مدیریت داده‌های پزشکی با کمک زنجیره بلوکی

زهرا امین مهر [۱]، فضل الله ادیب نیا [۲]

[۱] دانشجوی کارشناسی ارشد شبکه‌های کامپیوتری، فناوری اطلاعات، دانشگاه یزد، یزد
zahraaminmehr@stu.yazd.ac.ir
[۲] دانشیار دانشکده مهندسی کامپیوتر، فناوری اطلاعات، دانشگاه یزد، یزد
fadib@yazd.ac.ir

چکیده

در سال‌های اخیر، صنعت مراقبت‌های بهداشتی شاهد تحولی انقلابی با ادغام دستگاه‌های پزشکی به هم پیوسته، تجزیه و تحلیل داده‌ها و اتصال به اینترنت بوده است. اینترنت اشیاء پزشکی به شبکه‌ای از دستگاه‌های پزشکی، حسگرها، برنامه‌های کاربردی نرم‌افزاری و سیستم‌هایی اشاره دارد که برای بهبود ارائه مراقبت‌های بهداشتی، نظارت بر بیمار و رفاه کلی، به هم مرتبط هستند. این زیست‌بوم به هم پیوسته به دستگاه‌های پزشکی اجازه می‌دهد تا به طور یکپارچه با یکدیگر ارتباط برقرار کنند، اطلاعات مهم سلامتی را جمع آوری و تبادل کنند. با این حال، این داده‌ها بسیار حساس هستند و به یک سیستم ذخیره‌سازی و مدیریت ایمن و قابل اعتماد، نیاز دارند. در اینترنت اشیاء پزشکی چالشی که وجود دارد بحث امنیت و صحت داده‌ها و همچنین احراز هویت پزشکان و بیماران است. جهت برطرف نمودن این چالش، روش‌های مختلفی ارائه شده که هرکدام مزایا و معایبی دارند. معماری پیشنهادی در این مقاله ترکیبی از زنجیره بلوکی و پایگاه‌داده MongoDB است و معایب روش‌های دیگر را بهبود می‌بخشد. از جمله مزایای این مدل پیشنهادی مقیاس‌پذیری، کاهش سربار محاسباتی، حفظ حریم خصوصی و افزایش امنیت است.

کلمات کلیدی: امنیت، اینترنت اشیاء پزشکی، زنجیره بلوکی، محاسبات مه، MongoDB.

۱ مقدمه

اینترنت اشیاء پزشکی [۱] چشم‌انداز مراقبت‌های بهداشتی را با ترکیب قدرت دستگاه‌های متصل به هم و فناوری پیشرفته پزشکی متحول می‌کند. این فناوری شامل شبکه‌ای از دستگاه‌های پزشکی هوشمند، حسگرهای پوشیدنی و ابزارهای سلامت دیجیتال است که داده‌های بیمار را در زمان واقعی جمع‌آوری و به اشتراک می‌گذارد و تجزیه و تحلیل می‌کند. با اینترنت اشیاء پزشکی، متخصصان مراقبت‌های بهداشتی می‌توانند از راه دور بیماران را تحت نظر داشته باشند، علائم حیاتی را ردیابی کنند و اعلان‌هایی را در مورد مسائل

[1] Internet of Medical Things (IoMT)

