**پیاده‌سازی بلاک‌چین مراقبت‌های بهداشتی مبتنی بر توکن مبتنی بر بیمار با استفاده از اینترنت امن اشیاء پزشکی**

مریم یگانه

40212340076006

چکیده:

حفظ امنیت و حریم خصوصی در دنیای داده امروزی که به سرعت در حال رشد است به طور فزاینده ای دشوار می شود. ما از اینترنت اشیاء پزشکی (IoMT) برای تشخیص سریع و دریافت نتایج استفاده می کنیم. دستگاه های IoMT عملکرد بدن انسان را در پارامترهای مختلف اندازه گیری می کنند و داده ها را در سرورهای ابری جمع آوری، پردازش و ذخیره می کنند. یک کانال عمومی برای جمع‌آوری داده‌ها از انسان و ارسال آن به فضای ابری وجود دارد که بسیار غیرقابل اعتماد و در برابر حملات آسیب‌پذیر است. خطر دیگر ذخیره سازی داده ها در یک سیستم متمرکز است که می تواند در برابر خرابی تک نقطه ای آسیب پذیر باشد. بلاک چین برای ذخیره سازی امن داده ها به صورت غیرمتمرکز استفاده می شود تا از شکست تک نقطه ای جلوگیری شود. ما یک روش جمع‌آوری داده ایمن مبتنی بر IoMT را برای بیماران و ذخیره داده‌ها بر روی بلاک چین مطابق با مقررات حفاظت از داده‌های عمومی (GDPR) پیشنهاد می‌کنیم. در سیستم پیشنهادی، دستگاه‌های IoMT داده‌ها را از طریق دستیار دیجیتال شخصی بیمار (PDA) به ابر ارسال می‌کنند و سرور ابری داده‌ها را روی بلاک چین تراکنش می‌کند. ما یک الگوریتم انتخاب ماینر را برای جلوگیری از سوگیری در بلاک چین پیشنهاد می کنیم. ما حملات مختلف را بر روی کانال های باز بین دستگاه های IoMT و سرورهای ابری شبیه سازی می کنیم. این طرح بر روی یک بلاک چین سفارشی مبتنی بر پایتون پیاده سازی شده است. شبیه‌سازی اینترنت اشیا با استفاده از شبیه‌ساز اینترنت اشیا Bevywise و شبیه‌ساز انتقال تله متری صف پیام (MQTT) انجام می‌شود. پروتکل امنیتی با استفاده از Scyther تجزیه و تحلیل می شود.

کلمات کلیدی - احراز هویت، بلاک چین، مراقبت های بهداشتی، اینترنت اشیاء پزشکی (IoMT)، حریم خصوصی، امنیت.

نامگذاری

\*\*\*

1. مقدمه

آ. بهداشت و درمان و بلاک چین

در بخش مراقبت های بهداشتی، حفظ حریم خصوصی داده های بیمار بسیار مهم است. بلاک چین راهی برای ارائه ذخیره سازی داده های امن، تغییرناپذیر، ساختاریافته، تایید شده و قابل اعتماد است. فناوری بلاک چین برای ذخیره داده ها و ارسال یک کپی از آن داده ها به تمام گره های شبکه بلاک چین استفاده می شود، در حالی که در شبکه های بلاک چین بیمار محور، ما داده ها را از بیماران گرفته و در بلاک چین ذخیره می کنیم. به طوری که داده ها حاوی اطلاعات قابل شناسایی شخصی (PII) نباشند. بلاک چین بیمار محور بر مزایای بیماران و راحتی بیمار در طول فرآیند تراکنش و ایجاد بلاک تمرکز دارد. از آنجایی که به صورت رمزنگاری ایمن است و با استفاده از هش کردن تراکنش ها و بلوک ها ناشناس است، سیستم مراقبت های بهداشتی مبتنی بر بلاک چین قابل اعتماد و تأیید است و از اطلاعات قابل شناسایی بیماران محافظت می کند. داده های مراقبت های بهداشتی برای بسیاری از اهداف دیگر مانند بیمه درمانی و تحقیقات پزشکی استفاده می شود. پلتفرم بلاک چین که برای به اشتراک گذاری سوابق مراقبت های بهداشتی استفاده می شود، اغلب در سازمان های بیمه یا تحقیقاتی در مقایسه با بلاک چین بیمارستانی متمایز است. در بخش مراقبت های بهداشتی، رعایت مقررات حفاظت از داده های عمومی (GDPR) ضروری است. بلاک چین یک طرح حفاظتی مبتنی بر رمزگذاری بر اساس هش های رمزنگاری ارائه می دهد که سوابق ایمن را از نظر حملات دشمن و سناریوهای هک ایجاد می کند. به گفته حسن و صلاح [1]، سیستم های متمرکز از یک نقطه شکست رنج می برند. با این حال، از آنجایی که بلاک چین یک سیستم غیرمتمرکز است، از این مشکل مصون است.

ب. اینترنت اشیاء پزشکی (IoMT) و شبکه ناحیه بدن (BAN)

اینترنت اشیا (IoT) شبکه ای از دستگاه های کوچک است که با قدرت کمتر و حافظه کم کار می کنند، داده های خود را در ابرها پردازش می کنند و نتایج را به دستگاه های قابل حمل کاربر برمی گرداند. از آنجایی که این دستگاه‌های کوچک در یک محیط شبکه باز و ناامن کار می‌کنند و بنابراین در برابر هکرها آسیب‌پذیر هستند، امنیت اشتراک‌گذاری داده و اتصال باید در اولویت قرار گیرد. IoMT به دستگاه های مختلفی اطلاق می شود که برای اندازه گیری و انتقال داده ها به پزشکان از راه دور به منظور نظارت از راه دور سلامت بیماران استفاده می شود. از این دستگاه ها می توان برای اندازه گیری ضربان قلب، فشار خون، سطح اکسیژن خون، نوار قلب (ECG)، نوار مغزی (EEG) و صدمات استفاده کرد. این دستگاه ها برای انجام یک وظیفه خاص برای اهداف درمانی پزشکی و ارسال داده ها به سرور ابری متمرکز ساخته شده اند. BAN شبکه ای از دستگاه هایی است که برای اندازه گیری فعالیت های مختلف بدن استفاده می شود. BAN برای محاسبه و ذخیره داده ها برای تحقیقات و بهینه سازی آینده با سرور ابری متصل می شود. از آنجایی که فضای ابری نیز ظرفیت ذخیره سازی محدودی دارد، داده ها پس از یک دوره مشخص حذف می شوند. به گفته شو و همکاران. [2]، یک سیستم فیزیکی سایبری پزشکی تجهیزات پزشکی تعبیه شده را از طریق یک شبکه بی سیم کنترل می کند به طوری که داده های فیزیکی بیمار در زمان واقعی حس و نظارت می شود. هنگامی که بیمار وضعیت غیرعادی دارد، تجهیزات پزشکی اطلاعات هشدار اولیه را به موقع به موسسه پزشکی ارسال می کند.

