Information Technology Innovations and Applied Communication
Vol. 4, No. 1, Spring, 2026, Serial No. 9,pp.31-47

A Secure Access Control Scheme in Electronic Health Systems Using Attribute-Based Encryption and dual-blockchain Architecture

Peyman Veysi[1]; Fatemeh MotieShirazi[2]; Zahra MohammadHosseini Taheri[3]; Majid Bayat[*4]

* Associate Professor, Shahed University, Tehran, Iran

(**Received:** 17 March 2026, **Revised:** 24 April 2026, **Accepted:** 06 May 2026, **Published:** 22 May 2026)

ABSTRACT

The rapid evolution of technology has introduced significant challenges to information security and privacy preservation in electronic healthcare (e-health) systems. Efficient management of patient health data storage, sharing, and access represents a critical challenge for these systems. Addressing security concerns necessitates a comprehensive analysis of e-health architectures and communication paradigms prior to intervention. This study identifies the core structural foundations of e-health systems through an analysis of architectural designs over the past decade. Various clinical scenarios were examined, and access conditions for all stakeholders in the e-health healthcare process were defined. A secure, dynamic access control scheme leveraging dual blockchain, attribute-based encryption (ABE), and group signatures is proposed. Evaluation results indicate that the proposed scheme not only satisfies security requirements but also demonstrates acceptable performance and implementability. Security analysis against known attacks on permissioned blockchains revealed full resistance to 68% of attacks, partial resistance to 14%, and vulnerability to 18%.

Keywords: E-health, Access control, Blockchain, Attribute-based encryption, Group signature.

* Corresponding AuthorE-mail: mbayat@shahed.ac.ir

«نوآوری‌های فناوری اطلاعات و ارتباطات کاربردی»
سال چهارم، شماره ۱، فصل بهار ۱۴۰۵؛ ص ۴۷-۳۱.

علمی- پژوهشی

یک طرح کنترل دسترسی امن در سلامت الکترونیک با استفاده از زنجیره قالبی دوگانه

پیمان ویسی[۱]؛ زهرا محمدی[۲]؛ فاطمه مطیع شیرازی[۳]؛ مجید بیات*[٤]

۱- کارشناسی‌ارشد مهندسی کامپیوتر گرایش رایانش امن، دانشگاه شاهد، تهران، ایران.

۲- کارشناسی‌ارشد مهندسی کامپیوتر گرایش رایانش امن، دانشگاه شاهد، تهران، ایران.

۳- دانشجوی دکتری رایانش امن، دانشکده فنی و مهندسی، دانشگاه شاهد، تهران، ایران.

٤- دانشیار، گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه شاهد، تهران، ایران.

(**دریافت:** ۲۷ اسفند ۱٤۰٤ **بازنگری:** ۰٤ اردیبهشت ۱۴۰۵ **پذیرش:** ۱٦ اردیبهشت ۱٤۰۵ انتشار: ۰۱ خرداد ۱٤۰۵)

چکیده

پیشرفت سریع فناوری چالش‌های متعددی را در زمینه امنیت اطلاعات و حفظ حریم خصوصی ایجاد کرده و این چالش‌ها بر سامانه‌های سلامت الکترونیک نیز تأثیرگذار بوده است. مدیریت ذخیره‌سازی، اشتراک‌گذاری، و دسترسی به داده‌های سلامت بیماران از مهم‌ترین چالش‌های این سامانه‌ها به شمار می‌رود. برای رفع مشکلات امنیتی این حوزه، پیش از هر اقدامی، بررسی ساختار سامانه و چگونگی ارتباطات در سلامت الکترونیک ضروری است. در این پژوهش، با بررسی طرح‌های ساختاری سامانه‌های سلامت طی ده سال گذشته، هسته‌ی اصلی ساختار این سامانه‌ها شناسایی شده است. وضعیت‌های مختلف درمان مورد بررسی قرار گرفته و شرایط دسترسی برای هر یک از اعضای مرتبط با فرایند درمان در سامانه سلامت الکترونیک تشریح گردیده است. علاوه بر این، یک طرح کنترل دسترسی امن و پویا با استفاده از زنجیره قالبی دوگانه، رمزنگاری مبتنی بر ویژگی، و امضای گروهی ارائه شده است. نتایج بررسی‌ها نشان می‌دهد که طرح پیشنهادی، علاوه بر تأمین نیازهای امنیتی، از نظر کارایی و قابلیت اجرایی نیز عملکرد مطلوبی دارد. همچنین ارزیابی امنیتی در برابر حملات شناخته‌شده به زنجیره‌های قالبی دارای مجوز نشان داده است که طرح پیشنهادی در برابر ۶۸ درصد حملات کاملاً مقاوم، در برابر ۱۴ درصد دارای مقاومت نسبی، و در برابر ۱۸ درصد آسیب‌پذیر است.

کلید واژه‌ها: سلامت الکترونیک، کنترل دسترسی، زنجیره‌ی قالبی، رمزنگاری مبتنی بر ویژگی، امضای گروهی.

* رایانامه نویسنده مسئول: E-mail: mbayat@shahed.ac.ir

۱. مقدمه

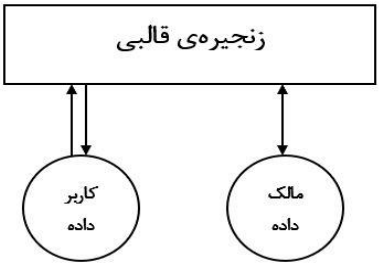
بر اساس تعریف سازمان بهداشت جهانی [1] (WHO) در سال ۲۰۲۵ میلادی، استفاده‌ی مقرون‌به‌صرفه و ایمن از فناوری‌های اطلاعات و ارتباطات در حمایت از سلامت و زمینه‌های مرتبط با سلامت، از جمله خدمات مراقبت‌های بهداشتی، نظارت بر سلامت، ادبیات سلامت، آموزش بهداشت، دانش و پژوهش در زمینه‌ی سلامت، سلامت الکترونیک نام دارد. به سامانه‌ای که اقدامات و فعالیت‌های مرتبط با سلامت در آن انجام می‌شود سامانه سلامت الکترونیک[2] گفته می‌شود. نسخه‌ای الکترونیکی از اطلاعات بیمار و سوابق مرتبط با سلامت بیمار را پرونده‌ی سلامت الکترونیک[3] بیمار می‌نامند[۱]. در سرتاسر جهان، بسیاری از دولت‌ها و مراکز بهداشتی از سامانه سلامت الکترونیک استفاده می‌کنند؛ ولی این سامانه با مشکلات و چالش‌هایی در حجم محاسبات، ذخیره‌سازی اطلاعات و امنیت آن‌ها، اشتراک‌گذاری امن داده‌ها، کنترل دسترسی در بخش‌های گوناگون سامانه سلامت الکترونیک، احراز اصالت، یکپارچگی داده‌ها، حفظ حریم خصوصی، امنیت مراکز مدیریتی و مشکلاتی ازاین‌قبیل همراه است که می‌تواند جان یک بیمار یا حتی یک جامعه را به خطر اندازد. امروزه پژوهشگران، متخصصان و مهندسان علوم رایانه و زمینه‌های مرتبط با امنیت فضای تبادل اطلاعات، برای حل مشکلات ذخیره‌سازی و جلوگیری از انواع حملات به سرورهای مرکزی، ساختار توزیع شده و مبتنی بر زنجیره‌ی قالبی[4] را برای سامانه سلامت الکترونیک ارائه می‌دهند و این ساختار به دلیل رفع مشکلاتی که گفته شد در حال گسترش است. بااین‌حال هنوز مشکلات مرتبط با اشتراک داده‌ی امن و کنترل دسترسی دقیق و امن نیاز به بررسی دارند. بر اساس مطالب ذکر شده، امروزه یکی از مشکلات مرتبط با سامانه سلامت الکترونیک کنترل دسترسی دقیق و امن در این سامانه است. در مبحث کنترل دسترسی در سلامت الکترونیک باید توجه داشت که محرمانگی و ناشناس بودن تراکنش‌ها، ارتباطات بین افراد و اطلاعات بیمار در سامانه جامع سلامت از دید افراد غیرمجاز کاملاً محفوظ و پنهان باشد. به دلایل گفته شده در بالا باید ساختار سامانه سلامت الکترونیک مبتنی بر زنجیره‌ی قالبی باشد؛ ازاین‌گذشته باید ناظری بر سامانه باشد تا امکان درمان صحیح و همچنین امکان شکایت برای همه‌ی اعضا وجود داشته باشد. در سامانه سلامت الکترونیک باید برای هر فرد یا نهاد باتوجه‌به نقشی که دارد دسترسی خاص و در زمان خاص تعریف شود برای مثال یک پرستار نباید توانایی دست‌کاری پرونده‌ی سلامت الکترونیک بیمار و تجویز دارو برای وی را داشته باشد؛ پزشک یک مرکز درمانی که در یک‌زمان مشخص درگذشته در درمان بیمار نقش داشته و اکنون در درمان بیمار هیچ نقشی ندارند، نباید توانایی دست‌کاری یا مشاهده‌ی اطلاعات مرتبط با درمان بیمار را داشته باشند. برای هرکس باید مشخص شود که توانایی خواندن و یا دست‌کاری چه بخشی از اطلاعات در چه زمانی را دارد. علاوه بر این هیچ‌یک از افراد و نهادهای مجاز نباید توانایی اعطای دسترسی غیرمجاز به فرد یا نهاد غیرقانونی دیگری را داشته باشد. محل ذخیره‌سازی اطلاعات بیمار باید ایمن باشد. امکان جعل در دسترسی به سامانه سلامت الکترونیک نباید وجود داشته باشد. افراد و نهادهای درگیر درمان باید کاملاً یکدیگر را بشناسند و از وجود یکدیگر کاملاً مطمئن باشند. باتوجه‌به مطالب گفته شده می‌توان گفت که کنترل دسترسی امن و دقیق به این معناست که ساختار طراحی شده، همه‌ی موارد زیر را در بر گیرد:

- مجوز دسترسی تنها توسط فرد یا نهاد کاملاً قانونی انجام پذیرد.
- زمان قانونی دسترسی برای هر فرد یا نهاد تعریف شده باشد.
- مقدار دسترسی برای هر فرد یا نهاد تعریف شده باشد و از اندازه‌ی تعریف شده نتواند تجاوز کند.
- دست‌کاری یا مشاهده‌ی بدون مجوز فرد یا نهادی که مجوز دسترسی نگرفته امکان‌پذیر نباشد.
- اشتراک پرونده‌ی سلامت الکترونیک و دیگر داده‌ها به‌صورت امن انجام پذیرد.
- اطلاعات به‌صورت امن ذخیره شوند.
- همراه با ساختار توزیع شده در سامانه سلامت الکترونیک باشد.
- هر سه اصل امنیت یعنی محرمانگی، یکپارچگی و دسترسی را فراهم کند.
- پرونده‌ی سلامت الکترونیک، تراکنش‌ها و دیگر اطلاعات مرتبط با سلامت بیمار برای افراد غیرمجاز ناشناس بماند.
- همه‌ی افراد و نهادهای مجاز از اطلاعات تراکنش‌های مرتبط با بیمار کاملاً آگاه باشند تا هیچ‌یک از این افراد یا نهادهای مجاز توانایی اجازه‌ی دسترسی به فرد یا نهاد غیرقانونی را نداشته باشند به دیگر سخن کسی توانایی دست‌کاری غیرمجاز نداشته باشد.
- همه‌ی افراد و نهادهای مجاز برای یکدیگر احراز اصالت شوند و به یکدیگر اطمینان کامل داشته باشند.
- افزایش امنیت، حجم محاسبات را بیش از اندازه افزایش ندهد.
- ذخیره و ردیابی تراکنش‌ها را داشته باشد.
- امکان جعل وجود نداشته باشد.
- قابلیت لغو، ابطال و حذف داشته باشد.

