دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۱، جلد ۲۰، شماره ۱ (۴۸-۵۸)
https://monadi.isc.org.ir

ارائه‌شده در هجدهمین کنفرانس بین‌المللی انجمن رمز ایران در دانشگاه اصفهان، ۱۰ و ۱۱ شهریور ۱۴۰۰

مدیریت پرونده الکترونیکی سلامت با حفظ حریم خصوصی مبتنی بر زنجیره بلوک★

مهسا رضائی و صادق دری نوگورانی*

دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:
پرونده الکترونیکی سلامت
حریم خصوصی
کنترل دسترسی
زنجیره بلوک
ابر

dor: 20.1001.1.24763047.1401.11.1.6.3

نوع مقاله: پژوهشی

چکیده

در سال‌های اخیر با گسترش فناوری شاهد توسعه و به‌کارگیری پرونده‌های الکترونیکی سلامت (EHR) و تأثیر آن بر روند زندگی بشر از جمله افزایش کیفیت مراقبت‌های درمانی، بهبود نتایج پژوهش‌های علمی و روش‌های درمانی هستیم. علی‌رغم تلاش‌های انجام‌شده، همچنان دسترس‌پذیری، امنیت و حفظ حریم خصوصی از دغدغه‌های بسیار مهم در این حوزه هستند. در این مقاله تلاش نموده‌ایم با کمک زنجیره بلوک و مزایای بالقوه‌ای که دارد، سامانه‌ای نامتمرکز و توزیع‌شده برای مدیریت پرونده الکترونیکی سلامت ارائه دهیم. در این سامانه اطلاعات بیمار در فضای ابری ذخیره می‌شود. همچنین مالک واقعی پرونده الکترونیکی، شخص بیمار است و با کمک قراردادهای هوشمند و رمزنگاری نحوه دسترسی به اطلاعات سلامتش را کنترل می‌کند. در راه‌حل پیشنهادی با کمک قرارداد هوشمند مشکل اشتراک‌گذاری و ذخیره‌سازی کلید بیمار حل‌شده است و چالش‌های ناشی از سپردن کنترل پرونده به بیمار نظیر تصمیم‌گیری برای بیماران زیر سن قانونی، در شرایط اضطراری و پس از فوت بیمار را برطرف نموده‌ایم. مقایسه باکارهای مرتبط نشان می‌دهد سامانه پیشنهادی بسیاری از مشکلات سامانه‌های رقیب را در عین حفظ سطح بالایی از حریم خصوصی مرتفع کرده است.

۱ مقدمه

در سامانه‌های سنتی نگهداری پرونده سلامت، ارائه‌دهندگان خدمات سلامت متفاوتی وجود دارند که از قالب‌های داده‌ای و استانداردهای مختلف برای ثبت پرونده بیمار استفاده می‌کنند، همچنین مبتنی بر پایگاه داده‌های خصوصی هستند که مشتمل بر اطلاعات تکراری و ناقص است. زمانی که بیمار بخواهد به ارائه‌دهنده دیگری مراجعه کند، باید شخصاً اطلاعاتش را جمع‌آوری و منتقل کند. از آنجا که انتقال اطلاعات به صورت فیزیکی یا از طریق رسانه‌های ذخیره‌سازی قابل‌حمل صورت می‌گیرد، علاوه بر صرف زمان و هزینه، خطر آسیب فیزیکی و گم‌شدن اطلاعات نیز وجود دارد.

سازمان بهداشت جهانی (WHO [1]) سلامت الکترونیک را به صورت زیر تعریف کرده است [۱]: «سلامت الکترونیکی به معنای انتقال منابع سلامت و مراقبت‌های بهداشتی از طریق وسایل الکترونیکی است که شامل سه حوزه اصلی است: ارائه اطلاعات پزشکی به فرد متخصص از طریق اینترنت و ارتباطات راه دور، استفاده از فناوری اطلاعات و تجارت الکترونیکی برای بهبود خدمات پزشکی از طریق آموزش افراد مرتبط و استفاده از تجارت الکترونیکی و کسب‌وکار الکترونیکی در مدیریت سامانه پزشکی.»

طی آمارهای اعلام‌شده از هر ۱۷ مرگ و میر ناشی از خطاهای پزشکی،

[1] World Health Organization

★از کمیته علمی هجدهمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول
آدرس‌های رایانامه: mahsa_rezaei@modares.ac.ir (مهسا رضائی)، dorri@modares.ac.ir (صادق دری نوگورانی)

۱۰ مورد آن به علت اطلاعات ناقص و اشتباه راجع به بیمار بوده است. استفاده از سامانه‌های الکترونیکی سلامت (EHR [1]) مزایایی همچون کاهش هزینه‌ها، افزایش کیفیت خدمات و ایمنی بیماران، کاهش خطاهای پزشکی و کاهش زمان دسترسی به اطلاعات مورد نظر را دارد. نکته حائز اهمیت دیگر در رابطه با سامانه‌های سنتی، عدم اعتماد و دسترسی ارائه‌دهندگان مختلف به روند درمان توسط سایر ارائه‌دهندگان است. این امر نه تنها موجب دوباره‌کاری می‌شود و زمان‌بر و هزینه‌بر است، بلکه بعضی از آزمایش‌ها غیرمجاز هستند و انجام مجددشان می‌تواند خطرناک باشد [۲]. در صورتی که پرونده قابل اعتمادی از بیمار در اختیار پزشک قرار گیرد، وی می‌تواند تشخیص دقیق‌تری داشته باشد و از تداخل یا حساسیت‌های دارویی در هنگام تجویز اطلاع پیدا کند. گذشته از این‌ها، با اتصال مراکز درمانی به سایر سازمان‌ها نظیر بیمه، مؤسسه‌های تحقیقاتی و تأمین‌کنندگان دارو، اطلاعات به راحتی و با هزینه کم به اشتراک گذاشته می‌شود.

علی‌رغم افزایش تمرکز بر امنیت پرونده‌های الکترونیکی سلامت و تلاش شهرهای بزرگ سراسر جهان برای بهبود زیرساخت‌های امنیتی و دسترسی در قالب شهرهای هوشمند، دستبرد و نقض حریم خصوصی اطلاعات بیماران همچنان به نحوی فراگیر از دغدغه‌های مهم پیش روی سامانه‌های الکترونیکی سلامت است. استفاده و افشای غیرمجاز داده‌ها منجر به ناامنی‌های جسمی و روانی برای افراد جامعه می‌شود [۳].

غالباً حریم خصوصی را به عنوان یک الزام از محرمانه بودن داده‌ها تلقی می‌کنند؛ زیرا حفظ حریم خصوصی نیاز به اطمینان از محرمانه بودن داده‌ها و کنترل دسترسی را در خود دارد؛ اگر از داده‌ها در مقابل دسترسی غیرمجاز محافظت نشود، حریم خصوصی تضمین نمی‌شود؛ اما علاوه بر این، برای حفظ حریم خصوصی کاربر باید خواسته‌های شخصی، قوانین و مقررات ملی و بین‌المللی و مسائل ویژه‌ای نظیر اجازه دسترسی در موارد اورژانسی باید لحاظ شود؛ بنابراین حفظ حریم خصوصی نیازمند سامانه‌هایی است که نه تنها از سیاست‌های کنترل دسترسی پشتیبانی کنند؛ بلکه باید تنظیمات موضوعی داده‌ها را هم پشتیبانی کنند. بسیاری از فنون حریم خصوصی پیشنهادی تنها در سامانه‌های متمرکز کاربرد دارند و به مشکل اصلی هماهنگ‌سازی داده‌ها با استفاده مؤثر از داده‌ها توجه نمی‌کنند. هدف از کنترل دسترسی حافظ حریم خصوصی آن است که افراد بتوانند بر نحوه دسترسی و چگونگی استفاده از اطلاعاتشان کنترل و نظارت داشته باشند. نیازمندی‌های کنترل دسترسی را می‌توان به صورت امکان وکالت و نمایندگی دادن، بازپس‌گیری نمایندگی، مقیاس‌پذیری، کنترل دسترسی ریزدانه، اعمال اصل حداقل مجوزها، انعطاف‌پذیری و تحمل عدم قطعیت دسته‌بندی کرد.

