که اطلاعات پزشکی آن‌ها جمع‌آوری شده و در اختیار نهادهای استفاده‌کننده از داده‌های PHR قرار می‌گیرد

۳-۲. معرفی جزئیات طرح پیشنهادی

در رمزگذاری مبتنی‌بر ویژگی آستانه‌ای، همه ویژگی‌ها در یک سطح از اهمیت قرار دارند و هیچ ویژگی نسبت به دیگری از برتری برخوردار نمی‌باشد. در حالی‌که در عمل برخی از ویژگی‌ها از اهمیت بالاتری نسبت به بقیه ویژگی‌ها برخوردارند. به‌عنوان نمونه تخصص یک پزشک از این‌که این پزشک وابسته به کدام بیمارستان است و یا مشخصات او چیست از اهمیت بالاتری برخوردار است. بنابراین، ما در طرح پیشنهادی SBA-PHR از یک طرح رمزنگاری ویژگی بر پایه سیاست کلید و مبتنی‌بر ویژگی آستانه‌ای سلسله مراتبی[1] برای رمزگذاری داده‌ها توسط نهادهای قانونی مانند بیمارستان‌ها استفاده می‌کنیم [۲۶]. همچنین برای رمزگذاری داده‌ها توسط بیماران از رمزنگاری ویژگی مبتنی‌بر پایه سیاست متن رمز CP_ABE که توسط بسن کارت و همکارانش پیشنهاد شده است استفاده می‌کنیم [۲۷].

طرح پیشنهادی ما دارای ۶ مرحله تعیین ویژگی‌ها و ساختار دسترسی، مرحله راه‌اندازی اولیه سامانه، مرحله رمزگذاری داده‌های PHR، مرحله رمزگشایی و استفاده از داده‌های PHR، مرحله اجماع و بررسی تراکنش‌ها در زنجیره‌بلوکی و مرحله ابطال حق دسترسی می‌باشد.

۳-۲-۱. مرحله تعیین ویژگی‌ها و ساختار دسترسی

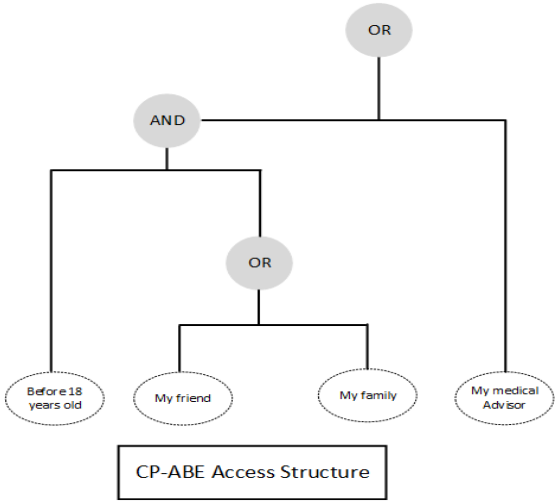
انتخاب مجموعه ویژگی‌ها و ساختار دسترسی مناسب اولین گام برای ایجاد یک سامانه رمزنگاری مبتنی‌بر ABE است. در سامانه پیشنهادی ما مجموعه ویژگی‌ها (U) به دو مجموعه مجزا برای KP-ABE و CP-ABE تقسیم‌بندی می‌شود. برای رمزنگاری KP-ABE ما یک مجموعه ویژگی مبتنی‌بر زمان را با استفاده از ویژگی‌های خاص پزشکی مانند پروفایل پزشکی و پروفایل مشخصات بیمار تعریف می‌کنیم (γ_{kp}). پروفایل پزشکی می‌تواند شامل پزشکان عمومی، جراحان، پرستاران، داروخانه‌ها و پروفایل مشخصات بیمار می‌تواند شامل سن، جنس و شماره شناسایی فرد باشد. برای رمزنگاری CP-ABE ما یک ساختار دسترسی متناسب با ویژگی‌هایی مانند دوستان، خانواده، مشاوران پزشکی، مراکز

1- Hierarchical Threshold Attribute Based Encryption

خدمات درمانی ایجاد می‌کنیم (Γ_{cp}).

فرض کنید Γ درختی باشد که یک ساختار دسترسی را ارائه می‌دهد. هر گره داخلی (گره غیربرگ) درخت یک دریچه آستانه‌ای[1] است که به‌وسیله یک مقدار آستانه‌ای و فرزندان آن توصیف می‌شود. اگر num_x را تعداد فرزندان و k_x را مقدار آستانه گره x در نظر بگیریم، آنگاه داریم $0 < k_x < num_x$. در این‌صورت وقتی $k_x = 1$ دریچه آستانه‌ای OR و وقتی $k_x = num_x$ دریچه آستانه‌ای برابر AND می‌باشد. هر گره برگ x از درخت نیز به‌وسیله یک ویژگی و یک مقدار آستانه‌ای $k_x = 1$ توصیف می‌شود.

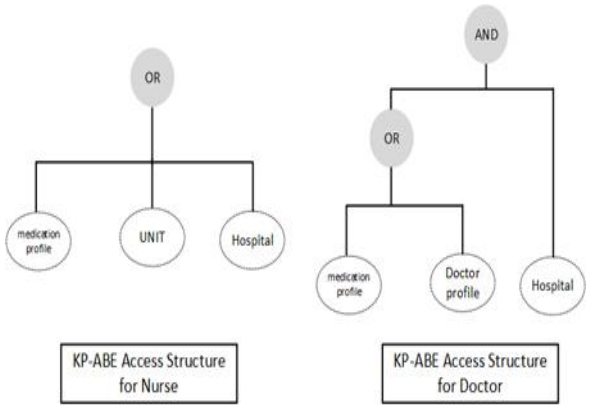
ما با انجام این کار، ویژگی‌ها را به دو دامنه جداگانه تقسیم می‌کنیم، یعنی دامنه عمومی که به خصوصیات ذاتی اطلاعات PHR اشاره دارد و دامنه شخصی که به اطلاعات شخصی شناسایی افراد موجود در سامانه PHR اشاره دارد. برای رمزنگاری KP-ABE هر ساختار دسترسی Γ_{kp} مشخص می‌کند که یک نهاد با ویژگی‌های مشخص می‌تواند به چه اطلاعاتی دسترسی داشته باشد. در شکل (۶) چند نمونه ساختار دسترسی برای نقش‌های مختلف ارائه شده است.



شکل (۶): ساختار دسترسی برای رمزنگاری KP-ABE

در رمزنگاری CP-ABE ساختار دسترسی Γ_{cp} مشخص می‌کند که یک متن رمزشده با برچسب‌های مشخص توسط چه نهادی می‌تواند رمزگشایی شود. به‌عنوان نمونه بیمار می‌تواند برای مشاهده اطلاعات مربوط به فشار خون خود، ساختار دسترسی مانند شکل (۷) ایجاد کند که در آن علاوه‌بر پزشکان بیمارستان چنانچه بیمار زیر سن قانونی است والدین او هم بتوانند این اطلاعات را دریافت کنند.

1- Threshold Gate



شکل (۷): ساختار دسترسی برای رمزنگاری CP-ABE

۳-۲-۲. مرحله راه‌اندازی اولیه سامانه

مرحله راه‌اندازی اولیه دارای دو بخش مجزا است، یک بخش توسط مرکز KGC برای ارتباط بیمارستان‌ها و نهادهای پزشکی مجاز با یکدیگر انجام می‌شود و بخش دیگر توسط هر بیمار برای ارتباط با نهادهای درمانی، پزشکان مشاور و یا افراد دلخواه صورت می‌گیرد.

مرحله راه‌اندازی اولیه سامانه برای KGC: این مرحله شامل دو بخش تعیین پارامترهای عمومی سامانه و تولید کلیدهای اصلی MK_{kp} برای رمزگذاری KP-ABE می‌شود (جریان (0-1) در شکل (۸)).

- تعیین پارامترهای عمومی سامانه:

KGC پارامترهای عمومی سامانه را که شامل تابع چکیده‌ساز، پارامترهای منحنی بیضوی و نگاشت دوخطی می‌شود را تعیین و به اطلاع کل شبکه می‌رساند.

فرض کنید G_1 یک گروه جمعی دوری تولیدشده توسط P و G_2 یک گروه ضربی دوری است. G_1 و G_2 دارای مرتبه عدد اول q هستند. فرض کنید $e : G_1 \times G_1 \rightarrow G_2$ یک زوج‌سازی دوخطی است.

فرض کنید $H_1 : \{0,1\}^* \rightarrow G_1$ یک نگاشت و $H_2 : \{0,1\}^* \rightarrow Z_q^*$ یک تابع چکیده‌ساز امن و $H_3 : G_1 \rightarrow \{0,1\}^*$ است.

- تولید کلیدهای اصلی MK_{kp} برای رمزگذاری KP-ABE:

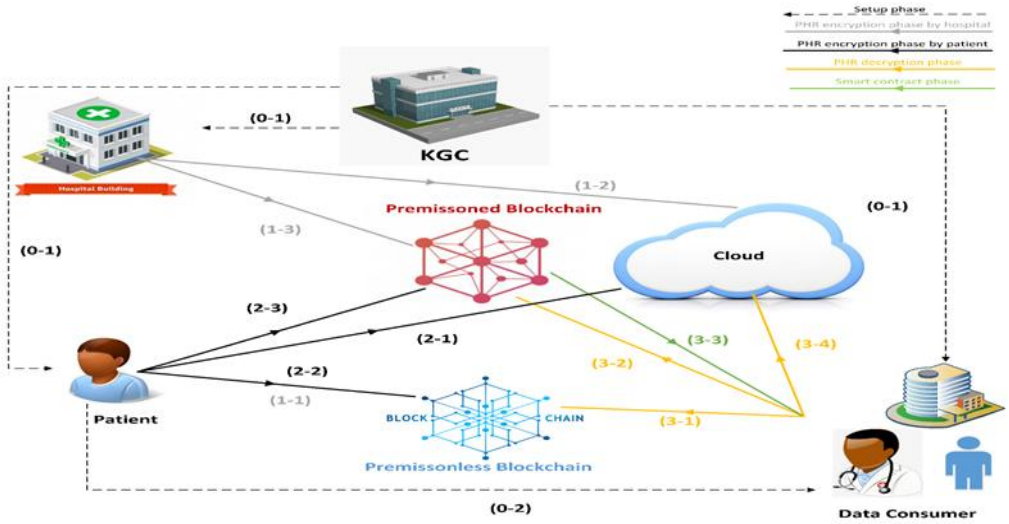
این الگوریتم توسط مرکز تولید کلید KGC و جهت تولید کلیدهای رمزنگاری مناسب برای نهادهای قانونی مانند بیمارستان‌ها اجرا می‌شود.

- KGC مجموعه‌ای از ویژگی‌های U را تعریف می‌کند و تمام

ویژگی‌های سامانه را مطابق با اهمیت آن‌ها به زیر مجموعه-های $u_0, u_1, \dots, u_m$ تقسیم می‌کند.