مطالعه مقالات مرتبط با سامانه سلامت الکترونیک از سال ۲۰۱۷ به بعد، نشان می‌دهد که همه‌ی طرح‌های سامانه سلامت

[1] World Health Organization
[2] Electronic Healthcare System (EHS)
[3] Electronic Health Record (EHR)
[4] Blockchain

الکترونیک، یک ساختار مشخص و مشترک یافت می‌شود. در این مقاله این ساختار به‌عنوان هسته و بدنه اصلی سامانه سلامت الکترونیک معرفی خواهد شد. این ساختار، شامل دو بخش اصلی کاربران و شبکه زنجیره‌ی قالبی است. شکل (۱) این ساختار را نشان می‌دهد.



شکل (۱). ساختار کلی سامانه سلامت الکترونیک

در مورد زنجیره‌ی قالبی، بیشتر مقالات، زنجیره قالبی کنسرسیومی را پیشنهاد دادند؛ ولی مقالاتی نیز وجود دارد که از زنجیره‌قالبی‌های خصوصی و یا دوگانه نیز استفاده کردند. در مورد کاربران، بر اساس نوع دسترسی افراد به سامانه سلامت الکترونیک، به دودسته کاربر داده و مالک داده تقسیم می‌شوند. برخی مقالات مالک و کاربر داده را به طور ثابت مشخص کرده‌اند برای مثال، پزشک را همیشه به‌عنوان مالک داده و بیمار را همیشه به‌عنوان کاربر داده معرفی کرده‌اند؛ ولی در اینکه واقعاً کدام‌یک کاربر و کدام‌یک مالک داده باشند، اختلافات بسیاری در مقالات وجود دارد. برخی مقالات نیز کاربر و مالک داده را به صوت پویا تعریف کرده‌اند. باتوجه‌به شرایط، نقش مالک یا کاربر داده برای یک کاربر خاص، تغییر می‌کند؛ برای مثال، یک مرکز درمانی در شرایط کلی به‌عنوان مالک داده شناخته می‌شود؛ ولی در برخی شرایط همکاری، به‌عنوان کاربر داده شناخته می‌شود.

ساختار مقاله به این شرح است که در بخش دوم؛ یعنی کارهای مرتبط، پیش‌زمینه پژوهش و مقالات مطالعه شده برای ارائه طرح پیشنهادی توضیح داده شده و مورد مقایسه قرار گرفته خواهد شد. سپس در بخش سوم، طرح کنترل دسترسی امن با استفاده از رمزنگاری مبتنی بر ویژگی، زنجیره قالبی، و امضای گروهی ارائه خواهد شد و معماری، پروتکل‌ها، ویژگی‌های امنیتی و حملات طرح پیشنهادی مورد بررسی قرار گرفته و با طرح‌های گفته شده مورد مقایسه قرار گرفته خواهد شد. در پایان در بخش چهارم مزایا و معایب طرح پیشنهادی ذکر خواهد شد و جهت‌گیری آینده برای بهبود طرح ارائه خواهد شد.

۲. کارهای مرتبط

در این بخش، طرح‌ها و مقالات سلامت الکترونیک که موردمطالعه قرار گرفته است و بر اساس آن‌ها طرح پیشنهادی ارائه شده، مورد بررسی قرار خواهد گرفت.

در سال ۲۰۲۳ روان و همکاران[۲،] یک طرح کنترل دسترسی ارائه داده که می‌تواند برای سامانه‌های مدیریت اعتماد غیرمتمرکز استفاده شود. این طرح به یک نهاد کاملاً قابل‌اعتماد نیاز ندارد و می‌تواند به طور مؤثر از حریم خصوصی کاربر و امنیت داده‌ها در سامانه‌های مدیریت اعتماد توزیع شده محافظت کند. این طرح از سیاست‌های دسترسی انعطاف‌پذیر و برون‌سپاری محاسباتی پشتیبانی می‌کند؛ بنابراین، می‌توان آن را در دستگاه‌های نهایی با منابع محاسباتی محدود مستقر کرد. طرح PM-CPABE را باهدف تقویت کنترل دسترسی توزیع شده و تولید کلید چند مرجعی را ارائه داده است. از ویژگی‌های امنیتی این طرح می‌توان به امنیت کلید کاربر، کنترل دسترسی توسط فرستنده‌ی داده یا به‌اختصار DS و مقاومت در برابر تبانی اشاره کرد. در سال ۲۰۲۲ دای و همکاران[۳]برای به اطمینان از ایمن بودن اشتراک داده‌ها بین کاربران، دستگاه‌ها و سامانه‌ها، حفظ حریم خصوصی و دستیابی به سایر ویژگی‌های موردنیاز ارائه دادند. چنین ویژگی‌هایی هنگام اشتراک‌گذاری داده‌های حساس، مانند اشتراک‌گذاری داده‌های مراقبت‌های بهداشتی و کنترل دسترسی که حاوی اطلاعات خصوصی است، ضروری هستند. ازاین‌رو، در این مقاله، طرح HAPPS، باهدف دستیابی به ویژگی‌های پنهان و حفاظت از امتیاز برای به‌اشتراک‌گذاری داده‌ها باقابلیت تأیید طراحی شده است، و از حریم خصوصی کاربر محافظت می‌کند. در سال ۲۰۲۱ ایگال و همکاران[۴] با استفاده از زنجیره‌ی قالبی کنسرسیومی و DDS و SRAC تلاش کردند معماری جدید سامانه سلامت الکترونیک مبتنی بر H-CPS نامتمرکز و باهدف کاهش تأخیر، ناشناس بودن، قابل‌ردیابی، حفظ حریم خصوصی همراه با نظارت بر بیمار با استفاده از BC، DDSS و محاسبات ترکیبی، کنترل دسترسی مبتنی بر حلقه SRAC ارائه دادند. از ویژگی‌های امنیتی این طرح می‌توان به ناشناس بودن، قابل‌ردیابی، تغییرناپذیری اشاره کرد. در سال ۲۰۲۲ ژانگ و همکاران[۵]لاش کردند تا با استفاده از زنجیره‌ی قالبی کنسرسیومی و رمزنگاری‌های MA-ABE و CP-ABE یک طرح کنترل دسترسی دقیق و امن باهدف جلوگیری از افشای اطلاعات و دسترسی غیرقانونی به پرونده‌ی سلامت الکترونیک بیمار، جلوگیری از تغییر غیرمجاز داده‌ها ارائه دهد. از ویژگی‌های امنیتی قابل‌توجه این طرح می‌توان به مقاوم‌بودن در برابر حملات IND-CPA و IND-CKA اشاره کرد. در سال ۲۰۲۳ وزید و همکاران[۶] تلاش کردند تا با استفاده از مدل استاندارد تصادفی ROR، ECDDHP و زنجیره‌ی قالبی کنسرسیومی، و با استفاده از هوش مصنوعی در EHS مبتنی بر محاسبات مه و باهدف کاهش هزینه محاسبات، و با استفاده از روش‌های هیورستیک ارتباطی امن به نام AISCM-FH ارائه دهند. از ویژگی‌های امنیتی این طرح می‌توان به مقاوم در برابر

حملات replay و MITM و جعل هویت و ESL ، ناشناس بودن، و جلوگیری از درز اطلاعات در EHS مبتنی بر محاسبات مه اشاره کرد. در سال ۲۰۲۳ سموئیل و همکاران[۷] در طرح کنترل دسترسی سلامت الکترونیک در اینترنت اشیا با استفاده از زنجیره‌ی قالبی کنسرسیومی، مسیریابی سیری، و رمزنگاری مبتنی بر شناسه (IBE)، و الگوریتم اجماع POEOI طرح GarliMedChain را ارائه داده و با درنظرگرفتن اعتماد بین گره‌ها، ردیابی با استفاده از مسیریابی سیری، درنظرگرفتن اجماع گره‌ها برای اطمینان از اشتراک‌گذاری ایمن داده توانسته به ناشناس بودن، کاهش هزینه‌ی محاسباتی، حفظ حریم خصوصی بیماران در اینترنت اشیا، ردیابی، جلوگیری از ردیابی توسط مهاجم، مقاوم در برابر دست‌کاری داده‌ها دست یابد. در سال ۲۰۲۳ بائو و همکاران[۸]طرح امضای گروهی قابل پیوند انتخابی و قابل‌ردیابی با نام مخفف SLTGS برای اشتراک‌گذاری امن داده در سامانه‌ی سلامت الکترونیک را ارائه دادند. این طرح از رمزنگاری مبتنی بر ویژگی سیاست متن رمزی استفاده کرده و از ویژگی‌های امنیتی این مقاله می‌توان به ناشناس بودن، قابلیت ردیابی، جعل‌ناپذیری، ردیابی و تبدیل کور اشاره کرد. این مقاله تلاش کرده قابلیت پیوند انتخابی و قابلیت ردیابی نیز در کنار یکدیگر در طرح امضای گروهی در اشتراک‌گذاری ایمن داده‌های سلامت را فراهم کند. در دسامبر ۲۰۲۳، پنگ و همکاران[۹]طرح یک پروتکل اشتراک‌گذاری EMR مبتنی بر زنجیره قالبی دوگانه با توافق‌نامه کلید احراز هویت سه‌جانبه مبتنی بر هویت برای اشتراک‌گذاری EMR در میان چندین بیمارستان، پروتکل توافق‌نامه کلید احراز هویت سه جانبه (TAKA) را ارائه داده است. این مقاله از دو نوع زنجیره قالبی کنسرسیومی و عمومی استفاده کرده و برای الگوریتم اجماع نیز از الگوریتم‌های اثبات کار و Hotstuff استفاده کرده است. از ویژگی‌های امنیتی این مقاله می‌توان به امنیت جلو و عقب، امنیت کلید جلسه، احراز هویت دوطرفه، امنیت قابل‌اثبات، عدم انکار، مقاومت در برابر حملات ماینینگ اشاره کرد. هدف ارائه‌ی این طرح، عدم استفاده از کلید متقارن برای کاربران در EHS، عدم الزام بیماران به ارسال کلید برای مراکز درمانی، کاهش ارتباطات بین مرکز مدیریت سامانه با کاربران برای تولید کلید، تأیید هویت بوده و همچنین تلاش کرده سربار محاسباتی و سربار ارتباطی کمی را کاهش دهد. در سال ۲۰۲۱ ژو و همکاران [۱۰] یک سامانه اشتراک‌گذاری EMR را با معرفی یک طرح رمزگذاری مبتنی بر ویژگی‌های قابل‌برگشت باسیاست دوگانه با مقاومت در معرض قرارگرفتن در معرض کلید رمزگشایی و ذخیره‌سازی قابل‌برگشت پیشنهاد کرده است. یک تعریف رسمی و مدل امنیتی را برای طرح پیشنهادی خود ارائه داده و تلاش کرده با استفاده از زنجیره‌ی قالبی کنسرسیومی و رمزنگاری مبتنی بر ویژگی سیاست دوگانه‌ی ترکیبی متن رمزی و کلیدی، طرح سلامت الکترونیک باقابلیت مقاومت در برابر دست‌کاری غیرمجاز و نیازمند لغو و ابطال به نام طرح DP-RABE ارائه داده است. در سال ۲۰۲۴ یانهوا و همکاران[۲۱] یک طرح کنترل دسترسی دقیق برای سامانه حل هویت ارائه داده است. این طرح از یک روش رمزگذاری شناسه جدید و الگوریتم رمزگذاری مبتنی بر ویژگی استفاده می‌کند که طبقه‌بندی داده‌ها و مدیریت مجوزهای انعطاف‌پذیر را برای شرکت‌های صنعتی امکان‌پذیر می‌کند. علاوه بر این، برای مبارزه با رفتارهای مخرب بالقوه کاربران، مانند دسترسی غیرمجاز یا سوءاستفاده از هویت، از فناوری زنجیره قالبی برای ردیابی کاربران مخرب و درعین‌حال محافظت از حریم خصوصی کاربران استفاده کرده و با استفاده از الگوریتم دوخطی دیفی هلمن امنیت طرح خود را ثابت کرده است. در سال ۲۰۲۴ داژیانگ و همکاران[۲۲] یک طرح کنترل دسترسی منعطف و دقیق[۱] و سالمندان برای داده‌های پرونده سلامت بیمار در مراقبت‌های بهداشتی هوشمند سالمندان[۲] ارائه شده است. این مقاله از رمزگذاری مبتنی بر ویژگی سیاست متن رمزی، مجوز شناسه‌ای[۳]، رگرسیون کلید دوگانه و زنجیره قالبی استفاده کرده است. این طرح توانسته از نظر هزینه زمانی و سربار محاسباتی عملکرد خوبی ارائه دهد. در سال ۲۰۲۵ هوی ین و همکاران[۲۳] یک ساختار مبتنی بر ویژگی با حفظ حریم خصوصی و کارآمد را باسیاست دسترسی کاملاً پنهان بر روی گروه سفارش اصلی[۴] بر اساس ساختار رمزنگاری مبتنی بر ویژگی ارائه کرده در سال ۲۰۲۴ داژیانگ - چن و همکاران[۲۲] یک طرح کنترل دسترسی منعطف و دقیق[۵] و سالمندان برای داده‌های پرونده سلامت بیمار در مراقبت‌های بهداشتی هوشمند سالمندان[۶] ارائه داده شد. این مقاله از رمزگذاری مبتنی بر ویژگی سیاست متن رمزی، مجوز شناسه‌ای[۷]، رگرسیون کلید دوگانه و زنجیره قالبی استفاده کرده است. این مقاله کنترل دسترسی چندبعدی داده‌های پرونده سلامت بیمار از نظر زمان تولید داده، و ویژگی‌های کاربر داده، دسترسی را تعیین کرده است. زمان و دوره دسترسی، یک الگوریتم تقسیم‌بندی نشانه جدید برای انتقال حقوق دسترسی بین پزشکان به طور مؤثر برای تشخیص و درمان چندجانبه طراحی شده است. این طرح توانسته به غیرقابل‌تشخیص بودن EHR متن رمزی تحت حملات متن ساده