ج. امنیت و حریم خصوصی در بلاک چین های مراقبت های بهداشتی

در بلاک چین مبتنی بر مراقبت های بهداشتی، می توان ارتباط بین گره بیمار و گره پزشک، گره بیمار و گره داروخانه، گره بیمار و گره آزمایشگاه تست و بالعکس امکان پذیر باشد. از آنجایی که داده‌های موجود در بلاک چین مبتنی بر IoMT به صورت ناشناس در گره ابری جمع‌آوری می‌شوند، هویت بیمار پنهان مانده است. لایه امنیتی بین دستگاه IoMT و بیمار، دستگاه قابل حمل بیمار و ابر، و گره سرور ابری و گزارش دسترسی مقامات مانند پزشک، پرستار، آزمایشگاه و داروخانه قرار دارد. به گفته کای و همکاران. [3]، گره های بلاک چین با استفاده از پیوندهای محکم امضای رمزنگاری و توابع هش به هم متصل می شوند و ارتباط بین گره ها با استفاده از این توابع رمزنگاری ایمن است. با توجه به تانگ و همکاران، احراز هویت بین داده‌های ذخیره شده در بلاک چین و گره‌های بلاک چین مورد نیاز است. [4]. برای محافظت از داده‌های بیمار، امنیت بلاک چین باید در برابر حملات چندشناسه ای و حمله فرد میانی بلاک‌چین‌های مبتنی بر ابر، و همچنین محافظت از حملات DDoS در گره‌های توزیع‌شده و انواع تهدیدات دیگر مقاوم باشد.

د. انگیزه و هدف

با توجه به وضعیت فوق، ما می‌خواهیم یک سیستم بلاک چین بیمار محور طراحی کنیم که داده‌های بیمار را از دستگاه‌های IoMT اندازه‌گیری می‌کند و با امنیت و احراز هویت نفوذ ناپذیر به سرورهای ابری در یک شبکه عمومی منتقل می‌کند. سرورهای ابری به عنوان گره های جمع آوری داده از دستگاه های IoMT عمل می کنند. گره های پزشک به عنوان تایید کننده بلوک ها عمل می کنند. اهداف اصلی این مقاله به شرح زیر است.

1) توسعه یک بلاک چین مبتنی بر IoMT بیمار محور برای جمع آوری و ذخیره داده های بیمار.

2) برای اندازه گیری الزامات امنیتی سیستم پیشنهادی.

3) برای پیشنهاد الگوریتم انتخاب ماینر بین سرور ابر و گره دکتر.

4) ابزار Scyther برای انجام تحلیل امنیتی سیستم پیشنهادی استفاده می شود. IoTSimulator زیرساخت اینترنت اشیا را شبیه سازی می کند. پایتون برای پیاده سازی بلاک چین استفاده می شود.

ه. سازماندهی مقاله

بررسی ادبیات این مقاله در بخش دوم توضیح داده شده است. بخش III سیستم پیشنهادی و الگوریتم های پیشنهادی را توضیح می دهد. پیاده سازی سیستم پیشنهادی در بخش IV توضیح داده شده است. بخش V نتایج و همچنین تجزیه و تحلیل امنیتی سیستم پیاده سازی شده را تشریح می کند. مقایسه سیستم پیشنهادی با سیستم‌های توسعه‌یافته قبلی در بخش ششم توضیح داده شده است. بخش هفتم این مقاله را با دامنه آینده به پایان می رساند.

1. بررسی ادبیات

بلاک چین های خصوصی، عمومی و کنسرسیومی همگی می توانند برای پیاده سازی مدیریت سوابق مراقبت های بهداشتی بر روی بلاک چین استفاده شوند. به گفته وانگ و همکاران. [5]، BAN بی‌سیم به‌عنوان یک قسمت جلویی در بلاک چین استفاده می‌شود، داده‌های سلامت بیمار را از طریق دستگاه‌های IoMT دریافت می‌کند، گره‌های حسگر را به هم متصل می‌کند و با یک شبکه بلاک چین در پشت صحنه تعامل می‌کند. کاربرانی که عضو سیستم هستند رابط جلویی را تشکیل می دهند. Rahoof و Deepthi [6] بلاک چین را در سیستم مدیریت مراقبت های بهداشتی به عنوان امن، مقیاس پذیر و کم ذخیره تعریف کردند. آنها یک طرح مبتنی بر ویژگی برای کار با بلاک چین و IPFS به عنوان یک سیستم ذخیره سازی داده مقیاس پذیر ایجاد کردند. براتی و رانا [7] استفاده از بلاک چین را در بازرسی دستگاه های اینترنت اشیاء برپایه GDPR توصیف کردند که برخی از قوانین GDPR را به قراردادهای هوشمند تبدیل می‌کند تا تأیید خودکار اشیاء هوشمند را که نقش‌های آن‌ها کنترل‌کننده یا پردازشگر داده‌ها هستند، تسهیل کند. ری و همکاران [8] معماری جریان داده IoBHealth مبتنی بر IoT را توصیف کردند که برای ادغام بلاکچین و داده‌های حسی IoT جمع‌آوری شده از بیماران، به گونه‌ای که به صورت امن توسط ارائه‌دهندگان خدمات بهداشتی و ذی‌نفعان مدیریت و دسترسی پیدا کنند، طراحی شده است.

کیم و همکاران [9] توضیح داد که سیستم مراقبت بهداشتی پیاده‌سازی شده با استفاده از یک شبکه بی‌سیم، در حین انتقال داده‌های بیماران از دستگاه‌های IoMT به سرور ابری در یک شبکه ناامن، یعنی اینترنت عمومی، یک لایه امنیتی اضافی اضافه می‌کند. برای محافظت در برابر هر شبکه ای، آنها یک پروتکل تبادل کلید تایید شده با رمز عبور کارآمد مبتنی بر بیومتریک (SBAKE) ابداع کردند. به گفته گارگ و همکاران. [10]، حسگرهای بدن داده ها را به دستگاه های تلفن همراه ارسال می کنند. در سناریوی بلاک چین، این دستگاه ها به عنوان گره بیمار به سرور ابری متصل می شوند. این مدل از مدیریت کلید با استفاده از ویژگی های هش رمزنگاری مختلف و عملیات XOR با هر موجودیت استفاده می کند. این مدل به تجزیه و تحلیل تهدیدات امنیتی و اقدامات متقابل آنها می پردازد. آنها از یک مدل بلاک چین خصوصی با استفاده از الگوریتم اجماع پروتکل ریپل (RPCA) و AVISPA برای تجزیه و تحلیل و تأیید این پروتکل استفاده کردند.

وانگ و همکاران [5] معماری لایه‌ای را برای اتصال گره‌ها و موجودیت‌ها در شبکه مراقبت‌های بهداشتی بلاک چین، ارائه تحلیل امنیت و عملکرد مدل پیشنهادی در شبیه‌سازی سیستم پیشنهادی، توضیح داد. با این حال، آنها نتوانستند مفهوم بلاک چین را در این مقاله حفظ کنند. کائو و همکاران [11] یک سیستم مراقبت بهداشتی بلاک چین مبتنی بر ابر را با یک طرح مدیریت کلیدی توسعه داد. ثبت نام بیمار در بیمارستان، تشخیص توسط پزشک و در نهایت، پزشک گزارش ها را در فضای ابری آپلود می کند. تراکنش های این سیستم در شبکه بلاک چین نگهداری می شوند. اتریوم به عنوان یک بلاک چین عمومی برای پیاده سازی مدل پیشنهادی استفاده می شود و برای کل تراکنش ها ۳۷ دلار آمریکا برای هر بیمار هزینه دارد.