زنجیره بلوک یک پایگاه داده توزیع‌شده است که فهرستی از رکوردها را به صورت بلوک نگهداری می‌کند و آن‌ها را از خطرات مداخله و دستکاری ایمن نگه می‌دارد. هر بلوک یک چکیده حفاظت‌شده از بلوک‌های پیشین را در خود دارد و این‌گونه امنیت رکوردها را فراهم می‌کند. زنجیره بلوک به صورت ذاتی در برابر دستکاری و تغیر داده‌ها مقاوم بوده و داده‌های رمز شده در بلوک‌ها قابل‌تغییر نمی‌باشند. علاوه بر استفاده از رمزنگاری، یکی دیگر از راهکارهای دستیابی به امنیت داده‌ها در زنجیره بلوک استفاده از قراردادهای هوشمند است. قرارداد هوشمند امکان ایجاد تراکنش‌های معتبر بدون واسط را فراهم می‌کند. این تراکنش‌ها قابل‌پیگیری، مطابق الگوریتم مشخص و توافق شده و غیرقابل‌برگشت هستند.

در این مقاله سامانه‌ای برای مدیریت پرونده الکترونیکی سلامت مبتنی بر زنجیره بلوک و قراردادهای هوشمند را معرفی می‌کنیم. در این سامانه مالکیت پرونده را به شخص بیمار سپرده‌ایم. در ادامه پس از مروری بر کارهای پیشین در بخش ۲، روش پیشنهادی را در بخش ۳ معرفی می‌کنیم. سپس در بخش ۴ به مقایسه بارکارهای مرتبط می‌پردازیم و نهایتاً در بخش ۵ مقاله را جمع‌بندی می‌کنیم.

۲ کارهای پیشین

در این بخش کارهای مرتبط با پرونده‌های سلامت الکترونیک را با تأکید بر کنترل دسترسی بررسی می‌کنیم. این بررسی به دو بخش ۱.۲ بدون استفاده از زنجیره بلوک و ۲.۲ با کمک از آن تقسیم می‌شود که در ادامه می‌آید.

۱.۲ بدون استفاده از زنجیره بلوک

یکی از مسائلی که در سامانه‌های مربوط به‌سلامت و درمان وجود دارد، تعداد زیاد کاربران است. برای حل این مشکل از کنترل دسترسی نقش-مبنا (RBAC [2]) در ترکیب با کنترل دسترسی خصیصه-مبنا (ABAC [3]) استفاده‌شده است [۴]. در [۵] مدلی پیشنهاد شده است که کنترل دسترسی مبتنی بر گروه (TMAC [4]) و (RBAC) را ترکیب می‌کند. برای بیان قوانین در یک بخش و وجود گروه‌های مختلفی که در یک بیمارستان وجود دارد از ایده‌های مطرح در مدل (TMAC) استفاده شده است. در صورتی که یک عامل بیمارستانی بر اساس نقش خود به تیمی تعلق داشته باشد مجوزهای همان گروه، بر اساس شرایط مکانی به او تعلق می‌گیرد؛ بنابراین اعطای مجوزهای لازم به افراد درون گروه، بر اساس اطلاعات زمینه‌ای صورت می‌پذیرد.

مدل ارائه‌شده در [۶] در کنار در نظر گرفتن حریم خصوصی بیماران به عنوان یکی از مهم‌ترین نیازمندی‌های کنترل دسترسی، بر روی برطرف کردن مسئله دسترسی به پرونده بیمار توسط پزشک بر اساس موقعیت فیزیکی پزشک متمرکز شده است. مسئله تشخیص شرایط اضطراری و اعطای دسترسی موقت به پزشک حاضر و همچنین مسئله اعطای وکالت دسترسی همه یا بخشی از حقوق دسترسی یک عامل بیمارستانی به عامل بیمارستانی دیگر، در قالب خانواده مدل کنترل دسترسی تفویض مبتنی بر گروه (TbDAC [5]) ارائه شده است. مدل ارائه شده در [۷]، از

[1] Electronic Health Record

[2] Role Based Access Control [3] Attribute-based access control [4] Team Based Access control [5] Team-based Delegation Access Control

زمانی که اولین سند برای بیمار در سامانه (HER) ثبت می‌شود، وی قادر است به صورت پویا نیازمندی‌های حریم خصوصی‌اش را در قالب (RBAC) و (BLP [1]) تعریف کند. برای دست‌یابی به کنترل دسترسی ریزدانه، انعطاف‌پذیری بالا و مقیاس‌پذیری به طور گسترده در [۸] از ویژگی‌های رمزنگاری خصیصه مبنا (ABE [2]) در سامانه ذخیره‌ساز ابری استفاده شده است. در [۸]، سه الزام امنیتی برآورده شده است: محرمانه بودن اطلاعات، مقاومت در برابر تقلب و حریم خصوصی خط‌مشی‌ها.

۲.۲ با کمک زنجیره بلوک

در روند بررسی و حل مشکلات امنیتی مدت زمان زیادی بر روی آسیب‌پذیری پایگاه‌های داده بیمارستان‌ها و بیمه‌ها کار شده است که نهایتاً بتوانند مسئله محرمانگی را پوشش دهند [۹]. از آنجا که این نهادها فقط مسئول حفظ و نگهداری اطلاعات هستند، صحت اطلاعات به مسئله جدی دیگری تبدیل شده است. در مدل ارائه شده در [۱۰] با کمک دو نوع از معاملات [3] T_{access} و T_{data} کنترل دسترسی به صورت خودکار صورت می‌گیرد و دیگر نیاز به اعتماد به شخص ثالثی ندارد. در [۱۱] مدلی ارائه شده است که با استفاده از زنجیره بلوک و مطابق با قوانین (HIPAA [4]) عمل می‌کند. در این روش، پرونده‌های بیماران در بلوک‌ها ذخیره نمی‌شود بلکه شاخص‌های پرونده بیمار با استفاده از توابع درهم‌سازی در بلوک‌ها نگه‌داری می‌شود. در [۱۲] رویکردی در نظر گرفته شده است که با کمک کارت‌های هوشمند و اثبات هیچ دانشی (ZKP [5]) امکان احراز هویت را به افراد ذینفع فراهم می‌سازد و آنان به‌وسیله قراردادهای هوشمند و رمزگذاری مجدد پروکسی امکان استفاده از خدمات را پیدا می‌کنند. یک کنترل دسترسی با کمک قرارداد هوشمند و سپس کنترل دسترسی سیستمی با (ABAC) بررسی خواهد شد [۱۳].

در شرایط اضطراری بیمار نمی‌تواند روند کنترل دسترسی را مدیریت نماید. برای رفع مشکل و رسیدگی به شرایط اضطراری مدل [۱۴] بر بستر زنجیره بلوک ارائه شده است تا بیمار بتواند با بهره‌مندی از مزایای بالقوه آن، شرایط خاص را مدیریت نماید. در مدل ارائه شده در [۱۵] به جای رمزگذاری اطلاعات ذخیره‌شده بر روی زنجیره بلوک با کلید بیمار، از یک کلید اشتراکی بین بیمار و پزشک استفاده می‌شود. این کلید توسط الگوریتم (SIFF) [۱۶]، (AES256) و تبادل کلید DiffieHellman ساخته می‌شود. نهادهای مشروع نیز پس از فوت بیمار توانایی بازسازی کلید را دارند.