- دنبالـه‌ای از مقـادیر آسـتانه‌ای $k_0, k_1, \dots, k_m$ را انتخـاب می‌کند.
- اعـداد تصـادفی $t_0, t_1, \dots, t_{|u|}, y \in Z_p$ را بـه‌عنـوان کلیـد مخفی $\mathrm{MK_{kp}}$ انتخاب می‌کند.
- مولـد g را در گـروه G_1 انتخـاب و مقـادیر $T_1 = g^{t_1}, \dots, T_{|u|} = g^{t_{|u|}}, Y = e(g,g)^y$. را محاسـبه می‌کند.
- پارامترهـای عمـومی سـامانه عبـارت‌انـد از: $params: \{G_1, G_2, e, g, k_0, k_1, \dots, k_m, T_0, T_1, \dots, T_{|u|}, Y\}$ که توسط مرکز تولید KGC کلید منتشر می‌شود.
- سپس KGC یک چندجملـه‌ای تصـادفی q از درجـه k_{m-1} به‌طوری که $q(0) = y$ انتخاب می‌کند.
- ویژگی‌های γ_{kp} را به زیرمجموعه‌های $\gamma_0, \gamma_1, \dots, \gamma_m$ طـوری تقسیم می‌کند که به‌ازای تمـام مقـادیر j از 0 تـا m داشـته باشیم $\gamma_j \subset U_j$.
- به‌ازای هر ویژگی i موجود در γ_{kp} که در سطح jام قرار دارد، مقدار $D_i = g^{\frac{q^{(k_{j-1})(i)}}{t_i}}$ را محاسبه مـی‌کنـد. ایـن محاسـبات به‌ازای تمام سطوح یعنی j از 0 تا m انجام می‌شود.
- مولفه‌های کلید خصوصی، $\{D_i\}_{i\in\gamma_{kp}}$ را به‌صورت محرمانه به کاربر با ویژگی‌های γ_{kp} تحویل می‌دهد.

مرحله راه‌اندازی اولیه سامانه برای بیماران: این مرحله نیـز دارای دو بخش تولید کلیدهای اصلی $\mathrm{MK_{Cp}}$ برای رمزگذاری CP-ABE و تولید کلیدهای عمومی و خصوصی به‌منظور امضای تراکنش‌هـا توسط بیمار است. (جریان (2-0) در شکل (۸)).



شکل (۸): معماری طرح پیشنهادی

- تولید کلیدهای اصلی $\mathrm{MK_{Cp}}$ برای رمزگذاری CP-ABE

این الگوریتم توسط بیمار جهت تولید کلیـدهای رمزگشـایی داده برای افراد و یا نهادهایی که بیمار خـود تمایـل دارد تـا اطلاعـات پزشکی خود را در اختیار آن‌ها قرار دهد انجام می‌شود.

- بیمار مجموعه‌ای از ویژگی‌های مورد نظر خـود را بـه‌صـورت $U = \{1, 2, \dots, n\}$، تعریف می‌کند.
- دو عدد تصادفی α و β از $\mathbb{Z}_p$ انتخاب می‌کند.
- پارامترهـای عمـومی PK بیمـار عبـارت‌انـد از: $PK = \{G_0, g, h = g^\beta, f = g^{1/\beta}, e(g,g)^\alpha\}$ که آن‌هـا را منتشـر می‌کند.
- کلید محرمانه $\mathrm{MK_{Cp}}$ بیمار عبارت است از : (β, g^α).
- بیمار به‌وسیله کلید محرمانه $\mathrm{MK_{Cp}}$ یک کلید خصوصی کـه سازگار با مجموعه ویژگی γ_{cp} است را به‌صـورت زیـر تولیـد می‌کند:
  - ابتدا یک عدد تصادفی $r \in \mathbb{Z}_p$ و سپس اعـداد تصـادفی $r_j \in \mathbb{Z}_p$ را برای هر ویژگی j عضو مجموعه γ_{cp} انتخاب می‌کند.
  - سپس کلید متناسب با مجموعه ویژگی γ_{cp} را به‌صـورت زیر محاسبه می‌کند.

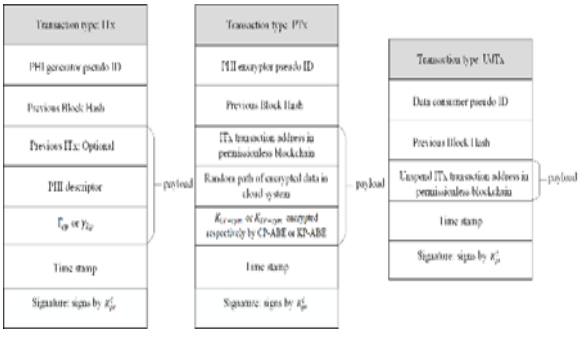
$$SK = (D = g^{(\alpha+r)/\beta}, \forall j \in \gamma_{cp}, D_j = g^r . H_1(j)^{r_j}, D'_j = g^{r_j})$$

- بیمار این مجموعه کلید را به‌صورت امن در اختیار افراد و یـا نهادهای مورد نظر خود قرار می‌دهد.
- تولیـد کلیـدهای عمـومی و خصوصـی بـه‌منظـور امضـای تراکنش‌ها.

کاربر کلیدهای عمومی و خصوصی مخصوص به خود را برای امضای تراکنش‌های مورد نظر تولید می‌کند. اگر کاربر تمامی تراکنش‌های ارسالی به شبکه را با یک کلید خصوصی امضا کند گمنامی کاربر در شبکه مورد تهدید واقع می‌شود. بنابراین، کاربر بر اساس سطح گمنامی مورد نظر خود هر تراکنش و یا دسته‌ای از تراکنش‌ها را باید با یک کلید خصوصی جدید امضا کند. تولید تعداد زیادی از کلیدهای خصوصی و عمومی کار دشواری است و نگهداری از آن‌ها برای کاربر پرهزینه خواهد بود. بنابراین، در طرح پیشنهادی ما از ویژگی تولید کلیدهای سلسله مراتبی[1] برای تولید کلیدهای امضا استفاده می‌شود، یعنی کاربر تنها یک بذر اولیه کلید تولید می‌کند و سپس سایر کلیدهای خصوصی و عمومی مورد نیاز خود را بر مبنای آن بذر اولیه تولید می‌کند. لذا کاربر باید تنها یک بذر را به‌صورت امن ذخیره کند که این موجب افزایش امنیت نگهداری از کلید خصوصی کاربر می‌شود.

- کاربر دو مقدار تصادفی $k, x \in_R Z_q^*$ را انتخاب می‌کند و سپس x را به‌عنوان بذر کلید خصوصی خود به‌صورت امن ذخیره‌سازی می‌کند.
- کاربر هر زمان که نیاز باشد تا تراکنشی را امضا کند iامین کلید خصوصی خود را به‌صورت $\mathrm{K}_{pr}^{i} = x + H_2(k||i)$ محاسبه می‌کند. سپس کلید عمومی متناظر با آن را به‌صورت $K_{pub}^{i} = \mathrm{K}_{pr}^{i} G_1 = xG_1 + H_2(k||i)G_1$ محاسبه می‌کند.
- $H_3(K_{pub}^{i})$ به‌عنوان شناسه مستعار کاربر در آن تراکنش محسوب می‌شود.

با توجه به خاصیت شبه‌تصادفی بودن توابع چکیده‌ساز با داشتن چندین کلید عمومی مختلف امکان برقراری ارتباط بین آن‌ها وجود ندارد و نمی‌توان تشخیص داد که بذر تولیدکننده آن‌ها یکسان است یا متفاوت. بنابراین، ویژگی پیوندناپذیری در ارتباطات کاربران به خوبی حفظ شده و گمنامی کاربران تضمین می‌شود (شکل (۹)).



شکل (۹): تولید کلیدهای سلسله مراتبی امضا

1- Hierarchical key generation

۳-۲-۳. مرحله رمزگذاری داده‌های PHR

دو نوع داده برای رمزگذاری در مدل پیشنهادی ما وجود دارد؛ یکی داده‌های پزشکی تولیدشده توسط بیمارستان که وابسته به یک بیمار است، اما توسط بیمارستان رمزگذاری می‌شود و دیگری داده‌های EHR[2] و یا داده‌هایی که بیمار خود تمایل دارد در اختیار افراد و یا نهادهای دیگری قرار دهد. نهاد تولیدکننده داده پزشکی پس از رمزگذاری داده‌ها یک تراکنش در زنجیره‌بلوکی premissinless که در آن شرح مختصری از داده تولیدشده و شرایط دسترسی به آن وجود دارد را ثبت می‌کند، سپس یک تراکنش دیگر که شامل مسیر ذخیره‌سازی داده‌ها و کلید رمزگذاری‌شده k_{sym} است در زنجیره‌بلوکی permissioned ثبت می‌کند. همچنین نهادهای استفاده‌کننده از داده برای دسترسی به مسیر ذخیره‌سازی داده‌ها و کلید رمزگذاری آن‌ها باید یک تراکنش در زنجیره‌بلوکی premissined برای راه‌اندازی قرارداد هوشمند ثبت کنند. در ادامه ساختار این تراکنش‌ها شرح داده شده است.

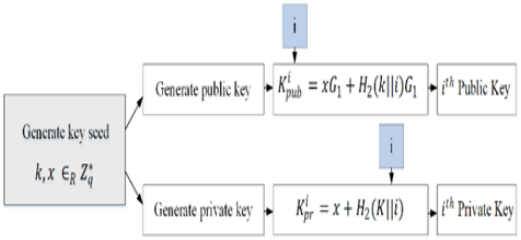
- انواع تراکنش‌های سامانه SBA-PHR

Information Transaction(ITx): این تراکنش توسط بیماران جهت اطلاع‌رسانی از محتوای داده‌های پزشکی در زنجیره‌بلوکی permissionless ثبت می‌شود که شامل شرح مختصری از داده‌های پزشکی ثبت‌شده، ساختار دسترسی مورد نظر برای دسترسی به این داده‌ها، شناسه مستعار تولیدکننده محتوای پزشکی و امضای او بر روی کل اطلاعات تراکنش است.

Permission Transaction (PTx): این تراکنش توسط بیمارستان و یا بیمار به‌منظور ارسال داده‌های پزشکی رمزگذاری‌شده و حق دسترسی مجاز کاربران در زنجیره‌بلوکی permissioned ثبت می‌شود. این تراکنش شامل مسیر تصادفی ذخیره‌سازی داده‌های رمزشده در ابر، کلید رمزنگاری متقارن داده‌ها که توسط رمزنگاری ABE رمز شده است و امضای تولیدکننده تراکنش بر روی این محتوا است.

Used Data Transaction (UdTx): این تراکنش توسط نهاده‌های استفاده‌کننده از داده‌های پزشکی به‌منظور دست‌یابی به اطلاعات پزشکی رمزشده در ابر در زنجیره‌بلوکی permissioned ثبت می‌شود. این تراکنش شامل شناسه مستعار نهاد استفاده‌کننده از داده‌ی پزشکی، امضای درخواست‌کننده اطلاعات پزشکی و آدرس تراکنشی در زنجیره‌بلوکی permissionless است که کاربر درخواست دسترسی به محتوای آن را دارد، می‌باشد. در شکل (۱۰) ساختار این تراکنش‌ها نشان داده شده است.

2- Electronic Health Record



شکل (۱۰): ساختار تراکنش‌ها

- رمزگذاری داده‌ها توسط بیمارستان:

بیمارستان داده‌های پزشکی مربوط به بیماران خود را برای دسترسی سایر نهادهای قانونی بر اساس ویژگی‌های اعلام شده توسط بیمار و بر اساس روش KP_ABE رمزگذاری می‌کند، که شامل مراحل زیر است.

- بیمار ویژگی‌های لازم برای رمزگشایی داده‌های PHR مربوط به خود را که در اختیار بیمارستان است را از مجموعه U مشخص می‌کند.(γ_{kp}).
- بیمار به‌منظور امضای تراکنش‌ها، یک زوج کلید عمومی و خصوصی مناسب بر اساس روش بیان‌شده در بخش ۴-۳-۲ تولید می‌کند (K_{pr}^{i} , K_{pk}^{i}).
- بیمار یک تراکنش ITx که شامل ویژگی‌های لازم برای رمزگذاری داده‌ها (γ_{kp}) و شرح مختصری از داده است تولید کرده و با کلید خصوصی K_{pr}^{i} این تراکنش را امضا می‌کند.
- بیمار این تراکنش ITx را در زنجیره‌بلوکی permissionless ذخیره می‌کند. (جریان (1-1) در شکل (۸)).
- بیمارستان یک کلید تصادفی K_{kp-sym} را برای رمزنگاری داده‌ها تولید کرده و داده‌های مربوط به بیمار p_i را به‌وسیله الگوریتم AES با آن رمز می‌کند.
- بیمارستان کلید K_{kp-sym} را بر اساس ویژگی (γ_{kp}) که توسط بیمار در تراکنش ITx در زنجیره‌بلوکی permissionless ثبت شده است، به کمک روش رمزنگاری KP_ABE رمزگذاری می‌کند.