خان و همکاران [12] یک چارچوب امن برای احراز هویت و رمزگذاری داده‌های حسگر پزشکی مبتنی بر اینترنت اشیا با استفاده از ECC تقویت‌شده، که مکانیزمی برای ارسال داده‌ها از گره حسگر بیمار به سرور ابری از طریق رادیو برد بلند (LoRa) ارائه می‌دهد پیشنهاد داده اند. آنها یک الگوریتم ECC بهبود یافته را برای حذف تهدیدات و بهبود امنیت انتقال داده های شبکه عمومی پیشنهاد کردند. Özyilmaz و Yurdakul [13] استفاده از دستگاه های کم مصرف را برای پیاده سازی برنامه های کاربردی مبتنی بر اینترنت اشیا با استفاده از اتریوم، ازدحام و قراردادهای هوشمند توضیح دادند. از آنجایی که اتریوم و ازدحام در این سیستم استفاده می شود، مصرف گاز در حین تراکنش ها مشکل ساز است. ژائوفنگ و همکاران [14] یک سیستم اینترنت اشیا و کلان داده را پیشنهاد کرد که یک سیستم مبتنی بر پاداش برای جمع‌آوری و استفاده از داده‌ها در بلاک چین‌های عمومی و مجاز است. برا و همکاران [15] طرحی را پیشنهاد کرد که در برابر حملات مختلف به دستگاه‌های IoT در طول انتقال شبکه عمومی با استفاده از 5G و بلاک چین مقاومت می‌کند. مقاله آنها عمدتاً بر روی هواپیماهای بدون سرنشین\*\*\*(پهباد)\*\*\* متمرکز بود و امنیت و تجزیه و تحلیل عملکرد را مورد بحث قرار داد. پولاپ و همکاران [16] مدلی با عوامل مبتنی بر مکانیسم کنسرسیوم برای طبقه بندی نتایج حاصل از بسیاری از راه حل های یادگیری ماشین پیشنهاد کرد. آنها از هوش مصنوعی به ویژه تکنیک های یادگیری فدرال برای نشان دادن به حداقل رساندن زمان استفاده کردند. سیستم آنها به این نتیجه رسید که می توانند زمان تشخیص را کاهش دهند. به گفته وانگ و همکاران. [17]، شبکه‌های حسگر پزشکی بی‌سیم (WMSN) دارای دو مشکل عمده به‌عنوان امنیت سرور متمرکز و امنیت لایه فیزیکی هستند. آنها ترکیبی از فناوری پیشرفته توابع غیرقابل کلون فیزیکی (PUF) و فناوری بلاک چین را پیشنهاد می کنند. طرح آنها از یک استخراج کننده فازی بیومتریک برای استخراج اطلاعات بیومتریک و انجام احراز هویت مناسب استفاده کرد.

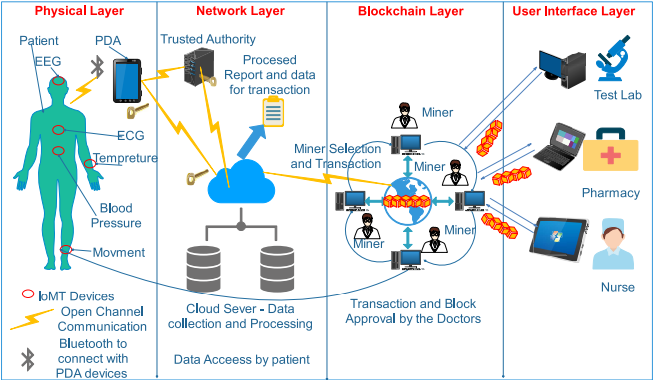
آ. شکاف تحقیق

بررسی متون بالا نشان داد که کمبود گره‌هایی وجود دارد که قادر به اشتراک‌گذاری اطلاعات باشند، مانند مکانیزم یک‌طرفه بلاک چین مراقبت‌های بهداشتی پزشکی که در آن پزشکان نمی‌توانند داده‌ها را برای بیمار ارسال کنند و داده‌های حاصل از حسگرها مستقیماً در بلاک چین نوشته می‌شوند. بنابراین، داده‌های بیمار بدون تأیید پزشکان روی بلاک چین می‌رود. ممکن است حسگرها کامل باشند، اما نیاز به یک نظارت انسانی قبل از تکمیل وظیفه داده‌های بیمار وجود دارد. شکاف‌های عمده ای در عدم اجرای بلاک چین و پیاده‌سازی سیستم اینترنت اشیاء بلادرنگ یا سرور ابری بدون بلاک چین، عدم ایجاد گره کافی برای اشتراک‌گذاری داده‌ها و تایید در زنجیره‌های بلوکی یافت می‌شود. ابر به عنوان ماینر عمل می کند، تراکنش‌های ورودی از گره بیمار را بدون مشاوره با پزشکان تأیید می‌کند. برخی از مقالات به فناوری IoMT اشاره کردند اما از بلاک چین استفاده نکردند و مقاله خود را با GDPR پیاده سازی نکردند. برخی از مقالات دارای سیستم بلاک چین بیمار محور نیستند، بنابراین بیمار نمی تواند سوابق را ببیند. در برخی از مقالات، بیمار کنترلی بر داده های خود ندارد. این نوع مقالات با استفاده از فناوری بلاک چین اجرا می شوند اما مطابق با GDPR نیستند. این شکاف های تحقیقاتی در مقاله پیشنهادی حل شده است.

ما در حال توسعه یک مدل زنجیره بلوکی برای ذخیره داده‌های بیمار از دستگاه‌های IoMT هستیم که از سرور ابری در طرح پیشنهادی استفاده می‌کنند، به‌جای ارسال فوری تراکنش‌ها به بلاک چین مانند سیستم‌های ساخته شده قبلی. قبل از تایید تراکنش ها، پزشکان داده ها را زیر نظر دارند. ماینرها ابتدا احراز هویت IoMT را تأیید می کنند و سپس تراکنش ها تأیید می شوند. طرح پیشنهادی در زمینه‌های ذخیره‌سازی داده، امنیت، اتصال، نظارت بلاک چین و داده‌های بیمار محور جدید است.

1. سیستم پیشنهادی

سیستم پیشنهادی شامل یک معماری لایه‌ای است که شامل لایه بیمار (لایه فیزیکی)، لایه شبکه، لایه بلاک چین و لایه رابط کاربر است. از شکل 1، می بینیم که لایه فیزیکی شامل دستگاه های IoMT در بدن بیمار است و لایه شبکه شامل برقراری ارتباط امن بین دستگاه شخصی بیمار و ابر است. لایه بلاک چین شامل انتقال داده ها از یک گره سرور ابری به بلاک چین و استخراج تراکنش ها و بلاک ها توسط ماینر انتخاب شده است. لایه رابط کاربری این سیستم شامل رابط های وب و برنامه های کاربردی است که توسط رابط های مختلف تحت کنترل انسان در این شبکه بلاک چین استفاده می شود. نمادهای استفاده شده در این مقاله در نامگذاری آورده شده است. هر لایه از این سیستم پیشنهادی در نکات زیر توضیح داده شده است.