بالقوه سلامت دریافت کنند. بیماران به لطف ابزارهای اینترنت اشیاء در مواقع ضروری قابل رصد هستند و همچنین ضرورت انجام معاینات روتین بهداشتی در بیمارستان‌ها کاهش می‌یابد. همچنین می‌توان اقامت در بیمارستان و هزینه‌های بستری مجدد را به حداقل رساند [۱]. از آنجا که داده‌ها در چندین موسسه پزشکی پراکنده هستند پردازش پرونده‌های پزشکی بیمار و احراز هویت بیماران و پزشکان به روشی ایمن بسیار دشوار است. از دست دادن اطلاعات شخصی و حساس بیمار و تشخیص احراز هویت نادرست، ممکن است پیامدهای قابل توجهی داشته باشد. علاوه براین، سیستم‌های پزشکی فعلی قادر به ایجاد شفافیت، قابلیت ردیابی، قابلیت اعتماد، تغییرناپذیری، حفظ حریم خصوصی و امنیت در هنگام رسیدگی به این پرونده‌ها نیستند [۲]. فناوری زنجیره بلوکی[۲] توانایی غلبه بر این مشکلات را در سیستم‌های مراقبت‌های بهداشتی امروز دارد [۱]. با این حال مقیاس‌پذیری، برگشت‌ناپذیری، هزینه زیاد و محاسبات فوق‌العاده بالا و غیره، چالش‌ها و نگرانی‌هایی هستند که زنجیره بلوکی با آن روبه‌رو است. در نتیجه، ایده‌ی پیشنهادی در این مقاله، ترکیبی از پایگاه‌داده توزیع‌شده MongoDB با فناوری زنجیره بلوکی و گره‌های مه است. بخش دوم مقاله به بررسی کارهای قبلی در حوزه زنجیره بلوکی می‌پردازد. در بخش سوم به پیش زمینه‌ای از زنجیره بلوکی، ساختار و مسائل آن و تعریفی از MongoDB پرداخته می‌شود. در بخش چهارم روش پیشنهادی بررسی شده است. و سرانجام، در بخش پنجم در مورد نتیجه‌گیری بحث می‌شود.

۲ کارهای انجام شده

اخیراً تحقیقات گسترده‌ای برای اطمینان از مراقبت‌های بهداشتی هوشمند با استفاده از اینترنت اشیاء پزشکی انجام شده است. با این حال، به دلیل جدید بودن اینترنت اشیاء پزشکی، در حال حاضر تحقیقات کمی در مورد بررسی امنیت در این زمینه در دسترس است. در این قسمت خلاصه ای از تلاش‌های قبلی در این زمینه بررسی می‌شود و به محدودیت‌ها و چالش‌های آنها اشاره می‌شود.

نویسندگان در سال ۲۰۱۷ در مقاله [۴-۳] پیشنهاد می‌کنند که حفظ حریم خصوصی داده‌های پزشکی تقریباً در اولویت قرار دارد، زیرا باعث به خطر افتادن وضعیت بیمار می‌شود. اگر این نقض اتفاق بیفتد، بر همه بیماران، ذی‌نفعان و اعتبارسنج‌ها تأثیر منفی می‌گذارد. برای جلوگیری از چنین وضعیتی، نویسندگان یک چارچوب مبتنی بر زنجیره بلوکی را برای محافظت از استقلال داده‌ها با استفاده از یک محیط ابری پیشنهاد می‌کنند. چارچوب پیشنهادی فقط به کاربران یا ذینفعان تایید شده اجازه دسترسی به یک سیستم را می‌دهد. اقدامات کاربران را می‌توان توسط چارچوب پیشنهادی مبتنی بر زنجیره بلوکی نظارت کرد. به اشتراک‌گذاری داده‌های بیمار با اتخاذ تکنیک‌های رمزنگاری تأیید می‌شود. این سیستم ارتباط بین کاربران و داده‌های حساس مراقبت‌های بهداشتی است. سیستم پیشنهادی آنها از یک زنجیره بلوکی سبک استفاده می‌کرد که تراکنش‌های سریع و کارایی مناسب را تضمین می‌کند. نویسندگان، پروتکل‌های ارتباطی و احراز هویت را به عنوان مطالعه بیشتر نگه داشته‌اند. سه لایه را در اینجا نگه داشته‌اند، یعنی لایه کاربر، لایه مدیریت سیستم و لایه ذخیره‌سازی. لایه کاربر شامل همه آن نهادها یا استخراج‌کنندگان زنجیره بلوکی است که سعی

[2] Blockchain

می‌کنند به داده‌ها دسترسی یا درخواست کنند. لایه مدیریت سیستم، مرکزی و مهم‌ترین لایه‌ای است که در آن تمامی ارتباطات برای تراکنش‌های امن برقرار می‌شود. آخرین لایه، یعنی لایه ذخیره‌سازی شامل کل داده‌هایی است که به‌طور ایمن در ابر برای کاربردهای متنوع بیشتر ذخیره می‌شوند. مشکل این پژوهش این است که احراز هویت و پروتکل ارتباطی کامل بررسی نشده است.

