مقاله پژوهشی

مجله انفورماتیک سلامت و زیست پزشکی
مرکز تحقیقات انفورماتیک پزشکی
دوره هفتم شماره چهارم. ص ۴۲۴-۴۱۳. ۱۳۹۹

ارائه مدلی برای احراز هویت توزیع شده در یک شبکه سلامت الکترونیک با استفاده از بلاک‌چین

شهریار محمدی[۱]*، نازنین قنبری[۲]

• **دریافت مقاله:** ۹۹/۴/۲ • **پذیرش مقاله:** ۹۹/۵/۲۰

مقدمه: یکی از مهم‌ترین و پرچالش‌ترین حوزه‌های نفوذ فناوری اطلاعات، حوزه بهداشت و سلامت می‌باشد. این نفوذ فراگیر منجر به توسعه شبکه‌های سلامت الکترونیک با تنوع خدمات و کیفیت‌های مختلف شده است. موضوع مدیریت امنیتی، حفظ محرمانگی و یکپارچگی داده و تبادل آن در فضای امن بین طرفین قابل اعتماد، به عنوان چالش شبکه‌های سلامت الکترونیک مطرح می‌باشد. با بررسی‌های انجام شده در مقاله‌های پیشین، ارائه مدلی جامع برای احراز هویت و تبادل امن اطلاعات و کارا به همراه رویکرد توزیع شده و پرهیز از نقطه یگانه شکست که بتواند نیازمندی‌های مختلف شبکه سلامت الکترونیک را پوشش دهد، به عنوان خلأ و نیازی قابل توجه به چشم می‌خورد. در این پژوهش سعی شده است با برطرف کردن محدودیت‌های مقاله‌های پیشین احراز هویت در شبکه سلامت الکترونیک و استفاده از مزایای مدل‌های احراز هویت در حوزه‌های کاربردی مختلف، مدل احراز هویت امنی برای شبکه سلامت الکترونیک معرفی شود.

روش: در این مطالعه مدل احراز هویت امن و توزیع شده‌ای برای شبکه سلامت با تلفیقی از زیرساخت کلید عمومی و بلاک چین طراحی و کاربردپذیری آن را در قالب یک مصداق (نسخه نویسی الکترونیکی) ارائه شد.

نتایج: این مدل نشان داد که تلفیق زیرساخت کلید عمومی به همراه بلاک‌چین می‌تواند احراز هویت امن، دوطرفه، مقیاس‌پذیر و توزیع شده با ویژگی پرهیز از نقطه یگانه شکست برای شبکه سلامت الکترونیک فراهم کند.

نتیجه‌گیری: می‌توان نتیجه گرفت، برای برطرف کردن نیازمندی‌های امنیتی شبکه سلامت الکترونیک باید به سمت مدل‌های احراز هویت نظیر به نظیر و عدم وابسته به سرور مرکزی رفت و مدل پیشنهادی نشان داد، ترکیب زیرساخت کلید عمومی با بلاک‌چین، می‌تواند مزایا و نیازمندی‌های امنیتی را پوشش دهد.

کلید واژه‌ها: سلامت الکترونیک، احراز هویت، بلاک چین، زیرساخت کلید عمومی، امنیت

• **ارجاع:** محمدی شهریار، قنبری نازنین. ارائه مدلی برای احراز هویت توزیع شده در یک شبکه سلامت الکترونیک با استفاده از بلاک چین مجله انفورماتیک سلامت و زیست پزشکی ۱۳۹۹؛ ۷(۴): ۲۴-۴۱۳.

۱. دکتری فناوری اطلاعات، دانشیار، گروه فناوری اطلاعات دانشکده صنایع، دانشگاه صنعتی خواجه نصیرالدین طوسی، تهران، ایران

۲. دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات، گرایش مدیریت سیستم‌های اطلاعاتی، گروه فناوری اطلاعات، دانشگاه صنعتی خواجه نصیرالدین طوسی، دانشکده صنایع، تهران، ایران

*** نویسنده مسئول:** شهریار محمدی

آدرس: تهران، میدان ونک، خیابان ملاصدرا، خیابان پرددیس، دانشکده مهندسی صنایع

• **شماره تماس:** ۰۲۱۸۸۴۶۵۰۳۰

• **Email:** mohammadi@kntu.ac.ir

مقدمه

ما در حال حرکت به سمت آینده‌ای هستیم که در آن فناوری‌های اطلاعات و ارتباطات در حوزه بهداشت و سلامت در زندگی مردم به طور کامل فراگیر خواهد شد. ترکیب فناوری اطلاعات و ارتباطات با سامانه‌های سنتی مراقبت از سلامت موجب شکل‌گیری سلامت الکترونیک شده است. سامانه‌های سلامت الکترونیک، زندگی روزانه مردم را با حذف کردن سامانه‌های کاغذی، به همراه مزایای فوق‌العاده‌شان تغییر داده و از طرفی کارایی، دقت و دسترس‌پذیری را افزایش داده‌اند. البته شبکه‌های سلامت الکترونیک با چالش‌های متعدی مانند: امنیت، حریم خصوصی شناسه‌ها، اطلاعات و پرونده‌های الکترونیک سلامت بیماران مواجه شده‌اند [۱].

با توجه به حساسیت‌های موجود در خدمات پزشکی، داده‌ها و اطلاعات ذخیره و رد و بدل شده در این بستر، حفظ امنیت سلامت الکترونیک بیش از هر سیستم دیگری اهمیت می‌یابد. مسائل مربوط به امنیت و حریم خصوصی مانع پذیرش گسترده سامانه‌های سلامت الکترونیک هستند. احراز هویت و حریم خصوصی داده‌ها نگرانی‌های ویژه‌ای در این حوزه قلمداد می‌شوند. وقتی نیازی به یک خدمت پزشکی و درمانی وجود دارد، شناسه بیمار باید احراز هویت شود. بدون یک مکانیزم احراز هویت مناسب افراد بیگانه می‌توانند هویت بیمار را جعل کنند و به اطلاعات او دسترسی پیدا کنند [۱]. در حالت کلی ۳ مکانیزم و اصل برای احراز هویت می‌توان مطرح کرد: نام کاربری و رمز عبور، زیرساخت کلید عمومی، بیومتریک [۲]. با توجه به اهمیت موضوع احراز هویت در شبکه‌های سلامت الکترونیک، پژوهش‌های بسیاری به ارائه مدل برای معرفی یک مکانیزم احراز هویت امن پرداخته‌اند.

تحقیقات اخیر فناوری اطلاعات در حوزه‌های کاربردی مختلف مانند: صنعت، اینترنت اشیاء، انرژی، سلامت و ... از ابزاری به نام بلاک چین (Block chain) بهره برده‌اند.