شکل 1

آ. لایه فیزیکی

قرار است دستگاه‌های IoMT در این لایه کار کنند، که یک چند جمله‌ای دو متغیره متقارن انحصاری

X1

با درجه t را روی یک میدان محدود (میدان Galois) GF(p) (=Z p) انتخاب می‌کند، جایی که ضرایب ai,j از GF(p) و Z p = 0.1.2.، . . . ، p – 1انتخاب می‌شود. ، که در آن p یک عدد اول مناسب بزرگ است و t بیشتر از تعداد کل دستگاه‌های IoMT است که روی بیمار قرار می‌گیرد. دستگاه‌های IoMT (Dev)، دستیار دیجیتال شخصی دستگاه همراه بیمار (PDA) و سرور ابری CS همگی در این مرحله ثبت می‌شوند.

1. ثبت دستگاه: اگر کلید مخفی مولد کلید جلسه معتبر (ASKG) برابر L و هویت دستگاه IoMT k برابر IDDevk باشد، شناسه مستعار دستگاه به عنوان

X2

تعیین می شود. سپس، ASKG مقدار (3) را محاسبه می کند

X3

که مطمئناً یک چند جمله ای تک متغیره با همان درجه t است. اکنون، ASKG مقدار (PIDDevk، χ(PIDDevk،y)) در حافظه دستگاه IoMT ذخیره می شود.

1. ثبت دستگاه شخصی: ثبت PDAl مورد نیاز است زیرا داده های جمع آوری شده از دستگاه های IoMT را به سرور ابری منتقل می کند. برای این منظور، ASKG هویت خود را به عنوان IDASKG دارد و اکنون شبه هویت ASKG را به صورت (4) محاسبه می کند.

X4

اجازه دهید هویت PDAl برابر IDPDAl باشد و توکن تولید شده برای PDAl برابر TKNPDAl باشد. سپس، ما شبه هویت PDAl را به صورت زیر محاسبه می کنیم.

X5

اکنون، اعتبارنامه های قطعی را به صورت

X6

محاسبه می کنیم که در آن TSPRPDAl مهر زمانی ثبت PDA در سرور مجاز ASKG

X7

است و سپس ASKG اطلاعات (PIDPDAl، TEMPCPDAl، PIDASKG، χ(PIDPDAl،y)) را قبل از استقرار این دستگاه PDA در پایگاه داده PDAl ذخیره می کند.

1. ثبت سرور ابری: ASKG هویت منحصر به فرد CSj را به عنوان IDCSj انتخاب می کند و شبه هویت را به صورت زیر محاسبه می کند.

X8

سپس، ASKG اطلاعات PIDCSj، PIDASKG را قبل از استقرار، در پایگاه داده سرور ابری ذخیره می کند.

امنیت و احراز هویت بین دستگاه ها: این قسمت مدیریت کلید بین IoMT به PDA و PDA به CS را توضیح می دهد. نمای کلی این قسمت در شکل 2 قابل مشاهده است.

1. مدیریت کلید بین Devk و PDAl:Devk زمان فعلی TSP1 را تولید می کند و (PIDDevk، TSP1) را از طریق کانال باز به PDAl ارسال می کند. PDAl داده (PIDDevk، TSP1) را در مهر زمانی TSP∗ 1 دریافت کرده است. تا کنون، تأیید تأخیر زمانی PDAl محاسبه می‌شود |TSP1 - TSP∗ 1| ≤ T . اگر آن معتبر باشد، PDAl مقدار TSP2 را تولید می کند و

X9

کلید خصوصی را به صورت

X10

و

X11

محاسبه می کند و سپس پیام PIDPDAl, MSG1, TSP2 را از طریق کانال عمومی به Devk ارسال می کند. پس از دریافت PIDPDAl، MSG1، TSP2 از PDAl در مهر زمانی TSP∗2، Devk حداکثر زمان تاخیر

X12

را تأیید می کند. اگر نتایج تأیید معتبر باشد،

X13

و کلید خصوصی را به صورت

X14

و

X15

محاسبه می‌کند. سپس، Devk تأیید می کند که آیا MSG 1 با MSG1برابر است یا خیر. اگر برابر است، پس شرط برای برقراری اتصال صحیح است. برای مراجعات بعدی، هر دو دستگاه کلیدهای خصوصی را به صورت Priv(Devk ,PDAl) و Priv(PDAl,Devk ). ذخیره می کنند.

1. مدیریت کلید بین PDAl و CS j: PDAl مقدار

X16

را در زمان TSP1 و M2 = h(M1||TSP1||PIDASKG) محاسبه می کند. PDAl مقادیر M1, M2, TCP1 را از طریق کانال باز به CSj ارسال می کند. مهر زمانی دریافت این پیام در CSj برابر TSP∗1 است. سپس، CSj اعتبار حداکثر تاخیر زمانی را با محاسبه |TSP1 − TSP∗1| ≤ T میسنجد. اگر معتبر باشد، CSj مقادیر

X17

و M 2 = h(M1||PIDASKG||TSP1) را محاسبه می کند، و سپس، CSj بررسی می کند که آیا M 2 با M2 برابر است یا خیر. اگر معتبر باشد، PDAl ارتباط با CSj را تأیید کرده است. در غیر این صورت، اتصال قطع می شود. پس از تأیید اتصال، CSj مقدار M3 = h(r||PIDCSj ) ⊕ PIDASKG را محاسبه می کند، که r به صورت تصادفی در سرور ابری CSj در زمان TSP2 تولید می شود. سپس، CSj کلید خصوصی خود را به صورت

Priv(CSj,PDAl) = h(h(r||PIDCSj)||PIDASKG||h(TKNPDAl ||TEMPCPDAl )||TSP1||TSP2)

و M4 = h(Priv(CSj,PDAl) ||TSP2) محاسبه میکند و سپس پیام M3, M4, TSP2 را از طریق کانال عمومی به PDAl ارسال می کند. پس از دریافت M3، M4، TSP2 از CSj در مُهر زمانی TCP∗2، PDAl باید اعتبار حداکثر زمان تأخیر را با محاسبه |TSP2 - TSP∗2 | ≤ T بسنجد; اگر این مورد با موفقیت تأیید شود، PDAl مقادیر h(r||PIDCSj ) = M3 ⊕ PIDASKG ، کلید خصوصی Priv(PDAl,CSj) = h(h(r||PIDCSj)||PIDASKG||h(TKNPDAl||TEMPCPDAl ||TSP1||TSP2)) و

X18

را محاسبه می کند. سپس، PDAl اعتبار M 4 = M4 را بررسی می کند. اگر معتبر باشد، CSj توسط PDAl احراز هویت می شود و محاسبه کلید جلسه صحیح است. علاوه بر این، PDAl X19 را در مُهر زمانی تولید شده TSP3 محاسبه می‌کند و پیام M5، TSP3 را از طریق کانال باز به CSj می‌فرستد. سپس، PDAl اعتبار M 4 = M4 را بررسی می کند. اگر معتبر باشد، CSj توسط PDAl احراز هویت می شود و محاسبه کلید جلسه صحیح است. علاوه بر این، PDAl مقدار

X19

را در مُهر زمانی تولید شده TSP3 محاسبه می‌کند و پیام M5، TSP3 را از طریق کانال باز به CSj می‌فرستد. پس از دریافت M5، TSP3 از PDAl، در مُهر زمانی TSP∗3، CSj مقدار |TSP3 - TSP∗3 | ≤ T برای اعتبار سنجی تأخیر زمانی محاسبه میکند؛ اگر معتبر باشد، مقدار

X20

را محاسبه کرده و M 5 = M5 را بررسی می کند. اگر معتبر باشد، PDAl کلید صحیح را محاسبه می کند. در نهایت، هر دو کلید Priv(CSj,PDAl) و Priv(PDAl,CSj) را برای استفاده در آینده ذخیره کنید.