Muhammad Asif Habib و همکاران [۵] در سال ۲۰۱۹ یک مدل کنترل دسترسی برای اطمینان از حریم خصوصی داده‌های پزشکی در برابر تهدیدات داخلی در سیستم سلامت هوشمند پیشنهاد کردند. این روش ارتباط بین پزشکان و بیماران را به روشی ایمن، خصوصی و کارآمد تضمین می‌کند. این سیستم در مقایسه با سایر مدل‌های کنترل دسترسی اخیر، عملکرد بهتری دارد. با این حال سیستم، انجام عملیات کپی و انتقال روی منبع دایرکتوری را تسهیل نمی‌کند.

Tarek Farikha و همکاران [۶] در سال ۲۰۲۱ بر روی ذخیره سوابق سلامت الکترونیکی تمرکز کردند که در آن داده‌های جمع‌آوری‌شده توسط دستگاه‌های مستقر شده حیاتی هستند. هدف آنها ارائه دسترسی توزیع‌شده، ایمن و مجاز به این داده‌های حساس با استفاده از فناوری زنجیره بلوکی در حال ظهور بود. در این مطالعه، یک معماری تعبیه‌شده در زنجیره بلوکی و اینترنت اشیاء برای یک برنامه مراقبت‌های بهداشتی برای ذخیره و بررسی پرونده الکترونیک بیمار طراحی شد. مشکل این روش این است که ابتدا بدون اعتبارسنجی و رمزنگاری داده‌ها در زنجیره بلوکی ذخیره می‌شوند که این موجب بروز تهدیدات امنیتی می‌شود.

۳ پیش زمینه

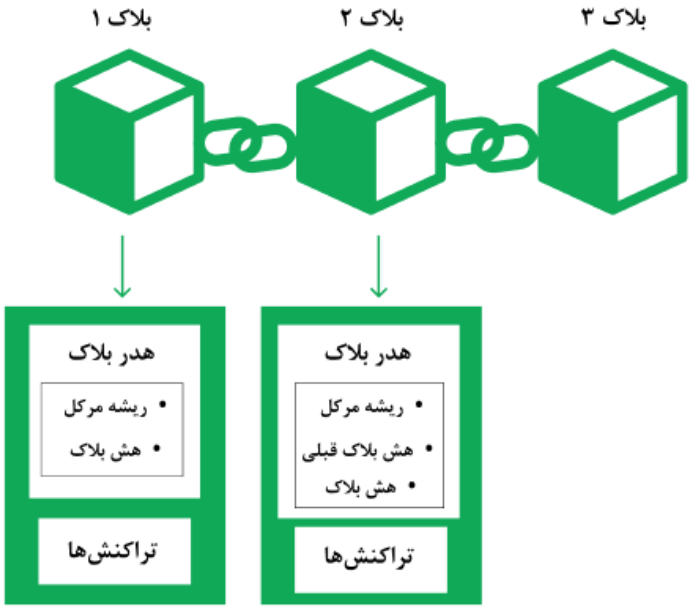
۱.۳ زنجیره بلوکی

این فناوری در سال ۲۰۰۸ معرفی و در سال ۲۰۰۹ توسط ناکاموتو برای حل مشکل هزینه دو برابر پول دیجیتال یا ارز رمزنگاری شده خود، یعنی بیت کوین پیشنهاد داد [۷]، اما این فناوری جدید برای کاربردهای مختلف دیگر نیز مورد استقبال قرار گرفت. زنجیره بلوکی شبکه‌ای نظیر به نظیر از بلوک‌های به هم پیوسته است که با اضافه شدن تراکنش‌های جدید به شبکه، دائماً در حال گسترش است. این فناوری با استفاده از روش غیرمتمرکز، امکان توزیع دانش و مالکیت مشترک هر قطعه از داده‌های توزیع‌شده را فراهم می‌کند. از مزایای زنجیره بلوکی می‌توان به امنیت، حفظ حریم خصوصی، یکپارچگی داده‌ها، تمرکززدایی، پایداری، ناشناس بودن، تغییرناپذیری و بدون نیاز به شخص ثالث اشاره کرد. این مزایا آن را به گزینه‌ای مناسب برای ذخیره اطلاعات پزشکی بیمار تبدیل کرده است [۸]. در نتیجه، زنجیره بلوکی این امکان را دارد که هزینه‌های قابل توجهی را کاهش و در عین حال کارایی را افزایش دهد [۷].