[1] Fine-Grained
[2] Smart Elderly Healthcare
[3] Permission token
[4] Prime order group:
منظور از گروه سفارش اصلی گروهی از کاربران انسانی است که در روند درمان بیمار دخالت دارند و داده‌های این اعضا نباید برای افراد خارج از روند درمان نباید این اعضا را در شبکه IoMT افشا شود.
[5] Fine-Grained
[6] Smart Elderly Healthcare
[7] Permission token

انتخابی و عدم پیوند و جعل‌ناپذیری نشانه‌ها تحت حملات تبانی کاربران داده دست یابد. در سال ۲۰۲۵، هوی - ین و همکاران[۲۳] یک ساختار مبتنی بر ویژگی با حفظ حریم خصوصی و کارآمد را باسیاست دسترسی کاملاً پنهان بر روی گروه سفارش اصلی بر اساس ساختار رمزنگاری مبتنی بر ویژگی ارائه دادند. این طرح ویژگی‌های حساس در ساختار دسترسی را توسط چندین طرح غیرضروری بدون به خطر انداختن صحت و امنیت پنهان می‌کند. علاوه بر این، عملکرد این طرح بسیار برتر از ویژگی طرح‌های نیمه پنهان است. جدول (۱) مقایسه بهترین طرح‌های گفته شده در این بخش که به طرح پیشنهادی نزدیک‌تر هست را نشان می‌دهد.

جدول (۱). مقایسه طرح‌ها

	[۴]	[۵]	[۶]	[۷]	[۸]	[۹]	[۱۰]
پیوندپذیری	×	×	×	×	✓	×	×
ابطال	✓	✓	×	×	✓	✓	✓
ناشناس	✓	✓	✓	✓	✓	✓	✓
پویایی	×	×	×	×	×	✓	×
مقاومت در برابر تبانی	✓	✓	✓	✓	✓	✓	✓
ردیابی	✓	✓	✓	✓	✓	✓	✓
تغییرناپذیری	✓	✓	✓	✓	✓	✓	✓
احراز هویت سه‌طرفه	×	×	×	×	×	×	✓
جستجوی امن	✓	×	✓	✓	×	✓	✓
عدم انکار	✓	✓	✓	✓	✓	✓	✓

در این بخش، نخست طرح‌های گوناگون کنترل دسترسی در سامانه‌ی سلامت الکترونیک در سه سال اخیر پرداخته شد. چند طرح سلامت الکترونیک منتشر شده در سال ۲۰۲۵م با یکدیگر مقایسه شد و در پایان، ویژگی‌های امنیتی سه تا از طرح‌های موردنظر معرفی و با دیگر طرح‌های سلامت الکترونیک مقایسه شد. باتوجه‌به مقایسه‌های انجام شده چنین نتیجه می‌دهد که بهترین ساختار برای سامانه‌ی سلامت الکترونیک، ساختار طرح بائو، و بهترین نوع رمزنگاری، رمزنگاری مبتنی بر ویژگی سیاست دوگانه، و بهترین شبکه‌ی ارتباطی نیز، شبکه‌ی زنجیره‌ی قالبی ترکیبی است.

۳. طرح پیشنهادی

در این بخش، طرح پیشنهادی برای کنترل دسترسی امن در سامانه سلامت الکترونیک ارائه می‌شود. این طرح از رمزنگاری مبتنی بر ویژگی و زنجیره‌ی قالبی کنسرسیومی استفاده می‌کند تا امنیت و پویایی نقش کاربران را تأمین کند. بررسی طرح‌های بخش دوم نشان داد که بهترین انتخاب، طرح با نقص‌هایی بوده که نیاز به اصلاحاتی مانند تغییر مالکیت داده در شرایط اورژانسی و همکاری پزشکان دارد؛ بنابراین، طرح پیشنهادی بهبودهایی برای رفع این مشکلات دارد و با استفاده از امضای گروهی و ترکیب زنجیره‌های قالبی خصوصی و کنسرسیومی، امنیت کامل را تضمین می‌کند.

۳-۱. معماری طرح پیشنهادی

باتوجه‌به ساختار سامانه‌ی سلامت الکترونیک، چهار وضعیت برای صدور مجوز دسترسی را در نظر گرفته شد و بر اساس این حالات، طرح پیشنهادی خود ارائه می‌شود. حالات چهارگانه به شرح زیر است:

۱. وضعیت عادی و بدون همکاری: بیمار توان صدور مجوز دسترسی به پرونده سلامت برای پزشک یا مرکز درمانی را دارد و مرکز درمانی برای درمان بیمار نیاز به همکاری با هیچ نهاد درمانی دیگری ندارد.

۲. وضعیت عادی و نیازمند همکاری: بیمار توان صدور مجوز دسترسی به پرونده سلامت برای پزشک یا مرکز درمانی را دارد؛ ولی مرکز درمانی برای درمان بیمار نیاز به همکاری با حداقل یک نهاد درمانی دیگر دارد.

۳. وضعیت اضطراری و بدون همکاری: بیمار توان صدور مجوز دسترسی به پرونده سلامت برای پزشک یا مرکز درمانی را ندارد و مرکز درمانی برای درمان بیمار نیاز به همکاری با هیچ نهاد درمانی دیگری ندارد.

۴. وضعیت اضطراری و نیازمند همکاری: بیمار توان صدور مجوز دسترسی به پرونده سلامت برای پزشک یا مرکز درمانی را ندارد و مرکز درمانی برای درمان بیمار نیاز به همکاری با حداقل یک نهاد درمانی دیگر دارد.

حالات ۱ و ۲ نشان می‌دهد که طرح پیشنهادی باید امکان صدور مجوز دسترسی برای بیمار را فراهم کند. حالات ۲ و ۴ نشان می‌دهد که در طرح پیشنهادی باید امکان همکاری دست‌کم دو نهاد درمانی در روند درمان را فراهم کند و حالات ۳ و ۴ نشان می‌دهد که طرح پیشنهادی باید توانایی مجوز دسترسی به پرونده سلامت بیمار برای مرکز درمانی در مواقع اضطراری را فراهم کند؛ وضعیت اضطراری، شرایطی است که باید بیمار فوراً درمان شود؛ ولی بیمار توانایی صدور مجوز دسترسی به

پرونده سلامت خود را برای عضو دیگر در سامانه سلامت ندارد. برای فهم بهتر وضعیت‌های تعریف شده، ماشین حالت رسم می‌شود. برای این کار، xy را به‌صورت زیر تعریف می‌شود.

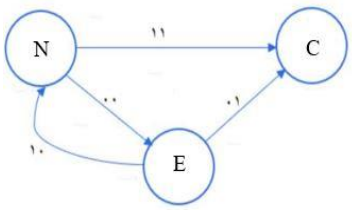
x	نیازمند صدور مجوز توسط بیمار
y	نیازمند صدور مجوز توسط دو کاربر

درصورتی‌که شرایط x یا y برقرار باشد، مقدار آن‌ها ۱ خواهد بود و در غیر این صورت، مقدار صفر را می‌گیرند. جدول (۲) شرایط و حالات چهارگانه را برای x و y نشان می‌دهد.

جدول (۲). مقادیر x و y برای شرایط چهارگانه بیمار

شرایط	y	x
۱	۰	۱
۲	۱	۱
۳	۰	۰
۴	۱	۰

پس می‌توان گفت برای رسم ماشین حالت، سه حالت کلی دارد: کاملاً عادی (N)، اورژانسی (E)، و همکاری (C). باتوجه‌به این موضوع، گراف ماشین حالت دارای سه گره خواهد بود. شکل ۲ ماشین حالت نوع دسترسی در وضعیت‌های مختلف به‌صورت xy را نشان می‌دهد.



شکل (۲). ماشین حالت مجوز دسترسی در شرایط گوناگون

برای اینکه طرح پیشنهادی همه‌ی حالات گفته شده را پوشش دهد، باید دست‌کم یک نهاد نظارتی در این طرح موجود باشد. از طرفی، برای شفافیت، قابلیت ردیابی، و پیوندپذیری انتخابی نیاز است که از امضای SLTG استفاده شود که خود نیازمند یک سرور تبدیل است. ازاین‌رو کاربران طرح ما شامل بیمار، پزشک، نهاد درمانی، و نهاد نظارتی است. همان‌طور که در بخش ۱ توضیح داده شد، همه‌ی کاربران باید در دودسته مالک داده و کاربر داده قرار گیرند. در طرح پیشنهادی، مالک داده به‌عنوان شخص یا نهادی تعریف می‌شود که توانایی صدور مجوز دسترسی و یا افزودن پرونده سلامت جدید را دارد و کاربرانی که توانایی صدور هیچ‌گونه مجوزی ندارند، به‌عنوان کاربر داده تعریف می‌شوند. بر اساس این تعریف، بیمار در حالات ۱ و ۲ به‌عنوان مالک داده محسوب می‌شود. در مورد پزشک و مراکز درمانی در وضعیت‌های ۳ و ۴، پزشک کاربر داده هست. در حالت ۲، پزشک یا مرکز درمانی که درخواست همکاری ارسال می‌کند مالک داده است و همکار، کاربر داده محسوب می‌شود. حالت ۴، مشابه حالت ۲ است با این تفاوت که در حالت ۴، فقط مرکز درمانی می‌تواند نقش مالک داده را بگیرد و پزشک، در نقش کاربر داده قرار دارد. نهاد نظارتی در همه حالات مالک داده محسوب می‌شود؛ ولی توانایی ویرایش پرونده سلامت را ندارد و فقط توانایی صدور مجوز، لغو و ابطال را دارد. بنا بر مطالب گفته‌شده، به این نتیجه می‌رسد که به دلیل پویایی نقش‌ها در شرایط گوناگون، باید از رمزنگاری مبتنی بر ویژگی باسیاست دوگانه (DP-ABE) استفاده شود. برای رسیدگی و ثبت سریع‌تر تراکنش‌های مرتبط با سلامت و نظارت، نیاز است از دوزنجیره قالبی خصوصی و کنسرسیومی استفاده گردد. زنجیره سلامت، زنجیره خصوصی است و زیر نظر وزارت بهداشت است و تراکنش‌های مرتبط با سلامت و درمان بیمار در این زنجیره ثبت می‌شود. باقی تراکنش‌ها، نظارتی است و در زنجیره کنسرسیومی برای نظارت ثبت می‌شود. به دلیل استفاده از زنجیره‌قالبی‌های نیازمند دسترسی، از مکانیزم اجماع PBFT در هر دوزنجیره استفاده می‌شود.