بدون استانداردهای مشترک برای جمع‌آوری اطلاعات، هویت افراد می‌تواند حتی از یک ارائه‌دهنده به ارائه‌دهنده دیگر متفاوت باشد [۱۷]. در [۱۸] هویت دیجیتالی برای فرد، سازمان یا وسایل الکترونیکی تعریف شده است. این هویت بر اساس ویژگی‌ها، حساب‌های بانکی و پرونده‌های پزشکی تعریف می‌شود؛ همچنین با کمک زنجیره بلوک از تغییرات و حذف اطلاعات جلوگیری شده است. شناسه غیرمتمرکز (DID [6]) یک شناسه هویتی مستقل از کاربرد و استاندارد شده توسط (W3C [7]) که معمولاً با کمک زنجیره بلوک پیاده‌سازی می‌شود، این شناسه می‌تواند جایگزین شناسه کاربری‌های معمول شود تا امنیت و حریم خصوصی افراد را تأمین نماید. پیاده‌سازی متن‌باز شناسه غیرمتمرکز در پروژه (Indy [8]) انجام شده است. در این سیستم هر کاربر دو نوع DID دارد. اولی از طرف نهادهای دولتی قابل تأیید است و دیگری یک شناسه کور شده است که برای حفظ حریم خصوصی بر بستر یک رابطه دیجیتالی استفاده می‌شود [۱۹].

در [۲۰] برای صرفه‌جویی در هزینه‌های مختلف، تمامی اطلاعات پزشکی بیماران در بلوک‌ها و به صورت متنی رمز شده قرار می‌گیرد؛ اما اطلاعات چندرسانه‌ای به صورت فهرستی رمز شده از محل نگه‌داری اطلاعات در بلوک‌ها قرار می‌گیرند.

۳ روش پیشنهادی

در این مقاله با استفاده از معماری چندلایه تلاش نموده‌ایم کنترل دسترسی، محرمانگی و حریم خصوصی بیمار را حفظ کنیم. در لایه اول، بیمار با تنظیم قراردادهای هوشمند پیش‌بینی شده مطابق دلخواه خود به صورت خصیصه‌مبنا (ABAC) مشخص می‌کند که چه کسانی به داده‌هایش دسترسی دارند. در لایه دوم، بیمار (مالک اطلاعات) مجوز کنترل دسترسی را تائید می‌نماید و در لایه بعدی اطلاعات با کمک الگوریتم AES256 رمز شده‌اند. در طراحی این قراردادها و مدیریت کلید رمزنگاری، مسائلی نظیر افراد زیر سن قانونی، شرایط اضطراری و بعد از فوت مد نظر قرارگرفته است. در ادامه جزئیات روش پیشنهادی به صورت کامل تشریح می‌شود (شکل ۲).

۱.۳ کاربران و الزامات سیستم

در سامانه پیشنهادی، هر کاربر می‌تواند نقش‌های متفاوتی داشته باشد. هر نقش مجموعه‌ای از الزامات خاص خود را می‌طلبد تا بتواند حریم خصوصی خود را در سامانه به نحو احسن کنترل کند. بر اساس مطالعات صورت پذیرفته توسط پژوهشگران این حوزه و بررسی‌های میدانی انجام شده [۲۱] می‌توان الزامات کنترل دسترسی در محیط‌های سلامت را به سه دسته اصلی تقسیم نمود:

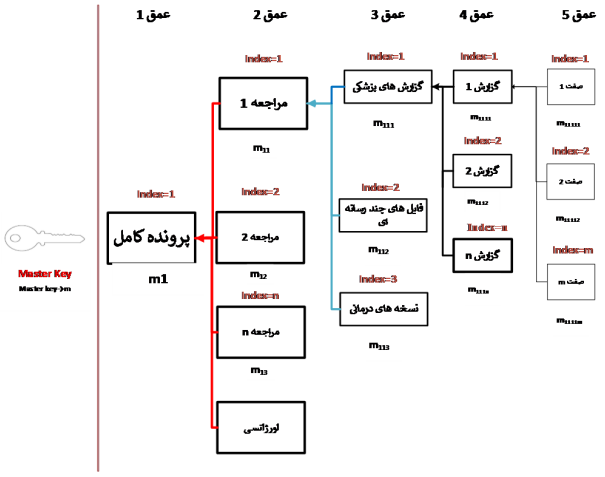
(۱) برای بیماری که اسناد به آن‌ها اشاره می‌کند.
(۲) برای سازمان‌های مراقبت بهداشتی که داده‌ها را مدیریت می‌کنند.
(۳) برای اعمال قوانین محلی، ملی، بین‌المللی و کسب اجازه بیمار

در این مقاله تمرکز اصلی ما بر روی بخش بیمار است، جهت سهولت راه‌اندازی سیستم روابط درون سازمانی را به خود سازمان‌های بهداشتی واگذار نموده‌ایم. همچنین روابط مابین سازمان‌های بهداشتی را بر اساس رضایت بیمار در صورت نیاز پیش خواهیم برد.

الزامات بیمار:

[1] Bell–LaPadula [2] Attribute -based Encryption [3] transaction [4] Health Insurance Portability and Accountability Act [5] Zero-Knowledge Proof [6] Decentralized Identifier

[7] https://www.w3.org/TR/did-core [8] https://github.com/hyperledger/indy-sdk



شکل ۱. تفکیک پرونده پزشکی بیمار

(۱) مالک داده‌ها است.
(۲) در هر زمان‌بندی باید بتواند دسترسی‌ها را تغییر دهد.
(۳) باید بتواند اسناد خود را از موارد خاص پنهان کند.

۲.۳ تفکیک پرونده الکترونیکی سلامت

به منظور مدیریت بهتر پرونده‌های الکترونیکی سلامت و اعمال کنترل دسترسی ریزدانه نیازمند تقسیم پرونده به بخش‌های متفاوتی خواهیم بود، در این مقاله یک کلید اصلی وجود دارد که در بالاترین سطح (کل پرونده‌ها) قرار می‌گیرد. در سطح بعدی بر اساس مراجعه بیمار به مرکز درمانی (پزشک) و مشابه روند درمان معمول، یک پرونده جدید به وجود می‌آید. در گام‌های بعدی پرونده به زیربخش‌های مختلف بر اساس نوع اطلاعات (متنی یا چندرسانه‌ای) و مجموعه‌ای از صفات تعریف‌شده، تفکیک می‌شود. (هر بیمار یک پزشک اصلی دارد که زیر نظر ایشان یک پرونده از خلاصه وضعیت بیمار ایجاد می‌گردد تا در مواقع اورژانسی بتواند روند درمان بیمار را پیش برد) (شکل ۱).

۱.۲.۳ اطلاعات هویتی

همراه سایر اطلاعات پزشکی بیمار بخشی به عنوان اطلاعات هویتی بیمار داریم که اطلاعاتی نظیر نحوه سرپرستی سایر افراد تحت پوشش بیمار، سرپرستان قانونی وی، اطلاعات بیمه درمانی و ... در آن وجود دارند. به منظر دسترسی به سابقه تغییرات، با به‌روزرسانی این اطلاعات لینک دسترسی به مقادیر قبلی پرونده در آن ذکر می‌شود.