- امضای تراکنش‌ها:

در طرح SBA-PHR برای امضای تراکنش‌های ثبت‌شده در زنجیره‌بلوکی از امضای دیجیتال ECDSA بر روی منحنی بیضوی استاندارد "secp256k1" استفاده می‌کنیم. طول کلید خصوصی K_{pr}^{i} در این امضا ۲۵۶ بیت و طول کلید عمومی K_{pub}^{i} برابر ۵۱۲ بیت است که با استفاده از روش فشرده‌سازی در ذخیره‌سازی نقاط منحنی بیضوی طول آن برابر ۲۵۷ بیت خواهد شد. همچنین طول خروجی امضا برابر ۵۱۲ بیت می‌باشد.

- رمزگذای کلید K_{cp-sym} به روش KP_ABE:

بیمارستان برای رمزگذاری کلید K_{kp-sym} تحت مجموعه ویژگی‌های γ_{kp} که از طرف بیمار مشخص شده است به روش زیر عمل می‌کند.

- مقدار تصادفی $s \in_R Z_p$ را انتخاب می‌کند.
- مقادیر $E_i = T_i^s$ و $E' = K_{kp-sym}Y^s$ را به‌ازای همه ویژگی‌های موجود در γ_{kp} محاسبه می‌کند.
- سپس کلید K_{kp-sym} توسط بیمارستان به‌صورت $E_{kp} = \left(\gamma_{kp}, E' = K_{kp-sym}Y^s, \{E_i = T_i^s\}_{i\in\gamma_{kp}}\right)$ رمز می‌شود.
- بیمارستان داده پزشکی بیمار را که توسط کلید K_{kp-sym} رمز شده را در مکان‌های تصادفی در سامانه ذخیره‌ساز ابری ذخیره می‌کند. (جریان (2-1) در شکل (۸)).
- بیمارستان یک تراکنش PTx شامل E_{kp} و محل ذخیره‌سازی داده‌ها در ابر تولید کرده و در زنجیره‌بلوکی خصوصی ذخیره می‌کند. (جریان (3-1) در شکل (۸)).

گره‌های vdN موجود در زنجیره‌بلوکی خصوصی این تراکنش PTx را بررسی می‌کنند و در صورتی که ویژگی استفاده‌شده در رمزگذاری K_{kp-sym} با ویژگی اعلام‌شده در تراکنش ITx متناظر آن در زنجیره‌بلوکی عمومی که از طرف بیمار ثبت شده است یکسان باشد، آنگاه این تراکنش به‌عنوان یک تراکنش معتبر در بلوک‌های زنجیره‌بلوکی خصوصی ثبت می‌شود.

- رمزگذاری داده توسط بیمار:

هر بیمار بر اساس سیاست‌های دسترسی مورد نظر خود می‌تواند تمام و یا بخشی از اطلاعات پزشکی خود را در اختیار افراد و یا نهادهای دیگر قرار دهد، برای این منظور بیمار از رمزنگاری CP_ABE استفاده می‌کند که مراحل انجام آن به شرح زیر است.

- بیمار برای رمزگذاری داده‌های EHR و یا آن اطلاعاتی که تمایل دارد در اختیار نهادهای دیگر قرار دهد، یک کلید تصادفی K_{cp-sym} تولید می‌کند.
- داده‌های مورد نظر خود را به‌وسیله کلید K_{cp-sym} و الگوریتم AES رمزگذاری می‌کند.
- داده‌های رمزگذاری‌شده را در مکان‌های تصادفی در ابر ذخیره می‌کند. (جریان (1-2) در شکل (۸)).
- بیمار ساختار دسترسی (Γ_{cp}) را بر اساس این‌که این اطلاعات برای چه نهادها و یا افرادی و با چه ویژگی‌هایی قابل استفاده باشد تعیین می‌کند.
- سپس بیمار کلید K_{cp-sym} را براساس ساختار دسترسی مورد نظر (Γ_{cp}) توسط رمزگذاری CP-ABE رمزگذاری می‌کند.

- رمزگذای کلید K_{cp-sym} به روش CP_ABE:

بیمار برای رمزگذاری کلید K_{cp-sym} بر اساس ساختار دسترسی (Γ_{cp}) به روش زیر عمل می‌کند.

- در ابتدا برای هر گره x (شامل برگ‌ها) در ساختار دسترسی (Γ_{cp}) یک چندجمله‌ای تصادفی q_x از درجه $d_x = k_x - 1$ انتخاب می‌کند. این چندجمله‌ای‌ها را به روش بالا به پایین یعنی با شروع از گره ریشه R به روش زیر انتخاب می‌کند.
  - برای چندجمله‌ای گره ریشه R، ابتدا یک عدد تصادفی $s \in Z_p$ انتخاب می‌کند و $q_R(0) = y$ قرار می‌دهد و d_R نقطه دیگر از این چندجمله‌ای را به‌طور کاملاً تصادفی انتخاب می‌کند.
  - برای گره‌های دیگر x، $q_x(0) = q_{parent(x)}(index(x))$ قرار می‌دهد و d_x نقطه دیگر از چندجمله‌ای را به‌طور تصادفی انتخاب می‌کند.
- اگر Y مجموعه گره‌های برگ در ساختار دسترسی (Γ_{cp}) باشد آنگاه متن رمز $K_{cp-sym} \in G_1$ تحت ساختار دسترسی (Γ_{cp}) به‌صورت زیر محاسبه خواهد شد.

$E_{cp} = \left(\Gamma_{cp}, \tilde{C} = K_{cp-sym} e(g,g)^{\alpha s}, C = h^s, \forall y \in Y: C_y = g^{q_y(0)}, C'_y = H_1\left(att(y)\right)^{q_y(0)}\right)$.

- بیمار به‌منظور امضای تراکنش‌ها، یک زوج کلید عمومی و خصوصی مناسب بر اساس روش بیان‌شده در بخش ۴-۳-۲ تولید می‌کند (K_{pr}^i, K_{pk}^i).
- سپس بیمار یک تراکنش ITx شامل ساختار دسترسی مجاز (Γ_{cp}) و شرح مختصری از داده ذخیره‌شده تولید کرده و توسط کلید خصوصی K_{pr}^i آن را امضا می‌کند و این تراکنش را در زنجیره‌بلوکی permissionless ثبت می‌کند. (جریان (2-2) در شکل (۸)).
- همچنین بیمار یک تراکنش PTx شامل مسیر ذخیره‌سازی داده در ابر و کلید رمزشده K_{cp-sym} توسط رمزگذاری CP-ABE تولید کرده و توسط همان کلید خصوصی K_{pr}^i آن را امضا کرده و در زنجیره‌بلوکی premissioned ثبت می‌کند (جریان (3-2) در شکل (۸)).
- گره‌های موجود در زنجیره‌بلوکی premissioned این تراکنش PTx را بررسی می‌کنند و در صورتی که ویژگی استفاده‌شده در رمزگذاری K_{cp-sym} با ویژگی اعلام‌شده در تراکنش ITx متناظر آن در زنجیره‌بلوکی permissionless که از طرف بیمار ثبت شده است یکسان باشد، آنگاه این تراکنش به‌عنوان یک تراکنش معتبر در بلوک‌های زنجیره‌بلوکی premissioned ثبت می‌شود.

۳-۲-۴. مرحله رمزگشایی و استفاده از داده‌های PHR

نهادهایی که تمایل به استفاده از داده‌های پزشکی را دارند با مشاهده‌ی تراکنش‌های ثبت‌شده در زنجیره‌بلوکی permissionless، اگر ویژگی‌های لازم برای دریافت آن اطلاعات را بر اساس ساختار دسترسی مجاز ثبت‌شده در تراکنش ITx متناظر آن داشته باشند، آنگاه فرآیند زیر را انجام می‌دهند. (جریان (1-3) در شکل (۸)).

نهاد استفاده‌کننده از داده یک تراکنش UdTx در زنجیره‌بلوکی premissioned ثبت می‌کنند که در آن درخواست استفاده از داده پزشکی مشخصی را دارد (جریان (2-3) در شکل (۸)).

- سپس یک قرارداد هوشمند را اجرا می‌کند که ورودی آن دو تراکنش است، یکی تراکنش UdTx ثبت‌شده توسط آن نهاد برای استفاده از داده‌های پزشکی و تراکنشی دیگری که در آن شرح کلی داده و ساختار دسترسی آن در زنجیره‌بلوکی permissionless آمده است (تراکنش ITx). (جریان (3-3) در شکل (۸)). این قرارداد هوشمند توسط گره‌های زنجیره‌بلوکی premissioned به اجرا در می‌آید.
- با اجرای قراداد هوشمند، گره‌های vdN موجود در فرآیند اجماع زنجیره‌بلوکی premissioned بررسی می‌کنند، که اگر تراکنش ITx اشاره‌شده در زنجیره‌بلوکی permissionless مصرف نشده باشد آنگاه خروجی این قرارداد هوشمند معتبر است و تراکنش PTx متناظر با تراکنش ITx ثبت‌شده در زنجیره‌بلوکی permissionless توسط گره bkN تحویل نهاد درخواست‌کننده می‌شود. تراکنش PTx شامل مسیر ذخیرسازی داده و کلید رمزشده آن با ویژگی‌های متناسب با نهاد درخواست‌کننده داده است.
- سپس نهاد استفاده‌کننده از داده بر اساس مسیر مشخص‌شده در تراکنش PTx حاصل از قرارداد هوشمند، داده‌های رمزگذاری را، از ابر بارگذاری می‌کند و کلید رمزگشایی آن داده‌ها را با استفاده از رمزنگاری KP-ABE و یا CP-ABE رمزگشایی می‌کند و به محتوای داده دسترسی پیدا می‌کند (جریان (4-3) در شکل (۸)).
  - رمزگشایی کلید K_{kp-sym} به روش KP_ABE:

دریافت‌کننده اطلاعات با ویژگی‌های γ_{kp}' متن رمزشده E_{kp} را که تحت ویژگی‌های γ_{kp} رمز شده است را توسط کلید خود به روش زیر رمزگشایی می‌کند.

- ویژگی‌های γ_{kp}' و γ_{kp} را به سطوح 0 تا m به‌صورت $\{\gamma_i\}_{i=0}^m$ و $\{\gamma_i'\}_{i=0}^m$ تجزیه می‌کند.

- به شرطی که رابطه $\left|\mathrm{U}_{j=0}^{i}\gamma_i \cap \mathrm{U}_{j=0}^{i}\gamma_i'\right| \geq k_i$ به‌ازای تمام مقادیر i از 0 تا m برقرار باشد. k_m تا از ویژگی‌های γ_i' را به‌عنوان γ_i'' طوری انتخاب می‌کند تا رابطه $\left|\mathrm{U}_{j=0}^{i}\gamma_i \cap \mathrm{U}_{j=0}^{i}\gamma_i''\right| \geq k_i$ به‌ازای تمام مقادیر $i = 0, \dots, m$ برقرار باشد.
- سپس با استفاده از این k_m تا ویژگی و مولفه‌های کلید خصوصی مربوط به آن‌ها ماتریس A معرفی‌شده در بخش ۳-۴ را تکمیل کرده و محاسبات زیر را انجام می‌دهد.

$$E'/\left(\prod_{i\in ID''}\left(e(D_i,E_i)\right)^{(-1)^{i_r}.\left|A_{i_r}\left(E_{kp},X,\varphi_0\right)\right|}\right)^{\left|A\left(E_{kp},X,\varphi\right)\right|^{-1}} \quad (1)$$

که i_r شماره سطر مربوط به ویژگی i در ماتریس A را بیان می‌کند.