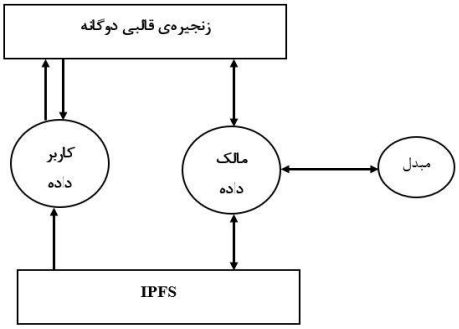
مالک و کاربر داده: بنا بر توضیحات داده شده در فصل دوم بیمار، مرکز درمانی، دولت و پزشک (به جز زمانی که به‌عنوان پزشک دوم و همکار شناخته می‌شود)، مالک داده خواهند بود و باقی اعضای مرتبط با سلامت، کاربر داده شناخته می‌شوند. البته اینجا نکته‌ای باید اضافه شود، زمانی که پزشک در مطب خود اقدام به درمان بیمار می‌کند، مطب پزشک که اعضای آن شامل منشی و پزشک است به‌عنوان مرکز درمانی شناخته می‌شود؛ ولی در این زمان پزشک اجازه‌ی تغییر وضعیت اورژانسی را ندارد و تغییر وضعیت اورژانسی که گفته شد تنها برای بیمارستان‌ها و درمانگاه‌ها است. سرور تبدیل: برای انجام امضای گروهی قابل پیوند انتخابی و قابل‌ردیابی استفاده می‌شود که طرز کار این امضا در فصل دوم توضیح داده شد و دقیقاً مطابق امضای گروهی] ۸ و ۲۰]است. زنجیره‌ی قالبی: در این طرح، از دو نوع زنجیره‌ی قالبی خصوصی و کنسرسیومی استفاده می‌شود. برای زنجیره‌ی قالبی خصوصی از اصطلاح زنجیره‌ی پزشکی (MEDchain) و برای زنجیره‌ی قالبی کنسرسیومی زنجیره‌ی نظارت (SUPchain) استفاده می‌شود.

زنجیره‌ی پزشکی (MEDchain): زنجیره‌ی قالبی پزشکی یک زنجیره‌ی قالبی خصوصی است که از سازوکار تحمل خطای بیزانسی عملی برای تولید قالب‌های پزشکی (Mblocks) تازه استفاده می‌کند. زنجیره‌ی قالبی پزشکی برای ثبت تراکنش‌های

مرتبط با پرونده‌های سلامت الکترونیک استفاده می‌شود. معاملات در قالب‌های پزشکی در یک ساختار دولایه ثبت می‌شود. مراکز درمانی تراکنش‌ها را از پزشکان موجود در مرکز درمانی جمع‌آوری می‌کند، سپس به تأیید و جمع‌آوری امضای مربوطه خود می‌پردازد تا لایه پایینی را تشکیل دهد؛ لازم به ذکر است که اینجا منظور از مرکز درمانی که ذکر شد مطب پزشک و یا باقی مراکز درمانی تفاوتی ندارد، اگر مطب پزشک بود خود پزشک این کار را انجام می‌دهد. سپس، گره‌های استخراج‌کننده این تراکنش‌ها را از مراکز دریافت می‌کنند و تأیید بیشتر و تجمع ثانویه علائم آنها را برای ایجاد لایه بالایی انجام می‌دهند. به‌جای ذخیره امضاهای فردی تراکنش‌ها، قالب پزشکی امضای نهایی را حفظ می‌کند و به طور مؤثر فضای ذخیره‌سازی زنجیره‌ی پزشکی را صرفه‌جویی می‌کند. با تأیید امضای گروهی، باقی نهادها به‌راحتی می‌توانند صحت تمام تراکنش‌ها در قالب پزشکی را تأیید کنند، بنابراین به طور قابل‌توجهی سربار محاسباتی را کاهش می‌دهند. زنجیره‌ی نظارت (SUPchain): زنجیره‌ی نظارت یک زنجیره‌ی قالبی کنسرسیومی است که از مکانیزم اجماع تحمل خطای بیزانسی عملی برای تولید قالب‌های نظارتی (Sblocks) استفاده می‌کند. هدف آن مدیریت تراکنش‌های نظارتی برای پیگیری شکایات، مجوزات در مواقع همکاری و ضروری است و هر مجوزی که صادر شود، جزئیات آن در این زنجیره ثبت خواهد شد. همچنین چکیده‌ی قالب‌های پزشکی را ثبت می‌کند و دسترسی اضطراری به پرونده‌های سلامت الکترونیک را در مواقع اورژانسی تسهیل می‌کند. علاوه بر این، زنجیره‌ی نظارت از درخت مرکل پاتریشیا[1] استفاده می‌کند تا یک فهرست ابطال ثابت از پزشکان در ذخیره‌سازی محلی هر مرکز درمانی (غیر از مطب پزشک) را حفظ کند. با تغییراتی در مدارک پزشکی، این فهرست را می‌توان به‌صورت پویا گسترش داد یا در صورت لزوم منقبض کرد. به‌منظور افزایش کارایی تأیید تراکنش، زنجیره‌ی نظارت امضای گروهی قابل‌ردیابی و قابل پیوند انتخابی مطابق توضیحات داده شده در فصل دوم را پیاده‌سازی می‌کند. همچنین در صورت نیاز، برای بررسی صاحب امضا، SUPchain اطلاعات صاحب امضای کور را از سرور تبدیل در خواست می‌کند و سرور تبدیل، اطلاعات را برای Supchain ارسال می‌کند.

۳-۲. ساختار کلی طرح پیشنهادی

در این بخش ساختار کلی طرح معرفی، و جزئیات آن بیان خواهد شد. شکل ۳ ساختار کلی طرح را نشان می‌دهد. مبدل در اینجا برای امضای گروهی توسط مالکان داده در زنجیره‌ی نظارت است.



شکل (۳). ساختار کلی طرح پیشنهادی

مراحل انجام کار در حالت کلی و عادی:

۱. مقداردهی اولیه
۲. ثبت‌نام اعضا و مبدل
۳. بارگذاری داده‌ها در زنجیره‌ی سلامت توسط مالکان داده
۴. بارگیری داده‌ها توسط کاربران داده از سامانه ذخیره‌سازی توزیع شده فایل
۵. عملیات پیوند
۶. انجام الگوریتم ردیابی

ریاضیات و توضیحات مراحل:

پیش از هر چیز، نیاز است تا اصطلاحات مورداستفاده در این بخش توضیح داده شود. جدول ۳ اصلاحات مورداستفاده را نشان می‌دهد.

جدول (۳). تعریف اصطلاحات مورداستفاده طرح

اصطلاحات	تعریف
σ	امضا
nym	نام مستعار
Con_i	شرایط کاربر i برای معالج
$gsk[uid]$	کلید خصوصی کاربر
gpk	کلید عمومی کاربر
kw	کلیدواژه
$\widehat{cnym}$	نام مستعار تبدیلی در Trace
m	پیام
c	متن رمزی
uid	شناسه کاربر
T	مهر زمان
Policy	شرایط نهادهای نظارتی

[1] Merkle Patricia Trie (MPT)

[1]. باتوجه‌به این موضوع که زنجیره‌ی نظارت یک زنجیره قالبی کنسرسیومی است، وزارت بهداشت یکی از

نهادهایی است که بر این زنجیره نظارت دارد و ازاین‌رو، مقداردهی اولیه‌ی هر دوزنجیره را انجام می‌دهد.

۲. باتوجه‌به این موضوع که زنجیره‌ی نظارت یک زنجیره قالبی کنسرسیومی است، علاوه بر وزارت بهداشت و قوه قضائیه و بیمه، سازمان ثبت‌احوال نیز بر آن نظارت دارد و وزارت بهداشت با استفاده از اطلاعاتی که سازمان ثبت‌احوال در مورد اشخاص ارائه داده، برای هر شخص، کلید موردنظر تولید می‌شود؛ به عبارتی دیگر، کلیدهای عمومی و خصوصی هر شخص از بدو تولد و ثبت مشخصات او در سازمان ثبت‌احوال کشور تولید می‌شود و شخص برای ورود، نیاز است اطلاعات ورود مانند کد ملی و یا شماره‌تلفن همراه را وارد کرده و وارد سامانه‌ی سلامت شود (به‌مانند ورود از طریق پنجره دولت من در ایران).

۳. پزشک و یا مرکز درمانی، بخشی از اطلاعات بیمار (مانند کد ملی و یا تلفن همراه بیمار) را جستجو می‌کند، شرایط و میزان دسترسی موردنیاز خود را اعلام می‌کند و وضعیت اورژانسی یا اضطراری را در حالت No یعنی در وضعیت عادی و غیراضطراری قرار می‌دهد. سپس، مرکز درمانی (مطب پزشک، درمانگاه و یا بیمارستان) $SUPchain.CreateTransaction\ (state: No, m, mpk, \sigma)$ را ثبت می‌کند؛ پس از تأیید، درخواست دسترسی مرکز درمانی به پرونده سلامت بیمار ثبت می‌شود. SUPchain درخواست را برای بیمار ارسال می‌کند و درصورتی‌که بیمار درخواست ارسالی پزشک توسط SUPchain را تأیید کرد و $SUPchain.CreateTransaction\ (state: No, m, mpk,\ \sigma)$ توسط بیمار ثبت شد، مجوز برای مرکز درمانی صادر، و روند درمان آغاز خواهد شد. پزشک یا مرکز درمانی پس از معاینه‌ی بیمار و افزودن اطلاعات به پرونده‌ی سلامت بیمار، داده‌های سلامت الکترونیک m را با ساختار دسترسی P به c رمزگذاری می‌کند، متن رمزی پرونده سلامت c_i را به نمایندگی از گروه امضا کرده و تاپل متن رمز، امضا، و نام مستعار را در زنجیره‌ی پزشکی یعنی در MEDchain ثبت می‌کند و $MEDchain.createTransaction(c, \sigma, nym)$ ایجاد می‌شود. سپس، صاحب داده، نشانی h را که توسط زنجیره‌ی سلامت بازگردانده شده است، توضیحات اطلاعات داده‌های $info$ و کلمات کلیدی مرتبط kw را در قرارداد جستجوی قرارداد هوشمند در زنجیره‌ی سلامت می‌نویسد.