ب. لایه شبکه

در این لایه فرآیند ثبت نام کاربر انجام می شود. این لایه شامل مرحله ثبت نام کاربر، ورود به سیستم و احراز هویت بین سرور ابری، PDA و دستگاه های IoMT است.

1. ثبت نام کاربر: اجازه دهید کاربر Ui هویت IDUi داشته باشد و دارای یک توکن هش شده 256 بیتی باشد که توسط اطلاعات بیومتریک کاربر (ui, vi) = Bio(Ui) تولید می شود که TKNUi = h(IDUi||ui) است. کاربر Ui مقادیر IDUi، TKNUi را به ASKG می فرستد تا ارتباط بین CSj و Ui را حفظ کند. اکنون، ASKG هویت شبه Ui را به صورت PIDUi = h(IDUi ||L) تولید کرده و همچنین

X21

را محاسبه کرده و به Ui ارسال می کند. برای ارتباط امن بین CSj و ASGK، یک کلید متقارن مشترک CKCS ASGK و CKASGK-CS توافق شده است.

1. ورود کاربر: برای ورود کاربر، اعتبار نامه قبلاً در ASKG و CSj وجود داشته است. هنگامی که کاربر با استفاده از اعتبار نامه (IDUi, TKNU) برای ورود به سیستم تلاش می کند،CSj مقدار ASKG را برای

X22

و PIDUi درخواست می کند و داده ها را در سرور ابری مطابقت می دهد. اگر مطابقت تأیید شود، کاربر وارد شده است، در غیر این صورت رد می شود.

ج. لایه بلاک چین

در این لایه، CSj به عنوان گره بلاک چین کار می‌کند و گره‌های دیگر بلاک‌چین‌ها پزشک، پرستار، داروخانه و آزمایشگاه‌ها هستند چرا که، در این سیستم پیشنهادی، سرور ابری تایید کننده یا استخراج کننده داده های ارائه شده توسط دستگاه های IoMT از طریق شبکه عمومی نیست. در این لایه، ECDSA به عنوان ابزار رمزنگاری و SHA-512 برای هدف هش استفاده می شود. پس از جمع‌آوری داده‌ها و پردازش آن داده‌ها در سرور ابری، CSj باید آن داده‌ها را به پزشک منتقل کند، که به عنوان گره تأییدکننده کار می‌کند. این بلاک چین باید یک ماینر را بر اساس الگوریتم اجماع انتخاب کند. بنابراین، مراحل زیر در انتخاب ماینر، الگوریتم اجماع، فرمت تراکنش، تایید تراکنش و ایجاد بلوک گنجانده شده است.

1. انتخاب ماینر: اجازه دهید بگوییم که 100 ماینر در شبکه وجود دارد و الگوریتم اجماع به همه آنها فرصت یکسانی برای استخراج داده ها می دهد. بنابراین، الگوریتم اجماع تاریخچه را در بلاک چین جستجو می‌کند و گره‌هایی را می‌یابد که هنوز هیچ تراکنش استخراج نکرده‌اند، و این گره‌ها به عنوان ماینر برای تراکنش‌هایی که توسط سرور ابری ارسال می‌شود، در دسترس هستند. این روش انتخاب ماینر در الگوریتم 1 توضیح داده شده است. در الگوریتم 1، ورودی شامل تمام گره های بلاک چین های گرفته شده است. ماینرهایی که قبلاً شانس استخراج داشتند، در بلاک چین جستجو می شوند. از تعداد کل ماینرها، ماینرها از نتایج جستجو حذف می شوند و خروجی همه ماینرهای موجود را برای فرآیند استخراج فراهم می کند.

\*\*\* الگوریتم 1\*\*\*

1. الگوریتم اجماع: الگوریتم 2 بر اساس شانس برابر برای تمام گره‌های ماینر در شبکه بلاک چین است. این الگوریتم تاریخچه بلاک چین را برای داده های استخراج شده قبلی جستجو می کند. آدرس ماینرها را با لیست ماینر مطابقت می دهد. سرور ابری ماینرهایی را که هنوز استخراج انجام نداده اند از لیست انتخاب می کند و این فرصت را به سرور ابری می دهد تا یکی از آن ماینرها را انتخاب کند. اولویت لیست با زمان اتصال گره در شبکه تنظیم می شود. این شبکه بر اساس بلاک چین دارای مجوز خصوصی است، بنابراین همه ماینرها از قبل تایید شده اند. وقتی همه ماینرها استخراج مساوی داشته باشند، الگوریتم اجماع لیست ماینرها را در دنباله پیوستن آنها بازنشانی می کند.

\*\*\* الگوریتم 2\*\*\*

1. فرمت تراکنش: اجازه دهید سرور ابری CSj داده‌های Dn را از دستگاه‌های مختلف IoMT جمع‌آوری کند و داده‌ها را پردازش کند و آن را برای پزشکان قابل درک کند. قالب تراکنش در شکل 3 نشان داده شده است و شامل شناسه فرستنده، یعنی PIDCSj، و شناسه گیرنده، یعنی شناسه پزشک است. نوع داده به معنای نوع تشخیص است. این شامل PII از نظر بله/خیر بولین، مهر زمانی تراکنش، هش سرایند تراکنش، رضایت بیمار به شکل بله/خیر و امضای فرستنده CSj است.

\*\*\* شکل 3\*\*\*

1. تایید تراکنش و ایجاد بلوک: وقتی تراکنش در صف ماینر فهرست می شود، ماینر تراکنش را برای رضایت بیمار بررسی می کند. اگر رضایت بیمار منفی باشد، تراکنش رد می شود. اگر رضایت مثبت باشد، تراکنش از نظر صحت گزارش تولید شده توسط ماشین بررسی می شود. اگر گزارش دقیق باشد، ماینر تراکنش را تایید کرده و آن را به بلوک اضافه می کند. هنگامی که یک بلوک استخراج می شود، به بلاک چین اضافه می شود و یک کپی از آن بلوک به عنوان PIDPDAl در تمام گره های بلاک چین، از جمله بیمار، توزیع می شود. در نتیجه، بیمار به داده های بلاک چین دسترسی دارد.

د. لایه رابط کاربری

در این لایه، بیماران، پزشکان، پرستاران، داروخانه‌ها و آزمایشگاه‌های آزمایش می‌توانند به داده‌ها با توجه به استفاده و سطوح کنترل دسترسی توسط برنامه‌های وب و برنامه‌های غیرمتمرکز (dApps) دسترسی داشته باشند. سطوح دسترسی برای گره های مختلف در جدول 1 نشان داده شده است.

