DOI: 10.48305/jims.v42.i783.0813

مجله دانشکده پزشکی اصفهان — سال چهل و دوم/شماره‌ی ۷۸۳/هفته‌ی سوم آبان ۱۴۰۳

تاریخ دریافت: ۱۴۰۲/۱۲/۱۹ — تاریخ پذیرش: ۱۴۰۳/۰۸/۰۳ — تاریخ چاپ: ۱۴۰۳/۰۸/۲۲

بررسی طرح‌های احراز هویت در سامانه‌های اطلاعات پزشکی مراقبت از راه دور

سید محمد دخیل علیان[۱]، معصومه صفخانی[۲]، فاطمه پیرمرادیان[۳]، بهزاد نظری[۴]

مقاله مروری

چکیده

مقدمه: پیشرفت‌های فناوری مبتنی بر اینترنت اشیاء، زندگی انسان‌ها را متحول کرده است و نظارت از راه دور بر سلامت بیماران نیز از این امر مستثنی نیست. توسعه‌ی شبکه‌ی بی‌سیم بدن، نقش کلیدی در پایش سلامت ایفا می‌کنند. شبکه‌ی بی‌سیم بدن شامل حسگرهای پزشکی است که قابلیت تعبیه بر روی بدن بیمار را دارند و علائم حیاتی بیماران را اندازه‌گیری نموده و آن‌ها را از طریق کانال بی‌سیم به سرورهای پزشکی ارسال می‌کنند. بنابراین، اطلاعات حساس ارسالی بیماران که بر روی کانال ارسال شده است، می‌تواند در برابر حملات مختلف آسیب‌پذیر باشد. بنابراین امنیت در پزشکی از راه دور همواره یک چالش بوده است. از این‌رو، طراحی پروتکل‌های امنیتی احراز هویت سبک‌وزن با کمترین هزینه به یک چالش تبدیل شده است.

نتیجه‌گیری: در این مقاله، به معرفی سامانه‌های اطلاعات پزشکی مراقبت از راه دور، شبکه‌ی بی‌سیم بدن، پروتکل‌های احراز هویت، معیارهای عملکرد و خصوصیات امنیتی این طرح‌ها پرداخته شده‌است. همچنین، طرح‌های احراز هویتی که اخیراً ارائه شده، معرفی گردیده است.

مشاهده شده است که میزان عملکرد هر یک از طرح‌های احراز هویت وابسته به مقاومت هر طرح در برابر حملات موجود، ویژگی‌های امنیتی، هزینه‌های محاسباتی و غیره است. در این مقاله به معرفی حملات مطرح در سامانه‌های اطلاعات پزشکی مراقبت از راه دور و خصوصیات امنیتی طرح‌های احراز هویت پرداخته شده است. یکی از موضوعات مهم دیگر که مورد مطالعه و تمرکز پژوهشگران در حوزه امنیت بوده است، کاهش سربار محاسباتی با استفاده از سامانه‌های رمزنگاری سبک‌وزن است که این کاهش سربار محاسباتی منجر به کاهش امنیت در پروتکل‌های حاضر نشود.

واژگان کلیدی: اینترنت اشیاء، سامانه، حریم خصوصی

ارجاع: دخیل علیان سید محمد، صفخانی معصومه، پیرمرادیان فاطمه، نظری بهزاد. **بررسی طرح‌های احراز هویت در سامانه‌های اطلاعات پزشکی مراقبت از راه دور.** مجله دانشکده پزشکی اصفهان ۱۴۰۳؛ ۴۲ (۷۸۳): ۸۱۳-۸۲۴.