در مطالعه پژوهش‌های پیشین [۵-۳] روال مشخصی برای ثبت‌نام اولیه کاربران و تأیید و مجوز دادن به افراد در نظر نگرفته‌اند. در حالی که تأیید اولیه کاربران برای ثبت‌نام و حضور در شبکه مورد مهمی در شبکه سلامت الکترونیک می‌باشد. در تعدادی از مطالعات [۱۰-۶] به نیازمندی‌های مهمی از جمله مقیاس‌پذیر بودن مدل، دارای قابلیت پرهیز از نقطه یگانه شکست اشاره نکرده‌اند و مدل پیشنهادی آن‌ها دارای این قابلیت نمی‌باشد و به یک سرور مرکزی برای انجام هر بار احراز هویت وابسته می‌باشد. برخی نیز [۱۰] از روش‌های بیومتریک برای احراز هویت استفاده کرده‌اند که شبیه‌سازی آن‌ها در مقیاس کوچک با نرم‌افزار متلب انجام شده است. مطالعه Wetzels و همکاران [۱۱] تنها به موضوع احراز هویت در کاربرد اینترنت اشیاء پرداخته‌اند که جامعیت لازم برای پاسخگویی به تمام نیازهای شبکه سلامت الکترونیک را ندارد. برای برطرف کردن محدودیت‌های مدل‌های احراز هویت در شبکه سلامت الکترونیک، مقاله‌هایی که به ارائه مدل احراز هویت در کاربردهای دیگر پرداخته بودند، مورد بررسی قرار گرفت. جدیدترین مقاله‌ها از بلاک‌چین و زیرساخت کلید عمومی برای احراز هویت استفاده کردند. پژوهش‌هایی نیز [۱۶-۱۲] از بلاک‌چین استفاده و به مقیاس‌پذیری و کارایی توجه کرده‌اند. مطالعه Prakasha و همکاران [۱۷] از زیرساخت کلید عمومی و مزایای آن بهره برده و البته عدم توجه به مقیاس‌پذیر بودن مدل و اتکا به سرور مرکزی برای احراز هویت از محدودیت‌های آن می‌باشد. در مطالعه Wang و همکاران Norta و همکاران [۱۸،۱۹] نیز به مرجعی برای ثبت‌نام و تأیید هویت افراد اشاره نشده است. دسته‌ای از مقالات [۱۳،۲۰] نیز مدل‌هایی برای احراز هویت در اینترنت اشیاء ارائه کرده‌اند.

در این پژوهش تلاش شده است در جهت برطرف کردن محدودیت‌های ذکر شده در مطالعه‌هایی که به ارائه مدل احراز هویت در شبکه سلامت الکترونیک پرداخته‌اند، از مزایا و روش‌های مدل‌هایی که احراز هویت امنی در شبکه‌های دیگر مانند صنعت، انرژی و ... ارائه کرده‌اند، استفاده شود. بررسی این پژوهش‌ها نشان می‌دهد ارائه مدلی به صورت ترکیبی از بلاک چین و زیرساخت کلید عمومی می‌توان مزایای مناسبی را به همراه آورد. برای اطمینان از این موضوع، به طراحی مدلی که اساس و چارچوب آن، الهام گرفته از روش کار پژوهش‌های [۱۸،۱۴،۲۱] می‌باشد.

زیرساخت کلید عمومی مجموعه‌ای از سخت‌افزار، نرم‌افزار، افراد، رویه‌ها و سیاست‌هایی می‌باشد که برای ایجاد، مدیریت، ذخیره‌سازی، توزیع و لغو گواهی‌های دیجیتالی (Digital certificate) بر اساس رمزنگاری نامتقارن مورد استفاده هستند [۸].

بلاک‌چین یک دفترچه عمومی شامل هش بلاک‌هایی می‌باشد که غیرقابل تغییر بوده و مجهز به برچسب زمانی می‌باشد که عملکرد ذخیره و به اشتراک‌گذاری داده‌ها را در یک حالت توزیع شده فراهم می‌کند [۲۲]. بلاک‌چین (از لحاظ ساختاری) دنباله‌ای از بلاک‌ها می‌باشد که لیست کاملی از رکوردهای تراکنشی را مانند دفتر عمومی معمولی نگه می‌دارد.

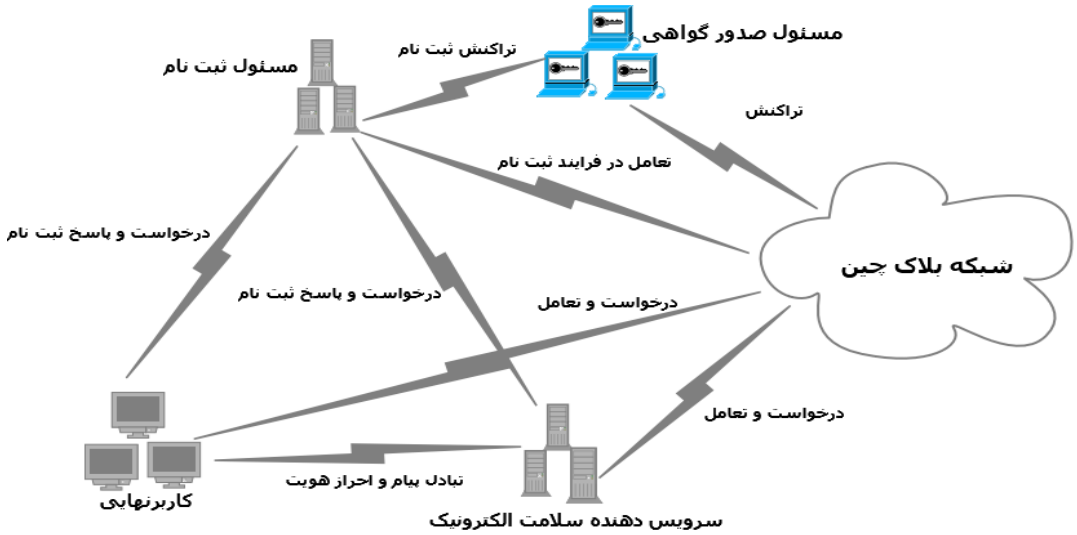
هر بلاک در هر لحظه با مرجعی به بلاک قبلی‌اش اشاره می‌کند که این مرجع (اشاره‌گر) مقدار هش (hash) بلاک قبلی کـه بـه آن بلاک والد (parent block) گفته می‌شود، می‌باشـد. اولـین بلاک در بلاک چین را بلاک منشأ می‌گویند [۲۳].