- رمزگذاری داده‌ها مالک داده، داده‌های سلامت الکترونیکی خود را دارد، به‌عنوان‌مثال، سوابق پزشکی الکترونیکی (EMR)، سوابق الکترونیکی سلامت (EHR)، یا داده‌های خدمات پزشکی. مالک داده یک ساختار دسترسی P را برای داده‌ها انتخاب می‌کند. سپس، $DP_ABE.Encrypt\ (P, m, mpk,\ Policy)$ را برای خروجی متن رمزی c اجرا می‌کند.
- امضاکردن. مالک داده، امضای گروهی را برای امضای متن رمزی c_i با اجرای $SLTGS.Sign(m, Con_i, gpk, gsk[uid])$ برای به‌دست‌آوردن امضا σ و نام مستعار انجام می‌دهد.
- بارگذاری داده‌ها سپس، مالک داده $IPFS.Upload(c)$ را برای به‌دست‌آوردن نشانی ذخیره‌سازی در IPFS اجرا می‌کند. داده‌ها به قطعات کوچک‌تر تقسیم می‌شوند و نشانی ذخیره‌سازی h به‌عنوان یک رکورد دائمی از داده‌ها عمل می‌کند.
- بارگذاری اطلاعات جستجو مالک داده، کلیدواژه‌های مرتبط $kw = (kw1, kw2, \ldots, kwl)$ را برای داده‌ها انتخاب می‌کند و ساختار دسترسی P و همچنین معرفی مختصری از داده‌ها را در توضیحات اطلاعات داده‌های $info$ می‌نویسد و سپس بارگذار می‌کند. توضیحات نشانی اطلاعات - واژگان کلیدی $(h, data\ info, kw)$ به قرارداد هوشمند $search_contract$ در زنجیره‌ی نظارت می‌رسد.

۴. کاربر داده می‌تواند واژگان کلیدی موردعلاقه‌ی خود را در قرارداد هوشمند $search_contract$ جستجو کند. پس از دریافت نشانی زنجیره‌ی نظارت مربوطه، آنها می‌توانند این داده‌های c را در زنجیره‌ی نظارت، یعنی $(h, info, kw)$ به دست آورند و برای تجزیه‌وتحلیل داده‌های سلامت الکترونیک، c به m را رمزگشایی کنند و درصورتی‌که نیاز به بررسی و افزودن انجام وظایف مربوطه (مانند بررسی و انجام وظایف توسط پرستار) تنها گزینه‌ی موارد قابل‌انجام را تأیید می‌کند.

- جستجوی واژگان کلیدی: کاربر داده واژگان کلیدی موردعلاقه خود را انتخاب کرده و آنها را در $search_contract.smartcontract$ جستجو می‌کند. او تاپل‌های پاسخگو (نشانی، اطلاعات توضیحات، کلمات کلیدی $\left\{\left(h_i, data_{info_i}, kw_i\right)\right\}_k$, $i \in [k]$ را دریافت می‌کند که در آن k نشان‌دهنده تعداد تاپل‌هایی است که شرایط جستجو را برآورده می‌کنند.
- دانلود داده‌ها: سپس کاربر داده ویژگی‌های خود را بررسی می‌کند A هر ساختار دسترسی $P_i, i \in [k]$ را برآورده می‌کند. اگر درست باشد، کاربر داده $DP_ABE.Decrypt(EHR, mpk, sk_A, Policy)$ را برای به‌دست‌آوردن m اجرا می‌کند. در پایان کاربر می‌تواند از روش تحلیل داده‌های بزرگ برای تحقیق استفاده کند.

تأکید می‌شود که کاربران می‌توانند بارها مقدار زیادی از داده‌ها را برای تجزیه‌وتحلیل این داده‌ها به دست آورند، تنها با دانستن اطلاعات موجود در آنجا که توسط یک عضو قانونی گروه تأیید شده است، بدون اینکه بدانند کدام یک است.

۵. اگر این داده‌ها متعلق به همان امضاکننده باشد، مالک داده فهرستی از پیام امضا - نام مستعار $\{(m_i, \sigma_i, nym_i)\}_n$ را به یک امضاکننده پیوند می‌دهد. این الگوریتم زمانی فراخوانی می‌شود که یک کاربر داده مجموعه‌ای از تاپل‌های $\{(m_i, \sigma_i, nym_i)\}_n$ داشته باشد و باید بداند که آیا این داده‌ها متعلق به همان مالک داده هستند یا خیر. برای مثال، اگر کاربر دو بار داده‌های خود را به اشتراک بگذارد، از جمله داده‌هایی که بسیار بیشتر از افرادی است که تنها یک بیماری دارند. ابتدا باید این تاپل‌ها به هم پیوند داده شود.

- یک جفت کلید کورکننده ایجاد می‌کند. کاربر داده $SLTGS.BKGen(pp)$ را برای تولید جفت کلید زودگذر خود $(bpk، bsk)$ اجرا می‌کند.
- کوری. کاربر داده این تاپل‌های پیام - امضا - نام مستعار را $\{(m_i, \sigma_i, nym_i)\}$ کور می‌کند. او $SLTGS.BKGen((gpk, bpk, (nym, m)))$ را اجرا می‌کند تا هر پیام مستعار تاپل $\{(cnymi, ci)\}_n$ را به دست آورد. سپس کاربر داده $\{(cnymi, ci)\}_n$ و یک شناسه تگ تازه منحصربه‌فرد ارسال می‌کند. برای این تبدیل توسط CS.
- تبدیل. مبدل، به‌منظور وارسی امضا، $\{(SLTGS.Convert(gpk, bpk, csk, \{(cnymi, ci)\}_n, id)\}_n$ را اجرا می‌کند تا تاپل‌های تبدیل شده را به دست آورد $\{(cnymi, ci)\}_n = (cnym1, c1), \ldots, (cnymn, cn)$ و آنها را برای کاربر ارسال می‌کند.
- کور کردن. سپس کاربر داده $\{(cnymi, ci)\}_n$ را به تاپل‌های $unblinded\ convertedpseudonym -$ $message\ \{(nymi, mi)\}_n$ باز می‌کند. اگر $nym_i = nym_j$ ، این داده‌ها متعلق به همان مالک داده است.

۶. صاحب داده می‌تواند هویت واقعی مالک داده را با فراخوانی $SLTGS.Trace$ برای به‌دست‌آوردن شناسه هویت اصلی و سپس جستجوی شناسه در قرارداد هوشمند $iden_contract$ برای دریافت org_info ردیابی کند.

- یک جفت کلید کورکننده ایجاد می‌شود. کاربر داده $SLTGS.BKGen(pp)$ را برای تولید جفت کلید زودگذر خود (bpk, bsk) اجرا می‌کند.
- کوری. کاربر داده با اجرای $Trace.Blind(gpk, bpk, nym)$ را کور می‌کند و آن را به همراه شناسه به CS ارسال می‌کند. توجه داشته باشید که id در این مرحله بسیار مهم است، زیرا اعداد تصادفی در هر شناسه تبدیل کاملاً متفاوت است.
- تبدیل. سرور تبدیل، به‌منظور انجام امضا $SLTGS.Trace.Convert(gpk, bpk, csk, \widehat{cnym}, id)$ را اجرا می‌کند تا $tuple\widehat{cnym}' := \widehat{cnym1}', \widehat{cnym2}'$ تبدیل شده را به دست آورد و آن را برای کاربر ارسال می‌کند.
- کوری: سپس کاربر داده با اجرای $SLTGS.Trace.Unblind(\widehat{cnym}')$ کور می‌کند. شناسه هویت اصلی مالک داده است.
- شناسه جستجو کاربر داده شناسه را در قرارداد جستجوی هوشمند جستجو می‌کند. او در نهایت اطلاعات سازمان مربوطه را دریافت خواهد کرد.

➢ مراحل انجام کار در حالت اورژانسی:

۱. مقداردهی اولیه؛
۲. ثبت‌نام مالک و کاربر داده و مبدل؛
۳. اعلام وضعیت اضطراری و اورژانسی توسط مرکز درمانی و ثبت درخواست در زنجیره‌ی نظارت: در این قسمت مرکز درمانی وضعیت اورژانسی را به زنجیره‌ی نظارت ارسال می‌کند؛ زنجیره نظارت و زنجیره‌ی نظارت به‌جای بیمار مجوز دسترسی به مرکز درمانی را صادر می‌کند و بیمار هیچ دخالتی در انجام این کار ندارد؛
۴. بارگذاری داده‌ها در زنجیره‌ی سلامت توسط مالک داده؛
۵. بارگیری داده‌ها توسط کاربران داده از زنجیره‌ی سلامت؛
۶. عملیات پیوند؛
۷. انجام الگوریتم ردیابی.

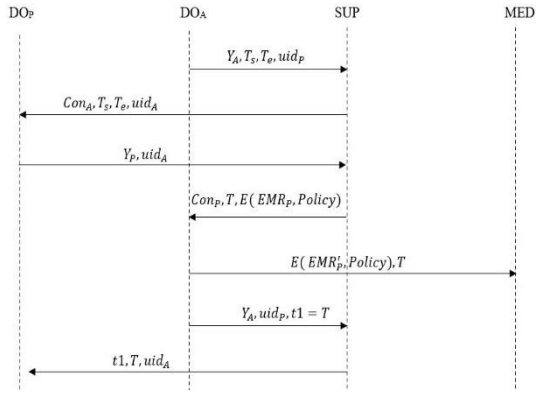
۳-۳. پروتکل‌ها

در این بخش، باتوجه‌به توضیحات بخش‌های ۳-۱ و ۳-۲ پروتکل‌های طرح پیشنهادی رسم، و توضیح داده خواهد شد.

پروتکل ۱) مرحله‌ی سوم: شرایط اول (کاملاً عادی): مرحله‌ی درمان بدون نیاز به همکاری در شرایط عادی (غیراورژانسی و خارج از حالت کما)

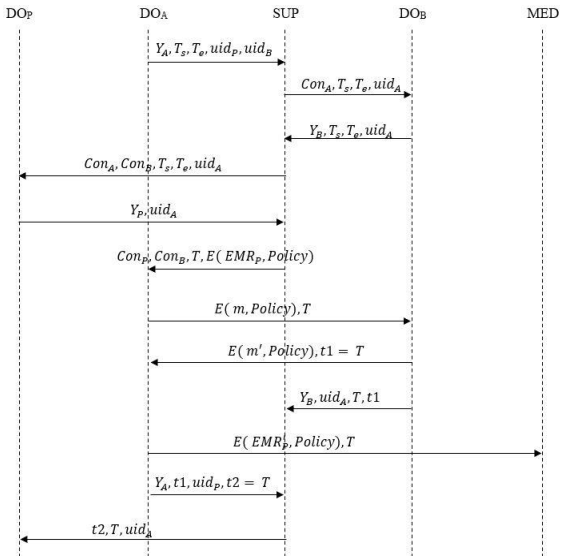
لازم به ذکر است که در پروتکل زیر، منظور از Y_i در واقع اطلاعاتی (اطلاعاتی نظیر نشانی، امضا، پیام، شرایط (اورژانسی یا

عادی)) است که کاربر i ارسال می‌کند که پیش‌تر توضیح داده شد که شامل چه اطلاعاتی است و منظور از Con_i نیز، شرایطی است که شخص یا نهاد i تعیین می‌کند. شکل (۴) پروتکل مرحله سوم در حالت عادی را نشان می‌دهد.



شکل (۴). پروتکل مرحله‌ی سوم: طرح پیشنهادی در حالت عادی و بدون نیاز به همکاری

پروتکل ۲: پروتکل شکل (۵)، شرایط عادی و نیازمند همکاری را نشان می‌دهد؛ منظور وضعیت دوم از چهار وضعیت ذکر شده برای درمان است.



شکل (۵). پروتکل مرحله‌ی سوم در حالت عادی و نیازمند همکاری

➢ پروتکل مرحله‌ی سوم در حالت اورژانسی:

طرز کار این پروتکل، دقیقاً مانند پروتکل شکل‌های (۴) و (۵) هست با این تفاوت که در این پروتکل، مرکز درمانی (فقط مراکز درمانی می‌توانند این کار را انجام دهند و پزشک تحت هیچ شرایطی اجازه‌ی فعال‌نمودن حالت اورژانسی و اضطراری را ندارد) هنگام ارسال درخواست، وضعیت را در حالت اضطراری قرار می‌دهد و SUPchain نیز درخواست نهاد را برای بیمار ارسال می‌کند. درصورتی‌که پاسخی از بیمار دریافت نشد، اطلاعات را برای نهاد درمانی ارسال می‌کند و روند درمان آغاز می‌شود.