۱.۱.۳ ساختار بلوک

بلوک یک ساختار داده است که شامل یک هدر و مجموعه‌ای از معاملات است. هدر آن شامل یک مهر زمان (لحظه تولید بلوک)، هش بلوک قبلی ، هش بلوک فعلی و ریشه مرکل است. با استفاده از هش بلوک قبلی و ریشه مرکل تراکنش‌ها، هش بلوک جدید محاسبه و یک زنجیره بلوک ایجاد می‌شود. این ساختار در شکل ۱

دیده می‌شود. معاملات ذخیره شده در این بلوک تغییر ناپذیر هستند. با دستکاری شدن یک تراکنش، هش ریشه مرکل که نمایانگر هش تمام معاملات نامزد است، نیز تغییر می‌کند. در نتیجه، کل شبکه به امنیت و یکپارچگی معاملات مربوطه کمک می‌کند [۹].



شکل ۱: ساختار بلوک زنجیره بلوکی

۲.۱.۳ پایگاه داده MongoDB

اصطلاح NoSQL اولین بار در سال ۱۹۹۸ توسط آقای کارلو استروزی برای نامگذاری پایگاه داده رابطه‌ای منبع باز سبک وزن استفاده شد. برخی از پایگاه داده‌های موجود از استانداردهای NoSQL پیروی می‌کنند. اصطلاح «نه فقط SQL» نیز برای این پایگاه داده‌ها استفاده می‌شود. آنها مکانیزم ذخیره‌سازی و بازیابی را با مدل‌های سازگاری محدودتری نسبت به پایگاه داده‌های رابطه‌ای سنتی ارائه می‌کنند. به دلیل طراحی ساده، مقیاس‌پذیری افقی و در دسترس بودن، پایگاه داده‌های NoSQL در سراسر جهان محبوبیت پیدا کرده‌اند. اخیراً آنها به طور گسترده در داده‌های بزرگ و برنامه‌های وب بلادرنگ مانند فیس بوک، یاهو، گوگل و آمازون استفاده می‌شوند [۱۰]. یکی از این پایگاه داده‌های محبوب MongoDB است.

MongoDB یک پایگاه داده اسناد منبع‌باز است که عملکرد بالا، در دسترس بودن بالا و مقیاس‌بندی خودکار را ارائه می‌دهد. رکورد در MongoDB یک سند است که یک ساختار داده‌ای است که از جفت فیلد و مقدار تشکیل شده است. اسناد MongoDB مشابه اشیاء JSON هستند. مقادیر فیلدها ممکن است شامل سایر اسناد، آرایه‌ها باشد [۱۱].

جدول ۱: مقایسه زنجیره بلوکی و پایگاه داده MongoDB

	MongoDB	زنجیره بلوکی
یکپارچگی داده	اگر اقدامات لازم انجام نشود، یک عامل مخرب به طور بالقوه می‌تواند داده‌ها را تغییر دهد.	در ساختار زنجیره بلوکی عملاً غیرممکن است که کسی بتواند بدون شکستن زنجیره، داده‌ها تغییر دهد.
معاملات	داده‌ها را می‌توان ایجاد کرد، خواند، به روز یا حذف کرد (عملیات CRUD)	داده‌ها را فقط می‌توان خواند یا به زنجیره بلوکی اضافه کرد.
عملکرد پرس و جو	پایگاه‌های داده دسترسی سریع به داده‌ها را فراهم می‌کنند.	روش‌های تأیید برای اطمینان از یکپارچگی داده‌ها می‌توانند پرس و جو و عملکرد کلی یک زنجیره بلوکی را کاهش دهند.
ساختار	پایگاه‌های داده به صورت مرکزی مدیریت می‌شوند و یک مدیر مالک و کنترل کننده داده‌ها است.	زنجیره بلوکی‌ها می‌توانند کاملا غیرمتمرکز باشند و به هیچ مرجع مرکزی تکیه نکنند.