\*\*\* جدول 1\*\*\*

1. پیاده سازی سیستم پیشنهادی

برای پیاده سازی، سیستم پیشنهادی به سه بخش تقسیم می شود: 1) اینترنت اشیا و ابر. 2) تأیید پروتکل امنیتی با استفاده از Scyther. و 3) پیاده سازی بلاک چین خصوصی با استفاده از بلاک چین مبتنی بر پایتون. جدول 2 الزامات سیستم را نشان می دهد. در ادامه به جزئیات این پیاده سازی می پردازیم.

\*\*\*جدول 2\*\*\*

آ. پیاده سازی اینترنت اشیا و ابر

ما از شبیه ساز اینترنت اشیا Bevywise برای ایجاد زیرساخت های اینترنت اشیا و ابر استفاده می کنیم. این یک ابزار شبیه سازی کاربر پسند است که به شما امکان می دهد ده ها هزار مشتری انتقال تله متری صف پیام (MQTT) را در یک سیستم واحد شبیه سازی کنید. عملکرد، کارایی و ظرفیت برنامه های کاربردی ابری و MQTT را آزمایش کنید. محیط آزمایش در جدول 3 توضیح داده شده است و شبیه ساز اینترنت اشیا از طریق میزبان محلی با اتصال ابری از طریق MQTT در میزبان محلی قابل دسترسی است. محیط شبیه سازی دارای 12 دستگاه IoMT با انواع و پیکربندی های مختلف می باشد. زمان اجرای شبیه سازی 480 ثانیه است و نتیجه در بخش 5 مورد بحث قرار گرفته است. جدول 3 فهرستی از دستگاه های IoMT مورد استفاده برای شبیه سازی را نشان می دهد.

\*\*\* جدول 3\*\*\*

ب. تست پروتکل با استفاده از Scyther

ما از Scyther برای آزمایش پروتکل امنیتی پیشنهادی استفاده می کنیم. Scyther ابزاری برای تجزیه و تحلیل خودکار پروتکل های رمزنگاری است. توانایی اجرای تایید نامحدود یکی از مزایای Scyther نسبت به سایر ابزارها است. به طور سنتی، ابزارها فقط ویژگی های امنیتی بیان شده را برای یک زیر مجموعه محدود از رفتارهای پروتکل قابل تصور (ممکن) ارزیابی می کردند، فرآیندی که به عنوان تأیید محدود شناخته می شود. روش اعمال شده در شکل 4 قابل مشاهده است.

\*\*\*شکل 4\*\*\*

ج. پیاده سازی بلاک چین

در سیستم پیشنهادی ما، بلاک چین توسط پایتون پیاده‌سازی می‌شود. گره های بلاک چین عبارتند از: پزشک، بیمار، پرستار، داروخانه و آزمایشگاه. نتیجه حاصل و تجزیه و تحلیل عملکرد این بلاک چین در بخش 5 مورد بحث قرار گرفته است.

1. تجزیه و تحلیل نتایج و امنیت

آ. تجزیه و تحلیل امنیتی

سیستم پیشنهادی در برابر حملات مختلف همانطور که در اجرای Scyther ثابت شده است، ایمن است. تجزیه و تحلیل امنیت به شرح زیر ارائه شده است.

1. ایمن در برابر حمله تکرار: ما از یک کلید احراز هویت بین دستگاه های IoMT به PDA و PDA به سرور ابری استفاده می کنیم. محاسبه کلید جلسه توسط یک مرجع قابل اعتماد انجام می شود. محاسبات و اعتبارسنجی زمان‌بندی برای برقراری اتصال انجام می‌شود تا مدیریت کلید معتبر انجام شود. در صورتی که مهاجم (Adversary) A نیاز به مدیریت کلید معتبر داشته باشد، این فرآیند مهم است.طرح پیشنهادی دارای حداکثر تاخیر انتقال T است. علاوه بر این، پخش مجدد پیام‌های ارسالی قدیمی هیچ گونه سود اطلاعاتی را برای مهاجم فراهم نمی‌کند، چیزی که برای «رویه احراز هویت و مدیریت کلید» در Devk، PDAl، CSj، و Ui در زمان T مورد نیاز بوده است. به این ترتیب این سیستم در برابر حملات تکراری ایمن است.
2. ایمن در برابر حمله Man-in-the-Middle: به یک مهاجم A اجازه دهید یک پیام درخواست احراز هویت MSA1، MSA2، TSP1 را استراق سمع کند، درحالی که MSA1 = h(TKNl||TEMPCPDAl 5 ⊕ PIDASKG و MSA2 = h(MSA1||TSP1||PIDASKG)⊕PDAl با مهر زمانی TSP1، که بین Ui و CSj رد و بدل شده است درست زمانی که A سعی می کند این پیام را به روز کند تا شبیه پیام احراز هویت اصلی شود، مانند MSA 1، MSA 2، TSP 1 که در آن MSA 1 = h(TKNl||TEMPCPDAl) ⊕ PID ASKG و MSA 2 = h(MSA 1||TSP 1||PID ASKG 52⊕ PDAl با کمک پارامترها انجام می شود. برای راه‌اندازی MITM، A می‌تواند تولید عدد تصادفی و مهر زمانی فعلی TSP 1 را آغاز کند. با این حال، در غیاب دانش کلید خصوصی و شناسه مستعار و L، A نمی تواند درخواست احراز هویت معتبر دیگری را ایجاد کند.
3. ایمن در برابر حمله جعل هویت: فرض کنید مهاجم A بخواهد با ایجاد یک پیام درخواست احراز هویت به نمایندگی از یک موجودیت معتبر در شبکه، خود را به عنوان آن موجودیت معرفی کند، مثلاً PDAl . پس از دریافت درخواست احراز هویت PDAl ، MSA1, MSA2, TSP1, که در آن MSA1 = h(TKNl|| 5EMPCPDAl) ⊕ PIDASKG و MSA2 = h(M1||TSP1|| 5IDASKG) ⊕ PDAl با برچسب زمانی TSP1 وجود دارند و به CSj ارسال شده‌اند، از آنجا که این پیام‌ها از طریق کلیدهای مخفی و کلید خصوصی بلندمدت PIDPDAl و PIDCSj تولید می‌شوند، A قادر به ایجاد یک "پیام درخواست احراز هویت" معتبر نمایانگر کاربر قانونی PDAl بدون داشتن دانش این مقادیر مخفی نیست. بنابراین، این سیستم در برابر انواع حملات جعل هویت مقاوم است.
4. ایمن در برابر نشت کلید موقت (ESL): کلید مخفی هر جلسه با استفاده از مهر زمانی در هر مرحله ارتباطی توسط CSj و Ui محاسبه می شود. در ایجاد کلید جلسه به صورت SecKey(CSj,Ui) = h(PIDPDAl||PDAl||TSP1||TSP2||h(PIDCS j ||PIDASKG))، از شناسه مستعار CSj و Ui استفاده می شود. همچنین از توکن کاربر استفاده می کند که توسط بیومتریک کاربر و کلید انتخابی تصادفی ایجاد می شود. توجه به این نکته حائز اهمیت است که کلیدهای مخفی کوتاه مدت و بلندمدت تولید شده برای ارتباط دارای شناسه مستعار هر گره ارتباطی و همچنین توابع هش در پیام ها هستند. بنابراین، کلید جلسه فقط در شرایطی آشکار می شود که A هر دو ارزش مخفی "کوتاه مدت" و "بلند مدت" را به خطر بیندازد. علاوه بر این، از آنجایی که کلیدهای جلسه با استفاده از مقادیر اعداد تصادفی و مهرهای زمانی متنوع در تمام جلسات محاسبه می شوند، حتی اگر یک کلید جلسه برای یک جلسه خاص آشکار شود، باعث آشکار شدن کلیدهای جلسه سایر جلسات نمی شود. به دلیل ادغام مقادیرهای مخفی کوتاه مدت و بلند مدت. این سیستم قادر به محافظت از حملات اطلاعات موقت جلسه و همچنین در برابر حملات ESL است.
5. مقاوم در برابر حمله داخلی با دسترسی ممتاز: اگر A تمام جزئیات ثبت‌نام Ui، CSj، Devk، و PDAl را بداند، باز هم نمی‌تواند کلید مخفی تولید شده به نام SecKey(CSj,Ui) = h(PIDPDAl || PDAl||TSP1||TSP2||h(PIDCSj ||PIDASKG)) توسط مدیر کلید جلسه را محاسبه کند و همچنین قادر به محاسبه مقادیر مخفی بلندمدت مختلف مانند مقادیر تصادفی، مهره های زمانی، کلیدهای مخفی و هویت‌ها، که قبلاً توضیح داده شده‌اند، نیست. کاربر داخلی با امتیاز از ASKG آگاهی نسبت به این اطلاعات ندارد. بنابراین، A نمی‌تواند "کلید جلسه" را به نمایندگی از یک موجودیت معتبر محاسبه کند. بنابراین، این سیستم در برابر حملات داخلی با امتیاز محافظت شده است.
6. ایمن در برابر حمله ضبط فیزیکی دستگاه: هر دستگاه دارای هویتی به عنوان χ(PIDDevk,y) است که برای کارهای مربوط به "احراز هویت و ایجاد کلید" با موجودیت های مختلف ارتباطی استفاده می شود. محافظت در برابر حمله ضبط فیزیکی دستگاه IoMT از نقطه نظر امنیتی یک الزام حیاتی است. اجازه دهید بگوییم که دستگاه‌های IoMT به‌طور فیزیکی توسط یک دشمن A به دام افتاده‌اند. ما ارزیابی «حمله ضبط فیزیکی IoMT» را به عنوان کسری از کل ارتباطات ایمن انجام می‌دهیم که در اثر گرفتن (دزدیده شدن فیزیکی) دستگاه‌های IoMT بدون احتساب ارتباطات، به خطر می‌افتد که در آن "Devk به خطر افتاده" به وضوح گسترش یافته است. به عنوان مثال، می‌توان احتمال تخصص A را برای رمزگشایی «ارتباطات امن» بین PDAl و Devk غیرقابل نفوذ زمانی که دشمنان قبلاً در معرض خطر قرار گرفته‌اند (تحت نفوذ حمله) محاسبه کرد. از یک Devk به سرقت رفته، مهاجم A هویت شبه اطلاعات و سایر پارامترها را به همراه کلید جلسه زوجی مخفی Priv(Devk,PDAl) که بین Devk و PDAl به اشتراک گذاشته شده است از حافظه خود استنتاج می کند تا متوجه شود که تمام PIDDevk و χ(PIDDevk,y) برای IoMT های مختلف متفاوت است. بنابراین، سرقت فیزیکی Devk توسط A تنها می تواند به او در به دست آوردن کلید جلسه مخفی بین آن Devk و PDAl کمک کند نه سایر کلیدهای جلسه. بنابراین، این سیستم بدون قید و شرط در برابر حمله ضبط فیزیکی IoMT ایمن است. این نتیجه آزمایش شده توسط Scyther تأیید می شود و نتیجه تأیید در شکل 5 نشان داده شده است.