مقدمه

تکامل سریع فناوری‌های شبکه و انقلاب دیجیتال، اکثر کشورهای جهان را تحت تأثیر قرار داده است. شبکه‌ی اینترنت اشیاء، یک مدل فناوری جدید است که به‌عنوان یک شبکه‌ی جهانی از دستگاه‌هایی که قادر به تعامل با یکدیگر هستند، در زمینه‌های مختلف به‌کارگرفته می‌شود. یکی از این زمینه‌ها، ارائه‌ی خدمات بهداشتی از راه دور و بر بستر اینترنت است که هزینه‌های بستری بیماران در بیمارستان‌ها و رفت‌وآمد را کاهش می‌دهد. مراقبت‌های بهداشتی در کشورهایی با جمعیت مسن‌تر توجه بیشتری را به خود جلب کرده است. از این‌رو، یکی از فناوری‌های اساسی در اینترنت اشیاء، سامانه‌های اطلاعات پزشکی مراقبت از راه دور است. این سامانه به بیماران اجازه می‌دهد که به صورت مجازی و از طریق اینترنت یا شبکه‌های تلفن همراه با پزشکان ارتباط برقرار کنند و به پزشکان اجازه ملاقات با بیماران و تبادل اطلاعات مهم با سایر پزشکان را می‌دهد. درواقع با پیشرفت روزافزون فناوری، پزشکان می‌توانند خدمات بهداشتی را از راه دور و بر بستر اینترنت به افراد ارائه دهند. ارائه‌ی این خدمات پزشکی و بهداشتی با استفاده از فناوری‌های ارتباطی، محدود به مکان و زمان نیست و از این‌رو بیمار می‌تواند بدون مراجعه به مراکز درمانی از این

۱- دانشیار، مهندسی برق و کامپیوتر، دانشکده‌ی مهندسی برق و کامپیوتر، دانشگاه صنعتی اصفهان، اصفهان، ایران

۲ –دانشیار، مهندسی کامپیوتر، دانشکده‌ی مهندسی کامپیوتر، دانشگاه تربیت دبیر شهید رجائی تهران، تهران، ایران

۳ –دکترا، مهندسی برق و کامپیوتر، دانشکده‌ی مهندسی برق و کامپیوتر، دانشگاه صنعتی اصفهان، اصفهان، ایران

۴- استادیار، مهندسی برق و کامپیوتر، دانشکده‌ی مهندسی برق و کامپیوتر، دانشگاه صنعتی اصفهان، اصفهان، ایران

نویسنده‌ی مسؤول: سید محمد دخیل علیان: دانشیار، مهندسی برق و کامپیوتر، دانشکده‌ی مهندسی برق و کامپیوتر، دانشگاه صنعتی اصفهان، اصفهان، ایران

Email: mdalian@iut.ac.ir

خدمات پزشکی و درمان بهره‌مند شود (۱-۳).

سامانه‌ی اطلاعات پزشکی مراقبت از راه دور، بستری را برای تعامل بین پزشکان، بیماران، تجهیزات و مکان‌های پزشکی فراهم می‌آورد که اینترنت اشیاء در راستای تحقق این هدف نقش چشمگیری داشته است. تاکنون کاربردهای متعددی از سامانه‌های اطلاعات پزشکی مراقبت از راه دور از جمله مراقبت‌های بهداشتی الکترونیکی، مانیتورینگ بیمار در خانه و غیره معرفی شده است. به‌عنوان مثال، یک سامانه‌ی سلامت الکترونیک ارزشمند می‌تواند در تصمیم‌گیری‌های آگاهانه پزشکی کمک کند. در سامانه‌های اطلاعات پزشکی مراقبت از راه دور، حسگرها وضعیت و اطلاعات زیستی و فیزیولوژیکی بیماران را اندازه گرفته و این اطلاعات را با استفاده از دستگاه‌های تلفن همراه، شبکه‌های بی‌سیم، بستر اینترنت و یا هر بستر و کانالی که قابلیت ارسال و دریافت داشته باشد به سرور ارسال می‌نمایند.

به‌طورکلی ساختار سامانه‌های اطلاعات پزشکی مراقبت از راه دور شامل چهار بخش اصلی پزشک، بیمار، بستر عمومی اینترنت و پایگاه داده سرور است. بیماران می‌توانند به سامانه وارد شوند تا سوابق پزشکی خود را بررسی نمایند و نتایج آزمایش‌ها و تاریخ داروهای تجویزی را دریافت کنند. پزشکان همچنین می‌توانند تاریخچه‌ی داروهای تجویزی و نتایج آزمایش‌ها را بررسی کنند.