روش

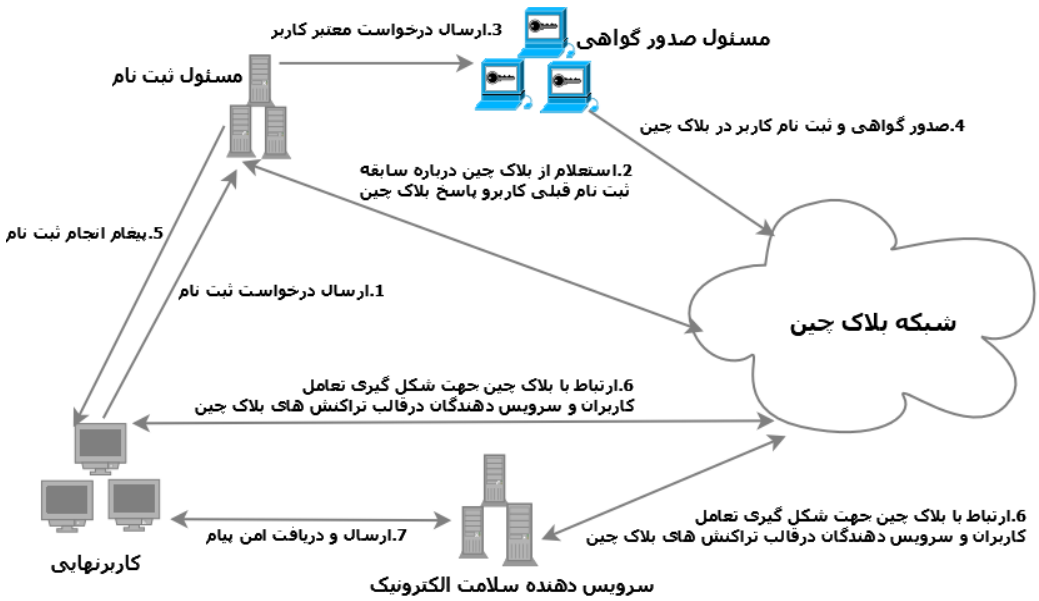
در مطالعه Wang و همکاران [۱۸] به ارائه مـدلی بـرای احـراز هویت امن با تأکید بر کاربرد مدل در حوزه انرژی پرداخته‌اند. به نظر می‌رسد در مدل زیرساخت، کلید عمومی را به همراه بـلاک چین استفاده کـرده اسـت. در حـالی کـه در آن مسـئول صـدور گواهی دیده نمی‌شود و مرجعی برای تأیید افراد بـرای ثبت‌نـام و ورود به شبکه در نظر گرفته نشده است؛ بنابراین سعی شد مـدل این مطالعه با اضافه کردن مسـئول صـدور گـواهی کـه وظیفـه صدور گواهی به افراد درخواست کننده را دارد، تغییر داده شود. از طرفی مـدل پیشـنهادی مطالعـه Zeb و همکـاران [۲۱] نقـش کـاربران ماننـد بیمـاران، پزشـکان و سـرویس‌دهندگان شـبکه سلامت الکترونیـک ماننـد سـرورهای پرونـده‌هـای الکترونیـک سلامت، نسخه‌نویسی الکترونیک را مشخص کـرده بـود و ایـن نقش‌ها در مدل پیشنهادی نظر گرفته شد؛ امـا در ایـن پـژوهش احراز هویت به طور کامل وابسته به سرور مرکزی می‌باشد و این مستعد نقطه یگانه شکست می‌باشد؛ زیرا اگر سرور به هر دلیلـی از کار بیفتد، احراز هویت کل مجموعه دچـار مشـکل مـی‌شـود. همچنین اگر قرار باشد تعداد کاربران زیـاد شـود، معلـوم نیسـت سرور تا چه اندازه بتواند پاسخگو باشـد. بـه همـین دلیـل مـدل پیشنهادی مقیاس‌پـذیر بـه نظـر نمی‌رسـد. بـرای ذخیره‌سـازی گواهی، نگهداری و توزیـع کلیـد و بـه دنبـال آن اجـرای احـراز هویت، به جای مکانیزم سنتی زیرساخت کلید عمومی، از پایگـاه داده توزیع شده بلاک‌چین بهره برده شد.

به منظور اثبات احراز شدن هویت فرستنده پیام بـرای گیرنـده پیـام، گـام‌هـای پیشـنهادی مشـابه روش کـار مطالعـه Zeb و همکاران [۲۱] به صورت فلوچارت‌هایی نشان داده شده است.

مطابق با مدل کلی شکل ۱ که مـدل تلفیقـی زیرسـاخت کلیـد عمومی و بلاک‌چین می‌باشد، فرآیند احراز هویت با تعامل اجزا با یکدیگر در شکل ۲ در سطح بالاتری نشان داده شده است.



شکل ۱: سطح صفر مدل پیشنهادی برای احراز هویت در شبکه سلامت الکترونیک



شکل ۲: سطح بالاتری از مدل پیشنهادی، ترتیب گام‌های انجام شده در شبکه

معرفی اجزا

کاربران نهایی: افرادی هستند که جهت استفاده و دسترسی به سرویس دهنده‌های سلامت الکترونیک درخواست خود را ارسال می‌کنند. به طور مثال یک پزشک برای استفاده از سرویس نسخه‌دهی و تجویز و ارسال نسخه به داروخانه باید ابتدا به عنوان کاربر پزشک ثبت نام شود و سپس با دریافت گواهی ثبت‌نام و احراز هویت به تجویز نسخه و ارسال آن در قالب پیام به داروخانه بپردازد.

سرویس‌دهندگان سلامت الکترونیک: سرویس‌دهنده‌هایی هستند که وظیفه انجام خدمت مشخصی را به کاربران دارند و از سویی فضای ذخیره‌سازی و امکانات محاسباتی لازم برای تحلیل‌های داده‌ای مورد نیاز را برای مسئولان مشخص فراهم می‌کند. سرویس دهنده اصلی نسخه‌نویسی الکترونیکی و سرور داروخانه مثالی در حوزه نسخه‌نویسی الکترونیک مطرح می‌شود و هویت پزشکان باید برای سرور داروخانه احراز شود تا پزشک صادرکننده نسخه شناسایی و قابل رهگیری شود.

مسئول ثبت‌نام: مسئول ثبت‌نام یک سرویس دهنده مورد اعتماد شبکه است و وظیفه ثبت‌نام کاربران جدید و برقراری ارتباط لازم با مسئول صدور گواهی برای ثبت‌نام و انتساب کلید عمومی و گواهی به کاربر می‌باشد. یکی از وظایف مهم آن چک کردن عدم ثبت‌نام قبلی کاربر می‌باشد و برای تمام سرویس‌های سلامت الکترونیک نقش ثابتی را ایفا می‌کند.

مسئول صدور گواهی: مسئول صدور گواهی، وظیفه بررسی شرایط کاربر برای ثبت‌نام و تأییدیه کاربر برای ثبت‌نام و انتساب گواهی و کلید عمومی به آن منطبق با سیاست‌های شبکه را بر عهده دارد و تراکنش‌های لازم را جهت ثبت‌نام با مسئول ثبت‌نام و بلاک چین انجام می‌دهد و برای تمام سرویس‌های سلامت الکترونیک نقش ثابتی را ایفا می‌کند.