- اثبات درستی رمزگشایی: رابطه رمزگشایی ۶ صحیح می‌باشد، زیرا که اگر کاربری با داشتن مجموعه ویژگی‌های γ_{kp} همه شرایط آستانه‌ای را برآورده کند، بنا به تعریف ویژگی‌های γ_{kp}' نیز همین خاصیت را نیز خواهد داشت و رمزگشایی به طریق زیر ممکن می‌شود.

$$E'/\left(\prod_{i\in ID''}\left(e(D_i,E_i)\right)^{(-1)^{i_r}.\left|A_{i_r}\left(E_{kp},X,\varphi_0\right)\right|}\right)^{\left|A\left(E_{kp},X,\varphi\right)\right|^{-1}}$$
$$= K_{kp-sym}e\,(g,g)^{sy}\Big/\left(\prod_{i\in\gamma_i''}\left(e(g^{\frac{g^{(k_{j-1})(i)}}{t_i}},g^{st_i})\right)^{(-1)^{i_r}.\left|A_{i_r}\left(E_{kp},X,\varphi_0\right)\right|}\right)^{\left|A\left(E_{kp},X,\varphi\right)\right|^{-1}}$$
$$= K_{kp-sym}e\,(g,g)^{sy}\Big/\left(\prod_{i\in\gamma_i''}\left(e(g,g)^{sq^{(K_{j-1})}{}_i}\right)^{(-1)^{i_r}.\left|A_{i_r}\left(E_{kp},X,\varphi_0\right)\right|}\right)^{\left|A\left(E_{kp},X,\varphi\right)\right|^{-1}}$$
$$= K_{kp-sym}e\,(g,g)^{sy}/e(g,g)^{s.\left(\sum_{i\in\gamma_i''}\frac{(-1)^{i_r}.q^{(K_{j-1})}(i)\left|A_{i_r}\left(E_{kp},X,\varphi_0\right)\right|}{\left|A\left(E_{kp},X,\varphi\right)\right|}\right)}$$
$$= K_{kp-sym}e(g,g)^{sy}/e(g,g)^{sy} = K_{kp-sym}$$

- رمزگشایی کلید K_{cp-sym} به روش CP_ABE:

دریافت‌کننده اطلاعات با دریافت ورودی‌های متن رمزی E_{cp} که شامل یک ساختار دسترسی (Γ_{cp}) است، کلید خصوصی $\mathrm{MK_{Cp}}$ که کلیدی برای مجموعه ویژگی‌های γ_{cp} است و پارامترهای عمومی سامانه PK به‌صورت زیر عمل رمزگشایی را انجام می‌دهد.

تابع رمزگشایی متن رمز $E_{cp} = (\Gamma_{cp}, \tilde{C}, C, \forall y \in Y: C_y, C_y')$، کلید خصوصی $\mathrm{MK_{Cp}}$ که وابسته به مجموعه ویژگی γ_{cp} می‌باشد و گره x از ساختار Γ_{cp} را به‌عنوان ورودی می‌پذیرد. این تابع را به‌ازای xای متفاوت که $i = att(x)$ است، به‌صورت زیر تعریف می‌کنیم. اگر x گره برگ باشد و $i \in \gamma_{cp}$ آنگاه مقدار تابع به‌صورت زیر محاسبه می‌شود [۲۸]:

$$DecryptNode\left(E_{cp}, \mathrm{MK_{Cp}}, x\right) = \frac{e(D_i,C_x)}{e(D_i',C_x')} = \frac{e(g^r.H_1(i)^{ri},g^{q_x(0)})}{e(g^{ri},H_1(i)^{q_x(0)})} = e(g,g)^{rq_x(0)}$$

- و اگر $i \notin \gamma_{cp}$ آنگاه $DecryptNode\left(E_{cp}, \mathrm{MK_{Cp}}, x\right) = \perp$
- و اگر x یک گره داخلی باشد، ابتدا تابع $DecryptNode\left(E_{cp}, \mathrm{MK_{Cp}}, z\right)$ را به‌ازای همه گره‌های z که فرزندان x هستند محاسبه و به‌عنوان F_z ذخیره می‌شود. سپس به‌طور دلخواه K_x تا از گره‌های فرزند z، که $F_z \neq \perp$ را در مجموعه S_x قرار می‌دهد. اگر چنین مجموعه‌ای وجود نداشته باشد تابع مقدار $\perp$ را برمی‌گرداند، در غیر این‌صورت محاسبات زیر را انجام می‌دهد که در آن $i = index(z)$ و $S_x' = \{index(z): z \in S_x\}$

$$F_x = \prod_{z\in S_x} F_z^{\Delta_{i,S_x'}(0)} = \prod_{z\in S_x}\left(e(g,g)^{r.q_z(0)}\right)^{\Delta_{i,S_x'}(0)}$$
$$= \prod_{z\in S_x}\left(e(g,g)^{r.q_{parent(z)}(index(z))}\right)^{\Delta_{i,S_x'}(0)}$$
$$= \prod_{z\in S_x} e(g,g)^{r.q_x(i).\Delta_{i,S_x'}(0)} = e(g,g)^{r.q_x(0)}.$$

- حال که تابع DecryptNode را تعریف کرده‌ایم، می‌توان تصور کرد که الگوریتم رمزگشایی تابع $DecryptNode\left(E_{cp}, \mathrm{MK_{Cp}}, R\right)$ را فراخوانی می‌کند. حال اگر ساختار دسترسی Γ_{cp} به‌وسیله ویژگی‌های مجموعه γ_{cp} برآورده شود مقدار تابع برابر است با:

$$DecryptNode\left(E_{cp}, \mathrm{MK_{Cp}}, R\right) = e(g,g)^{rqR(0)} = e(g,g)^{rs}. \quad (3)$$

که در این صورت می‌توان به راحتی با محاسبات زیر به متن اصلی دسترسی پیدا کرد.

$$\tilde{C}/(e(C,D)/A) = \tilde{C}/(e(h^s, g^{\alpha+r/\beta}/e(g,g)^{rs}) = K_{cp-sym}$$

۳-۲-۵. مرحله اجماع و بررسی تراکنش‌ها در زنجیره‌بلوکی

مکانیزم اجماع هسته اصلی فناوری زنجیره‌بلوکی محسوب می‌شود زیرا تعیین می‌کند که آیا بلوک جدید اعتبار دارد و آیا رکوردهای شبکه را حفظ می‌کند. بنابراین، فرآیند اجماع زنجیره‌بلوکی بر امنیت و قابلیت اطمینان کل سامانه تاثیر می‌گذارد. هر دو نوع زنجیره‌بلوکی استفاده‌شده در سامانه SBA-PHR از نوع زنجیره‌بلوکی خصوصی است و نوع دسترسی به آن‌ها یکی به‌صورت permissioned و دیگری به‌صورت permissionless است. روش اجماع استفاده‌شده در هر دو زنجیره‌بلوکی مبتنی‌بر روش‌های اجماع PBFT است. گره‌های عضو هر یک از زنجیره‌بلوکی‌ها که می‌تواند از رایانه‌های مختلف بیمارستان، بیماران و یا نهادهای پزشکی مختلف باشند، در هر بازه با اجرای پروتکل اجماع مبتنی‌بر BPFT یک گره را برای ثبت بلوک نهایی در شبکه انتخاب می‌کنند. این گره موظف به ثبت تراکنش‌های تاییدشده توسط اکثر گره‌های شبکه در بلوک نهایی

زنجیره‌بلوکی است. همه گره‌های شبکه زنجیره‌بلوکی تمامی تراکنش‌های ثبت‌شده در شبکه را بررسی می‌کنند و امضای این تراکنش‌ها را مورد بررسی قرار می‌دهند. بنابراین، اگر بیش از ۲/۳ همه شرکت کنندگان در فرآیند اجماع بلوک‌های تکرارشده در شبکه را تایید کنند، آن بلوک‌ها در شبکه اعتبار پیدا می‌کنند.

یک تراکنش صحیح در زنجیره‌بلوکی خصوصی permissionless تراکنشی است که صرفاً امضای آن معتبر باشد و ارجاع درستی به چکیده بلوک قبلی شبکه داده باشد. بنابراین، گره‌های عضو زنجیره‌بلوکی صرفاً اعتبار یک تراکنش را با بررسی صحت امضای آن و بررسی اعتبار چکیده بلوک قبلی شبکه مورد بررسی قرار می‌دهند.

یک تراکنش صحیح در زنجیره‌بلوکی خصوصی permissioned علاوه‌بر صحت امضای تولیدکننده آن و اعتبار چکیده بلوک قبلی شبکه باید حاوی یک تراکنش مصرف‌نشده در زنجیره‌بلوکی خصوصی permissionless نیز باشد و رمزگذاری محتوای تراکنش منطبق بر ساختار دسترسی اشاره‌شده در آن تراکنش انجام شده باشد. بنابراین، گره‌های vdN عضو زنجیره‌بلوکی permissioned علاوه‌بر بررسی صحت امضای تراکنش‌های ثبت‌شده در این زنجیره‌بلوکی، معتبر بودن تراکنش اشاره‌شده از زنجیره‌بلوکی permissionless و تطبیق ساختار دسترسی آن را در رمزنگاری محتوای تراکنش ثبت‌شده در زنجیره‌بلوکی permissioned را نیز بررسی می‌کنند. چنانچه این بررسی موفقیت‌آمیز باشد قرارداد هوشمند خروجی معتبری تولید خواهد کرد که توسط گره bkN در اختیار نهاد درخواست‌کننده قرار می‌گیرد

۳-۲-۶. مرحله به‌روزرسانی و ابطال حق دسترسی

تغییر ساختار دسترسی و یا حذف ویژگی‌های داده‌شده به یک کاربر در رمزگذاری مبتنی‌بر ویژگی با چالش‌های زیادی روبه‌رو است و به سهولت و با سرعت امکان‌پذیر نیست. اما در سامانه SBA-PHR برای آن که کاربر بتواند ساختار دسترسی که برای رمزگذاری داده‌های مشخصی ایجاد کرده است را باطل کند و یا به دلایلی آن‌ها را تغییر دهد، کافی است تراکنشی را که در آن ساختار دسترسی را برای داده‌های مشخصی در زنجیره‌بلوکی عمومی قبلاً ثبت کرده است را مصرف کند.

مصرف یک تراکنش به این صورت است که منبع تولیدکننده داده (در اینجا می‌تواند بیمار و یا بیمارستان تلقی شود) یک تراکنش جدید با کلید خصوصی امضای همان تراکنش قبلی که در آن ساختار دسترسی مجاز را تعیین کرده است، ایجاد می‌کند و در این تراکنش جدید به تراکنش قبل اشاره می‌کند. گره‌های بررسی‌کننده زنجیره‌بلوکی به راحتی با بررسی ساختار درخت مرکل می‌توانند از استفاده شدن یک تراکنش در داخل یک تراکنش دیگر مطلع شوند. بنابراین، اگر چنین باشد یعنی آن تراکنش توسط تولیدکننده آن باطل شده است و دیگر اعتباری ندارد. بنابراین، خروجی قرارداد هوشمند شکست می‌خورد و در نتیجه تراکنشی که در آن مسیر ذخیره‌سازی داده و کلید رمزگذاری‌شده آن قرار دارد به کاربر تحویل داده نمی‌شود. در این صورت کاربر علاوه‌بر داشتن ساختار دسترسی مجاز در رمزنگاری ABE به علت تغییر سیاست نهاد تولیدکننده داده نمی‌تواند به داده دسترسی پیدا کند. بنابراین، ما با استفاده از فناوری زنجیره‌بلوکی و استفاده از مفهوم تراکنش‌های مصرف‌شده روند ابطال و به‌روزرسانی حق دسترسی در رمزنگاری ABE به‌کار رفته در طرح SBA-PHR را بهبود بخشیدیم.