در شکل ۱ معماری این سامانه جهت ارائه‌ی خدمات پزشکی از راه دور مبتنی بر شبکه‌ی بی‌سیم بدن نشان داده شده است. همه‌ی این خدمات مستلزم فراهم شدن بستر و پروتکلی است که کاربران موجود در این سامانه احراز هویت متقابل شوند تا خدمات ارائه شده مورد سوء استفاده قرار نگیرد و گمنامی و حریم خصوصی آن‌ها مصون از تهدیدات اینترنتی و امنیتی باشد. سامانه‌های اطلاعات پزشکی مراقبت از راه دور، بستری مناسب را جهت خدمات پزشکی مبتنی بر شبکه‌ی بی‌سیم بدن فراهم می‌کنند. به طورکلی، فرایند استفاده از خدمات این سامانه مستلزم ثبت‌نام اولیه بیمار در سرور است. سپس برای هر بار استفاده از خدمات ارائه شده‌ی از راه دور بایستی بیمار برای سرور احراز هویت شود. در هر بار نشست در مرحله‌ی احراز هویت با سرور، بین طرفین یک کلید توافق می‌گردد که به واسطه‌ی کلید توافق شده بیمار قادر است اطلاعات را ارسال و دریافت نماید. لازم به ذکر است، مرحله‌ی احراز هویت مستلزم تأیید اعتبار متقابل است تا خدمات ارائه شده مورد سوء استفاده قرار نگیرند.

به طور کلی، معماری شبکه‌ی بی‌سیم بدن مبتنی بر دو لایه است. لایه‌ی اول آن مبتنی بر شبکه‌ای با برد کوتاه همراه با حسگرهای پزشکی مناسب بر روی بدن بیمار است. این حسگرها جهت جمع‌آوری اطلاعات زیستی بیماران به دستگاه‌هایی مانند تلفن همراه متصل می‌شوند. سپس در لایه‌ی دوم، این دستگاه‌ها با استفاده از بستر اینترنت، اطلاعات جمع‌آوری شده را به پایگاه داده سرور ارسال می‌کنند. همانطور که ارتباط بین تلفن همراه و کارت هوشمند در بستر اینترنت عمومی اتفاق می‌افتد و اطلاعاتی که در شبکه بی‌سیم بدن ارسال می‌شوند، اطلاعات بسیار حساسی هستند و پتانسیل بالایی را جهت اعمال حمله دارند، بنابراین، کل سامانه‌ی آسیب‌پذیر به تهدیدات اینترنت باز می‌باشد. پس محرمانه بودن، یکپارچگی این اطلاعات، حفظ حریم خصوصی، انکارناپذیری و به ویژه ناشناس بودن در پیاده‌سازی یک سامانه‌ی اطلاعات پزشکی مراقبت از راه دور بسیار حائز اهمیت است. در سال‌های اخیر، محققان بر روی شبکه‌های بی‌سیم بدن تمرکز کرده‌اند. زیرا بیمار خدمات مراقبت بهداشتی بهتری را از طریق نظارت و تشخیص از راه دور دریافت می‌کند. امنیت و حریم خصوصی به‌عنوان ملزومات حیاتی برای شبکه‌ی بی‌سیم بدن محسوب می‌شود، زیرا اطلاعات مهمی را در اختیار بیماران قرار می‌دهد. لازم به ذکر است که پزشکی هوشمند در کنار مزایای چشمگیرش، خطرات امنیتی و مشکلات حریم خصوصی بسیاری را به دنبال دارد.

شکل ۱: معماری سامانه‌های اطلاعات پزشکی مراقبت از راه دور (۳).

بستری که برای خدمات پزشکی از راه دور تعبیه می‌شود مبتنی بر فناوری شناسایی فرکانس رادیویی است. این فناوری شامل سه مؤلفه‌ی اصلی است: برچسب، برچسب‌خوان و سرور پایگاه داده. در این فناوری، برچسب به اشیاء و افرادی که قرار است اطلاعات را به پایگاه داده ارسال کنند متصل می‌شود. این اطلاعات می‌تولند سیگنال‌های مربوط به دستگاه و یا داده‌های فیزیولوژیکی بدن بیمار باشد. خدماتی مانند اطلاع از وضعیت بیمار، دریافت اطلاعات دارویی، بیماری‌های واگیردار، نوزادان تحت درمان، آزمایشات و غیره می‌تواند بخشی از خدمات ارائه شده در سامانه‌های اطلاعات پزشکی مراقبت از راه دور باشد.