بلاک‌چین: به عنوان قلب تپنده امن‌سازی و بهبود کارایی شبکه عمل می‌کند. به ازای صدور گواهی توسط مسئول صدور گواهی برای هر شخص، یک بلاک در بلاک‌چین به ازای آن ایجاد می‌شود. وظیفه بلاک‌چین ثبت و ضبط گواهی‌ها و کلید عمومی کاربران ثبت‌نام شده، ارائه بستر امن برای رد و بدل شدن پیام‌ها در قابل تراکنش‌ها و کمک به طرفین برای بازیابی کلید عمومی طرف مقابل و کمک به احراز هویت می‌باشد. انجام اعمال ثبت، به‌روزرسانی و لغو عضویت کاربران را طبق درخواست مسئول صدور گواهی انجام می‌دهد. درخواست‌های مربوط به احراز هویت، به بلاک‌چین منتهی می‌شود. در این پژوهش ۲ رویکرد برای نقش بلاک‌چین در دل فرایند احراز هویت در نظر گرفته شده است.

روال کلی کار در مدل پیشنهادی به این صورت می‌باشد که کاربران نهایی که نیازمند دریافت خدمت و همچنین سرویس دهنده‌های معین که وظیفه سرویس‌دهی را بر عهده دارند پس از ثبت‌نام توسط مسئول ثبت‌نام و تأیید مسئول صدور گواهی در بلاک‌چین ثبت‌نام شده و کلید عمومی به آن‌ها اختصاص داده

می‌شود. این فرآیند پیش‌نیاز فرآیند اصلی، یعنی احراز هویت است. در این سیستم نیاز به روزرسانی اطلاعات کاربران و سرویس دهنده‌ها و لغو ثبت‌نام آن‌ها نیز به درخواست و فرمان مسئول صدور گواهی انجام می‌شود و تغییرات لازم در بلاک‌چین اعمال می‌شود.

نتایج

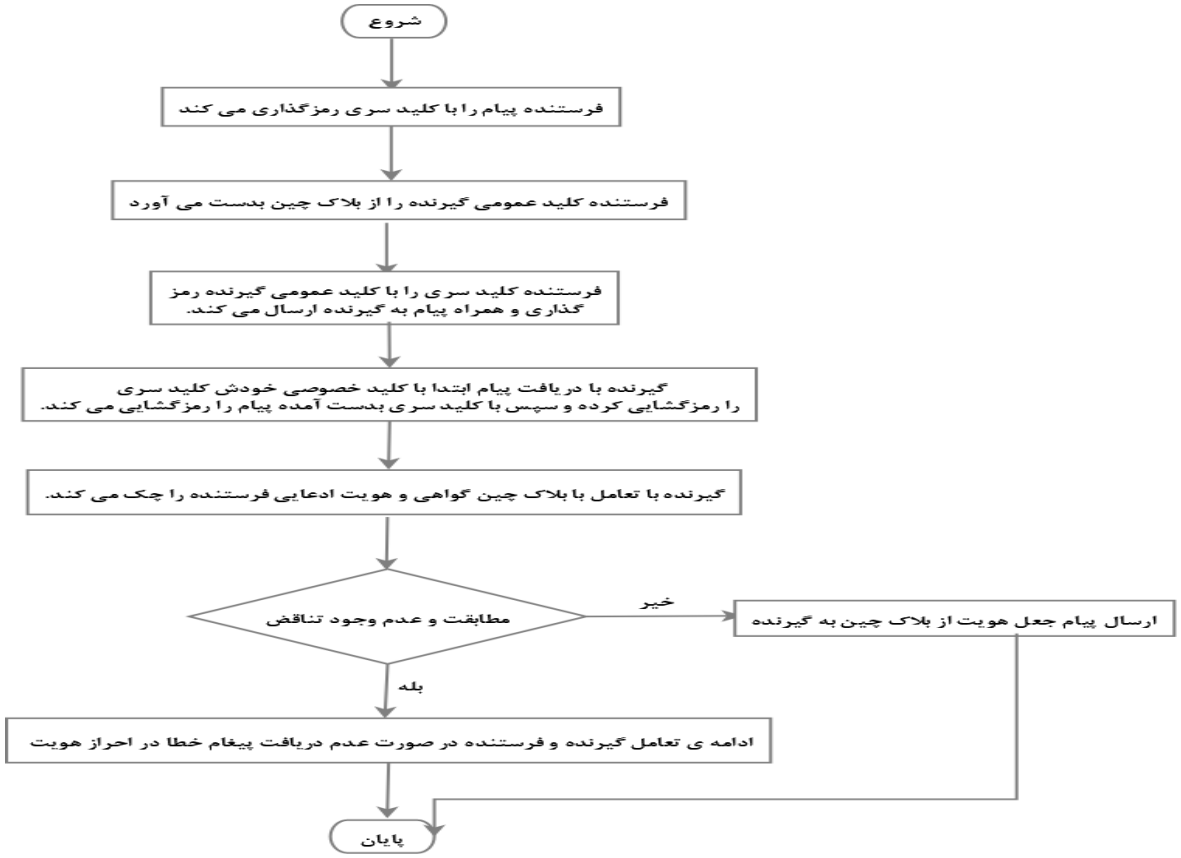
تحلیل کارایی و امنیتی مدل

طبق روش و مدل کلی پیشنهادی شکل ۱ و ۲، نحوه رد و بدل شدن پیام‌ها و شکل‌گیری تراکنش‌ها در قالب ۲ پیشنهاد مطرح می‌شود. فرآیند گام به گام احراز هویت طبق روش پیشنهادی، در این قسمت ارائه می‌شود. در ادامه، ابتدا هریک از پیشنهادها شرح داده شده سپس به ازای هریک فلوچارتی که نشان دهنده گام‌های اصلی هریک می‌باشد، ترسیم شده است.