۴. تحلیل امنیتی طرح پیشنهادی

در این بخش، بررسی می‌شود که چگونه طرح پیشنهادی SBA-PHR می‌تواند به‌طور موثر با اهداف طراحی‌شده در "مدل معماری" مطابقت داشته باشد. برای این منظور ما امنیت طرح‌های رمزنگاری CP-ABE و KP-ABE استفاده‌شده در این معماری را به‌صورت فرمال اثبات کرده و نشان می‌دهیم این طرح‌ها در مدل اوراکل تصادفی دارای امنیت قابل اثبات هستند. همچنین عملکرد صحیح پروتکل را در منطق BAN به اثبات رسانده و نشان می‌دهیم پروتکل به درستی به اهداف امنیتی خود دست پیدا می‌کند.

۴-۱. تحلیل امنیتی طرح رمزنگاری KP_ABE

قضیه: با فرض سختی حل مسئله DMBDH در زمان چندجمله‌ای طرح رمزنگاری KP_ABE در مدل شناسه منتخب امن است.

برهان: فرض کنید A مهاجمی باشد که در بازی ارائه‌شده برای طرح رمزنگاری KP-ABE با احتمال ε پیروز می‌شود. آنگاه با به‌کار بردن مهاجم A چالشگر C را طوری طراحی می‌کنیم که مسئله DMBDH را با احتمال $\varepsilon/2$ حل کند.

فرض کنید چالشگر C یک نمونه تصادفی $(g, A = g^a, B = g^b, C = g^c, Z) \in G_1 \times G_2$ از مسئله سخت DMBDH را دریافت کرده است [۲۹-۳۰]. در ادامه نشان خواهیم داد که چالشگر C چگونه با استفاده از مهاجم A در طول بازی می‌تواند جواب مسئله DMBDH را به‌دست آورد. مدل‌سازی بازی ارائه شده به‌صورت زیر است.

آماده‌سازی: C پارامتر Y را برابر $Y = e(g,g)^a$ قرار می‌دهد و برای هر ویژگی i در سامانه مقادیر T_i را به‌صورت زیر مقداردهی می‌کند.

- اگر $i \in \alpha$ باشد، یک عدد تصادفی $\beta_i \in Z_p$ انتخاب می‌کند

و T_i را برابر $C^{\beta_i} = g^{c\beta_i}$ قرار می‌دهد.
- در غیراین‌صورت یک عدد تصادفی $\omega_i \in Z_p$ انتخاب می‌کند و T_i را برابر g^{ω_i} قرار می‌دهد.
- سپس پارامترهای عمومی را به A تحویل می‌دهد.

فاز ۱: در این مرحله A می‌تواند کلید خصوصی برای ویژگی‌های متعدد γ_{kp}' را به شرطی که اشتراک آن‌ها با γ_{kp} حداقل در یکی از شروط آستانه‌ای صدق نکند، درخواست نماید. به عبارت دیگر باید $0 \le i \le m$ وجود داشته باشد که به‌ازای آن داشته باشیم $|\cup_{j=0}^{i}\gamma_i \cap \cup_{j=0}^{i}\gamma_i'| \ge k_i$. فرض کنید مجموعه ویژگی γ_{kp}' چنین شرطی را برآورده می‌کند. C کلید خصوصی ویژگی‌های γ_{kp}' را مطابق مراحل زیر تولید می‌کند:

- مقدار α را برابر $\gamma_{kp}' \cap \gamma_{kp}$ تعریف می‌کند.
- یک ویژگی بی‌تاثیر $0 \in u_0$ تعریف می‌کند.
- مقدار α' را طوری انتخاب می‌کند که $|\alpha'| = k_m - 1, \alpha \subseteq \gamma_{kp}'$ و $\alpha', \alpha' \subset \gamma_{kp}'$ و ویژگی‌های موجود در $\alpha' \cup \{0\}$ تمام مقادیر آستانه‌ای را برآورده کند.
- مجموعه S را برابر مقدار $\alpha' \cup \{0\}$ تعریف می‌کنیم.
- مولفه‌های کلید خصوصی برای ویژگی‌های $i \in \alpha'$ را به روش زیر محاسبه می‌کند.
  - اگر $i \in \alpha$ باشد، آنگاه یک عدد تصادفی $s_i \in Z_p$ انتخاب، سپس مقدار $D_i = g^{s_i}$ را محاسبه می‌کند.
  - اگر $i \in \alpha' - \alpha$ باشد آنگاه یک عدد تصادفی $\lambda_i \in Z_p$ انتخاب کرده و سپس مقدار $D_i = g^{\frac{\lambda_i}{\omega_i}}$ را محاسبه می‌کند.

در واقع C به‌طور ضمنی یک چندجمله‌ای $q(x)$ از درجه $k_m - 1$ با انتخاب $k_m - 1$ نقطه تصادفی به‌علاوه نقطه $q(0) = a$ تعریف می‌کند. به‌طوری که اگر $i \in \alpha$ مقدار تابع برابر $q^{(k_{j-1})}(i) = c\beta_i s_i$ و برای ویژگی‌های $i \in \alpha' - \alpha$ مقدار تابع برابر $q^{(k_{j-1})}(i) = \lambda_i$ است. j شماره سطحی است که ویژگی i در آن قرار دارد. C به روش زیر مولفه‌های کلید خصوصی مطابق با ویژگی‌های $i \in ID' - \alpha'$ را تولید می‌کند:

$$D_i = g^{\frac{q^{(k_{j-1})}(i)}{w_i}}$$

که j شماره سطحی است که ویژگی i در آن قرار دارد. بنابراین، طبق روش بالا C توانست مطابق با طرح اصلی، کلید خصوصی برای ویژگی γ_{kp}' تولید کند.

درخواست: مهاجم A دو پیام M_0 و M_1 با طول یکسان را به چالشگر C می‌دهد. سپس C یک بیت v را به‌طور تصادفی انتخاب می‌کند و پیام M_v را با استفاده از ویژگی γ_{kp} رمز می‌کند و متن رمز E_{kp} را به A می‌دهد. متن رمز به‌صورت زیر است:

$$E_{kp} = (\gamma_{kp}, E' = M_v Z, \{E_i = B^{\beta_i}\}_{i \in ID})$$

فاز ۲: در این مرحله نیز A می‌تواند درخواست‌هایی همانند آنچه در فاز اول انجام داده را انجام دهد و C نیز به همان روش پاسخ دهد.

حدس: در این مرحله A مقدار بیت v' را به‌عنوان پاسخ بر می‌گرداند. اگر $v = v'$ باشد، چالشگر مقدار یک را به نشانه تساوی Z با مقدار $e(g,g)^{ab/c}$ برمی‌گرداند. در غیر این‌صورت مقدار صفر را برای نشان دادن این‌که Z یک عدد تصادفی در گروه G_2 است را برمی‌گرداند. حال نشان می‌دهیم اگر A در بازی بالا با احتمال ε برنده شود، آنگاه C می‌تواند مساله سخت DMBDH را با احتمال $\varepsilon/2$ حل نماید.

اگر $z = e(g,g)^{\frac{ab}{2}}$ باشد، آنگاه $E' = M_v e(g,g)^{ar'}$ و برای هر ویژگی $i \epsilon \gamma_{kp}$، $E_i = B^{\beta_i} = g^{b\beta_i} = g^{\frac{b}{c}c\beta_i} = (T_i)^{r'}$ است که در آن $r' = \frac{b}{c}$. بنابراین، متن رمز یک رمزگذاری تصادفی از متن M_v تحت ویژگی γ_{kp} خواهد بود. در این حالت مزیت (احتمال برد) A بنابر تعریف برابر ε است، یعنی $\Pr[v = v'] = 1/2 + \varepsilon$.

در غیر این‌صورت، اگر Z برابر مقدار $e(g,g)^z$ به‌ازای یک عدد تصادفی $z \in Z_p$ شود، آنگاه $E' = M_v e(g,g)^z$. از آنجایی‌که Z یک عدد تصادفی است، E' از دید A یک عنصر تصادفی از گروه G_2 است و شامل هیچ گونه اطلاعاتی از M_v نیست. در این حالت مهاجم هیچ اطلاعی در مورد v به‌دست نمی‌آورد، در نتیجه $\Pr[v = v'] = 1/2$. بنابراین، احتمال چالشگر C برای حل مساله DMBDH برابر است با:

$$Adv_C^{DMBDH} = \left|Pr\left[C(g, g^a, g^b, g^c, e(g,g)^{ab/c}) \middle| v = v'\right] - Pr[C(g, g^a, g^b, g^c, Z) | v = v']\right| = \frac{1}{2}\left(\frac{1}{2} + \varepsilon\right) - \frac{1}{2}.\frac{1}{2} = \frac{\varepsilon}{2}$$

۴-۲. تحلیل امنیتی طرح رمزنگاری CP_ABE

در مدل امنیتی طرح CP_ABE مشابه مدل امنیتی طرح‌های رمزنگاری مبتنی‌بر شناسه به مهاجم این اجازه را می‌دهد تا کلیدهای خصوصی را درخواست کند که قادر به رمزگشایی متن رمز چالش نباشد. در ادامه بازی امنیتی به‌کار رفته در طرح بسن کارت و همکارانش را برای اثبات امنیت رمزنگاری CP_ABE شرح داده و نشان می‌دهیم طرح رمزنگاری CP_ABE به‌کار رفته در طرح پیشنهادی SBA-PHR در این مدل امنیتی دارای اثبات امنیتی است. این بازی بین چالشگر و مهاجم انجام می‌شود و

دارای مراحل زیر است.

آماده‌سازی: چالشگر الگوریتم آماده‌سازی را اجرا می‌کند و پارامترهای عمومی را به مهاجم می‌دهد.

فاز ۱: مهاجم کلیدهای خصوصی برای مجموعه ویژگی‌های $\gamma_0, \gamma_1, \dots, \gamma_m$ را درخواست می‌کند.

چالش: مهاجم دو پیام M_0 و M_1 با طول یکسان را به چالشگر می‌دهد. علاوه‌بر آن مهاجم یک ساختار دسترسی $\Gamma_{cp}{}^*$ را نیز اعلام می‌کند به‌طوری که هیچ یک از مجموعه ویژگی‌های $\gamma_0, \gamma_1, \dots, \gamma_m$ در فاز ۱ ساختار دسترسی $\Gamma_{cp}{}^*$ را برآورده نکنند. سپس چالشگر یک بیت b را به‌طور تصادفی انتخاب می‌کند و پیام M_b را تحت ساختار دسترسی $\Gamma_{cp}{}^*$ رمز می‌کند و متن رمزی $E_{cp}{}^*$ را به مهاجم می‌دهد.

فاز۲: در این مرحله فاز ۱ تکرار می‌شود با این محدودیت که هیچ یک از مجموعه ویژگی‌های $\gamma_0, \gamma_1, \dots, \gamma_m$ ساختار $\Gamma_{cp}{}^*$ را برآورده نکنند.

پاسخ: مهاجم یک بیت b' را به‌عنوان پاسخ برمی‌گرداند.

بنابراین، احتمال برد مهاجم در این بازی برابر است با:

$$Pr[\ Bsucceeds\ ] = pr[b = b'] - \frac{1}{2}$$

مانند تمامی طرح‌های رمزگذاری مبتنی‌بر ویژگی، تبانی کاربران یکی از چالش‌های اصلی در طراحی سامانه‌هایی رمزنگاری مبتنی‌بر ویژگی است. در رمزنگاری ABE استفاده‌شده در طرح پیشنهادی ما همانند طرح ساهای و واترز کلیدهای خصوصی کاربران به‌صورت تصادفی تولید شده است تا از مشارکت آن‌ها جلوگیری شود، همچنین در طرح بسن کارت استفاده شده در طرح SBA-PHR تسهیم راز به‌جای کلید خصوصی در متن رمز گنجانده شده است.