پیشرفت‌های زیاد در زمینه‌ی خدمات پزشکی، سامانه‌های پایش سلامت پوشیدنی را ایجاد کرده است که در این سامانه‌ها تعداد زیادی حسگر برای جمع‌آوری داده استفاده می‌شوند. یک سامانه پایش سلامت پوشیدنی شامل سه شرکت‌کننده است: مدیر شبکه، سرور کاربرد و کاربر شبکه‌ی بی‌سیم بدن. شبکه‌ی بی‌سیم بدن، نقش اصلی در صنعت پزشکی برای اطلاع از وضعیت سلامت بیماران بازی می‌کند. شبکه‌ی بی‌سیم بدن شامل حسگرهای پزشکی مختلف است. از آن‌جایی که این حسگرها برای اندازه‌گیری اطلاعات حساس بیماران در کانال‌های ناامن استفاده می‌شوند، کل سامانه در برابر تهدیدات آسیب‌پذیر است و در نتیجه حفظ حریم خصوصی افراد، حفظ گمنامی کاربران و دیگر خواص امنیتی تبدیل به یک چالش بزرگ در پیاده‌سازی یک سامانه امن مناسب شده است و بنابراین باید گمنامی و حریم خصوصی کاربران مصون از تهدیدات امنیتی باشد. بنابراین در سال‌های اخیر طرح‌های مختلفی جهت تضمین امنیت داده توسعه یافته است (٤، ٥).

بنابراین، مفهوم احراز هویت امن برای سامانه‌های اطلاعات پزشکی، مراقبت از راه دور ضروری است. تشخیص آسیب‌پذیری‌های امنیتی در سامانه‌ها و جایگزینی آن‌ها با ویژگی‌های قوی امنیتی امری ضروری است. بااین‌حال، تشخیص دقیق در علم پزشکی می‌تواند برای پزشکان یک کار دلهره‌آور باشد. از آنجایی‌که پزشکان به پرونده‌ی الکترونیک سلامت بیمار مانند آزمایشات، اطلاعات صورتحساب، تاریخچه‌ی پزشکی، داروها و جزئیات بیمه دسترسی ندارند.

در این مقاله، در بخش اول معرفی سامانه‌های اطلاعات پزشکی مراقبت از راه دور و در بخش دوم تاریخچه‌ی کارهای انجام شده مورد بررسی قرار گرفته است. همچنین، به اهمیت موضوع و هدف از نگارش این مقاله در بخش سوم، به معرفی طرح‌های احراز هویت در سامانه‌های اطلاعات پزشکی مراقبت از راه دور در بخش چهارم و طرح‌های احراز هویت، معیارهای عملکرد و خصوصیات امنیتی این طرح‌ها در فصل پنجم پرداخته و در انتها در بخش پنجم نتیجه‌گیری بیان شده است.

تاریخچه‌ی کارهای انجام شده

در سال‌های اخیر پروتکل‌های احراز هویت و توافق کلید بسیاری ارائه شده است که در میان آن‌ها تنها آن دسته از پروتکل‌ها که کارآیی بالایی دارند ماندگار می‌شوند. در این بخش، هدف بررسی پروتکل‌های ارائه شده‌ی اخیر در سامانه‌های اطلاعات پزشکی مراقبت از راه دور و بررسی امنیت آن‌ها است. درواقع، پروتکل‌ها راهی جهت برقراری تعامل و ارتباط میان کاربران و سرور هستند که شامل مراحل مختلفی است. یک پروتکل امن باید بتواند در یک کانال ناامن امنیت را تضمین کند. مهم‌ترین معیاری که در طراحی و کاربردی بودن یک طرح احراز هویت مهم است، امنیت و حفظ حریم‌خصوصی افراد شرکت‌کننده در پروتکل است. در ادامه به معرفی برخی از طرح‌های احراز هویت در این حوزه و تحلیل امنیتی آن‌ها پرداخته شده است.

ابزارهای رمزنگاری مختلف مانند توابع چکیده‌ساز، رمزنگاری خم بیضوی، امضای دیجیتال، توابع آشوبی، زوج‌نگار دوخطی و برخی عملیات سبک‌وزن دیگر مانند XOR همگی برای طراحی یک طرح احراز هویت امن استفاده می‌شوند.