۲.۲.۳ پرونده اورژانسی

پرونده اورژانسی بیمار شامل اطلاعاتی نظیر داروهای مصرفی، فهرستی از بیماری‌های مهم (مد نظر کادر پزشکی برای درمان فوری) درجه حاد بودن بیماری و درنهایت حساسیت‌های داروی بیمار است، اطلاعات این بخش توسط یک پزشک متخصص (پزشک اصلی و مورد اعتماد بیمار) تکمیل می‌شود و بر اساس روند درمان بیماری‌های در حال حاضر بیمار طبق دوره‌های از پیش تعیین شده یا معالجات صورت پذیرفته شده باید بروز رسانی شود.

۳.۳ رمزنگاری اطلاعات

رمزنگاری اطلاعات پزشکی بیمار در چند گام صورت می‌پذیرد. بیمار پرونده را از کوچک‌ترین بخش آن طبق شکل ۱ به سمت کل پرونده رمزنگاری خواهد نمود، رمزنگاری با استفاده از الگوریتم AES256 با یک کلید تصادفی است. همچنین محل نگهداری کلیدها به همراه شناسه‌های که آنان را از یکدیگر متمایز می‌کند در دستگاه مورد استفاده کاربر مانند تلفن همراه وی خواهد بود که باز به تشخیص بیمار می‌توان فایل پشتیبان کلیدها را در هر مکان امن دیگری منتخب خود کاربر است، ذخیره نمایند.

۱.۳.۳ رمزنگاری و مدیریت کلید پرونده اورژانسی

پرونده اورژانسی بیمار نیز به روش AES256 رمز خواهد شد، اما تفاوتی که با سایر قسمت‌ها دارد در این است که کلید پرونده اورژانسی بیمار بیومتریک است و از طریق اسکن اثرانگشت بیمار به دست خواهد آمد؛ که طبق الگوی توابع درهم‌سازی [1] تبدیل به یک عبارت ۲۵۶ بیتی می‌شود، بعد از گذر از شرایط بحرانی نسبت به وضعیت بیمار تصمیم‌گیری از جانب وی یا افراد مورد اعتمادش صورت می‌گیرد.

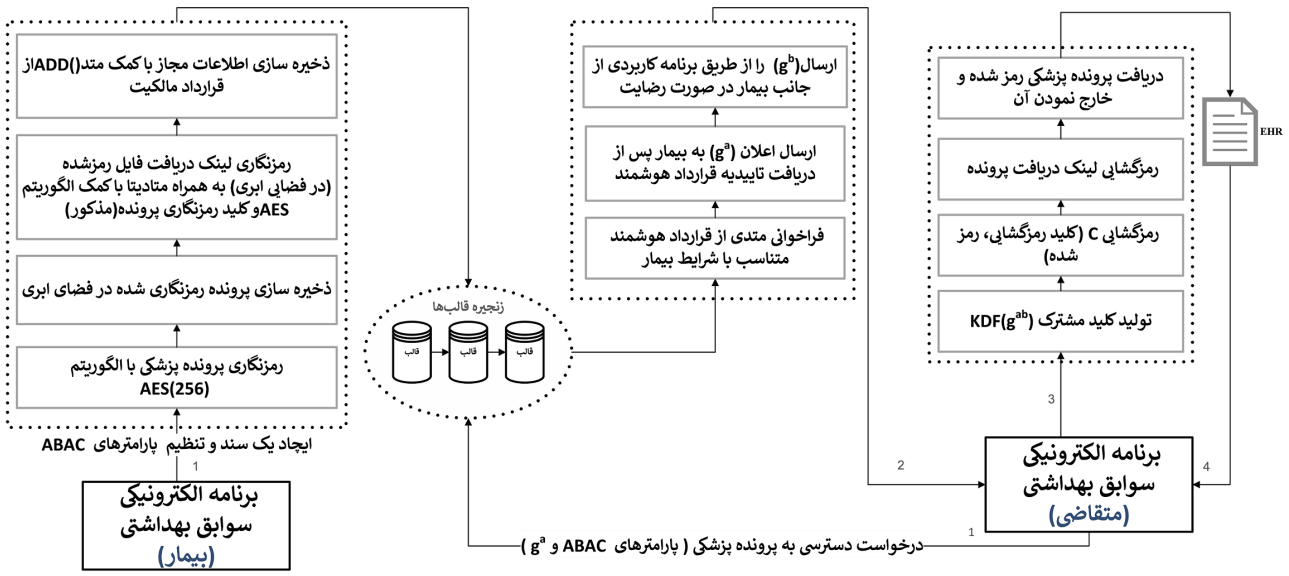
۴.۳ ذخیره‌سازی اطلاعات

به منظور مدیریت بهتر پرونده‌های الکترونیکی سلامت باید محل و نحوه ذخیره‌سازی اطلاعات را مشخص نماییم. پرونده بیمار از فایل‌های متنی و چندرسانه‌ای تشکیل شده است. اگر بنا باشد تمام محتویات پرونده بیمار در بلوک ذخیره کنیم، با حجم زیادی از اطلاعات روبرو خواهیم شد که در نهایت منجر به کاهش کارآیی سیستم می‌گردد.

وظیفه ذخیره‌سازی اطلاعات رمز شده بر عهده بیمار است، با پایان روند درمان مثلاً مرکز درمانی مربوط با ترخیص بیمار و در صورت نیاز تعیین نوبت ملاقات مجدد گزارش درمان را به همراه یک چکیده امضاشده [2] در اختیار بیمار قرار می‌دهد. چکیده امضاشده جهت حصول اطمینان برای هر دو طرف رابطه است: عدم انکار برای مرکز درمانی و جلوگیری از دستکاری توسط بیمار.

اطلاعات متادیتا [3] در دو دسته به صورت آشکارا و رمز شده قرار می‌گیرند. اطلاعاتی نظیر عنوان پرونده، نوع آن، تاریخ پرونده آشکارا ذخیره می‌شوند، اما اطلاعاتی که ممکن است موجب نقض حریم خصوصی بیمار شوند به صورت رمز شده قرار می‌گیرند. هر پرونده نیز که در فضای ابری ذخیره می‌گردد یک URL [4] برای دسترسی آسان‌تر خواهد داشت که به صورت رمز شده همراه سایر متا دیتا در زنجیره بلوک ذخیره می‌گردد و لازم به ذکر است که URL و سایر متادیتا ناقص حریم خصوصی هر پرونده با خود کلید خود پرونده رمز می‌گردند.

[1]hash function [2]hash-based signature [3]metadata [4]Uniform Resource Locator



شکل ۲. عملکرد سامانه (نحوه ذخیره اطلاعات توسط بیمار در فضای ابر و سپس ذخیره اطلاعات پرونده به زنجیره بلوک توسط بیمار – نحوه دریافت اطلاعات توسط متقاضی از زنجیره بلوک با کمک قرارداد هوشمند و رمزگشایی آن)

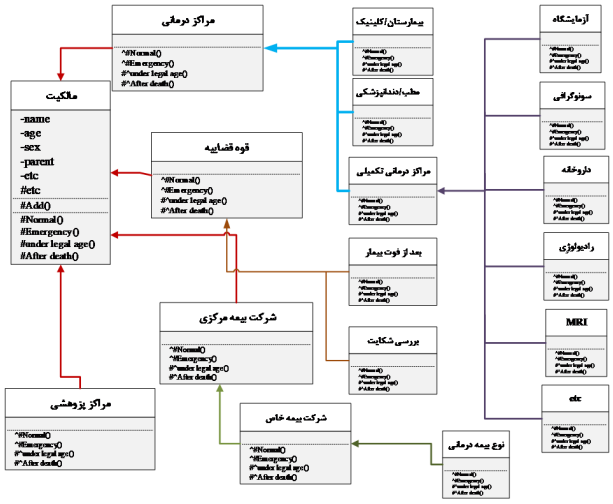
۵.۳ قراردادهای هوشمند

قراردادهای هوشمند اولین لایه کنترل دسترسی و حفاظت از حریم خصوصی را برای بیماران انجام می‌دهند. یکی از مهم‌ترین علت‌های استفاده از قرارداد هوشمند حذف طرف ثالث از بررسی و اعطای مجوز است. با کمک قرارداد هوشمند بیمار می‌تواند اطمینان حاصل نماید که مجوزهای صادره از طرف وی به صورت قطعی اعمال شده‌اند و قابل تغییر نخواهند بود. همچنین دسترسی‌هایی که به پرونده بیمار صورت گرفته شده است به صورت تراکنش در زنجیره بلوک موجود و قابل استناد است که برای ما شفافیت‌پذیری و نظارت‌پذیری را به همراه خواهد داشت.