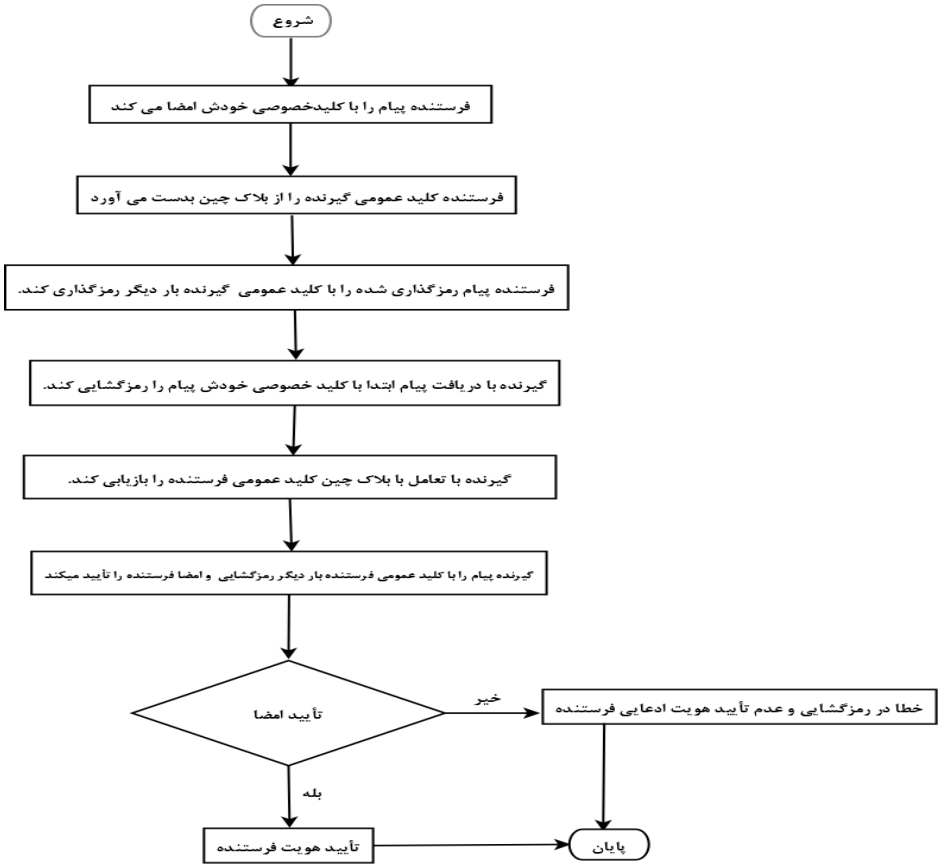
۱) پیشنهاد می‌شود که ارسال کننده پیام را با کلید سری رمزگذاری کند و کلید سری را هم با کلید عمومی گیرنده رمزنگاری کند و هر دو را به گیرنده بفرستد. گیرنده با دریافت محموله ابتدا با کلید خصوصی خودش کلید سری را رمزگشایی می‌کند سپس با استفاده از کلید سری پیام را رمزگشایی می‌کند. بدین‌ترتیب محرمانگی پیام حفظ می‌شود و از طرفی چون این پیام در قالب تراکنش‌های بلاک‌چین رد و بدل شده (با در نظر گرفتن امن بودن بلاک چین) شخصی خارج از شبکه امکان ارسال پیام را ندارد و چون در نظر می‌گیریم که در تراکنش‌های ارسالی آدرس فرستنده و گیرنده مشخص و به دلیل امن بودن و غیرقابل‌تغییر بودن محتوا امکان تغییر آدرس فرستنده امکان‌پذیر نیست. هیچ شخص (صاحب بلاکی) نمی‌تواند با هویت و آدرس بلاک دیگری به ارسال پیام اقدام کند؛ بنابراین گیرنده با دریافت پیام که حاوی گواهی و شناسه گیرنده نیز می‌باشد به طور خودکار با اتصال و تعامل با بلاک‌چین هویت ادعاشده از شخص را اعتبار سنجی می‌کند که در صورت هرگونه خطا و کشف جعل هویت، بلاک چین پیغام مبتنی بر احراز هویت نادرست یا جعل هویت را به گیرنده ارسال می‌کند. در غیر این صورت گیرنده با اعتماد به فرستنده ادامه تعامل را پی می‌گیرد. فلوچارت شکل ۳ ترتیب گام‌های انجام شده برای ارسال پیام و احراز هویت (پس از ثبت‌نام) را به صورت جزئی‌تر و با نمای بصری نشان می‌دهد.

۲) برای رد و بدل کردن پیام‌ها و احراز هویت فرستنده پیام برای دریافت کننده آن، شخص فرستنده پیام را با کلید خصوصی خودش پیام را امضا کند و سپس با کلید عمومی گیرنده رمزگذاری می‌کند. فرستنده کلید عمومی گیرنده را در کوتاه‌ترین زمان ممکن با تعامل با بلاک‌چین به دست می‌آورد. گیرنده با دریافت پیام ابتدا آن را با کلید خصوصی‌اش رمزگشایی کرده (تأمین محرمانگی پیام) و سپس با توجه به هویت اولیه اعلام شده از سمت فرستنده کلید عمومی‌اش را از بلاک‌چین بازیابی کرده و پیام را با کلید عمومی فرستنده رمزگشایی می‌کند و اگر رمزگشایی به درستی انجام شود و در واقع امضا فرستنده را تأیید می‌کند؛ یعنی هویت ارسال کننده به درستی احراز شده و با هویت اعلام شده یکسان است. شکل ۴ گام‌های این قسمت از احراز هویت را به صورت ترتیبی نشان می‌دهد. همان‌طور که ذکر شد به ازای تأیید ثبت‌نام هر فرد توسط مسئول صدور گواهی، به ازای آن یک بلاک در بلاک‌چین ذخیره می‌شود که شامل گواهی دیجیتال و کلید عمومی منتسب به شخص می‌باشد. حسن استفاده از بلاک‌چین برای ذخیره و بازیابی گواهی دیجیتال و کلید عمومی این است که این رویه همانند رویه سنتی زیرساخت کلید عمومی با ارجاع به مسئول صدور گواهی انجام نمی‌شود و بار کاری مسئول صدور گواهی را کاهش می‌یابد؛ به عبارت دیگر اجرای هر بار مکانیزم احراز هویت (پس از ثبت‌نام اولیه) بدون وابستگی به مسئول صدور گواهی انجام می‌پذیرد.