با این‌حال، رمزنگاری خم بیضوی به‌عنوان یک الگوریتم کلید عمومی مدرن، مزایایی نسبت به سایر الگوریتم‌های رمز کلید عمومی مانند RSA دارد. اکثر پروتکل‌های احراز هویت ارائه شده‌ی اخیر مبتنی بر رمزنگاری خم بیضوی هستند. به دلیل اینکه سطح امنیت مشابهی را در مقایسه با الگوریتم‌های رمزنگاری RSA با اندازه‌ی کلید کوچک‌تر فراهم می‌کنند، به‌طوری‌که خم بیضوی امنیت را با کلید ١٦٠ بیتی فراهم می‌کند، درحالی‌که همین میزان سطح امنیت در RSA با کلید ٤٠٩٦ بیتی فراهم می‌شود. همچنین زمان محاسبه عملیات نمایی RSA بسیار بیشتر از عملیات خم بیضوی است. پس میزان پیچیدگی محاسباتی کاهش می‌یابد. در جدول ١ طبقه‌بندی طرح‌های احراز هویت ارائه‌شده‌ی اخیر، پروتکل بهبودیافته‌ی آن‌ها و ویژگی‌های امنیتی نقض‌شده‌ی هر طرح مشخص گردیده است. این جدول نشان می‌دهد که در حوزه‌ی طراحی و تحلیل پروتکل‌های احراز هویت نمی‌توان پروتکل‌های طراحی‌شده را بدون تحلیل قبول و استفاده نمود. فقط صرف طراحی و ارائه‌ی پروتکل و عدم تحلیل آن اطمینان انسان‌ها جلب نمی‌شود. بنابراین، می‌بایست پروتکل‌های طراحی شده را گروه‌های تحقیقاتی مستقل و سومی مورد بررسی قرار دهند که این بررسی امنیت توسط افراد دیگر موجب جلب اعتماد می‌گردد. در جدول ١ پروتکل‌های ارائه‌شده‌ی اخیر برای به‌کارگیری در سامانه‌های اطلاعات پزشکی مراقبت از راه دور بیان شده است.

جدول ۱: پروتکل‌های ارائه شده‌ی اخیر برای به‌کارگیری در سامانه‌های اطلاعات پزشکی مراقبت از راه دور.

نام طرح	سال	نوع حمله	روش احراز هویت	طرح بهبودیافته	نام طرح	سال	نوع حمله	روش احراز هویت	طرح بهبودیافته
Liu و همکاران (۱۲)	۲۰۱۶	حمله‌ی جعل هویت	رمزنگاری خم بیضوی	Li و همکاران (۱۳)	Ostad-Sharif و همکاران (۲۵)	۲۰۱۹	حمله‌ی حدس گذرواژه، حمله‌ی داخلی الویت‌دار و حمله تکرار	رمزنگاری خم بیضوی	Nikooghadam و Amintoosi (۲۶)
Chiou و همکاران (۱۴)	۲۰۱۶	عدم وجود گمنامی کاربر و عدم وجود رازمانی پیش سوی کامل	رمزنگاری خم بیضوی	Deebak و Al-Turjman (۱۵)	Karthigaiveni و Indrani (۲۷)	۲۰۱۹	حمله‌ی تکرار و منع خدمت	رمزنگاری خم بیضوی	Alzahrani (۲۸)
Om و Chandrakar (۱۶)	۲۰۱۷	–	رمزنگاری خم بیضوی	–	Jia و همکاران (۲۹)	۲۰۱۹	حمله‌ی جعل هویت با کلید تسخیرشده	رمزنگاری خم بیضوی	Li و همکاران (۳۰)
Li و همکاران (۱۳)	۲۰۱۷	عدم وجود رازمانی پیش سوی کامل	رمزنگاری خم بیضوی	Sowjanya و همکاران (۹)	Sowjanya و همکاران (۹)	۲۰۱۹	حمله افشای مقادیر مخفی توسط مهاجم داخلی غیرفعال، حمله جعل هویت، حمله تکرار و عدم وجود ویژگی مقیاس‌پذیری	رمزنگاری خم بیضوی	ECCPWS و ECCPWS^{+} (۳۱)
Yessad و همکاران (۱۷)	۲۰۱۷	–	رمزنگاری خم بیضوی	–	Mehmood و همکاران (۳۲)	۲۰۱۹	حمله جعل هویت با کلید تسخیرشده	رمزنگاری/ رمزگشایی متقارن/ نامتقارن	ECKCI (۱۹)
Wu و همکاران (۱۸)	۲۰۱۷	–	رمزنگاری خم بیضوی	–	Alzahrani و همکاران (۳۳)	۲۰۲۰	حمله جعل هویت با کلید تسخیرشده	رمزنگاری/ رمزگشایی متقارن/ نامتقارن	Hajian و همکاران (۳۴)
Xiong و همکاران (۱۰)	۲۰۱۷	حمله جعل هویت با کلید تسخیرشده	رمزنگاری خم بیضوی	ECKCI (۱۹)	Xiong و همکاران (۱۰)	۲۰۲۱	عدم وجود رازمانی پیش سوی کامل و حمله جعل	رمزنگاری/ رمزگشایی متقارن/ نامتقارن	Hosseinzadeh و همکاران (۳۶)
Li و همکاران (۲۰)	۲۰۱۸	حمله جعل هویت، پیوندپذیری و عدم وجود گمنامی کاربر	رمزنگاری خم بیضوی	Mohit و همکاران (۲۱)	Guo و همکاران (۳۷)	۲۰۲۳	–	رمزنگاری/ رمزگشایی متقارن/ نامتقارن	–
Qi و همکاران (۲۲)	۲۰۱۸	–	رمزنگاری خم بیضوی	–	ECCPWS	۲۰۲۳	–	رمزنگاری خم بیضوی	–
Amin و همکاران (۲۳)	۲۰۱۸	حمله جعل هویت و تکرار	رمزنگاری خم بیضوی	Ravanbakhsh و Nazari (۲۴)	ECCPWS^{+}	۲۰۲۳	–	رمزنگاری خم بیضوی	–
Ravanbakhsh و Nazari (۲۴)	۲۰۱۸	عدم وجود رازمانی پیش سوی کامل	رمزنگاری/ رمزگشایی متقارن/ نامتقارن	Ostad-Sharif و همکاران (۲۵)	ECKCI (۱۹)	۱۹ ۲۰۲۴	۰	رمزنگاری خم بیضوی	–