قراردادهای هوشمند اولین لایه کنترل دسترسی و حفاظت از حریم خصوصی را برای بیماران انجام می‌دهند. درخواست دسترسی به پرونده در ابتدا به قرارداد هوشمند مناسب ارائه می‌شود و قرارداد با توجه به ترجیحاتی که توسط بیمار تعیین شده است، نوع و خصیصه‌های متقاضی و شرایط موجود تصمیم می‌گیرد که اجازه دسترسی به بخش مورد نظر از پرونده به صورت بالقوه وجود دارد یا خیر. در صورت مثبت بودن، آدرس ذخیره‌سازی بخش به صورت رمز شده، چکیده محتوا (برای صحت‌سنجی) و نحوه دریافت کلید رمزگشایی در اختیار متقاضی قرار می‌گیرد. این کار مستقیماً توسط بیمار یا به صورت غیرمستقیم از طریق نمایندگان انجام می‌شود که در بخش بعد توضیح داده می‌شود.

برای سهولت تعیین ترجیحات توسط بیمار، قراردادهایی ویژه کنترل دسترسی انواع مختلف عوامل (مانند شرکت‌های بیمه، مراکز پژوهشی و درمانی و نهادهای قضایی) و بررسی خصیصه‌های آن‌ها در نظر گرفته‌شده است (شکل ۲) و عامل درخواست‌کننده درخواست خود را به قرارداد متناسب می‌فرستد.

در این سلسله‌مراتب قراردادها بیمار می‌تواند تصمیم‌گیری نماید که



شکل ۳. سلسه‌مراتب قراردادها (#: متد محافظت شده[1]، ۸: کلاس ارثبری[2]، →: ارثبری و متدها بدون بدنه هستند و با توجه به شرایط قراردادها بازنویسی[3] می‌شوند.)

جزئیات هر قرارداد تا چه حد مشخص باشد و بر اساس سلایق خود قرارداد هوشمند را تنظیم نمایید و یا در صورت عدم تکمیل این قراردادها لینک دسترسی به قوانین والد در آنان قرار می‌گیرد تا در صورت نیاز قوانین والد خود را اجرا نمایند. همچنین به منظور افزایش حریم خصوصی بیمار و همچنین بهره‌وری کامل از قرارداد هوشمند از ثبت هرگونه اطلاعات هویتی و پزشکی بیمار پرهیز کرده‌ایم.

۱.۵.۳ قرارداد مالکیت

اولین و برجسته‌ترین قرارداد هوشمندی که بیمار با آن سروکار خواهد داشت قرارداد مالکیت است، این قرارداد شامل ۵ رویه است، اولین آنان

[1]protected method [2]inheritance [3]override

متد Add است که با کمک آن مالک قرارداد هوشمند اطلاعات مربوط به پرونده پزشکی خود را بر روی زنجیره بلوک ذخیره می‌کند و چهار رویه دیگر دریافت اطلاعات شرایط مختلف را پوشش می‌دهند: درخواست دسترسی در شرایط عادی، دسترسی به پرونده بیمار قبل از سن قانونی، دسترسی در شرایط اورژانسی و دسترسی پس از مرگ. مثلاً در شرایط اضطراری که بیمار قادر به شناسایی محیط و تصمیم‌گیری نیست، درخواست باید از طریق فراخوانی رویه شرایط اورژانسی انجام شود.

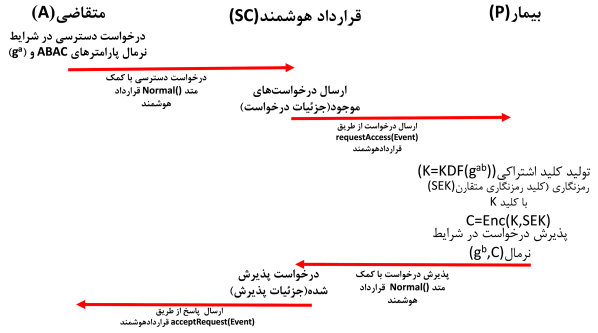
در اولین سطح از ارث‌بری نحوه دسترسی مراکز مختلف به اطلاعات بیمار مورد بررسی قرار می‌گیرد، رویه‌ها خصیصه‌های درخواست‌کننده و مورد درخواست را با ترجیحات بیمار (ABAC) تطبیق می‌دهند و در صورتی که ناسازگار باشند درخواست را رد می‌کنند. در غیر این صورت، آن را از طریق ثبت کردن یک رویداد روی زنجیره بلوک برای تأیید در اختیار بیمار (بسته به شرایط نمایندگان وی) می‌گذارند (جزئیات این کار در ادامه توضیح داده می‌شود.) با توجه به روابط ارث‌بری قراردادها، بیمار می‌تواند میان مجوزهای سازمان‌های مختلف تمایز ایجاد نماید. همچنین اگر رویه‌ی از جانب بیمار تکمیل نشود بر اساس شرایط پیش‌فرض عمل می‌شود.

۲.۵.۳ کسب اجازه و توزیع کلید

در این بخش روند کسب اجازه و انتقال کلید رمزگشایی را از سمت مالک پرونده شرح می‌دهیم. متقاضی پرونده (مرکز درمانی) درخواست خود را طبق پروتکل زیر به قرارداد هوشمند می‌دهد و قرارداد واسطه میان مالک و متقاضی است.

روند کار بدین صورت است که متقاضی در هنگام ارسال درخواست، یک زوج کلید دیفی هلمن می‌سازد و همراه با اطلاعات ورودی (پارامترهای ABAC) به رویه بررسی درخواست دسترسی) رویه (Normal) می‌دهد. در صورتی که متقاضی واجد شرایط بود، قرارداد هوشمند یک رویداد (requestAccess) در زنجیره بلوک ثبت می‌کند که ضمن اعلام تأیید مجوزهای متقاضی توسط قرارداد هوشمند، کلید عمومی را در اختیار بیمار می‌گذارد.

بیمار از طریق نرم‌افزاری که در اختیار دارد، متوجه رویداد و درخواست می‌شود. اگر درخواست پیرو مراجعه و با رضایت بیمار است، آن را تأیید می‌کند. در این صورت یک زوج کلید دیفی هلمن جدید ایجاد می‌کند و با استفاده از کلید عمومی دیفی هلمن متقاضی یک کلید متقارن مشترک می‌سازد. سپس کلید رمزگشایی بخش مورد درخواست از پرونده بر روی ابر را با این کلید مشترک رمز می‌کند و به همراه کلید عمومی دیفی هلمن خود به قرارداد هوشمند از طریق رویه Normal() می‌فرستد. قرارداد هوشمند نیز با دریافت تأییدیه، این اطلاعات را به همراه رمز شده URL پرونده در فضای ابری در قالب یک رویداد (acceptRequest) بر روی زنجیره بلوک ثبت می‌کند. متقاضی از رویداد مطلع می‌شود، کلید مشترک دیفی هلمن را می‌سازد، کلید رمزگشایی پرونده و URL را رمزگشایی می‌کند و نهایتاً به بخش از پرونده که درخواست کرده بود دسترسی پیدا می‌کند.