به‌طور روشن حمله‌کننده برای این‌که بتواند متن رمز را رمزگشایی نماید باید بتواند عبارت $e(g,g)^{\alpha s}$ را کشف نماید. به‌منظور تحقق این امر باید مولفه C از متن رمز و مولفه D از کلید خصوصی کاربر را با هم جفت نماید. که این کار مقدار مطلوب $e(g,g)^{\alpha s}$ را نتیجه می‌دهد اما این مقدار به‌وسیله $e(g,g)^{rs}$ مخفی شده است. مقدار $e(g,g)^{\alpha s}$ تنها زمانی می‌تواند آشکار شود که کاربر بتواند مولفه صحیحی از کلید را برای برآورده کردن تسهیم راز موجود در متن رمز در اختیار داشته باشد. از آن‌جایی که مقدار مخفی‌شده به‌طور تصادفی در کلید خصوصی یک کاربر خاص تعبیه شده است، حمله‌های تبانی به این طرح موثر نمی‌باشند. با توجه به مدل امنیتی به‌کار برده شده در طرح، مشخص است که این طرح نسبت به حملات انتخاب متن آشکار امن می‌باشد و حتی می‌تواند به‌طور کارا توسط اعمال روش‌های اراکل تصادفی شبیه طرح [۳۱] امنیت این طرح نسبت به حملات انتخاب متن رمز گسترش پیدا کند.

۴-۳. تحلیل امنیتی طرح پیشنهادی بر اساس منطق BAN

در این بخش برای تجزیه و تحلیل صحت پروتکل پیشنهادی از منطق BAN استفاده می‌شود. منطق BAN که در سال ۱۹۸۹ توسط برو[1] و همکارانش [۳۲] ارائه شده است، یک منطق مبتنی‌بر باور و عمل است. این منطق یک روش فرمال برای بررسی درستی باورهای پروتکل نزد نهادهای مورد اعتماد در اجرای پروتکل و تکامل این باورها از طریق فرایندهای ارتباطی به‌منظور شناسایی دقیق نقاط ضعف پروتکل می‌باشد. در جدول (۱) علائم اختصاری به‌کار رفته در منطق BAN ارائه شده است.

جدول (۱): علائم منطق BAN

نماد	توضیح
$P\| \equiv X$	P عبارت X را باور دارد؛ یعنی P می‌تواند بر مبنای درستی X تصمیم‌گیری کند.
$P \lhd X$	P عبارت X را می‌بیند؛ یعنی می‌تواند آن‌را بخواند و ذخیره کند.
$P\| \sim X$	P عبارت X را زمانی گفته است؛ یعنی P یک بار X را گفته است و زمانی که آن را گفته است آن را باور هم داشته است.
$P\| \Rightarrow X$	P در مورد X اختیار دارد؛ یعنی اگر P گفت که X را باور دارد صحت آن را می‌پذیریم.
$\#X$	عبارت X تازه است؛ یعنی X قبل از اجرای این مرحله از پروتکل هرگز ارسال نشده است.
$P \overset{K}{\leftrightarrow} Q$	یک کلید مشترک مانند K بین P و Q به اشتراک گذاشته شده است.
$\overset{k}{\mapsto} P$	K کلید عمومی P می‌باشد و کلید خصوصی متناظر با آن K^{-1} است.
$\{X\}_K$	عبارت X توسط کلید K رمز شده است.
$\underset{>_Y}{<X}$	عبارت X با فرمول Y ترکیب شده است؛ این بدان معنی است که Y یک راز است و حضور آن هویت هر کسی که $<X>_Y$ را گفته است را بیان می‌کند.
(X,Y)	فرمول X یا Y بخشی از فرمول (X,Y) است.

- فرضیات اولیه:

فرضیات اولیه شامل دارایی‌های اولیه موجودیت‌ها، توانایی آن‌ها و باور اولیه آن‌ها نسبت به لحظه آغازین پروتکل می‌باشد که به شرح زیر است:

فرضیات اولیه مربوط به بیمار P_i:

1 Burrows

$A_{1.1} P_i| \equiv | \xrightarrow{k_{pup}^{P_i}} P_i$:
$A_{1.2}$: $P_i| \equiv \#k_{pup}^{P_i}$
$A_{1.3}$: $P_i| \equiv \#K_{cp-sym}$
$A_{1.4}$: $P_i| \equiv U_k| \equiv < \gamma_{cp} >_{SK_i}$

فرضیات اولیه مربوط به بیمارستان :H_j

$A_{2.1}$: $H_j| \equiv | \xrightarrow{k_{pup}^{H_j}} H_j$
$A_{2.2}$: $H_j| \equiv \#k_{pup}^{H_j}$
$A_{2.3}$: $H_j| \equiv \#K_{kp-sym}$
$A_{2.4}$: $H_j| \equiv U_k| \equiv < \gamma_{kp} >_{D_j}$

فرضیات مربوط به کاربر U_k:

U_k کاربری است که قصد استفاده از داده‌های پزشکی را دارد.

$A_{3.1}$:$U_k| \equiv | \xrightarrow{k_{pup}^{U_k}} U_k$
$A_{3.2}$:$U_k| \equiv \#k_{pup}^{U_k}$
$A_{3.3}$:$U_k| \equiv < \gamma_{cp} >_{SK_i}$
$A_{3.4}$: $U_k| \equiv < \gamma_{kp} >_{D_j}$

فرضیات مربوط به گره‌های زنجیره‌بلوکی:

$A_{4.1}$: $B| \equiv P_i| \equiv | \xrightarrow{k_{pup}^{P_i}} P_i$
$A_{4.2}$: $B| \equiv H_j| \equiv | \xrightarrow{k_{pup}^{H_j}} H_j$
$A_{4.3}$: $B| \equiv U_k| \equiv | \xrightarrow{k_{pup}^{U_k}} U_k$
$A_{4.4}$: $B| \equiv P_i| \Rightarrow k_{pup}^{P_i}$
$A_{4.5}$: $B| \equiv H_j| \Rightarrow k_{pup}^{H_j}$
$A_{4.6}$: $B| \equiv U_k| \Rightarrow k_{pup}^{U_k}$
$A_{4.7}$: $B| \equiv U_k| \equiv < \gamma_{cp} >_{SK_i}$
$A_{4.8}$: $B| \equiv U_k| \equiv < \gamma_{kp} >_{D_j}$
$A_{4.9}$: $B| \equiv P_i| \equiv < \gamma_{cp} >_{SK_i}$
$A_{4.10}$: $B| \equiv H_j| \equiv < \gamma_{kp} >_{D_j}$
$A_{4.11}$: $B| \equiv P_i| \equiv \#k_{pup}^{P_i}$
$A_{4.12}$: $B| \equiv H_j| \equiv \#k_{pup}^{H_j}$
$A_{4.12}$: $B| \equiv U_k| \equiv \#k_{pup}^{U_k}$

اهداف مورد انتظار پروتکل:

اهداف مورد انتظار شامل هدف‌هایی می‌شود که مجموعه آن‌ها امنیت پروتکل پیشنهادی را تضمین می‌کند. این اهداف شامل باور موجودیت‌های مشارکت‌کننده در پروتکل از اجرای صحیح فرآیندها می‌باشد. مانند باور گره‌های اجراکننده اجماع در زنجیره‌بلوکی به صحت تراکنش‌های ارسال‌شده و یا باور بیمار از این‌که فقط نهادهای مجاز و مورد انتظار او قادر به رمزگشایی داده هستند. این اهداف مورد انتظار به شرح زیر می‌باشد.

G_1: $B| \equiv P_i| \sim IT_x$
G_2: $B| \equiv P_i| \sim PT_x$
G_3: $B| \equiv H_j| \sim PT_x$
G_4: $B| \equiv \#(IT_x, PT_x)$
G_5: $B| \equiv \#IT_x$
G_6: $U_k \lessdot PHI$
G_7: $U_k| \equiv P_i| \sim IT_x$
G_8: $U_k| \equiv P_i| \sim PT_x$
G_9: $U_k| \equiv H_j| \sim PT_x$

ایده‌آل‌سازی جریان‌های پروتکل:

در ایده‌آل‌سازی پروتکل هر بخش از اجرای پروتکل بر اساس منطق BAN مدل‌سازی شده و یک تعریف رسمی مبتنی‌بر نمادگذاری منطق BAN از جریان‌های پروتکل ارائه می‌شود.

مرحله رمزگذاری داده‌ها توسط بیمارستان:
M(1.1); $(P_i \rightarrow B)$: $B \lessdot < IT_x >_{k_{pr}^{P_i}}$
M(1.2); $(H_j \rightarrow C)$: $C \lessdot \{PHI\}_{K_{kp-sym}}$
M(1.3); $(H_j \rightarrow B)$: $B \lessdot < PT_x >_{k_{pr}^{H_j}}, B \lessdot \{K_{kp-sym}\}_{D_j}$

مرحله رمزگذاری داده‌ها توسط بیمار:
M(2.1); $(P_i \rightarrow C)$: $C \lessdot \{PHI\}_{K_{cp-sym}}$
M(2.2); $(P_i \rightarrow B)$: $B \lessdot < IT_x >_{k_{pr}^{P_i}}$
M(2.3); $(P_i \rightarrow B)$: $B \lessdot < PT_x >_{k_{pr}^{P_i}}, B \lessdot \{K_{cp-sym}\}_{SK_i}$

مرحله رمزگشایی داده‌ها:
M(3.1); $(B \rightarrow U_k)$: $U_k \lessdot < IT_x >_{k_{pr}^{P_i}}$
M(3.2); $(U_k \rightarrow B)$: $B \lessdot \left(< UdT_x >_{k_{pr}^{U_k}}, SC \right)$
M(3.3); $(B \rightarrow U_k)$: $U_k \lessdot < PT_x >_{k_{pr}^{P_i}}$
OR $U_k \lessdot < PT_x >_{k_{pr}^{H_j}}$
M(3.4); $(C \rightarrow U_k)$: $U_k \lessdot < PHI >_{K_{kp-sym}}$
OR $U_k \lessdot < PHI >_{K_{cp-sym}}$

تفسیر اهداف امنیتی پروتکل:

بر مبنای فرضیات اولیه، جریان‌های ایده‌آل‌سازی پروتکل و قوانین منطق BAN، تفسیر اهداف امنیتی پروتکل به شرح زیر است.

قضیه ۱: گره‌های موجود در شبکه زنجیره‌بلوکی باور دارند که بیمار P_i یک زمانی تراکنش IT_x را تولید کرده است.

اثبات:

$(J1)$: $\frac{P| \equiv Q| \Rightarrow X,\ P| \equiv Q| \equiv X}{P| \equiv X}$ بر اساس فرضیات $A_{4.1}$ و $A_{4.4}$ و قانون داریم:

$$(T1): \frac{B| \equiv P_i| \Rightarrow k_{pup}^{P_i},\ B| \equiv P_i| \equiv | \xrightarrow{k_{pup}^{P_i}} P_i}{B| \equiv | \xrightarrow{k_{pup}^{P_i}} P_i}$$

یعنی گره‌های شبکه زنجیره‌بلوکی باور دارند که کلید $k_{pup}^{P_i}$ کلید عمومی متناظر با کلید خصوصی $k_{pr}^{P_i}$ و مربوط به بیمار P_i است. بنابراین، بر اساس پیام M(1.1) که گره‌های زنجیره‌بلوکی در آن یک تراکنش IT_x را با امضای کلید خصوصی $k_{pup}^{P_i}$ دریافت کرده‌اند، نتیجه T2 و قانون $(RM2)$: $\frac{P| \equiv | \xrightarrow{K} Q,\ P \lessdot \{X\}_{K^{-1}}}{P| \equiv Q| \sim X}$ داریم:

$$(T2): \frac{B| \equiv | \xrightarrow{k_{pup}^{P_i}} P_i \ , \ B \lhd \{IT_x\}_{k_{pr}^{P_i}}}{B| \equiv P_i| \sim IT_x}$$

یعنی گره‌های زنجیره‌بلوکی به این باور می‌رسند که P_i یک زمانی تراکنش IT_x را ایجاد کرده است. بنابراین، هدف G_1 برآورده می‌شود. به همین طریق اهداف G_2، G_3، G_7، G_8 و G_9 نیز اثبات می‌شود.