اهمیت موضوع و هدف آن

با سوق یافتن مراکز پزشکی به سمت فناوری‌های پیشرفته‌تر، حفاظت از محرمانه بودن، حفظ امنیت، یکپارچگی، حفظ حریم خصوصی افراد و اشخاص جویای خدمات از راه دور در سامانه‌های اطلاعات پزشکی مراقبت از راه دور و احراز هویت متقابل بیماران و پزشکان چالش‌های بزرگی است و اهمیت جنبه‌های امنیتی و حفاظت از داده‌ها برای مراقبت‌های بهداشتی قابل اعتماد بیمار هرگز نباید نادیده گرفته شود. بنابراین، حملات مختلف از جمله حمله‌ی جعل هویت، حمله‌ی تکرار، حمله‌ی تغییر، استراق سمع و غیره را می‌توان با یک مهاجم مخرب انجام داد. برقراری ارتباط و تبادل اطلاعات در سامانه‌های اطلاعات پزشکی مراقبت از راه دور، منوط به تأیید هویت کاربران توسط سرورهای پزشکی است و احراز هویت بیمار و متخصصین مراقبت‌های بهداشتی تکنیکی برای شناسایی افراد درگیر است.

در راستای تحقق این هدف، طراحان طرح‌های توافق کلید و احراز هویت بسیاری را معرفی نموده‌اند. کارآیی این طرح‌ها به دربرداشتن ویژگی‌های خاصی از قبیل حفظ حریم خصوصی، ناشناس‌بودن کاربر، ردیابی‌ناپذیری، یکپارچگی و محرمانگی وابسته است. بنابراین ضرورت و اهمیت، ارائه و معرفی طرح‌های احراز هویت و توافق کلید مقاوم در برابر حملات شناخته شده است که نیازمند کار بیشتر در حوزه امنیت در پایگاه‌های داده بیمارستانی توسط محققان است. به طور کلی، حسگرهای پزشکی شرایط فیزیولوژیکی بیمار را اندازه‌گیری کرده و اطلاعات به دست آمده را به یک تلفن هوشمند ارسال می‌کنند. سپس این اطلاعات ارسال‌شده به سرورهای ارائه‌دهنده خدمات بهداشتی از طریق اینترنت عمومی منتقل می‌شوند. سرور مربوطه اطلاعات پزشکی محافظت شده یا PHI بیمار را نگهداری می‌کند. دسترسی به این اطلاعات پزشکی تحت سیاست‌های پیاده‌شده توسط سرور سیاست‌گذاری می‌شود و تنها پس از احراز هویت از طرف سرور دسترسی‌ها اعطاء می‌شود. در مراقبت پزشکی الکترونیکی، بیمار به PHI برای نظارت بر وضعیت سلامت خود، پزشک برای تجویز نسخه و داروساز جهت بررسی داروهای تجویزی دسترسی پیدا می‌کند. در شرایط اضطراری نیز می‌توان یک آمبولانس را برای ارائه‌ی کمک به بیمار قبل از رسیدن به بیمارستان فراخواند.