۳-۴. ارزیابی امنیتی

در این بخش، باتوجه‌به توضیحات داده شده، ویژگی‌های امنیتی طرح بررسی شده و سپس طرح در برابر انواع حملات شناخته‌شده به شبکه زنجیره قالبی بررسی می‌شود.

۱- ناشناس بودن: استفاده از امضای SLTG در این طرح، باعث شده که کاربران این توانایی را داشته باشند که تراکنش‌های خود را به‌صورت ناشناس انجام دهند و هویت واقعی آن‌ها تنها در شرایط خاص (ردیابی انتخابی) توسط مراجع معتبر (SUPchain) قابل افشا است. حتی اعضای گروه نیز نمی‌توانند هویت یکدیگر را تشخیص دهند، مگر در شرایط خاص (مانند ردیابی انتخابی).

۲- شفافیت: زنجیره قالبی کنسرسیومی شفافیت محدودی ارائه می‌دهد، زیرا اطلاعات آن فقط برای اعضای مجاز شبکه (مانند نهادهای نظارتی یا سازمان‌های بهداشتی) قابل‌مشاهده است. در زنجیره قالبی خصوصی شفافیت کمتر است، زیرا اطلاعات درمانی محرمانه هستند و تنها برای افراد مجاز (مانند پزشکان یا بیماران) قابل دسترسی‌اند. این ترکیب از شفافیت محدود برای نظارت و حریم خصوصی بالا برای داده‌های حساس، یک تعادل مناسب ایجاد کرده است.

۳- قابلیت ردیابی: ویژگی ردیابی انتخابی در SLTGS به مراجع معتبر (مانند نهادهای نظارتی) این امکان را می‌دهد که در شرایط خاص هویت کاربر را ردیابی کنند. این قابلیت برای جلوگیری از سوءاستفاده و پیگیری فعالیت‌های غیرمجاز در سامانه سلامت الکترونیک ضروری است. همچنین تراکنش‌ها در زنجیره قالبی کنسرسیومی ثبت می‌شوند که امکان ردیابی فعالیت‌ها را در چارچوب قوانین فراهم می‌کند.

۴- پویایی: مطابق توضیحات داده شده، در طرح پیشنهادی، نوع مالک و یا کاربر داده به‌صورت کاملاً ثابت تعریف نشده‌اند و در شرایط خاص، با مجوز نهاد نظارتی تغییر می‌کند.

۵- قابلیت حذف و ابطال: در طرح ما SUPchain می‌تواند رفتار کاربران را زیر نظر بگیرد و در صورت تشخیص رفتار مشکوک ارتباطات با کاربر و مجوز ایجاد دسترسی توسط کاربر را لغو می‌کند. همچنین با استفاده از مکانیزم اجماع PBFT ، رفتار مشکوک کاربران می‌تواند به‌صورت جمعی

تأیید شود. سپس سامانه می‌تواند اطلاعات مربوط به لغو دسترسی کاربر را در شبکه ثبت کند که این امر مانع از سوءاستفاده مجدد کاربر از سامانه می‌شود. باتوجه‌به اینکه کاربران از امضای SLTGS استفاده می‌کنند، لغو می‌تواند به‌نحوی انجام شود که دیگر اجازه ایجاد یا تأیید تراکنش‌های جدید در گروه به کاربر متخلف داده نشود.

۶- پیوندپذیری: امضای SLTG از پیوندپذیری انتخابی تراکنش‌ها پشتیبانی می‌کند. اگر یک کاربر تراکنش‌های متعددی را انجام دهد، تحت شرایط خاص (مانند تحلیل داده‌ها توسط یک نهاد مجاز)، می‌توان این تراکنش‌ها را به هم مرتبط کرد. این ویژگی می‌تواند برای ردیابی الگوهای درمانی یا سوءاستفاده احتمالی استفاده شود، بدون اینکه ناشناس بودن کلی کاربران نقض شود.

در جدول (۴) مقایسه طرح پیشنهادی با برترین طرح‌های پیشینه پژوهش نشان داده شده است. منظور از PS در جدول (۴) طرح پیشنهادی است.

جدول (۴). مقایسه سایر طرح‌ها با طرح پیشنهادی

	[۴]	[۵]	[۶]	[۷]	[۸]	[۹]	[۱۰]	PS
پیوندپذیری	×	×	×	×	✓	×	×	✓
ابطال	✓	✓	×	×	✓	✓	✓	✓
ناشناس	✓	✓	✓	✓	✓	✓	✓	✓
پویایی	×	×	×	×	×	✓	×	✓
مقاومت در برابر تبانی	✓	✓	✓	✓	✓	✓	✓	✓
ردیابی	✓	✓	✓	✓	✓	✓	✓	✓
تغییرناپذیری	✓	✓	✓	✓	✓	✓	✓	✓
احراز هویت سه‌طرفه	×	×	×	×	×	×	✓	✓
جستجوی امن	✓	×	✓	✓	×	✓	✓	✓
عدم انکار	✓	✓	✓	✓	✓	✓	✓	✓

در جدول (۵) مرتبه و پیچیدگی زمانی، و هزینه محاسباتی نوع زنجیره قالبی یا زنجیره‌های قالبی، مکانیزم یا مکانیزم‌های اجماع، نوع رمزنگاری، نوع امضا به‌ویژه برای امضای SLTGS و معماری طرح‌های[۴]تا[۱۰]که بهترین طرح‌های موجود بودند، هزینه محاسباتی و پیچیدگی زمانی کلی مورد تحلیل قرار گرفته و با طرح پیشنهادی در جدول (۵) مورد مقایسه قرار گرفته است. در جدول (۵)، منظور از n تعداد گره‌ها در زنجیره قالبی، d سختی استخراج، a تعداد ویژگی‌ها، p تعداد شروط در سیاست رمزنگاری، m تعداد پیام یا درخواست، و k طول کلید رمزنگاری است. همان‌طور که پیش‌تر ذکر شد، منظور از PS در جدول (۵)، طرح پیشنهادی است.

جدول (۵). مقایسه پیچیدگی زمانی و هزینه محاسباتی طرح پیشنهادی با سایر طرح‌ها

	پیچیدگی زمانی	هزینه محاسباتی
PS	$\theta(n^2) + \theta(p+a) + \theta(1)$	$\theta(n^2) + \theta(p.a) + \theta(k)$
[۴]	$\theta(2^d) + \theta(p)$	$\theta(2^d) + \theta(p.k)$
[۵]	$\theta(2^d) + \theta(p)$	$\theta(2^d) + \theta(p.k)$
[۶]	$\theta(2^d) + \theta(p)$	$\theta(2^d) + \theta(p.k)$
[۷]	$\theta(2^d) + \theta(1) + \theta(m)$	$\theta(2^d) + \theta(k) + \theta(m.k)$
[۸]	$\theta(2^d) + \theta(1) + \theta(p)$	$\theta(2^d) + \theta(p.k) + \theta(k)$
[۹]	$\theta(2^d) + \theta(n) + \theta(p)$	$\theta(2^d) + \theta(n) + \theta(p.k)$
[۱۰]	$\theta(2^d) + \theta(p+a)$	$\theta(2^d) + \theta(p.a)$

۳-۵. حملات

حملات به شبکه‌های زنجیره قالبی شامل دودسته عام و خاص هستند. دسته عام، حملاتی مانند سیبیل که هر نوع از شبکه زنجیره قالبی باتوجه‌به مکانیزم اجماع و سیاست‌های امنیتی ممکن است در برابر این حمله آسیب‌پذیر باشد و ربطی به نوع زنجیره‌ی قالبی ندارد. دسته دوم حملاتی هستند که فقط نوع خاصی از شبکه‌های زنجیره قالبی در برابر این حملات آسیب‌پذیر است که این حملات بستگی به نوع شبکه زنجیره قالبی (مثل خصوصی یا عمومی بودن) دارد. در این بخش مقاومت طرح پیشنهادی نسبت به انواع حملات عام و حملات مرتبط با نوع شبکه زنجیره قالبی طرح خود بررسی خواهد شد.

۱- حمله سیبیل[1] :

در این حمله، یک مهاجم چندین هویت جعلی در یک شبکه غیرمتمرکز ایجاد می‌کند تا کنترل شبکه را به دست بگیرد. به‌طورکلی در برابر این حمله مقاوم است. در سامانه‌های زنجیره قالبی کنسرسیومی و خصوصی که از PBFT استفاده می‌کنند، حملات سیبیل به دلیل نیاز به حضور گره‌های معتبر و تأیید شده در شبکه، مشکل‌ساز می‌شوند. همچنین، در زنجیره‌قالبی‌های کنسرسیومی، اعضای شبکه معمولاً شناخته‌شده و قابل‌اعتماد هستند و بنابراین می‌توان گفت که طرح پیشنهادی، به دلیل استفاده از مکانیزم اجماع PBFT می‌تواند حملات سیبیل را تا حد قابل‌توجهی کاهش دهد و به‌طورکلی می‌توان گفت که در برابر این دسته از حملات مقاوم است؛ ولی ازآنجاکه در این طرح از زنجیره‌قالبی‌های خصوصی و کنسرسیومی استفاده شده،

[1] Sybil Attack

باتوجه‌به اینکه در برابر حملات رشوه و یا کارتل آسیب‌پذیر است، درصورتی‌که انجام این حملات روی شبکه موفق باشد، در برابر حمله سیبیل نیز، آسیب‌پذیر خواهد شد.

۲- هدررفت دوگانه[1]:

در این حمله، یک مهاجم یک ارز دیجیتال یا توکن را بیش از یک‌بار خرج می‌کند. این کار معمولاً با ارسال یک تراکنش معتبر و هم‌زمان ایجاد یک تراکنش متقلبانه برای بازگرداندن توکن‌های خرج‌شدن انجام می‌شود. استفاده از PBFT به‌عنوان مکانیزم اجماع، حملات دوگانه‌سازی را متوقف می‌کند؛ زیرا در این مکانیزم اجماع، تنها گره‌هایی که موردتأیید اکثریت قرار می‌گیرند، می‌توانند تراکنش‌ها را تأیید کنند؛ بنابراین امکان تأیید یک تراکنش دوباره وجود ندارد. در نتیجه طرح پیشنهادی به دلیل استفاده از مکانیزم اجماع PBFT در برابر این حمله کاملاً مقاوم است.

۳- حمله مسابقه‌ای[2]:

این حمله، زمانی رخ می‌دهد که یک مهاجم دو تراکنش متناقض را به طور هم‌زمان به شبکه ارسال می‌کند، یکی به یک پذیرنده (که پرداخت را فوری تأیید می‌کند) و دیگری به خودش (برای خرج دوباره همان ارز دیجیتال یا توکن). اگر پذیرنده قبل از تأیید زنجیره قالبی کالا یا خدمات را ارائه دهد، ممکن است قربانی این حمله شود. به دلیل استفاده از PBFT و ساختارهای غیرمتمرکز و پیوسته در زنجیره قالبی، انجام حملات مسابقه‌ای که در آن مهاجم تلاش می‌کند تراکنش‌های خود را سریع‌تر از بقیه منتشر کند، بسیار دشوار است. در نتیجه طرح پیشنهادی به دلیل استفاده از امضای SLTG و مکانیزم اجماع PBFT در برابر این حمله کاملاً مقاوم است.

۴-حمله فینی[3]:

در این حمله، ماینر ابتدا یک تراکنش را استخراج کرده؛ ولی آن را به شبکه ارسال نمی‌کند. سپس با استفاده از همان توکن‌ها یک تراکنش جدید برای قربانی ارسال می‌کند. اگر قربانی بدون تأیید کافی تراکنش را بپذیرد، ممکن است دچار ضرر شود. این حمله نیاز به استخراج یک قالب خاص و تأخیر در انتشار تراکنش‌ها دارد. اما استفاده از PBFT با اجماع سریع و بر اساس تأیید گره‌ها، امکان موفقیت این حمله بر طرح پیشنهادی را کاهش می‌دهد.