۳.۱.۳ مقایسه زنجیره بلوکی و MongoDB

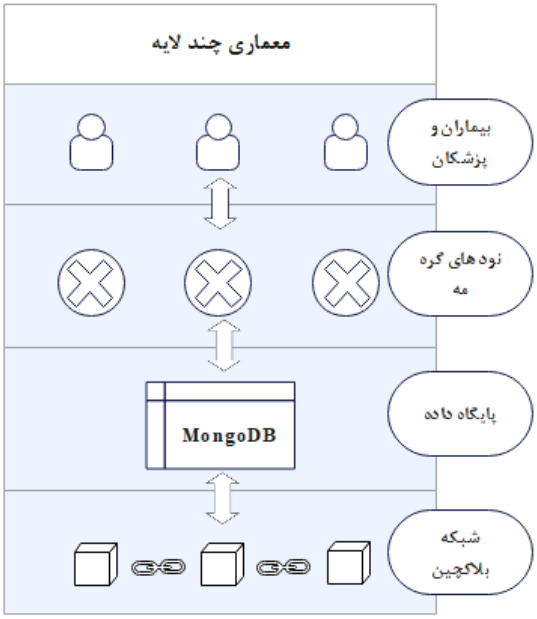
در جدول ۱، مقایسه‌ای بین MongoDB و زنجیره بلوکی انجام می‌دهیم. هدف نهایی یک زنجیره بلوکی، ذخیره اطلاعات است که آن را به یک پایگاه داده تبدیل می‌کند. زنجیره بلوکی‌ها تنها از طریق نحوه ذخیره داده‌ها با سایر انواع پایگاه داده‌ها متفاوت هستند. در حالی که زنجیره بلوکی‌ها را می‌توان یک پایگاه داده در نظر گرفت، یک پایگاه داده معمولاً یک زنجیره بلوکی نیست. پایگاه‌های داده معمولاً از بلوک‌های امضا شده برای ذخیره داده‌ها استفاده نمی‌کنند [۱۲]. زنجیره بلوکی مقیاس‌پذیری کمی دارد و هزینه ذخیره‌سازی در آن زیاد است. از طرفی پایگاه داده MongoDB نیز نمی‌تواند به اندازه زنجیره بلوکی امنیت داده‌ها را تضمین کند لذا پایگاه داده MongoDB و زنجیره بلوکی هر کدام به تنهایی قادر به ارائه یک راه حل کاملاً غیرمتمرکز نیستند و هر کدام مزایا و معایب خود را دارند. برای همین با ادغام زنجیره بلوکی و MongoDB می‌توان از مزایای آن‌ها بهره برد و محدودیت‌های آنها را برطرف کرد. خلاصه‌ای از مقایسه این دو در جدول ۱ بررسی شده است.

۲.۳ معماری روش پیشنهادی

روش پیشنهادی شامل یک معماری سه لایه جهت ادغام زنجیره بلوکی و MongoDB برای مدیریت داده‌ها در حوزه اینترنت اشیاء پزشکی است. شکل ۲ مدل پیشنهادی را نشان می‌دهد که شامل سه لایه می‌باشد و در ادامه به معرفی هر یک از این لایه‌ها پرداخته می‌شود.

لایه مه: این لایه جهت جمع‌آوری اطلاعات پزشکان و بیماران است. گره‌های مه[۳] می‌توانند اطلاعات پزشکی را با استفاده از حسگرهای مختلف جمع‌آوری کنند و در پایگاه داده ذخیره نمایند. این اطلاعات می‌توانند از طریق دستگاه‌هایی مانند سیستم‌های نظارت بر اطلاعات پزشکی به شبکه مه ارسال شوند و جهت

[3] Fog



شکل ۲: معماری روش پیشنهادی

بهبود کیفیت مراقبت از بیماران به پزشکان و پرستاران در بیمارستان کمک کنند. در کل، گره‌های مه با استفاده از حسگرهای مختلف می‌توانند به شیوه‌ای موثر در جمع‌آوری و ثبت اطلاعات پزشکی و سلامتی فرد کمک کنند.