معرفی طرح‌های احراز هویت در سامانه‌های اطلاعات پزشکی مراقبت از راه دور

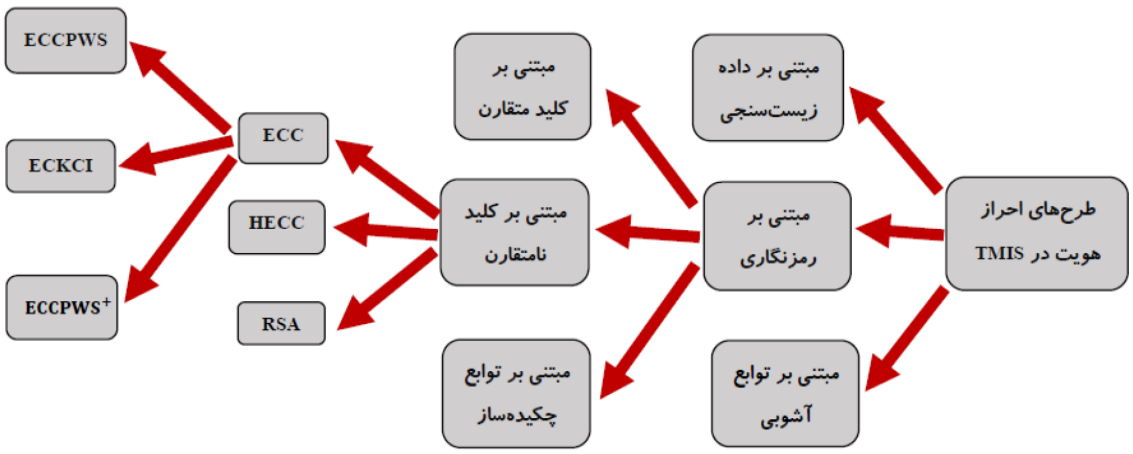
ارائه‌ی تمامی خدمات از راه دور مستلزم احراز هویت متقابل افراد شرکت‌کننده در سامانه‌های اطلاعات پزشکی مراقبت از راه دور است. تأیید اعتبار و توافق در تمامی طرح‌های احراز هویت در راستای شناسایی هویت کاربر و بیمار برای سرور پزشکی حائز اهمیت فراوانی است. حال این فرایند می‌تواند به هر نحوی طراحی و پیاده‌سازی شود. چارچوبی که به وسیله‌ی آن احراز هویت صورت می‌پذیرد پروتکل احراز هویت نام دارد. در شکل ۲ طبقه‌بندی طرح‌های احراز هویت در سامانه‌های اطلاعات پزشکی مراقبت از راه دور نشان داده شده است (۶، ۷).

طرح‌های احراز هویت مبتنی بر رمزنگاری

در این نوع از طرح‌ها، تمامی پیام‌های مبادله شده جهت شناسایی هویت کاربر و توافق کلید به صورت رمز شده در کانال ارسال می‌شوند که تنها کاربر مجاز و سرور قادر به رمزگشایی این پیام‌های ارسالی با کلید توافق شده هستند. طرح‌های احراز هویت مبتنی بر رمزنگاری می‌توانند مبتنی بر رمزنگاری کلید متقارن، رمزنگاری کلید عمومی یا نامتقارن و توابع چکیده‌ساز باشند (۸-۱۰).

طرح‌های احراز هویت مبتنی بر رمزنگاری کلید متقارن

رمزنگاری کلید متقارن، روشی سریع و کارآمد به‌شمار می‌آید. به



شکل ۲: طبقه‌بندی طرح‌های احراز هویت در سامانه‌های اطلاعات پزشکی مراقبت از راه دور (۸).