شکل ۴. تبادل کلید بین متقاضی و بیمار با کمک قرارداد هوشمند در شرایط نرمال

۳.۵.۳ تسهیم راز و استفاده از نمایندگان

در شرایط زیر ممکن است بیمار به شبکه متصل نباشد و/یا نتواند کلید رمزگشایی پرونده را مستقیماً به متقاضی تحویل دهد:

(۱) سن پایین‌تر از سن قانونی است، پس توانایی تصمیم‌گیری و صدور و کنترل مجوزها را ندارد.
(۲) در شرایط نیست که توان تصمیم‌گیری یا فعالیت داشته باشد.
(۳) فوت‌شده است.

در شرایط اورژانسی خلاصه پرونده در اختیار اورژانس قرار می‌گیرد؛ اما در صورت استمرار وضعیت نامساعد بیمار (حالت ۲ فوق) یا هر یک از دو مورد دیگر، از فرایندی که در ادامه ذکر می‌شود استفاده می‌کنیم. برای فراهم کردن امکان دسترسی به پرونده در این شرایط، کلید رمزنگاری AES256 را از قبل بین نمایندگان بیمار به صورت دو از چند تسهیم می‌کنیم تا در شرایط مورد نیاز بتوانند آن را بازسازی کنند. تسهیم راز دو از چند برای جلوگیری از سوءاستفاده است تا لازم باشد دستکم دو عامل در بازسازی کلید مشارکت داشته باشند. تصمیم‌گیری در مورد اینکه آیا خود بیمار باید کلید رمزگشایی را به متقاضی بدهد یا خیر؛ و نیز تشخیص نمایندگان بیمار چنانکه پیش‌تر ذکر شد، توسط قراردادهای هوشمند انجام می‌شود.

پروتکل تبادل کلید شرح داده‌شده شرایط عادی را می‌توان با نمایندگان بیمار به منظور دستیابی رمز شده به سهم آن‌ها از کلید رمزگشایی نیز انجام داد. بدین صورت که متقاضی هنگام اجرای قرارداد هوشمند رویه مخصوص درخواست دسترسی متناسب با شرایط بیمار را فراخوانی می‌کند. در این مرحله، رویداد درخواست برای همه نمایندگان بیمار صادر می‌شود. هر یک از این افراد در صورت تأیید درخواست، سهم خود از کلید را با روش پیش‌تر توضیح داده‌شده رمز می‌کنند و از طریق قرارداد هوشمند به متقاضی می‌دهند. در صورتی که لااقل دو نماینده این کار را کرده باشند، متقاضی می‌تواند کلید را بازسازی کند.

پروتکل شرح داده‌شده به واسطه قرارداد هوشمند صورت می‌گیرد و حتی اگر فرض بر آن باشد که مهاجم بتواند بدون اجرای قرارداد هوشمند به URL رمز شده پرونده دسترسی پیدا کند، کلیدی ندارد که بتواند آن را رمزگشایی کند. علاوه بر این، سوابق دسترسی به پرونده بیمار و حتی نمایندگانی که درخواست‌ها را تأیید کرده‌اند نیز به صورت شفاف بر روی

زنجیره بلوک ثبت می‌شود و امکان بازرسی وجود دارد. با توجه به اینکه فرکانس چنین درخواست‌هایی بالا نیست، سرباری بر روی زنجیره بلوک ندارد. همچنین تأخیر ثبت و رسیدگی به رویدادها (دو تراکنش) نیز در کاربرد دسترسی به پرونده سلامت قابل تحمل است.

۶.۳ ابطال کلید

زمانی که دسترسی صورت می‌گیرد و کلید به کادر درمان سپرده می‌شود ممکن است کادر درمان بلافاصله اطلاعات را دریافت و از رمز خارج نمایند؛ و نمی‌توان این اطلاعات را به‌سادگی باز پس گرفت. باید توجه داشته باشیم که هرچند ممکن است اقلامی به پرونده سلامت افزوده شوند اما اطلاعات موجود تغییر نمی‌کنند. پزشک در طول درمان به‌طور عادی و بدون دخالت سامانه پیشنهادی به پرونده ذخیره‌شده در محل خود دسترسی کامل دارد و تغییرات را مشاهده و بررسی می‌کند. زمانی که لازم است به بخشی دیگر از پرونده دسترسی داشته باشد، بیمار جزئی‌ترین کلید را از آن بخش در اختیار پزشک قرار می‌دهد و حتی در صورتی که پرونده درخواستی در حال تکمیل شدن باشد پزشک درخواست دهنده به موارد تکمیلی دسترسی ندارد.

تنها استثنا، پرونده اورژانسی است که همواره به‌روز نگه داشته می‌شود. با هر بار بروز رسانی، پرونده قدیمی از فضای ابری حذف می‌شود؛ پرونده جدید با URL جدید ذخیره می‌شود؛ و آدرس جدید در قرارداد هوشمند ثبت و در اختیار متقاضی احتمالی قرار می‌گیرد.

در پایان یک درمان بر اساس مقررات جاری در خصوص نگهداری اطلاعات سلامت و نیز با توجه به نظر بیمار فقط مواردی که لازم باشد از پرونده نزد مرکز درمانی نگه داشته می‌شود و سایر موارد باید امحا شود. در صورت تخلف نیز پیگیری این موضوع باید از طریق قانونی انجام شود و سوابق دسترسی ثبت‌شده روی زنجیره بلوک می‌تواند به عنوان سند استفاده شود.

۴ ارزیابی

در این بخش ابتدا سامانه را با سایر کارهای مرتبط مقایسه خواهیم نمود و در ادامه شکاف‌های ارتباطی، نحوه دسترسی‌پذیری به سامانه و هزینه‌های ناشی از این سامانه را بررسی می‌کنیم.

۱.۴ مقایسه کیفی

با بررسی مدل‌های کلاسیک [۴–۷] به سختی می‌توان اصل حداقل مجوزها (فقط میزانی از مجوز دسترسی به اطلاعات را در اختیار متقاضی قرار دهیم تا بتواند کار خود را به پایان برساند) و کنترل دسترسی ریزدانه (تفکیک مجوز دسترسی برای هر بخش پرونده به صورت مستقل) را اعمال نمود؛ و غیرقابل انعطاف و مقیاس ناپذیر (با حجم بالای اطلاعات و روابط سازمانی مشکل خواهند داشت) هستند؛ بنابراین می‌توان گفت هیچ یک از این مدل‌ها به تنهایی نمی‌توانند نیازهای کنترل دسترسی در محیط را برطرف کنند. مسأله مهم دیگر در روش‌های کلاسیک بررسی شده آن است که صدور و لغو مجوزها به دست بیمار نیست و در عوض، باید انتظار داشته باشیم که سامانه حافظ حریم خصوصی بیماران باشد.

در مواردی که از رمزنگاری ABE استفاده شده است (مانند [۸])، مزیت رعایت اصل حداقل مجوزها و کنترل دسترسی ریزدانه را داریم ولی از معضل عدم کارایی و عدم وجود مکانیزم لغو دسترسی رنج می‌بریم. در حالی که در روش پیشنهادی اعطای هر دسترسی مستلزم بررسی برخط توسط قرارداد هوشمند و اعلام رضایت بیمار است. مدل [۱۰] فقط با کمک انجام معاملات سعی در برقراری حریم خصوصی نموده است و انعطاف‌پذیری تحت تأثیر قرار گرفته است. همچنین اگر فقط به کنترل دسترسی مبتنی بر قراردادهای هوشمند متکی باشیم، هر فردی که به داده‌های زنجیره بلوک دسترسی داشته باشد می‌تواند قرارداد(ها) را دور بزند و به پرونده بیمار دست یابد.