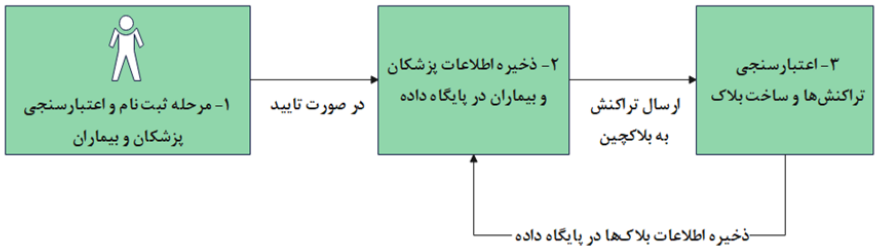
لایه پایگاه داده MongoDB: لایه پایگاه داده MongoDB در ایده پیشنهادی مسئولیت ذخیره و مدیریت داده‌های موجود در زنجیره بلوکی را برعهده دارد. این لایه جهت ذخیره‌سازی اطلاعاتی مانند اطلاعات ثبت نام، احرازهویت بیماران و پزشکان و اطلاعات بلاک‌های زنجیره بلوکی است. این لایه به صورت مستقل از زنجیره بلوکی عمل کرده و به زنجیره بلوکی ارتباطی ندارد، اما با توجه به نیازهای زنجیره بلوکی و ایده ادغام این دو فناوری، برخی امکانات، نظیر ذخیره‌سازی و هماهنگ سازی داده، مدیریت منابع، مدیریت تراکنش‌ها و حفاظت اطلاعات مورد نیاز و غیره برای ارتباط با زنجیره بلوکی را فراهم می‌کند.

لایه زنجیره بلوکی: این لایه امکان ثبت و تایید تراکنش‌ها بر روی یک سیستم غیرمترکز و معتبر را فراهم می‌کند و جهت ذخیره درهم اطلاعات و اختصاص جفت کلید عمومی و خصوصی استفاده می‌شود.

زنجیره بلوکی مورد استفاده در این پژوهش، زنجیره بلوکی بیت‌کوین است. بیت‌کوین یکی از معروف‌ترین نوع زنجیره بلوکی‌ها است و برای اینترنت اشیاء پزشکی نیز مزایای ویژه‌ای نظیر امنیت بالا، شفافیت، تقلب‌ناپذیری، مقرون به صرفه و غیره را دارد.

۴ مراحل روش پیشنهادی

در ابتدا بیماران، پزشکان و دستگاه‌های پزشکی هوشمند در گره‌های مه ثبت نام می‌کنند و سپس اطلاعات و مشخصات آنها در قالب تراکنش‌های جهت اعتبارسنجی به Mongoose ارسال می‌شوند. زمانی که هویت موجودیت‌ها تائید شد به عنوان یک معامله برای ایجاد بلاک به زنجیره بلوکی فرستاده می‌شوند و به هر موجودیت ثبت شده یک جفت کلید عمومی و خصوصی اختصاص داده می‌شود. کلید خصوصی به عنوان شناسه موجودیت‌ها عمل می‌کند و کلید عمومی موجودیت‌ها در گره‌های مه نگهداری می‌شود. در نتیجه هر موجودیتی جهت ایجاد تعامل در سیستم، نیاز به احراز هویت دارد در غیر این‌صورت اجازه ورود و تعامل ندارد که این مکانیزم تهدیدات گره‌های مخرب را برای تعامل با شبکه اینترنت اشیاء پزشکی کاهش می‌دهد. بعد از اعتبارسنجی تمامی اطلاعات بیماران و پزشکان و همچنین اطلاعات بلاک‌های زنجیره بلوکی در پایگاه داده MongoDB به دلیل مقیاس‌پذیری بالا ذخیره می‌شود و تنها کلید خصوصی و درهم اطلاعات در زنجیره بلوکی ذخیره می‌شوند. مراحل انجام روش پیشنهادی در شکل ۳ نشان داده شده است.