قضیه ۲: گره‌های زنجیره‌بلوکی باور دارند که تراکنش‌های IT_x و PT_x توسط P_i و بر اساس ساختار دسترسی مورد نظر P_i تولید شده است.

اثبات: طبق قضیه ۱ گره‌های زنجیره‌بلوکی باور دارند که تراکنش‌های IT_x و PT_x زمانی توسط P_i تولید شده است. همچنین طبق فرض $A_{4.11}$ گره‌های زنجیره‌بلوکی باور دارند که $k_{pup}^{P_i}$ تازه است. بنابراین، طبق قانون $(F4): \frac{P| \equiv \#X}{P| \equiv \#<X>_Y}$ که بیان می‌کند اگر که P باور داشته باشد که بخشی از یک گزاره تازه است، آنگاه باور دارد که تمام آن گزاره تازه است و فرض $A_{4.4}$ داریم:

$$(T3): \frac{B| \equiv \#k_{pup}^{P_i} \ , \ B| \equiv P_i| \Rightarrow k_{pup}^{P_i}}{B| \equiv \# < IT_x >_{k_{pr}^{P_i}} \ , \ B| \equiv < PT_x >_{k_{pr}^{P_i}}}$$

بنابراین، طبق رابطه T4 هدف G_5 اثبات می‌شود.

$$(T4): \frac{B| \equiv \# < IT_x >_{k_{pr}^{P_i}}}{B| \equiv \#IT_x}$$

همچنین طبق رابطه T3 و قانون $(F1): \frac{P| \equiv \#X}{P| \equiv \#(X,Y)}$ داریم:

$$(T5): \frac{B| \equiv \#IT_x}{B| \equiv (IT_x, PT_x)}$$

بنابراین، هدف G_4 نیز اثبات شد.

قضیه ۳: بیمار P_i اطمینان داشته باشد که کاربر U_k با ویژگی‌های مناسب می‌تواند به داده‌های PHI دسترسی داشته باشد.

اثبات: طبق پیام M(3.1) کاربر U_k می‌تواند تراکنش IT_x را از شبکه زنجیره‌بلوکی دریافت کند و اگر ویژگی‌های لازم در آن تراکنش را داشته باشد نتیجه قرارداد هوشمند SC معتبر بوده و طبق پیام M(3.3) تراکنش PT_x را دریافت می‌کند، که شامل مسیر ذخیره‌سازی داده در ابر و اطلاعات کلید K_{kp-sym} و یا K_{cp-sym} به‌صورت رمزگذاری‌شده می‌باشد. بنابراین، کاربر U_k می‌تواند طبق پیام M(3.3) و M(3.4) داده‌های رمزگذاری‌شده را از ابر دریافت کند.

$$(T6): \frac{U_k \lhd < PT_x >_{k_{pr}^{P_i}}}{U_k \lhd \{K_{cp-sym}\}_{SK_i}, U_k \lhd \{PHI\}_{K_{cp-sym}}}$$

$$OR \ \frac{U_k \lhd < PT_x >_{k_{pr}^{H_j}}}{U_k \lhd \{K_{kp-sym}\}_{D_j}, U_k \lhd \{PHI\}_{K_{kp-sym}}}$$

لذا طبق فرضیات $A_{3.3}$ و $A_{3.4}$ و نتیجه T6 داریم:

$$(T7): \frac{U_k \lhd \{K_{kp-sym}\}_{D_j} \ , \ U_k| \equiv < \gamma_{kp} >_{D_j}}{U_k \lhd K_{kp-sym}}$$

$$(T8): \frac{U_k \lhd K_{kp-sym} \ , \ U_k \lhd \{PHI\}_{K_{kp-sym}}}{U_k \lhd PHI}$$

به همین طریق برای داده‌هایی که توسط بیمار رمزگذاری شده‌اند نیز داریم:

$$(T9): \frac{U_k \lhd \{K_{cp-sym}\}_{SK_i}, U_k| \equiv < \gamma_{cp} >_{SK_i}}{U_k \lhd K_{cp-sym}}$$

$$(T10): \frac{U_k \lhd K_{cp-sym}, U_k \lhd \{PHI\}_{K_{cp-sym}}}{U_k \lhd PHI}$$

بنابراین، هدف دست‌یابی کاربر به اطلاعات پزشکی PHI محقق شد یعنی هدف G_6 اثبات گردید.

۴-۴. مقایسه ویژگی‌های امنیتی

در این بخش طرح پیشنهادی SBA-PHR را با برخی از طرح‌های اخیر که برای اشتراک‌گذاری داده‌های پزشکی پیشنهاد شده است، از منظر ویژگی‌های امنیتی مقایسه و در جدول (۲) ارائه شده است.

جدول (۲): مقایسه ویژگی‌های امنیتی طرح پیشنهادی

Propertes	Yang[33]	Zhang[34]	BBDS [35]	MeDShare[10]	Peterson[11]	BSPP[36]	SBA-ABE
Blockchain based	✗	✗	✓	✓	✓	✓	✓
Access control	✓	✓	✓	✓	✓	✓	✓
Immediate accees revocation	✗	✗	✗	✗	✗	✗	✓
Data auditing	✓	✓	✓	✓	✗	✓	✓
Privacy preservation	✓	✓	✓	✓	✓	✓	✓
Patient anonymity	✓	✗	✓	✓	✓	✓	✓
No online registration center	✗	✓	✗	✗	✗	✗	✓
Perfect forward secrecy	✗	✗	✗	✗	✓	✓	✓

۵. کارایی

در این بخش به بررسی کارایی سامانه از نقطه نظر پیچیدگی محاسبات مورد نیاز برای عملیات‌های رمزگذاری، رمزگشایی و امضای تراکنش‌ها و فضای ذخیره‌سازی لازم در شبکه برای انواع تراکنش‌ها در زنجیره‌بلوکی می‌پردازیم.

۵-۱. تحلیل سربار ذخیره‌سازی طرح پیشنهادی

با توجه به این‌که تراکنش‌های ثبت‌شده در شبکه یا حاوی کلید رمزگذاری و مسیر ذخیره‌سازی اطلاعات PHI در زنجیره‌بلوکی permissioned و یا شامل توضیحی از اطلاعات PHI و ساختار دسترسی آن‌ها در زنجیره‌بلوکی permissionless می‌باشد؛ بنابراین، حجم اطلاعات ذخیره‌شده در زنجیره‌بلوکی از اهمیت بالایی برخوردار است. حجم اطلاعات ذخیره‌شده در بلوک‌های زنجیره‌بلوکی به حجم اطلاعات موجود در یک تراکنش وابسته است. در جدول (۳) اندازه بلوک‌های زنجیره‌بلوکی‌های permissioned و permissionless و اندازه انواع تراکنش‌های ITx، UdTx و PTx آورده شده است. ما اندازه اعضای گروه G_1 و G_2 را به ترتیب با $|G_1|$ و $|G_2|$ و اندازه اعضای $\mathbb{Z}_p$ را با $|Q|$ نشان می‌دهیم و t تعداد ویژگی‌های مورد انتظار برای رمزگشایی داده‌ها می‌باشد که حداکثر مقدار آن برابر با k_m است.

اندازه بلوک با یک بایت نوع زنجیره‌بلوکی را مشخص می‌کند و اندازه هر بلوک با ۴ بایت مشخص می‌شود. اندازه شناسه بلوک که برای آدرس دهی بلوک استفاده می‌شود و اندازه چکیده بلوک قبلی برابر ۳۲ بایت است. نوع هر تراکنش (ITx, UdTx or PTx) به‌وسیله یک بایت در آن تراکنش مشخص می‌شود. شناسه مستعار تولیدکننده هر تراکنش برابر است با $H_3(K^i_{pub})$ که اندازه آن ۳۲ بایت است. اندازه مهر زمانی برابر ۴ بایت در نظر گرفته شده است. امضای ECDSA بر روی منحنی بیضوی secp256k1 داری دو مولفه ۳۲ بایتی است که در مجموع ۶۴ بایت را در هر تراکنش به خود اختصاص می‌دهد.

اندازه محتویات تراکنش در تراکنش‌های مختلف متفاوت است که در جدول (۴) اندازه آن برای تراکنش‌های ITx، UdTx و PTx آورده شده است. همان‌طور که در جدول (۴) مشخص است اندازه محتویات تراکنش مربوط به تراکنش UdTx همواره ثابت است اما اندازه محتویات تراکنش‌های ITx و PTx به‌صورت خطی با تعداد ویژگی‌های سامانه افزایش می‌یابد. علت این امر این است که اندازه ساختار دسترسی که برای رمزگشایی داده‌ها تعیین می‌شود با افزایش تعداد ویژگی‌های مورد نیاز برای رمزگشایی داده‌ها به‌صورت خطی افزایش می‌یابد. بنابراین، افزایش تعداد ویژگی‌های مورد نیاز برای رمزگذاری داده‌ها منجر به افزایش خطی طول پیام رمز می‌شود. در جدول (۴) t تعداد ویژگی مورد نیاز برای رمزگشایی داده‌ها می‌باشد که حداکثر مقدار آن برابر با k_m خواهد بود.

جدول (۳): فضای ذخیره‌سازی بلوک‌های زنجیره‌بلوکی طرح پیشنهادی

Payload					
ITx		**UdTx**	**PTx**		
PHI descriptor	Γ_{cp}or γ_{kp}	Not spent ITx address	ITx address	Path of encrypted data	$E_{kp}or\ E_{cp}$
512 byte	$t\|Q\|$	32 byte	32 byte	8 byte	(Y_{kp}, E', E_i) $t\|Q\| + \|G_2\| + t\|G_1\|$ Or $(\Gamma_{cp}, \tilde{C}, C, C_y, C'_y)$ $t\|Q\| + \|G_2\| + \|Q\| + t\|G_1\| + \|G_1\|$

جدول(۴): فضای ذخیره‌سازی مورد نیاز برای هر نوع تراکنش طرح پیشنهادی

Permission or Permissionless Block

Block header				**Transaction**				
Block type	Block identity	Block size	Previous block hash	Transaction type	Pseudo ID	Payload	Time stamp	Signature
1 byte	32 byte	4byte	32 byte	1 byte	32 byte	ITx or UdTx or PTx	4byte	64 byte

۵-۲. تحلیل پیچیدگی محاسباتی طرح پیشنهادی

در این بخش پیچیدگی محاسباتی الگوریتم‌های تولید کلید، رمزگذاری و رمزگشایی مورد نیاز در رمزنگاری KP-ABE و CP-ABE استفاده‌شده در طرح SBA-PHR و الگوریتم تولید و بررسی امضای دیجیتال را تحلیل و بررسی می‌کنیم. در جدول (۵) پیچیدگی محاسباتی مورد نیاز برای الگوریتم‌های فوق آورده

شده است. همان‌طور که در جدول (۵) مشخص است. پیچیدگی محاسباتی مورد نیاز برای تولید کلید، رمزگذاری و رمزگشایی پیام‌ها وابستگی خطی به تعداد ویژگی‌های مورد انتظار (t) دارد. بنابراین، حداکثر مقدار t برابر با k_m خواهد بود. k_m حداکثر تعداد ویژگی ممکن برای دسترسی به داده‌ها می‌باشد.

در الگوریتم رمزنگاری CP-ABE نیاز به دو عملیات توان‌رسانی برای هر ویژگی مورد نظر در ساختار دسترسی Γ_{cp} و حداکثر یک عملیات زوج‌سازی و یک عملیات ضرب اسکالر داریم. همچنین در الگوریتم تولید کلید آن نیازمند دو عملیات توان‌رسانی برای هر ویژگی کاربر هستیم. الگوریتم رمزگشایی CP-ABE نیز در ساده‌ترین شکل نیازمند دو عمل زوج‌سازی برای هر ویژگی در ساختار دسترسی Γ_{cp} و حداکثر یک عملیات توان‌رسانی در طول مسیر از گره برگ تا ریشه می‌باشد.