روش‌های [۱۱]، [۱۲] و [۱۳] تا حد بسیار خوبی حافظ حریم خصوصی بیمار هستند و با کمک قراردادهای هوشمند و مالکیت بیمار توانسته‌اند کنترل دسترسی ریزدانه، اصل حداقل مجوزها و انعطاف‌پذیری را به وجود آورند، ولی به شرایط مختلف سیستم مانند شرایط اورژانسی و بعد از فوت بیمار توجه چندانی نداشته‌اند. سایر مقاله‌های بررسی‌شده ([۱۴، ۱۵]) به صورت موردی شرایط اضطراری و یا بعد از فوت بیمار را مدنظر خود قرار داده‌اند. همچنین در روش‌های مبتنی بر زنجیره بلوک بررسی‌شده، به کاربران سیستم فقط از جایگاه بیمار پرداخته و به سایر نقش‌ها و شرایط احتمالی آنان توجهی نشده است.

یکی از نقاط قوت روش پیشنهادی آن است که با استفاده از دو لایه کنترل دسترسی، بیمار می‌تواند ضمن تعیین کردن شرایط دسترسی عمومی از طریق قرارداد هوشمند، کنترل کاملی روی پرونده خود داشته باشد و به راحتی و در لحظه تک‌تک دسترسی‌ها به پرونده پزشکی‌اش کنترل نماید. خلاصه‌ای از شاخص‌های کیفی روش پیشنهادی در مقایسه با سایر روش‌ها در جدول ۱ آمده است.

۲.۴ دسترسی‌پذیری

شکاف‌های ارتباطی و چالش‌های به اشتراک‌گذاری اطلاعات، مانع جدی برای نوآوری در مراقبت‌های بهداشتی و کیفیت مراقبت از بیمار می‌باشند. ارائه‌دهندگان، بیمارستان‌ها، شرکت‌های بیمه و حتی ادارات در همان سازمان‌های بهداشتی، قطع ارتباط ناشی از تأخیر یا عدم جریان اطلاعات را تجربه می‌کنند. بیماران معمولاً در مراکز مختلف نظیر کلینیک‌های خصوصی، مراکز مراقبت فوری منطقه‌ای، بیمارستان‌های سازمانی و درمان از راه دور مراقبت می‌شوند. یک ارائه‌دهنده ممکن است فعالیت‌های مربوط به‌سلامت صدها یا بیشتر بیمار را دنبال کند؛ بنابراین دستیابی به اطلاعات به‌روز و کامل پزشکی در صورت تقاضای بیمار پرزحمت است. درروش پیشنهادی با ذخیره اطلاعات در زنجیره بلوک و ابر، بدون نیاز به سرور مرکزی عمل می‌شود. همچنین همه اعضای شبکه یک نسخه از اطلاعات زنجیره بلوک را در اختیار دارند؛ بنابراین مشکل دسترسی‌پذیری

جدول ۱.

منابع	پرونده فیزیکی	پرونده الکترونیکی بدون استفاده از زنجیره بلوک								پرونده الکترونیکی با استفاده از زنجیره بلوک						مقاله حاضر
		[۴]	[۵]	[۶]	[۷]	[۸]	[۱۰]	[۱۱]	[۱۲]	[۱۳]	[۱۴]	[۱۵]	
حریم خصوصی	✘	✘	✘	✘	✘	✔	✔	✔	✔	✔	✔	✔	✔
کنترل دسترسی ریزداده	✘	✘	✘	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔
اصل حداقل مجوزها	✘	✘	✘	✘	✘	✔	✘	✔	✔	✘	✔	✔	✔
انعطاف‌پذیری	✘	✘	✘	✘	✘	✘	✘	✔	✔	✘	-	-	✔
مالکیت بیمار	✘	✘	✘	✘	✔	✔	✔	✔	✘	✔	✔	✔	✔
قبل از سن قانونی	-	-	-	-	-	-	✘	✔	✘	✘	-	-	✔
شرایط اضطراری	-	-	-	-	✔	-	✘	✘	✘	✘	✔	-	✔
فوت بیمار	-	-	-	-	-	-	✘	✘	✘	✘	-	✔	✔
از دست رفتن اطلاعات	✘	✘	✘	✘	✘	✘	✔	✔	✔	✔	✔	✔	✔

را بهبود بخشیده‌ایم.

۳.۴ انتخاب نوع زنجیره بلوک

جهت پیاده‌سازی ساز و کار پیشنهادی بر روی زنجیره بلوک عمومی و خصوصی یا کنسرسیومی نظرات متفاوتی وجود دارد که در ادامه آن‌ها را بررسی می‌کنیم:

زنجیره بلوک خصوصی/کنسرسیومی: به دلیل آنکه هر کاربری اجازه حضور در این زنجیره را ندارد می‌توان تجربه بهتری از حفظ حریم خصوصی و امنیت را داشت، همچنین می‌توان تعداد معاملات زیاد و سریع را در سیستم به دست آوریم که جهت حفظ زندگی یک فرد بسیار ارزشمند خواهد بود.

زنجیره بلوک عمومی: بررسی‌های انجام‌شده نشان می‌دهد که ساختارهای خصوصی و کنسرسیومی هزینه بالای بر سازمان‌های درمانی تحمیل خواهد نمود و سازمان‌ها از پذیرش سیستم سر باز خواهند زد. همچنین تجربه نشان داده است که مجری خواستار برپایی قوانین مطابق با منافع خود خواهد بود که ممکن است هم‌راستا با منافع بیمار و ترجیحات وی نباشد.

با توجه به آنچه شرح داده شد ترجیح داده‌ایم سیستم را بر روی زنجیره بلوک عمومی و معروف (اتریوم) پیش ببریم تا هم از اعمال هزینه مازاد بر سیستم جلوگیری شود و هم شخص بیمار تصمیم‌گیرنده نهایی در این سیستم باشد. البته سیستم حاضر را می‌توان بر روی یک زنجیره بلوک خصوصی/کنسرسیومی نیز پیاده‌سازی نمود.

۴.۴ بررسی هزینه‌های سیستم

به‌طور متوسط هر تراکنش استاندارد 85 Gwei [1] سوخت مصرف می‌کند که می‌توان گفت اندازه هر بلوک به طور متوسط شامل ۳۰۰ تراکنش خواهد شد. با توجه به مدت زمان درج یک بلوک، ۱۵ تراکنش در ثانیه انجام می‌شود [2]. همچنین می‌توانیم امیدوار باشیم با جایگزینی الگوریتم اثبات سهام به جای اثبات کار در اتریم مشکلات مقیاس‌پذیری تا حد بسیار خوبی برطرف شوند و شاهد رشد تعداد تراکنش‌ها در ثانیه باشیم.

طبق آمار مرکز آمار ایران [3] پیش‌بینی می‌شود که در حال حاضر ۱۵۰ هزار مرکز درمانی فعال در کشور وجود دارد و با توجه با آمار روزانه مراجعه به مراکز درمانی از هر ۱۰۰۰ ایرانی حداکثر ۲ نفر نیاز به مراقب‌های درمانی دارند (حدود ۱۷۰ هزار بیمار در روز). همچنین حدود ۶۰ میلیون ایرانی از خدمات بیمه درمانی بهره‌مند هستند و می‌توان تخمین زد که روزانه بالغبر ۹۰ هزار درخواست دسترسی شرکت‌های بیمه خواهیم داشت. متأسفانه آمار دقیقی از تعداد شکایات پزشکی و درخواست‌های مراکز پزشکی در دسترس نیست.