۵- دزدی محاسباتی[4]:

زمانی رخ می‌دهد که مهاجم به طور مخفیانه از منابع محاسباتی قربانی)مانند CPU یا GPU برای استخراج ارز دیجیتال استفاده می‌کند. این حمله معمولاً از طریق بدافزارها یا اسکریپت‌های مخفی در وبگاه‌ها انجام می‌شود و باعث کاهش عملکرد سامانه قربانی و افزایش مصرف برق می‌شود. دزدی محاسباتی به سرقت قدرت محاسباتی و منابع شبکه اشاره دارد. استفاده از PBFT و DP-ABE در طرح پیشنهادی باعث می‌شود که تنها گره‌های معتبر و تأیید شده قادر به انجام تراکنش‌ها باشند و دزدی محاسباتی از گره‌های مخرب غیرممکن می‌شود.

۶- حمله منع سرویس توزیع‌شده[5]:

زمانی رخ می‌دهد که مهاجم با ارسال حجم زیادی از ترافیک جعلی از چندین منبع، یک سرور، شبکه یا سرویس را هدف قرار می‌دهد تا آن را از دسترس خارج کند. این حمله باعث کندی یا ازکارافتادن سامانه می‌شود. آسیب‌پذیر. سامانه‌های زنجیره قالبی، حتی با استفاده از PBFT، ممکن است در برابر حملات DDoS آسیب‌پذیر باشند؛ زیرا این حملات ممکن است گره‌ها را با درخواست‌های بسیار زیاد هدف قرار دهد. هرچند که PBFT برخی از این حملات را کاهش می‌دهد، اما در برابر حملات مقیاس‌پذیر همچنان آسیب‌پذیر است؛ بنابراین، طرح پیشنهادی در برابر این حمله کاملاً آسیب‌پذیر است.

۷- حمله تغییر زمان[6]:

مهاجم با تغییر زمان گزارش‌شده توسط گره‌های مخرب، زمان شبکه را دست‌کاری می‌کند. در شبکه‌های کنسرسیومی که گره‌ها معتبر و کنترل‌شده هستند، هماهنگی دقیق زمان‌سنجی در شبکه به کاهش احتمال وقوع حملات تغییر زمان کمک می‌کند. در چنین سیستمی، احتمال دست‌کاری زمان به شدت کاهش می‌یابد. درصد کاهش یا افزایش دست‌کاری در این نوع از حملات، بستگی به نوع مکانیزم اجماع، نوع شبکه، و دقت نظارت دارد. استفاده از امضای SLTG و مکانیزم اجماع PBFT و شبکه‌های خصوصی و کنسرسیومی و نظارت دقیق بر کاربران در طرح پیشنهادی باعث می‌شود که این طرح در برابر این حمله، کاملاً مقاوم باشد.

۸- حمله بازپخش[7]:

یک مهاجم داده‌های یک تراکنش معتبر را ضبط کرده و بدون تغییر مجدداً به شبکه ارسال می‌کند. این حمله می‌تواند باعث انجام دوباره یک تراکنش بدون رضایت کاربر شود. با

[1] Double-Spending
[2] Race Attack
[3] Finney Attack
[4] Cryptojacking
[5] DDoS
[6] Timejacking
[7] Replay Attack

استفاده از امضای SLTGS و سیاست‌های رمزنگاری DP-ABE، هر تراکنش به طور دقیق ثبت و پیوند داده می‌شود، بنابراین امکان بازپخش آن غیرممکن است. در نتیجه به دلیل استفاده از امضای SLTGS، رمزنگاری DP-ABE، و مکانیزم اجماع PBFT در طرح پیشنهادی، این طرح در برابر این حمله کاملاً مقاوم است.

۹- حمله به سازمان خودگردان غیرمتمرکز (دائو) [1]:

به حمله‌ای اشاره دارد که در سال ۲۰۱۶ روی یک سازمان خودگردان غیرمتمرکز روی شبکه اتریوم انجام شد. در این حمله، مهاجم از یک باگ بازگشتی در قرارداد هوشمند استفاده کرد و توانست بخش زیادی از سرمایه را بدون اجازه از قرارداد خارج کند. حملات به سازمان‌های خودگردان غیرمتمرکز ممکن است منجر به فساد یا کلاهبرداری شوند. در شبکه‌های کنسرسیومی، تصمیم‌گیری‌ها توسط گروه‌های شناخته‌شده انجام می‌شود و این ساختار از حملات مشابه حمله دائو جلوگیری می‌کند. در نتیجه به دلیل استفاده از شبکه کنسرسیومی در طرح پیشنهادی، این طرح در برابر حملات دائو کاملاً مقاوم است.

۱۰- حمله ورود مجدد [2]:

زمانی رخ می‌دهد که یک قرارداد هوشمند به طور ناخواسته و در هنگام اجرای یک تراکنش، به خود فراخوانی می‌کند. این نوع حمله معمولاً زمانی اتفاق می‌افتد که یک قرارداد پس از انجام تراکنش، قبل از به‌روزرسانی وضعیت خود، از یک قرارداد دیگر درخواست پرداخت می‌کند. حملات ورود مجدد می‌توانند زمانی که سامانه‌ها به طور نادرست پیاده‌سازی شوند، آسیب‌پذیر باشند. در صورت استفاده از قراردادهای هوشمند، تدابیر امنیتی باید به‌درستی پیاده‌سازی شوند تا از وقوع این حملات جلوگیری شود.

به دلیل استفاده از مکانیزم اجماع PBFT در طرح پیشنهادی، این طرح در برابر این حمله کاملاً مقاوم است.

۱۱- حمله کسوف [3]:

مهاجم تمامی نودهای یک شبکه را در معرض دید خود قرار می‌دهد و ارتباط نود هدف را تنها با گره‌های تحت کنترل خود برقرار می‌کند. این حمله باعث می‌شود که نود هدف نتواند اطلاعات صحیح از شبکه دریافت کند، زیرا تمام داده‌ها و تراکنش‌ها از گره‌های جعلی عبور می‌کنند. حمله کسوف به قطع ارتباطات و ایجاد وقفه در روند اجماع اشاره دارد. استفاده‌ی طرح پیشنهادی از PBFT که بر تأیید گره‌های معتبر تکیه دارد، این نوع از حملات را غیرممکن می‌سازد، زیرا برای اجرای چنین حمله‌ای باید تأییدات تمام گره‌ها مختل شود.

۱۲- حمله مسیریابی [4]:

زمانی رخ می‌دهد که مهاجم با دست‌کاری در پروتکل‌های مسیریابی شبکه، ترافیک داده‌ها را به گره‌های مخرب هدایت می‌کند. حملات مسیریابی در شبکه‌های عمومی ممکن است موجب تغییر مسیر داده‌ها شوند. در شبکه‌های کنسرسیومی با گره‌های شناخته‌شده و قابل‌اعتماد، حملات مسیریابی به طور قابل‌توجهی کاهش می‌یابد. در نتیجه به دلیل استفاده از PBFT و شبکه کنسرسیومی در طرح پیشنهادی، این طرح در برابر حمله مسیریابی مقاوم است.

۱۳- حمله رشوه‌دهی [5]:

حملات رشوه‌دهی در شبکه‌های مبتنی بر PBFT ممکن است درصورتی‌که گره‌ها تحت‌تأثیر فشار یا رشوه قرار گیرند، منجر به فساد شوند؛ بنابراین، نظارت دقیق و شفافیت در این شبکه‌ها برای جلوگیری از چنین حملاتی ضروری است. در نتیجه طرح پیشنهادی در برابر این حمله، آسیب‌پذیر است.

۱۴- حمله رأی‌گیری [6]:

در حملات رأی‌گیری، هدف تقلب در فرایند رأی‌گیری است. با استفاده از امضای SLTGS و DP-ABE در طرح پیشنهادی، این فرایند به طور دقیق کنترل می‌شود و امکان تقلب در رأی‌گیری کاهش می‌یابد.

۱۵- حمله تعقیب‌کننده [7]:

یک مهاجم به طور مداوم تراکنش‌های یک کاربر خاص را در شبکه زنجیره قالبی دنبال می‌کند. استفاده از DP-ABE و امضای SLTGS در طرح ارائه شده می‌تواند از تعقیب‌کنندگان جلوگیری کند؛ زیرا هر فرد فقط به داده‌های مجاز دسترسی خواهد داشت و اطلاعات مربوط به ویژگی‌های شخصی در دسترس نخواهد بود. در نتیجه طرح پیشنهادی در برابر این حمله مقاوم است.

۱۶- حمله رأی‌گیری موازی [8]:

حمله رأی‌گیری موازی به ثبت چندین رأی به طور هم‌زمان اشاره دارد. با استفاده از SLTGS، رأی‌ها به‌دقت ثبت و پیوند داده می‌شوند و احتمال آسیب‌پذیری طرح پیشنهادی در برابر این حمله به طور مؤثری کاهش می‌یابد.

[1] Decentralized Autonomous Organization (DAO) Attack
[2] Reentrancy Attack
[3] Eclipse Attack
[4] Routing Attack
[5] Bribery Attack
[6] Voting Attack
[7] Stalker Attack
[8] Attack of Parallel Voting

۱۷- حمله لحظه آخر[1]:

حمله لحظه آخر در سامانه‌هایی که به تصمیم‌گیری‌های لحظه‌ای وابسته هستند، می‌تواند به مشکلاتی منجر شود. به‌منظور جلوگیری از این حملات، باید زمان تصمیم‌گیری دقیقاً سنجیده و تأیید شود. باتوجه‌به استفاده از مکانیزم اجماع PBFT در طرح پیشنهادی، می‌توان به این نتیجه رسید که طرح پیشنهادی در برابر این حمله مقاوم است.

۱۸- آسیب‌پذیری منطقی رأی‌گیری[2]:

آسیب‌پذیری‌های منطقی در فرایندهای رأی‌گیری ممکن است منجر به تقلب شوند. استفاده از DP-ABE و SLTGS در طرح پیشنهادی این آسیب‌پذیری‌ها را از بین می‌برد؛ زیرا تمام فرایندهای تأیید و شفافیت به‌دقت پیاده‌سازی شده‌اند. در نتیجه طرح ارائه شده در برابر این حملات کاملاً مقاوم است.

۱۹- حمله کارتل[3]:

باتوجه‌به ویژگی‌های PBFT و ساختار کنسرسیومی و خصوصی و همچنین وجود شفافیت در شبکه، حمله کارتل به طور قابل‌توجهی کاهش می‌یابد، زیرا ایجاد یک هم‌پیمانی قوی بین نهادهای مختلف در چنین شبکه‌هایی دشوار است؛ بنابراین، طرح پیشنهادی مقاومتی خوب در برابر این نوع حمله دارد؛ ولی کاملاً مقاوم نیست.

۲۰- حمله ۵۱ درصد[4]

حملات ۵۱ درصد زمانی رخ می‌دهند که مهاجم بیش از نیمی از گره‌ها را کنترل کند. با استفاده از PBFT که تحمل خطای بیزانسی را مدیریت می‌کند، طرح پیشنهادی در برابر این حمله مقاوم است.

۲۱- حملات BFT:

حملات BFT (توافق بیزانسی) به حملاتی اطلاق می‌شود که در آن برخی گره‌ها مخرب هستند. استفاده از PBFT به‌گونه‌ای است که حتی در صورت وجود گره‌های مخرب، شبکه می‌تواند به کار خود ادامه دهد. در نتیجه استفاده از PBFT باعث مقاومت طرح پیشنهادی در برابر این حمله شده است.

۲۲- حمله بازگشتی[5]:

حملات بازگشتی به حملاتی گفته می‌شود که به فرایندهای قبلی حمله می‌کنند. سیاست‌های رمزنگاری دقیق و شرایط دسترسی مبتنی بر ویژگی‌ها، از این نوع حملات جلوگیری می‌کنند و استفاده از رمزنگاری DP-ABE باعث مقاومت طرح پیشنهادی در برابر این حمله شده است.