شکل ۳: مراحل انجام روش پیشنهادی

۱.۴ مرحله ثبت نام و اعتبارسنجی

ابتدا با استفاده از کلاس اسکیما[۴] Mongoose و تبدیل آن به مدل، یک سری بخش‌ها برای ثبت نام کاربر اعم از بخش ایمیل، بخش نام و بخش رمز در نظر می‌گیریم.

پس در ابتدا برای ثبت نام یک کاربر، نام و رمز و ایمیل کاربر باید برای Mongoose ارسال شود و با توجه به توضیحات بالا این مقادیر با اسکیما Mongoose جهت اعتبارسنجی بررسی می‌شود.

در مرحله قبل از ثبت نام کاربر جدید باید ابتدا بررسی کنیم که چنین کاربری با این آدرس ایمیل در پایگاه داده وجود دارد یا خیر. اگر وجود داشته باشد باید پیغامی حاوی متن «کاربری با این آدرس ایمیل در حال حاضر وجود دارد و ثبت نام جدید با این آدرس ایمیل امکان‌پذیر نمی‌باشد» نشان داده شود. اگر کاربر وجود نداشته باشد و اعتبارسنجی به درستی انجام شده باشد ثبت نام با موفقیت انجام می‌شود.

[4] Schema

بعد از ثبت نام و انجام فرایند اعتبارسنجی باید مشخصات کاربر در پایگاه داده ذخیره شود. اما بخش رمز به همین صورتی که از کاربر دریافت شده است در پایگاه داده ذخیره نمی‌شود بلکه قبل از ذخیره، با استفاده از روش درهم رمزنگاری می‌شود تا برای هیچ دو ورودی یکسان خروجی یکسانی نیز نداشته باشیم. در هنگام درهم کردن رمز یک Salt به درهم اضافه می‌شود تا امنیت درهم را بیشتر کند و باعث افزایش پیچیدگی شود.

در نهایت اگر اطلاعات ارسالی از کاربر برای ثبت نام مطابق با اسکیما Mongoose باشد، پیغامی حاوی متن «ثبت نام کاربر با موفقیت انجام شد» نمایش داده خواهد شد و این اطلاعات در پایگاه داده MongoDB نیز با موفقیت ذخیره می‌شود.

۲.۴ ورود کاربران

بعد از ورود موفقیت‌آمیز هر کاربر، یک Jason Web Tocken (JWT) به هر کدام از کاربران تعلق می‌گیرد. Jason Web Token در واقع یک شناسه منحصر به فرد است که به کاربر داده می‌شود تا پس از آن کاربر برای هربار ورود با استفاده از این شناسه احرازهویت گردد و اجازه ورود داشته باشد.

۳.۴ مرحله ارسال تراکنش به زنجیره بلوکی

برای اینکه زنجیره بلوکی تشکیل شود نیاز به حداقل ساخت یک بلاک داریم. اولین بلاکی که ساخته می‌شود و در زنجیره قرار می‌گیرد بلاک صفر است. این بلاک شامل بخش درهم قبلی به دلیل اینکه اولین بلاک زنجیره است نمی‌باشد. در اولین مرحله باید بررسی کنیم که بلاک صفر وجود دارد یا خیر. اگر وجود نداشته باشد باید اول این بلاک ساخته شود. بعد از اینکه این بلاک ساخته شد شبکه زنجیره بلوکی آماده دریافت تراکنش‌ها است.

بعد از ارسال تراکنش‌ها به شبکه زنجیره بلوکی، باید درهم تمامی این بلاک‌ها جهت یکپارچگی زنجیره و افزایش امنیت محاسبه، بررسی و تایید شوند. با توجه به اینکه حجم داده‌های ارسالی از اینترنت اشیاء پزشکی بالاست و مقیاس‌پذیری زنجیره بلوکی کم است ما از پایگاه داده MongoDB جهت ذخیره‌سازی اطلاعات شبکه زنجیره بلوکی استفاده می‌کنیم [۱۳]. در نهایت اطلاعات زنجیره بلوکی در MongoDB ذخیره می‌شود.