با یک تقریب و فرض اینکه برای رسیدگی به هر درخواست دو تراکنش لازم است و یک تراکنش جهت ذخیره‌سازی اطلاعات مورد نیاز است. ۱۱ تراکنش در ثانیه برای این موارد در نظر گرفت. اگر یک تراکنش در ثانیه هم برای مرکز قضایی و پژوهشی در نظر بگیریم، سامانه ما برای استفاده در کشور، به ۱۲ تراکنش در ثانیه نیاز دارد.

بر خلاف سایر سامانه‌های زنجیره بلوکی بررسی‌شده اطلاعات قراردادهای سامانه پیشنهادی ما از نظر حجم اطلاعات که از صاحب قرارداد هوشمند دارد و همچنین حجم کم اطلاعات ذخیره‌شده بر روی زنجیره بلوک می‌توان تعداد تراکنش در ثانیه بیشتری را به دست آوریم. همچنین می‌توان با تنظیم قیمت گس، برای تراکنش‌ها اولویت تنظیم کرد به این صورت که درخواست‌های ثبت پرونده قیمت پیشنهادی پایین‌تری داشته باشند و تراکنش‌های اورژانسی را با پیشنهاد قیمت بالاتر از حد معمول، سریع‌تر پردازش کرد.

[1] 10^{-9} Ether

[2] https://etherscan.io [3] http://yun.ir/5ybo08

۵ نتیجه‌گیری

با طراحی قراردادهای هوشمند و الگوریتم تولید کلید تصادفی به همراه نمایندگان توانسته‌ایم مسائل و مشکلات اشتراک‌گذاری را رفع کنیم. همچنین با تفکیک پرونده پزشکی بیمار به قسمت‌های مختلف و رمزنگاری جداگانه، مراکز و سازمان‌های مرتبط با نظام سلامت فقط می‌توانند به صورت موردی به اطلاعات دسترسی پیدا کنند. اگر چه نگه‌داری پرونده‌های پزشکی در فضای ابری یا پرداخت گس انجام تراکنش‌ها نیازمند صرف هزینه است؛ اما در مقابلِ هزینه‌های ناشی از عدم اعتماد سازمان‌ها و دوباره‌کاری‌های روند درمان و هزینه‌های جانی و مالی که بیماران بابت نقض حریم خصوصی می‌پردازند بسیار اندک است.

مراجع

[1] Ida, Imen Ben, Jemai, Abderrazak, and Loukil, Adlen. A survey on security of iot in the context of ehealth and clouds. in *2016 11th International Design & Test Symposium (IDT)*, pp. 25–30. IEEE, 2016.

[2] Zhang, Peng, Schmidt, Douglas C, White, Jules, and Lenz, Gunther. Blockchain technology use cases in healthcare. in *Advances in computers*, vol. 111, pp. 1–41. Elsevier, 2018.

[3] Atherton, Jim. Development of the electronic health record. *AMA Journal of Ethics*, 13(3):186–189, 2011.

[4] Yarmand, Mohammad H, Sartipi, Kamran, and Down, Douglas G. Behavior-based access control for distributed healthcare systems. *Journal of Computer Security*, 21(1):1–39, 2013.

[5] Hashemibeni, F. Privacy preserving access control in iot for ehealth, Sep. 2017.

[6] Ghofrani, F. Access control system with the power of access to electronic health, Sep. 2017.

[7] Pussewalage, Harsha S Gardiyawasam and Oleshchuk, Vladimir A. An attribute based access control scheme for secure sharing of electronic health records. in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–6. IEEE, 2016.

[8] Zhong, Hong, Zhu, Wenlong, Xu, Yan, and Cui, Jie. Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage. *Soft Computing*, 22(1):243–251, 2018.

[9] Atherton, Jim. Development of the electronic health record. *AMA Journal of Ethics*, 13(3):186–189, 2011.

[10] Zyskind, Guy, Nathan, Oz, et al. Decentralizing privacy: Using blockchain to protect personal data. in *2015 IEEE Security and Privacy Workshops*, pp. 180–184. IEEE, 2015.

[11] Dagher, Gaby G, Mohler, Jordan, Milojkovic, Matea, and Marella, Praneeth Babu. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable cities and society*, 39:283–297, 2018.

[12] Sharma, Bhavye, Halder, Raju, and Singh, Jawar. Blockchain-based interoperable healthcare using zero-knowledge proofs and proxy re-encryption. in *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, pp. 1–6. IEEE, 2020.

[13] Guo, Hao, Li, Wanxin, Nejad, Mark, and Shen, Chien-Chung. Access control for electronic health records with hybrid blockchain-edge architecture. in *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 44–51. IEEE, 2019.

[14] Rajput, Ahmed Raza, Li, Qianmu, Ahvanooey, Milad Taleby, and Masood, Isma. Eacms: Emergency access control management system for personal health record based on blockchain. *IEEE Access*, 7:84304–84317, 2019.

[15] Tian, Haibo, He, Jiejie, and Ding, Yong. Medical data management on blockchain with privacy. *Journal of medical systems*, 43(2):1–6, 2019.

[16] Zheng, Yuliang, Hardjono, Thomas, and Pieprzyk, Josef. The sibling intractable function family (siff): Notion, construction and applications. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, 76(1):4–13, 1993.

[17] Zhang, Peng, Schmidt, Douglas C, White, Jules, and Lenz, Gunther. Blockchain technology use cases in healthcare. in *Advances in computers*, vol. 111, pp. 1–41. Elsevier, 2018.

[18] Schouten, J. Opportunities for blockchain-based identity in healthcare, Oct. 2017.

[19] Windley, Phillip. How sovrin works. *Sovrin Foundation*, pp. 1–10, 2016.

[20] Li, Hongyu, Zhu, Liehuang, Shen, Meng, Gao, Feng, Tao, Xiaoling, and Liu, Sheng. Blockchain-based data

preservation system for medical data. *Journal of medical systems*, 42(8):1–13, 2018.

[21] Buschmann, Frank, Henney, Kevlin, and Schmidt, Douglas C. *Pattern-oriented software architecture, on patterns and pattern languages*. John wiley & sons, 2007.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2022, Volume 20, Number 1 (pp. 48–58)
https://monadi.isc.org.ir

Presented at the ISCISC 2021 in University of Isfahan, Isfahan, Iran

Management of Electronic Health Records with Preservation of Privacy using the Blockchain Technology★

Mahsa Rezaei and Sadegh Dorri Nogoorani *

Faculty of Electrical and Computer Engineering, Tarbiat Modares University, Tehran, Iran

ARTICLE INFO.

Keywords:
Electronic Health Record (EHR), privacy, access control, blockchain, cloud

dor: 20.1001.1.24763047.1401.11.1.6.3

Type: research paper

ABSTRACT

The development and use of electronic health records (EHR) have had remarkable impacts on human life, such as improvements in the quality of medical care, better research results, and enhancements in treatment methods. Despite these improvements, availability, security and privacy concerns have remained to be very important in this field. In this article, we propose a decentralized and distributed system for electronic health records management with the help of the blockchain technology and its potential benefits. In this system, patient information is stored in the cloud. Also, the real owner of the electronic records is the patient, and with the help of smart contracts and encryption, he/she controls how to access his/her health information. In the proposed solution, the problem of sharing and storing the patients' keys has been solved with the help of smart contracts. In addition, we proposed solutions to special cases which are raised by transferring the control of the records to the patients such as permissions for underage patients, in emergency situations, and after the death of the patient. Comparison of the related works shows that the proposed system has solved the problems of competing systems while maintaining a high level of privacy.

★ The ISCISC 2021 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: mahsa_rezaei@modares.ac.ir (Mahsa Rezaei), dorri@modares.ac.ir (Sadegh Dorri Nogoorani)