\*\*\* شکل 5\*\*\*

ب. نتایج شبیه سازی ها

1. شبیه سازی اینترنت اشیا: مجموع دستگاه های IoMT در شبیه سازی ما 12 عدد، کل پیام های گرفته شده 110 و کل زمان سپری شده 480 ثانیه است. این نتیجه شبیه سازی را می توان در شکل های 6 و 7 و جدول 4 مشاهده کرد.

\*\*\* شکل 6\*\*\*

\*\*\*شکل 7\*\*\*

\*\*\*جدول 4\*\*\*

2. شبیه سازی بلاک چین: نتایج شبیه سازی نشان می دهد که گره با مدت زمان افزایش می یابد و تعداد بیماران افزایش می یابد. همانطور که در شکل 8 نشان داده شده است، ما صد گره به عنوان ماینر داریم که از آنها برای استخراج تراکنش ها و بلاک ها استفاده می کنند. پس از تکمیل اولین ماینینگ، 99 ماینینگ باقیمانده در دسترس خواهند بود. با این حال، هنگامی که 100 ماینر تکمیل شد، از در دسترس بودن 100 ماینر دوباره شروع به کار میکند. از شکل 9 می بینیم که استخراج یک تراکنش از یک سرور ابری 2 میلی ثانیه طول می کشد و برای مجموع 100 تراکنش برای 100 ماینر، 200 میلی ثانیه طول می کشد. ایجاد بلاک چین در جدول 5 به تفصیل آمده است.

\*\*\* شکل 8\*\*\*

\*\*\*شکل 9\*\*\*

\*\*\*جدول 5\*\*\*

6. مقایسه با سیستم های توسعه یافته قبلی و نتایج

از جدول 6، می‌توان دید که سیستم پیشنهادی ما در مقایسه با سیستم‌های توسعه‌یافته قبلی پیچیده نیست و بیمار پسند است. سیستم پیشنهادی بر اساس الگوریتم اجماع مبتنی بر احراز هویت است. بنابراین، پیچیدگی موارد حل پازل در سیستم پیشنهادی دخیل نیست. در اینجا، پیچیدگی به معماری بلاک چین نیز اشاره دارد که برای ذخیره داده های بیمار توسعه یافته است. ما پیچیدگی ذخیره سازی داده های بیمار مبتنی بر بلاک چین را با توسعه یک رابط کاربری و نمونه سازی طرح پیشنهادی به روشی کاربرپسند کاهش می دهیم. مقایسه تعداد پیام‌ها در سیستم‌های توسعه‌یافته قبلی و سیستم پیشنهادی در شکل 10 نشان داده شده است. شکل 11 مقایسه زمان ارتباط (ms) در سیستم‌های توسعه‌یافته قبلی و سیستم پیشنهادی را نشان می‌دهد. مقایسه بیت‌های پیام در سیستم‌های توسعه‌یافته قبلی و سیستم پیشنهادی در شکل 12 نشان داده شده است. از جدول 7، می‌توان دید که سیستم پیشنهادی در مقایسه با سیستم‌های توسعه‌یافته قبلی امن است [4]، [9]-[ 12]، [15]، [18].