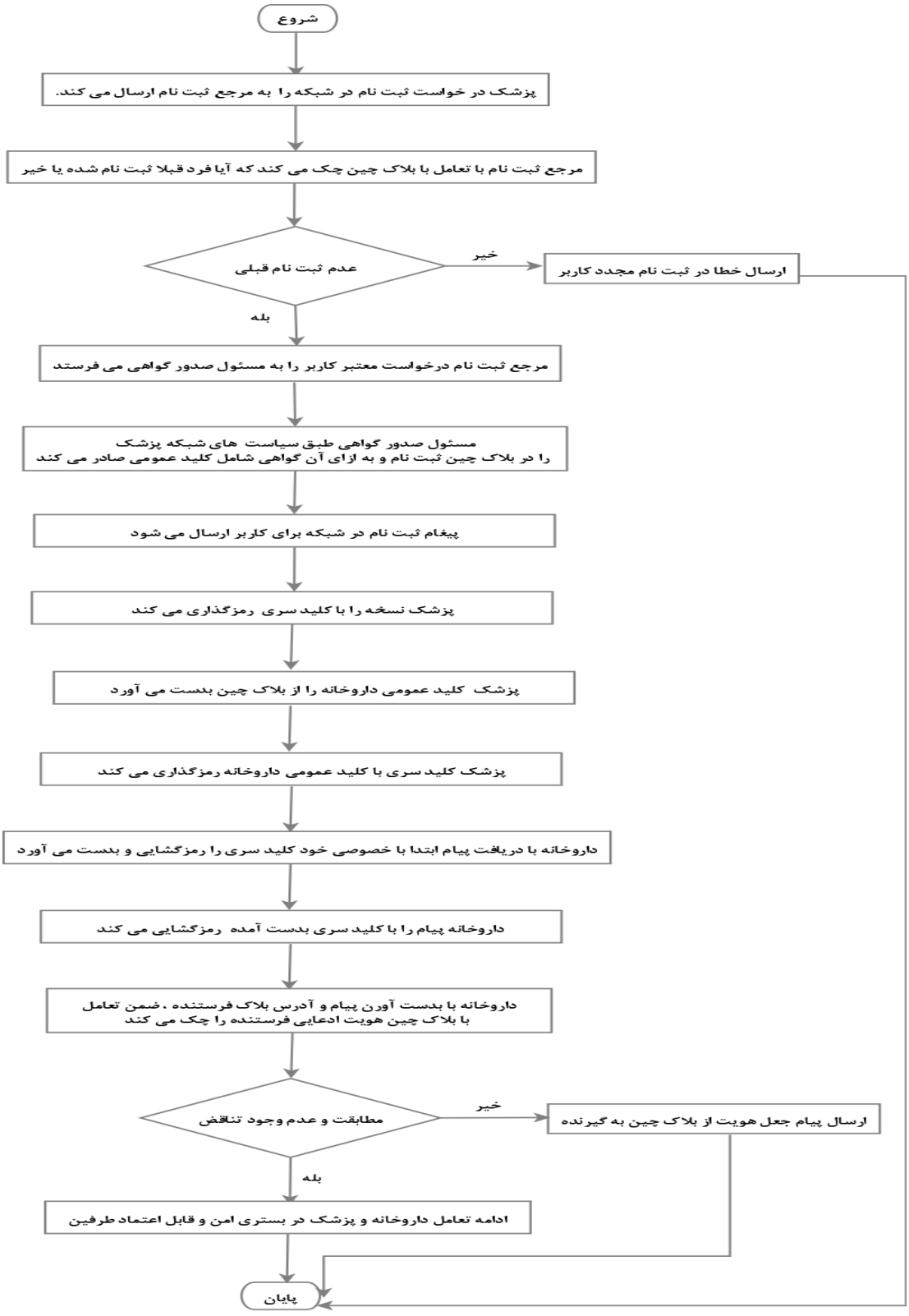
در این قسمت، به منظور ملموس‌تر شدن کاربرد مدل پیشنهادی، یکی از رایج‌ترین و اساسی‌ترین خدمات شبکه سلامت الکترونیک که در پژوهش‌ها نیز برای آن مکانیزمی ارائه نشده بود، در نظر گرفته شد و گام‌های ثبت‌نام و احراز هویت پیشنهادی را طبق دو پیشنهاد ارائه شده برای این مصداق کاربردی پیاده شد. نتیجه آن فلوچارت شماره ۵ طبق پیشنهاد ۱ و فلوچارت ۶ طبق پیشنهاد ۲ می‌باشد.



شکل ۳: فلوچارت تعاملات فرستنده و گیرنده و بلاک چین در پیشنهاد ۱



شکل ۴: تعاملات فرستنده، گیرنده و بلاک چین در پیشنهاد ۲



شکل ۵: گام‌های طی شده برای نسخه‌نویسی الکترونیک طبق پیشنهاد ۱

شکل ۶: گام‌های طی شده برای نسخه‌نویسی الکترونیک طبق پیشنهاد ۲

به طور خلاصه یافته‌ها و مزایای حاصل از مدل و مکانیزم پیشنهادی این‌طور بیان می‌شود:

- ✓ احراز هویت امن و دوطرفه (به استناد گام‌های مطرح شده در فلوچارت‌ها)
- ✓ احراز هویت نظیر به نظیر، عدم وابستگی به سرور مرکزی و دارای قابلیت پرهیز از نقطه یگانه شکست (به دلیل انجام احراز هویت بین طرفین بدون دخالت شخص سوم و انجام تراکنش‌ها در قالب تراکنش‌های بلاک‌چین)
- ✓ احراز هویت مقیاس‌پذیر (به دلیل عدم وابستگی به یک سرور مرکزی و اضافه شدن کاربران در قالب بلاک‌های بلاک‌چین)
- ✓ در نظر گرفتن نقش کاربران سلامت الکترونیک در شبکه
- ✓ استفاده از فضای توزیع شده برای ذخیره، بازیابی داده‌های مهم و پراستفاده برای احراز هویت مانند کلید عمومی یا گواهی‌ها
- ✓ حفظ محرمانگی و یکپارچگی گواهی‌ها و داده‌های مهم شبکه به دلیل استفاده از الگوریتم‌های رمزگذاری که در فلوچارت‌ها به آن اشاره شده است.
- ✓ کنترل ثبت‌نام کاربران مجاز در شبکه توسط مسئول صدور گواهی
- ✓ حفظ یکپارچگی پیام‌های رد و بدل شده در شبکه (به دلیل وجود بستر امن بلاک‌چین برای انجام تراکنش‌ها)

همان‌طور که بیان شد، خدمات سلامت الکترونیک به لحاظ تعداد و تنوع در حال زیاد شدن می‌باشد و ضرورت استفاده و فراگیری آن‌ها در حال گسترش می‌باشد. این گسترش ما را با چالش‌های مختلف حفظ محرمانگی داده‌ها، امنیت، سرعت و ... رو به رو می‌کند. به طوری که مدیریت امنیتی و احراز هویت در شبکه‌های سلامت الکترونیک مختلف همواره مورد توجه پژوهشگران و مطالعات پیشین بوده است. اغلب پژوهش‌ها سعی در نظر گرفتن برخی خدمات خاص، مانند پرونده‌های الکترونیک سلامت، دورا پزشکی و کاربرد اینترنت اشیاء در سلامت بوده‌اند تا بتوانند با ارائه مدلی به امن‌سازی و احراز هویت قابل‌اعتماد به عنوان رکن اصلی امنیت در شبکه کمک کنند. در حالی که باید به این خدمات به صورت یکپارچه نگاه کرد و مدلی برای امنیت و احراز هویت ارائه داد که برای تمام خدمات قابل استفاده باشد. به دنبال استفاده از زیرساخت کلید عمومی، بلاک‌چین یکی از فناوری‌های موردتوجه قرار گرفته در مطالعه اخیر به شمار می‌آید. در جدول ۱ به صورت خلاصه مزایا و نیازمندی‌های در نظر گرفته شده در مدل پیشنهادی این مطالعه با برخی از مطالعات دیگری که به حل چالش احراز هویت در شبکه سلامت الکترونیک پرداخته‌اند، مقایسه شده است. Wetzels و همکاران [۱۱] که به ارائه مدل احراز هویت پرداخته‌اند، کاربرد مدل پیشنهادیشان تنها مناسب شبکه اینترنت اشیاء می‌باشد؛ اما پژوهش‌هایی که کاربردهای عمومی‌تر شبکه سلامت الکترونیک دارند در جدول ۱ با مدل پیشنهادی این مطالعه مقایسه شده‌اند.