در رمزنگاری KP-ABE تعداد عناصر گروه در پارامترهای عمومی سامانه به‌طور خطی با ویژگی‌های سامانه افزایش می‌یابد. بنابراین، به تعداد ویژگی‌های مورد نظر در ساختار دسترسی Γ_{kp} نیاز به عملیات توان‌رسانی در تولید کلیدهای سامانه داریم. همچنین در الگوریتم رمزنگاری نیازمند $t+1$ عملیات توان-رسانی و حداکثر یک عملیات ضرب اسکالر منحنی بیضوی هستیم و در الگوریتم رمزگشایی KP-ABE به تعداد ویژگی‌های مورد نظر نیازمند عملیات زوج‌سازی و حداکثر یک عملیات توان-رسانی هستیم.

با توجه به الگوریتم امضای ECDSA نیازمند یک عملیات ضرب اسکالر و یک عملیات معکوس‌گیری برای فرایند امضا و دو عملیات ضرب اسکالر و یک عملیات معکوس‌گیری برای فرایند وارسی امضا هستیم. فرایند تولید و وارسی امضا فارغ از ویژگی‌های مورد نظر هر کاربر همواره پیچیدگی محاسباتی ثابتی دارد.

جدول (۵): پیچیدگی محاسباتی طرح پیشنهادی

	Key generation	Encryption / verification	Decryption / sign
KP-ABE	tT_{exp}	$(t+1)T_{exp}+T_{mul}$	$tT_{pair}+T_{exp}$
CP-ABE	$(2t+1)T_{exp}$	$T_{pair}+2tT_{exp}+T_{mul}$	$2tT_{pair}+T_{exp}$
ECDSA	$2T_{mul}$	$2T_{mul}+T_{inv}$	$T_{mul}+T_{inv}$

جدول (۶): نمادگذاری پیچیدگی محاسباتی

Time complexity of operators
T_{mul}: scaler multiplication
T_{exp}: exponential
T_{pair}:pairing
T_{inv}: inverse

۶. نتیجه‌گیری

در این مقاله، یک پروتکل جدید و امن برای به اشتراک‌گذاری داده‌های پزشکی به‌صورت کارآمد بین بیماران، بیمارستان‌ها و نهادهای استفاده‌کننده از داده‌های پزشکی ارائه شد. پروتکل پیشنهادی شامل به‌کارگیری روش‌های رمزنگاری مبتنی‌بر ویژگی و ترکیب آن با فناوری زنجیره‌بلوکی است. در طرح پیشنهادی جدید برای کنترل سطح دسترسی دقیق و دانه‌ای بیماران بر روی داده‌های پزشکی خود، از دو نوع رمزنگاری مبتنی‌بر ویژگی KP-ABE و CP-ABE استفاده شده است همچنین برای افزایش کارایی شبکه در انتقال موثرتر داده‌های پزشکی و بهبود روش‌های ابطال حق دسترسی در رمزنگاری مبتنی‌بر ویژگی به‌صورت آنی از فناوری زنجیره‌بلوکی استفاده کرده‌ایم. طرح پیشنهادی ما شامل دو زنجیره‌بلوکی خصوصی مبتنی‌بر روش اجماع PBFT به‌صورت premissionless و permissioned است، که یکی برای انتشار اطلاعات عمومی داده‌های پزشکی و ساختار دسترسی مجاز آن‌ها و دیگری برای در

اختیار قرار دادن اطلاعات کلید و مکان ذخیره‌سازی داده‌ها در سامانه‌های ذخیره‌ساز ابری می‌باشد.

مقایسه ویژگی‌های امنیتی طرح پیشنهادی ما با سایر طرح‌های مشابه نشان می‌دهد که طرح SBA-PHR علاوه‌بر

ویژگی محرمانگی داده کاربر، گمنامی بیماران و حفظ حریم خصوصی نهادها، ویژگی ابطال‌پذیری آنی حق دسترسی که یکی از چالش‌های رمزنگاری مبتنی‌بر ویژگی است را نیز برآورده می‌کند. همچنین سربار محاسباتی طرح SBA-PHR نشان می‌دهد که با افزایش تعداد ویژگی‌های مطلوب برای دسترسی به اطلاعات پزشکی، پیچیدگی طرح به‌صورت خطی افزایش می‌یابد اما با توجه به کران m برای حداکثر تعداد ویژگی‌های مطلوب مقیاس‌پذیری طرح حفظ شده است.

اثبات ارائه‌شده مبتنی‌بر منطق BAN صحت عملکرد طرح پیشنهادی ما را به اثبات می‌رساند و همچنین اثبات‌های فرمال ارائه‌شده برای رمزنگاری KP-ABE و CP-ABE امنیت اولیه‌های رمزنگاری طرح SBA-PHR را در مدل اوراکل تصادفی نشان می‌دهد.

۷. مراجع

[1] Wu, Hsin-Te, and Chun-Wei Tsai. "Toward Blockchains for Health-Care Systems: Applying the Bilinear Pairing Technology to Ensure Privacy Protection and Accuracy in Data Sharing," IEEE Consumer Electronics Magazine vol. 7.4, pp. 65-71, 2018.

[2] L. Cartwright-Smith, E. Gray, and J. H. Thorpe, "Health information ownership: legal theories and policy implications," Vand. J. Ent. & Tech. L., vol. 19, p. 207, 2016.

[3] Kshetri, Nir. "Blockchain's roles in strengthening cybersecurity and protecting privacy," Telecommunications Policy 41.10, pp. 1027-1038, 2017.

[4] Azaria, Asaph, et al., "Medrec: Using blockchain for medical data access and permission management," Open and Big Data (OBD), International Conference on. IEEE, pp. 25-30, 2016.

[5] Dagher, Gaby G., et al., "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," Sustainable Cities and Society, vol. 39, pp. 283-297, 2018.

[6] Yue, Xiao, et al., "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," Journal of medical systems, vol. 40.10, pp. 218, 2016.

[7] Banerjee, Mandrita, Junghee Lee, and Kim-Kwang Raymond Choo, "A blockchain future for internet of things security: a position paper," Digital Communications and Networks, vol. 4.3, pp. 149-160, 2018.

[8] K. Harleen, et al., "A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment," Journal of medical systems, vol. 42.8, pp. 156, 2018.

[9] X. Yue, H. Wang, D. Jin, et al., "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," Journal of Medical Systems, vol. 40(10), p. 218, 2016.

[10] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 757–767, July 2017.

[11] P. Kevin, et al., "A blockchain-based approach to health information exchange networks," Proc. NIST Workshop Blockchain Healthcare, vol. 1, 2016.

[12] D. Alevtina, et al., "Secure and trustable electronic medical records sharing using blockchain," AMIA Annual Symposium Proceedings, vol. 2017, American Medical Informatics Association, 2017.

[13] Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," In Proc. Int. Conf. Smart Technologies, pp. 763–768, 2017.

[14] A. Shamir, "Identity-based cryptosystems and signature protocols," Proceedings of CRYPTO1984, vol. 196, LNCS, California, USA, 1984, pp. 47–53, 1984.

[15] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," Proceedings of CRYPTO'01, LNCS, vol. 2139, California, USA, pp. 213–229, 2001.

[16] A. Sahai and B. Waters, "Fuzzy identity-based encryption," In EUROCRYPT2005, vol. 3494, Cramer R (ed.), LNCS. Springer: Heidelberg, pp. 457–473, 2005.

[17] G. Vipul, et al., "Attribute-based encryption for fine-grained access control of encrypted data," Proceedings of the 13th ACM conference on Computer and communications security, Acm, 2006.

[18] Nakamoto, Satoshi, "Bitcoin: A peer-to-peer electronic cash system," Consulted, vol. 1, 2012, 2008.

[19] A. Kosba, et al., "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," IEEE symposium on security and privacy (SP). IEEE, 2016.

[20] C. Cachin, "Architecture of the hyperledger blockchain fabric," In Workshop on Distributed Cryptocurrencies and Consensus Ledgers, 2016.

[21] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," Ripple Labs Inc White Paper, vol. 5, 2014.

[22] H. Sukhwani, J. M. Mart´ınez, X. Chang, et al., "Performance modeling of PBFT consensus process for permissioned blockchain network (hyper- ledger fabric)," In: Reliable Distributed Systems, pp. 253-255, 2017.

[23] C. Miguel and B. Liskov, "Practical Byzantine fault tolerance," OSDI., vol. 99, 1999.

[24] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals prob- lem," ACM Transactions on

[31] D. Hankerson, S. Vanstone, and A. J. Menezes, "Guide to elliptic curve cryptography," New York, Springer, 2004.

[32] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," In: Advances in cryptology CRYPTO, New York: Springer, pp. 213–229, 2001.

[33] Y. Yang and M. Ma, "Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-Health clouds," IEEE Transactions on Information Forensics and Security, vol. 11(4), pp. 746–759, 2016.

[34] J. Zhang, N. Xue, and X. Huang, "A secure system for pervasive social network-based healthcare," IEEE Access 4(99), pp. 9239–9250, 2016.

[35] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-Based data sharing for electronic medical records in cloud environments," Information 8(44), pp. 1–16, 2017.

[36] Zhang, Aiqing, and Xiaodong Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," Journal of medical systems, vol. 42.8, p. 140, 2018.

Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.

[25] N. Szabo, "Smart contracts: Building blocks for dig- ital markets," EXTROPY: The Journal of Transhumanist Thought, vol. 16, 1996.

[26] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," Security and Privacy, SP'07. IEEE Symposium on. IEEE, 2007.

[27] Fujisaki, Eiichiro, and Tatsuaki Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," Annual International Cryptology Conference, Springer, Berlin, Heidelberg, 1999.

[28] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," Proc. R. Soc. Lond. A 426.1871, pp. 233-271, 1989.

[29] N. Aitzhan and D. Svetinovic, "Security and privacy in decentralized en- ergy trading through multi-signatures, blockchain and anonymous messag-ing streams," IEEE Transactions on Dependable and Secure Computing, PP(99):1, 2016.

[30] S. H. Hosseinian Barzi and H. Maleki, "Hierarchical Fuzzy Identity-Based Encryption," Electronic and Cyber Defense Magazine, vol. 6, no. 3, 2018. (in Persian)

Journal of Electronical & Cyber Defence
Vol. 8, No. 1, 2020, Serial No. 29

A Novel and Secure Model for Sharing Protected Health Record (PHR) Based on Blockchain and Attribute Based Encryption

S. M. Pournaghi*, M. Bayat, Y. Farjami, Z. Hatefi, N. Hamian

*Department of Computer Engineering, University of Qom, Qom, Iran

(Received: 03/12/2018, Accepted: 05/03/2019)

ABSTRACT

Wireless body area networks (WBANs) include many tiny sensor nodes which are planted in or around a patient's body. These sensor nodes can collect biomedical data from the patient and transmit these valuable data to a data sink or a personal digital assistant. Later, health care service providers can get access to these data through authorization. The biomedical data are usually personal and private. Consequently, data confidentiality and user privacy are of primary concerns for WBAN. One of the most important factors for providing security in e-healthcare networks, is authentication protocols which allow both parties to authenticate each other. Recently, regarding this issue, Challa et al.[1] presented an efficient elliptic curve based provably secure three-factor key agreement and authentication protocol for wireless healthcare sensor networks. In this paper, firstly we identify some security flaws of the Challa et al.'s scheme such as privileged-insider attacks, lack of forward secrecy and user traceability. Then, we present a three-factor authentication scheme for (WBANs) and evaluate the security properties of our scheme formally via "ProVerif". Presented security analysis and comparisons show that the proposed scheme is an efficient secure authentication scheme for WBANs.

Keywords: Authentication, E-Health, Key Agreement, Security, Privacy, ProVerif

* Corresponding Author Email: sm.pournaghi@gmail.com