باتوجه‌به توضیحات داده شده در این بخش، می‌توان گفت که حملات طرح پیشنهادی به سه دسته تقسیم می‌شوند: کاملاً مقاوم، آسیب‌پذیر و مشروط.

➢ **حملات آسیب‌پذیر:**

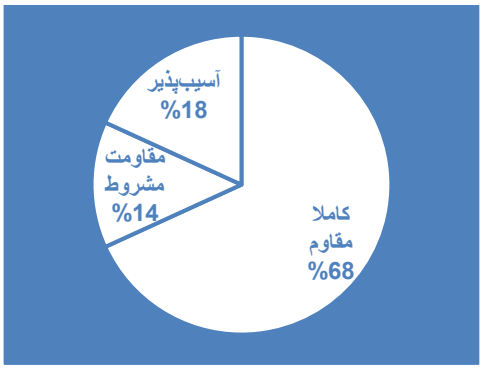
حملات انکار خدمات توزیع‌شده (DDOS)، رشوه، حمله لحظه آخر و کارتل از این دسته حملات هستند که به دلیل استفاده از زنجیره‌قالبی‌های خصوصی و کنسرسیومی، طرح پیشنهادی می‌تواند در برابر این دسته از حملات آسیب‌پذیر باشد.

➢ **حملات مشروط:**

حملات سیبیل، مقاومت در برابر حملات BFT و دزدی محاسباتی از این دسته حملات هستند چرا که به‌طورکلی طرح ما در برابر این حملات مقاوم است؛ ولی درصورتی‌که انجام یکی از حملات DDOS ، رشوه، حمله لحظه آخر و یا کارتل روی طرح ما موفق شود، طرح ما در برابر این سه حمله نیز، آسیب‌پذیر خواهد شد.

➢ **حملات کاملاً مقاوم:**

به جز هفت حمله دودسته قبل که توضیح داده شد، طرح پیشنهادی در برابر باقی حملات، کاملاً مقاوم است. شکل (۶) نمودار دسته‌بندی جزئی طرح پیشنهادی به حملات بررسی شده را نشان می‌دهد و شکل (۷) دسته‌بندی کلی را نشان می‌دهد.

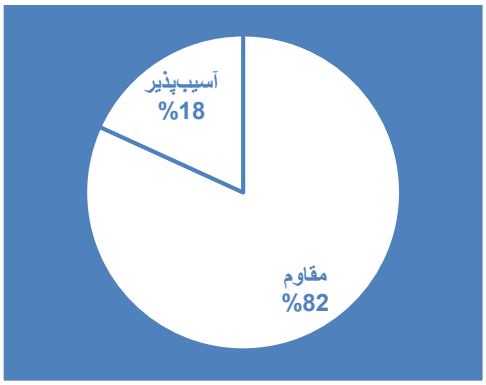


شکل (۶). دسته‌بندی جزئی مقاومت طرح پیشنهادی حملات بررسی شده

در این بخش بیست و دو حمله را برای طرح خود بررسی شد که از این تعداد، طرح پیشنهادی در برابر پانزده حمله یعنی ۶۸ درصد از حملات کاملاً مقاوم، در برابر سه حمله یعنی ۱۴ درصد دارای مقاومت مشروط، و در برابر چهار نوع حمله یعنی ۱۸ درصد حملات بررسی شده آسیب‌پذیر است؛ این موضوع نشان می‌دهد به‌طورکلی در برابر ۸۲ درصد حملات شناخته شده به زنجیره قالبی مقاوم است؛ بنابراین می‌توان ادعا کرد که طرح

[1] Attack of the Last Moment
[2] Logical Vulnerability of Voting
[3] Cartel Attack
[4] 51 percent Attack
[5] Collusion Resistance

پیشنهادی برای کنترل دسترسی در سامانه سلامت الکترونیک، طرحی امن محسوب می‌شود.



شکل (۷). دسته‌بندی کلی مقاومت طرح پیشنهادی حملات بررسی شده

۴. نتیجه‌گیری

طرح‌های کنترل دسترسی در سامانه سلامت الکترونیک در بخش دوم مورد بررسی قرار گرفت و بهترین آن‌ها به‌عنوان پایه طرح پیشنهادی انتخاب شد. طرح کنترل دسترسی امن در سلامت الکترونیک با استفاده از رمزنگاری مبتنی بر ویژگی دوگانه، امضای گروهی قابل‌ردیابی و قابل پیوند انتخابی، و زنجیره قالبی دوگانه ارائه گردید. در این طرح، چهار وضعیت مختلف برای تعیین دسترسی در سامانه سلامت الکترونیک در نظر گرفته شد و بر اساس این شرایط، بخش‌های مختلف ساختار طرح تعریف شدند. در این طرح، از دو نوع زنجیره قالبی خصوصی و کنسرسیومی استفاده شده است. زنجیره خصوصی برای ثبت تراکنش‌های مربوط به‌سلامت، و زنجیره کنسرسیومی برای ثبت تراکنش‌های نظارتی به کار گرفته می‌شود. همچنین، باتوجه‌به وظایف و دسترسی‌های موردنیاز کاربران، مالک و کاربر داده به‌صورت پویا تعریف شدند و مراحل طرح پیشنهادی برای دو وضعیت عادی و اورژانسی، به همراه حالت‌های نیازمند همکاری و بدون همکاری، تشریح گردید. در این مقاله، یک طرح کنترل دسترسی امن با ویژگی‌های انعطاف‌پذیری، قابلیت ردیابی، شفافیت، ناشناس بودن، قابلیت حذف و لغو و ابطال، جستجوی امن، و پیوند انتخابی ارائه شد. در این مقاله، بیست و دو حمله از معروف‌ترین حملات به زنجیره‌های قالبی برای طرح پیشنهادی بررسی شد که در برابر شصت و هشت درصد از آن‌ها کاملاً مقاوم، در برابر چهارده درصد مقاومت مشروط و در برابر هجده درصد آسیب‌پذیر بود.

۵. مراجع

مقاله‌های چاپ‌شده در مجلات:

[1] World Health Organization (WHO), "eHealth," World Health Organization. Available: https://www.emro.who.int/health-topics/ehealth/. [Accessed: Jan. 20, 2025].

[2] C. Ruan, C. Hu, R. Zhao, Z. Liu, H. Huang, and J. Yu, "A policy-hiding attribute-based access control scheme in decentralized trust management", IEEE Internet of Things Journal, vol. 10, no. 20, pp. 17656–17665, Oct. 2023.

[3] W. Dai, S. Tuo, L. Yu, K.-K. R. Choo, D. Zou, and H. Jin, "HAPPS: A hidden attribute and privilege-protection data-sharing scheme with verifiability", IEEE Internet of Things Journal, vol. 9, no. 24, Dec. 2022.

[4] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control", IEEE Internet Things Journal, vol. 8, no. 14, Jul. 2021.

[5] L. Zhang, T. Zhang, Q. Wu, Y. Mu, and F. Rezaeibagha, "Secure decentralized attribute-based sharing of personal health records with blockchain", IEEE Internet Things Journal, vol. 9, no. 14, Jul. 2022.

[6] M. Wazid, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and M. Guizani, "AISCM-FH: AI-enabled secure communication mechanism in fog computing-based healthcare", IEEE Trans. Inf. Forensics Security, vol. 18, 2023.

[7] O. Samuel, A. B. Omojo, S. M. Mohsin, P. Tiwari, D. Gupta, and S. S. Band, "An anonymous IoT-based E-health monitoring system using blockchain technology," IEEE Systems Journal, vol. 17, no. 2, pp. 2422–2433, Jun. 2023.

[8] Z. Bao, D. He, H. Wang, M. Luo, and C. Peng, "A Group Signature Scheme with Selective Linkability and Traceability for Blockchain-Based Data Sharing Systems in E-health Services", IEEE Internet of Things Journal, 2023.

[9] G. Peng, A. Zhang, and X. Lin, "Patient-centric fine-grained access control for electronic medical record sharing with security via dual-blockchain," IEEE Trans. Netw. Sci. Eng., vol. 10, no. 6, pp. 3908–3921, Nov./Dec. 2023.

[10] S. Xu, J. Ning, Y. Li, Y. Zhang, G. Xu, X. Huang, and R. H. Deng, "A secure EMR sharing system with tamper resistance and expressive access control," IEEE Trans. Dependable Secure Comput., vol. 20, no. 1, pp. 53–67, Jan. 2021.

[11] L. Zhang, Y. Zhu, W. Ren, Y. Zhang, and K.-K. R. Choo, "Privacy-preserving fast three-factor authentication and key agreement for IoT-based e-health systems", IEEE Trans. Services Comput, vol. 16, no. 2, Mar./Apr. 2023.

[12] M. Wang, Y. Guo, C. Zhang, C. Wang, H. Huang, and X. Jia, "MedShare: A privacy-preserving medical data sharing system by using blockchain," IEEE Trans. Serv. Comput., vol. 16, no. 1, pp. 438–451, Jan./Feb. 2021.

[13] J. Liu, W. Jiang, R. Sun, A. K. Bashir, M. D. Alshehri, Q. Hua, and K. Yu, "Conditional anonymous remote healthcare data sharing over

blockchain," IEEE J. Biomed. Health Informatics, vol. 27, no. 5, pp. 2231–2242, May 2023.
[14] J. Li, D. Li, and X. Zhang, "A secure blockchain-assisted access control scheme for smart healthcare system in fog computing", IEEE Internet Things Journal, vol. 10, no. 18, Sep. 2023.
[15] E. Chen, Y. Zhu, Z. Zhou, S.-Y. Lee, W. E. Wong, and W. C.-C. Chu, "Policychain: A decentralized authorization service with script-driven policy on blockchain for internet of things", IEEE Internet Things Journal, vol. 9, no. 7, Apr. 2022.
[16] H. Gao, H. Huang, L. Xue, F. Xiao, and Q. Li, "Blockchain-enabled fine-grained searchable encryption with cloud-edge computing for electronic health records sharing", IEEE Internet Things Journal, vol. 10, no. 20, Oct. 2023.
[17] A. S. Rajasekaran, M. Azees, and F. Al-Turjman, "A comprehensive survey on blockchain technology", Sustainable Energy Technologies and Assessments, vol. 52, Aug. 2022, Art. no. 102039.
[18] D. Chaum, E. van Heyst, "Group signatures", in Advances in Cryptology—EUROCRYPT'91: Workshop on the Theory and Application of Cryptographic Techniques, Brighton, UK, Apr. 8–11, 1991, pp. 257–265, Springer, Berlin, Heidelberg.
[19] G. Wu, S. Wang, Z. Ning, and B. Zhu, "Privacy-preserved electronic medical record exchanging and sharing: A blockchain-based smart healthcare system," IEEE J. Biomed. Health Informatics, vol. 26, no. 5, pp. 1917–1927, May 2021.
[20] L. Garms and A. Lehmann, "Group signatures with selective linkability", in International Conference on Practice and Theory of Public Key Cryptography (PKC), Springer, 2019, pp. 190–220.
[21] Y. He, Z. Yan, and T. Yuan, "Attribute-based access control scheme for secure identity resolution in prognostics and health management", IEEE Internet Things Journal, 2024.
[22] D. Chen, L. Zhang, Z. Liao, H.-N. Dai, N. Zhang, X. Shen, and M. Pang, "Flexible and fine-grained access control for EHR in blockchain-assisted e-healthcare systems," IEEE Internet Things J., 2024.
[23] H. Yin, Y. Zhu, H. Deng, L. Ou, Z. Qin, and K. Li, "Privacy-preservation enhanced and efficient attribute-based access control for smart health in cloud-assisted Internet of Things," IEEE Internet Things Journal, 2025.