جدول ۱: مقایسه مزایای مدل پیشنهادی با دیگر پژوهش‌ها

مدل پیشنهادی این مقاله	[۲۱]	[۹]	[۴]	[۲۴]	[۳]	نیازمندی و مزیت
✓				✓		درنظرگرفتن مرجع اولیه برای ثبت‌نام و مجوزدهی به کاربران
✓	✓		✓			درنظرگرفتن کاربران مختلف در شبکه
✓		✓			✓	احراز هویت دوطرفه (احراز هویت فرستنده پیام)
✓		✓			✓	مقیاس‌پذیری مدل
✓		✓			✓	احراز هویت توزیع‌شده (پرهیز از نقطه یگانه شکست)
✓	✓	✓	✓	✓	✓	حفظ محرمانگی، حریم خصوصی و یکپارچگی داده‌ها

بحث و نتیجه‌گیری

با توجه به نتایج و تحلیل مدل پیشنهادی بر اساس تکمیل پژوهش‌های پیشین، می‌توان با بهره‌گیری از اصول احراز هویت مبتنی بر زیرساخت کلید عمومی و مزایای بلاک‌چین به طور هم‌زمان، مدل احراز هویت امن‌تر، کاراتر و قابل اطمینان‌تری داشته باشیم که مزایای آن در بخش یافته‌ها تحلیل شد و نیازمندی‌های امنیتی بیشتری نسبت به مطالعات پیشین می‌توان در این مدل پوشش داد که در جدول ۱ به مهم‌ترین آن‌ها اشاره شده است. می‌توان نتیجه گرفت، برای برطرف کردن نیازمندی‌های امنیتی شبکه سلامت الکترونیک که موضوع حریم خصوصی، محرمانگی و یکپارچگی داده‌ها و از سویی در نظر گرفتن کاربران مختلف در شبکه، پرهیز از نقطه یگانه شکست،

حضور مرجعی برای ثبت‌نام و تأیید اولیه کاربران، احراز هویت دوطرفه و مقیاس‌پذیر قابل اهمیت می‌باشد، باید به سمت مدل‌های احراز هویت نظیر به نظیر و عدم وابسته به سرور مرکزی رفت و مدل پیشنهادی نشان داد، ترکیب زیرساخت کلید عمومی با بلاک‌چین، می‌تواند مزایا و نیازمندی‌های ذکر شده را پوشش دهد.

این مدل گرچه توانایی اجرا در شبکه‌های مختلف سلامت الکترونیک را دارا است؛ اما خدمات حوزه سلامت الکترونیک در حال متنوع شدن هستند. به همین دلیل می‌توان این بررسی را انجام داد که آیا مدل ارائه شده برای احراز هویت، می‌تواند در کاربردهای دیگر هم مورد استفاده قرار بگیرد. اگرچه در طراحی این مدل به احراز هویت نظیر به نظیر، دوطرفه و قابل اعتماد و مقیاس‌پذیر به همراه برخی دیگر از ملاحظات دست یافته‌ایم؛ اما از لحاظ سرعت اجرا، می‌توان مدل را با الگوریتم‌های مختلفی از جمله موارد ارائه شده در مطالعه‌های [۱،۱۸،۱۶،۲۵] پیاده‌سازی و در پژوهش‌های آینده ویژگی سرعت را در الگوریتم‌های رمزگذاری مختلف مقایسه کرد. همچنین در این مطالعه درباره نحوه پیاده‌سازی بلاک‌چین اشاره نشده است و می‌توان این مدل را در انواع بلاک‌چین‌های خصوصی و عمومی پیاده‌سازی کرد و نتایج حاصل را با هم مقایسه کرد. از جهتی دیگر می‌توان کاربردپذیری مدل احراز هویت پیشنهادی را برای حوزه‌های دیگر مانند دولت الکترونیک، صنعت و ... بررسی کرد و برای انطباق مدل در کاربردهای دیگر، مدل را بهبود بخشید. همچنین با پررنگ‌تر شدن اهمیت دورکاری کادر درمان و ارائه خدمات از راه دور به بیماران در شرایط بروز اپیدمی مانند اپیدمی کووید ۱۹ در جهان، می‌توان خدمات جدیدتری که به صورت دوراپزشکی در حال اجرا می‌باشند یا پتانسیل اجرایی شدن را دارا هستند، بررسی کرده و درباره کارایی مدل احراز هویت پیشنهادی در این دسته خدمات امکان‌سنجی کرد و چنان چه مدل پیشنهادی نیاز به اصلاح و به‌روزرسانی دارد، مدل را بهبود داد.

تعارض منافع

این پژوهش با حمایت‌های معنوی دانشکده صنایع دانشگاه خواجه‌نصیرالدین طوسی در قالب یک پروژه پژوهش در راستای پایان‌نامه دانشجویی انجام شد و هیچ‌گونه تعارض منافعی در آن وجود ندارد.

References

1. Huang P, Li B, Guo L, Jin Z, Chen Y. A robust and reusable ecg-based authentication and data encryption scheme for ehealth systems. Global Communications Conference (GLOBECOM); 2016 4-8 Dec; Washington, DC, USA: IEEE; 2016. p. 1-6. doi: 10.1109/GLOCOM.2016.7841541

2. Thakur M. Authentication, authorization and accounting with Ethereum block chain [dissertation]. Finland: University of Helsinki: 2017.

3. Cao S, Zhang G, Liu P, Zhang X, Neri F. Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. Information Sciences 2019;485:427-40.

4. Elmufti K, Weerasinghe D, Rajarajan M, Rakocevic V, Khan S. Timestamp authentication protocol for remote monitoring in ehealth. Second International Conference on Pervasive Computing Technologies for Healthcare; 2008 Jan- Feb 30-1; Tampere, Finland: IEEE; 2008. p. 73-6. doi: 10.1109/PCTHEALTH.2008.4571031

5. Thiranant N, Lee H. A design of security framework for eHealth authentication system using QR Code. Advanced Science and Technology Letters 2013;38:32-5. doi: 10.14257/astl.2013.38.07

6. Wetzels M, Ayoola I, Bogers S, Peters P, Chen W, Feijs L. Consume: A privacy-preserving authorisation and authentication service for connecting with health and wellbeing APIs. Pervasive and Mobile Computing 2018;43:20-6. https://doi.org/10.1016/j.pmcj.2017.11.002

7. Wang X, Bai L, Yang Q, Wang L, Jiang F. A dual privacy-preservation scheme for cloud-based eHealth systems. Journal of Information Security and Applications 2019;47:132-8. https://doi.org/10.1016/j.jisa.2019.04.010