\*\*\* جدول 6\*\*\*

\*\*\* شکل 10\*\*\*

\*\*\*شکل 11\*\*\*

\*\*\*شکل 12\*\*\*

\*\*\* جدول 7\*\*\*

7. نتیجه و چشضم انداز اینده

اینترنت اشیا نقش مهمی در رشد سریع زندگی مبتنی بر داده ایفا می کند. خدمات مراقبت های بهداشتی نیز با استفاده از دستگاه های IoMT برای انجام اقدامات و رتبه بندی بیماران از راه دور آسان می شود. این رتبه‌بندی‌ها می‌تواند به پزشکان و محققان کمک کند حتی در موقعیت‌های مشابه COVID-19 کار خود را انجام دهند. سیستم پیشنهادی ما بیمار محور است زیرا بیمار می‌تواند داده‌های خود را ببیند، و مفهوم رضایت برای اشتراک‌گذاری داده‌ها اینجاست. ما از دستگاه‌های اینترنت اشیا برای ضبط داده‌ها از BAN بیمار استفاده کردیم و به‌طور ایمن آن‌ها را در سرور ابری به اشتراک گذاشتیم، جایی که داده‌ها برای استفاده بیشتر پردازش می‌شوند و توسط سرور ابری به گره پزشک ماینر منتقل می‌شوند. گره پزشک، تراکنش و بلاک را استخراج کرد و سوابق را به تمام گره‌های بلاک چین ارسال کرد. در آینده، ما می‌توانیم از دستگاه‌های IoMT بدون تماس برای دریافت اطلاعات از راه دور از بیماران استفاده کنیم تا از انتشار هر گونه ویروسی مانند COVID-19 جلوگیری کنیم. در آینده می‌توانیم با استفاده از سیستم بازخورد، ویژگی‌های زیادی مانند کیف پول سخت‌افزاری بیماران و مجموعه‌ای از پزشکان را بر اساس شهرت آنها اضافه کنیم. سیستم پیشنهادی ما در مقایسه هزینه و عملکرد بهتر است.

مراجع

برای افزودن نوآوری‌های مقاوم در برابر کامپیوترهای کوانتومی به پروتکل، می‌توانیم از الگوریتم‌های رمزنگاری پساکوانتومی مانند رمزنگاری مبتنی بر شبکه‌های مشبک (Lattice-based Cryptography) استفاده کنیم. یکی از این الگوریتم‌ها، Kyber، است که به عنوان یک رمزنگاری کلید عمومی پساکوانتومی شناخته می‌شود.

**توضیح نوآوری‌ها**

1. **استفاده از رمزنگاری پساکوانتومی**:
   * از توابع PQ\_Encrypt و PQ\_Decrypt برای رمزنگاری و رمزگشایی داده‌ها استفاده شده است.
   * یک کلید مشترک (PQ\_Key) برای رمزنگاری پساکوانتومی داده‌ها بین کاربر (U) و سرور ابری (CS) استفاده شده است.
2. **ادعاها برای ویژگی‌های امنیتی**:
   * ادعاها برای بررسی اینکه داده‌های حساس مانند کلیدهای جلسه، شناسه‌ها و نانس‌ها محرمانه باقی می‌مانند، اضافه شده‌اند.
   * این ادعاها تضمین می‌کنند که پروتکل در طول ارتباط محرمانگی و صحت را حفظ می‌کند.

این کد Scyther یک پروتکل ورود مجاز امن را نشان می‌دهد که بر محرمانگی و صحت داده‌های انتقالی بین کاربر (U) و سرور ابری (CS) تمرکز دارد. نوآوری‌ها با استفاده از رمزنگاری پساکوانتومی و استفاده از نانس‌ها یک چارچوب امنیتی قوی‌تر را فراهم می‌کنند.

/\* تعریف توابع و ثابت‌ها \*/

const exp: Function;

const hash: Function;

const XOR: Function;

const PQ\_Encrypt: Function;

const PQ\_Decrypt: Function;

const h1: Function;

const plus: Function;

const mod: Function;

hashfunction h;

/\* تعریف پروتکل \*/

protocol AuthorizedLogin(U, CS) {

role U {

const IDi, Pu, Bu, SIDj, k, s, b, g, p, IDu, l: fresh;

N1: Nonce;

var N2: Nonce;

const PQ\_Key: Key; // کلید مشترک برای رمزنگاری پساکوانتومی

/\* ماکروها \*/

macro b = h(b);

macro k = mod(exp(g, b), p);

macro PIj = h(XOR(XOR(h(IDi), h(h(Di, h(si))), plus(h(N2), 1)), h(IDi, k)));

macro Llj = XOR(h(N2), h(IDu, k));

/\* ارتباطات \*/

send\_1(U, CS,  PQ\_Encrypt(XOR(h(SIDi, N1), h(IDu)), PQ\_Key), N1); // C1

recv\_2(CS, U, PQ\_Decrypt(XOR(h(N2), h(N1, 1)), PQ\_Key)); // C2

send\_3(U, CS, PQ\_Encrypt(h(XOR(XOR(h(IDu), h(h(IDu), h(s))), plus(h(N2), 1)), h(IDu, k)), PQ\_Key)); // PIj

send\_4(U, CS, PQ\_Encrypt(Llj, PQ\_Key));

/\* ادعاها \*/

claim\_i1(U, Secret, XOR(h(SIDj, N1), h(IDu))); // C1

claim\_i2(U, Secret, XOR(h(N2), h(N1, 1))); // C2

claim\_i3(U, Secret, h(XOR(XOR(h(IDu), h(h(IDu), h(s))), plus(h(N2), 1)), h(IDu, k))); // PIj

claim\_i4(U, Secret, h(s)); claim\_i10(U, Secret, k);

claim\_i11(U, Secret, h(IDu));

claim\_i12(U, Secret, N1);

claim\_i5(U, Secret, h(N2));

claim\_i13(U, Secret, Lij);

claim\_i8(U, Alive);

claim\_i9(U, Weakagree);

claim\_i10(U, Commit, CS, N1, N2);

}

role CS {

const IDi, Pi, N2, Bi, SIDj, k, s, b, g, p, I, IDu;

var N1: Nonce;

fresh N2: Nonce;

const PQ\_Key: Key; // کلید مشترک برای رمزنگاری پساکوانتومی

/\* ارتباطات \*/

recv\_1(U, CS,  PQ\_Encrypt(XOR(h(SIDj, N1), h(IDu)), PQ\_Key), N1); // C1

send\_2(CS, U, PQ\_Decrypt(XOR(h(N2), h(N1, 1)), PQ\_Key)); // C2

recv\_3(U, CS,  PQ\_Encrypt(h(XOR(XOR(h(IDu), h(h(IDu), h(s))), plus(h(N2), 1)), h(IDu, k)), PQ\_Key)); // PIj

recv\_4(U, CS, PQ\_Encrypt(Lij, PQ\_Key));

/\* ادعاها \*/

claim\_r13(CS, Secret, Lij);

claim\_r1(CS, Secret, XOR(h(SIDj, N1), h(IDi))); // C1

claim\_r2(CS, Secret, XOR(h(N2), h(N1, 1))); // C2

claim\_r3(CS, Secret, h(XOR(XOR(h(IDi), h(h(IDi), h(s))), plus(h(N2), 1)), h(IDi, k))); // PIj claim\_r4(CS, Secret, h(s));

claim\_r10(CS, Secret, k);

claim\_r4(CS, Secret, h(IDi));

claim\_r9(CS, Weakagree);

}

}