۵ نتیجه‌گیری

در این پژوهش با هدف افزایش سرعت، مقیاس‌پذیری و امنیت در شبکه‌های اینترنت اشیاء پزشکی روشی مبتنی بر ادغام زنجیره بلوکی و پایگاه داده MongoDB ارائه شد. در این پژوهش چون هزینه ذخیره‌سازی و اعتبارسنجی در زنجیره بلوکی زیاد است و همچنین مقیاس‌پذیری زنجیره بلوکی کم است از پایگاه داده MongoDB جهت حل این مشکل استفاده شد. پایگاه داده MongoDB چون یک پایگاه داده توزیع‌شده است دارای مقیاس‌پذیری و انعطاف بالایی است.

هدف این ایده، بهبود سرعت، امنیت و مقیاس‌پذیری سیستم زنجیره بلوکی با به کارگیری قدرت و کارآیی

پایگاه داده MongoDB است. با اجرای این پژوهش در این حوزه، امکان ارائه یک راهکار نوآورانه برای افزایش سرعت، امنیت و مقیاس‌پذیری سیستم‌ها وجود دارد. این ایده می‌تواند بهبود قابل توجهی در عملکرد و کارایی سیستم‌ها را به ارمغان بیاورد و در نهایت منجر به ساختاری بهتر و هماهنگ‌تر در استفاده از زنجیره بلوکی و MongoDB برای حوزه‌های مختلف شود.

مراجع

[1] Ali F, El-Sappagh S, Islam SR, Ali A, Attique M, Imran M, Kwak KS. An intelligent healthcare monitoring framework using wearable sensors and social networking data. Future Generation Computer Systems. 2021 Jan 1;114:23-43.

[2] J. Sengupta, S. Ruj, and S. Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," Journal of Network and Computer Applications, vol. 149, p. 102481, Jan. 2020, doi: 10.1016/j.jnca.2019.102481.

[3] A. Saha, R. Amin, S. Kunal, S. Vollala, and S. K. Dwivedi, "Review on 'Blockchain technology based medical healthcare system with privacy issues,'" Security and Privacy, vol. 2, no. 5, Sep. 2019, doi: 10.1002/spy2.83.

[4] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments," Information, vol. 8, no. 2, p. 44, Jun. 2017, doi: 10.3390/info8020044.

[5] M. A. Habib et al., "Privacy-based medical data protection against internal security threats in heterogeneous Internet of Medical Things," International Journal of Distributed Sensor Networks, vol. 15, no. 9, p. 155014771987565, Sep. 2019, doi: 10.1177/1550147719875653.

[6] T. Frikha, A. Chaari, F. Chaabane, O. Cheikhrouhou, and A. Zaguia, "Healthcare and Fitness Data Management Using the IoT-Based Blockchain Platform," Journal of Healthcare Engineering, vol. 2021, pp. 1–12, Jul. 2021, doi: 10.1155/2021/9978863.

[7] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," IJWGS, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/IJWGS.2018.095647.

[8] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," IEEE Access, vol. 7, pp. 147782–147795, 2019.

[9] P. Pandey and R. Litoriya, "Securing E-health Networks from Counterfeit Medicine Penetration Using Blockchain," Wireless Pers Commun, vol. 117, no. 1, pp. 7–25, Mar. 2021, doi: 10.1007/s11277-020-07041-7.

[10] P. Pandey and R. Litoriya, "Securing E-health Networks from Counterfeit Medicine Penetration Using Blockchain," Wireless Pers Commun, vol. 117, no. 1, pp. 7–25, Mar. 2021, doi: 10.1007/s11277-020-07041-7.

[11] A. Chauhan, "A Review on Various Aspects of MongoDb Databases," International Journal of Engineering Research & Technology, vol. 8, no. 5, May 2019, doi: 10.17577/IJERTV8IS050031.

[12] https://www.mongodb.com/databases/blockchain-database

[13] S. Pal, "Implementation of simple Blockchain using NodeJS & MongoDB," Jun. 2020. https://www.linkedin.com/pulse/implementation-simple-blockchain-using-nodejs-mongodb-sougata-pal/