8. Farahani B, Firouzi F, Chang V, Badaroglu M, Constant N, Mankodiya K. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Generation Computer Systems 2018;78:659-76. https://doi.org/10.1016/j.future.2017.04.036

9. Al Omar A, Rahman MS, Basu A, Kiyomoto S. Medibchain: A blockchain based privacy preserving platform for healthcare data. The 10th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage 2017 Dec 12; Guangzhou, China: Springer, Cham; 2017. p. 534-43. doi: 10.1007/978-3-319-72395-2_49

10. Yakubov A, Shbair W, Khan N, Medinger C, Hilger J. BlockPGP: A Blockchain-based Framework for PGP Key Servers. International Journal of Networking and Computing 2020;10(1):1-24. doi: 10.15803/ijnc.10.1_1

11. Wetzels M, Ayoola I, Bogers S, Peters P, Chen W, Feijs L. Consume: A privacy-preserving authorisation and authentication service for connecting with health

and wellbeing APIs. Pervasive and Mobile Computing 2018;43:20-6.
12. Lin C, He D, Huang X, Choo KK, Vasilakos AV. BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. Journal of Network and Computer Applications 2018;116:42-52. https://doi.org/10.1016/j.jnca.2018.05.005
13. Ourad AZ, Belgacem B, Salah K. Using blockchain for IOT access control and authentication management. In Internet of Things 2018 Jun 25 Springer; 2018. p. 150-64. doi: 10.1007/978-3-319-94370-1_11
14. Suralkar S, Udasi S, Gagnani S, Tekwani M, Bhatia M. E-Voting Using Blockchain With Biometric Authentication. International Journal of Research and Analytical Reviews 2019; 6(1): 72-81.
15. Pal O, Alam B, Thakur V, Singh S. Key management for blockchain technology. ICT Express 2019. https://doi.org/10.1016/j.icte.2019.08.002
16. Kabra N, Bhattacharya P, Tanwar S, Tyagi S. MudraChain: Blockchain-based framework for automated cheque clearance in financial institutions. Future Generation Computer Systems 2020;102:574-87. https://doi.org/10.1016/j.future.2019.08.035
17. Prakasha K, Gowda P, Acharya V, Muniyal B, Khandelwal M. Enhanced Authentication and Key Agreement Mechanism Using PKI. 9th International Conference on Applications and Techniques in Information Security; 2018 Nov 9; Nanning, China: Springer: Singapore; 2018. p. 40-51. doi: 10.1007/978-981-13-2907-4_4
18. Wang J, Wu L, Choo KK, He D. Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure. IEEE Transactions on Industrial Informatics 2019;16(3):1984-92. doi: 10.1109/TII.2019.2936278
19. Norta A, Matulevičius R, Leiding B. Safeguarding a formalized blockchain-enabled identity-authentication protocol by applying security risk-oriented patterns. Computers & Security 2019;86:253-69. doi: 10.1016/J.COSE.2019.05.017
20. Rahim K, Tahir H, Ikram N. Sensor based puf iot authentication model for a smart home with private blockchain. International Conference on Applied and Engineering Mathematics; 2018 4-5 Sep; Taxila, Pakistan: IEEE; 2018. p. 102-8. doi: 10.1109/ICAEM.2018.8536295
21. Zeb K, Saleem K, Al Muhtadi J, Thuemmler C. U-prove based security framework for mobile device authentication in eHealth networks. 18th International Conference on e-Health Networking, Applications and Services (Healthcom) 2016 Sep 14-16; Munich, Germany: IEEE; 2016. p. 1-6. doi: 10.1109/HealthCom.2016.7749518
22. Conti M, Hassan M, Lal C. BlockAuth: BlockChain based distributed producer authentication in ICN. Computer Networks 2019;164:106888. https://doi.org/10.1016/j.comnet.2019.106888
23. Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems 2018;82:395-411. https://doi.org/10.1016/j.future.2017.11.022
24. Sahi A, Lai D, Li Y. Security and privacy preserving approaches in the eHealth clouds with disaster recovery plan. Comput Biol Med 2016.
25. Slagell A, Bonilla R, Yurcik W. A survey of PKI components and scalability issues. In2006 IEEE International Performance Computing and Communications Conference; 2006 Apr 10—12; Phoenix, AZ, USA: IEEE; 2006. p. 10. doi: 10.1109/.2006.1629442

Original Article

Journal of Health and Biomedical Informatics
Medical Informatics Research Center
2021; 7(4): 413-424

A Distributed Authentication Model for an E-Health Network Using Blockchain

Mohammadi Shahriar[1]*, Ghanbari Nazanin[2]

• **Received:** 22 Jun 2020 • **Accepted:** 10 Aug 2020

Introduction: One of the most important and challenging areas under the influence of information technology is the field of health. This pervasive influence has led to the development of electronic health (e-health) networks with a variety of services of different qualities. The issue of security management, maintaining confidentiality and data integrity, and exchanging it in a secure environment between trusted parties is a challenge for e-health networks. Reviewing previous studies revealed that providing a comprehensive and efficient model for authentication and secure exchange of information with a distributed approach while avoiding the single point of failure, which can meet the various needs of the e-health network, was necessary to fill the gap. In this study, it was attempted to introduce a secure authentication model for the e-health network by overcoming the limitations of previous articles on authentication in the e-health network and using the benefits of authentication models in various fields.

Method: In this study, a secure and distributed authentication model was designed for the health network with a combination of blockchain and public-key infrastructure and its usability was presented in the form of an applicable instance (electronic prescribing).

Results: This model showed that combining public-key infrastructure with blockchain can provide a secure, two-way, scalable, and distributed authentication with avoiding a single point of failure for the e-Health network.

Conclusion: It can be concluded that in order to meet the security requirements of the e-health network, it is necessary to use peer-to-peer authentication models which are not dependent on a central server and the proposed model indicated that combining public-key infrastructure with blockchain can bring benefits and fulfill security requirements.

Keywords: E-Health, Authentication, Blockchain, Public-Key Infrastructure, Security

• **Citation:** Mohammadi S, Ghanbari N. A Distributed Authentication Model for an E-Health Network Using Blockchain. Journal of Health and Biomedical Informatics 2021; 7(4): 413-24. [In Persian]

1. Ph.D. in Information Technology, Associate professor, Information Technology Dept., Faculty of Industrial Engineering, K.N.Toosi University of Technology, Tehran, Iran
2. M.Sc. Student in Information Technology- Information Systems Management, Information Technology Dept., Faculty of Industrial Engineering, K.N.Toosi University of Technology, Tehran, Iran
***Corresponding Author:** Shahriar Mohammadi
Address: Faculty of Industrial Engineering, Pardis St., Molla Sadra St., Vanak Square, Tehran, Iran
• **Tel:** 02188465030 • **Email:** mohammadi@kntu.ac.ir