دلیل این‌که در آن از یک کلید مشترک برای رمزنگاری و رمزگشایی پیام‌ها استفاده می‌شود. درصورتی‌که تعداد پیام‌ها زیاد باشد، این روش در پردازش بسیار مناسب است. الگوریتم‌های AES و DES نمونه‌ای از الگوریتم‌های رمزنگاری مبتنی بر کلید متقارن می‌باشند.

طرح‌های احراز هویت مبتنی بر رمزنگاری کلید نامتقارن

در این نوع الگوریتم، از دو کلید جهت رمزنگاری و رمزگشایی پیام‌ها استفاده می‌شود، که یکی از کلیدها به‌عنوان کلید عمومی برای رمزنگاری پیام‌ها و کلید دیگر به عنوان کلید خصوصی برای رمزگشایی پیام‌ها استفاده می‌شود. در مقایسه با الگوریتم کلید متقارن، این الگوریتم موجب تفکیک شدن امنیت و هویت شده و در احراز هویت هستارها به یکدیگر مؤثر است. به عنوان نمونه رمزنگاری خم بیضوی یک الگوریتم رمزنگاری کلید عمومی است که نسبت به سایر الگوریتم‌های کلید عمومی با امنیت مشابه از یک کلید با طول کوچک‌تر استفاده می‌کند. بنابراین، این نوع رمزنگاری امروزه از جذابیت خاصی برخوردار است. الگوریتم‌های احراز هویت مبتنی بر کلید عمومی به چند دسته به صورت زیر تقسیم می‌شوند.

- الگوریتم رمزنگاری RSA و DSA
- الگوریتم رمزنگاری خم بیضوی یا ECC
- الگوریتم رمزنگاری فوق خم بیضوی یا HECC

رمزنگاری خم بیضوی، یک الگوریتم رمزنگاری کلید عمومی است که نسبت به رمزنگاری مبتنی بر RSA از یک کلید با اندازه‌ی کوچک‌تر استفاده می‌کند. پس رمزنگاری خم بیضوی نسبت به RSA امنیت مشابهی را با اندازه‌ی کلید کوچک‌تر فراهم می‌کند.

- طرح‌های احراز هویت مبتنی بر توابع چکیده‌ساز

توابع چکیده‌ساز توابعی یک‌طرفه هستند که به منظور فشرده‌سازی و تولید چکیده‌ای منحصربه‌فرد از پیام‌ها با طول دلخواه به‌کار می‌روند.

طرح‌های احراز هویت مبتنی بر داده‌ی زیست‌سنجی

یکی از عوامل افزایش امنیت، در نظر گرفتن عامل زیست‌سنجی در طرح‌های احراز هویت است. استفاده‌ی همزمان از خواص فیزیولوژیکی و زیستی کاربر مثل اثرانگشت، عنبیه چشم، DNA و خواص رفتاری کاربر مثل امضاء و صدا در طرح‌های احراز هویت مبتنی بر دو عامل از عوامل افزایش میزان امنیت است. ترکیب داده‌های زیست‌سنجی بیمار با سایر روش‌های احراز هویت موجب ارائه‌ی یک سامانه مبتنی بر چند عامل شده است. مبتنی بر این داده‌های زیست‌سنجی، کلیدهای مختلفی در رمزنگاری وجود دارد که این کلیدها به کلیدهای زیست‌سنجی معروف هستند. ویژگی منحصربه‌فرد این کلیدها به‌صورت زیر است (۱۱).

دشوار بودن جعل این کلیدها

دشوار بودن حدس این کلیدها

عدم نیاز به حفظ آن‌ها

به کار بردن داده‌ی زیست‌سنجی در فرایند احراز هویت عملیات‌هایی را به پروتکل اضافه می‌کند. ولی مزایای بیان شده در بالا نباید نادیده گرفته شود. فرایند طرح‌های احراز هویت مبتنی بر داده‌های زیست‌سنجی در شکل ۳ نشان داده شده است.

پروتکل‌های احراز هویت

به طورکلی طرح‌های احراز هویت از دیدگاه تعداد عامل‌های درگیر در فرایند احراز هویت به سه دسته کلی تقسیم شده‌اند (۱۲، ۲۹، ۳۰).

طرح‌های احراز هویت مبتنی بر یک عامل

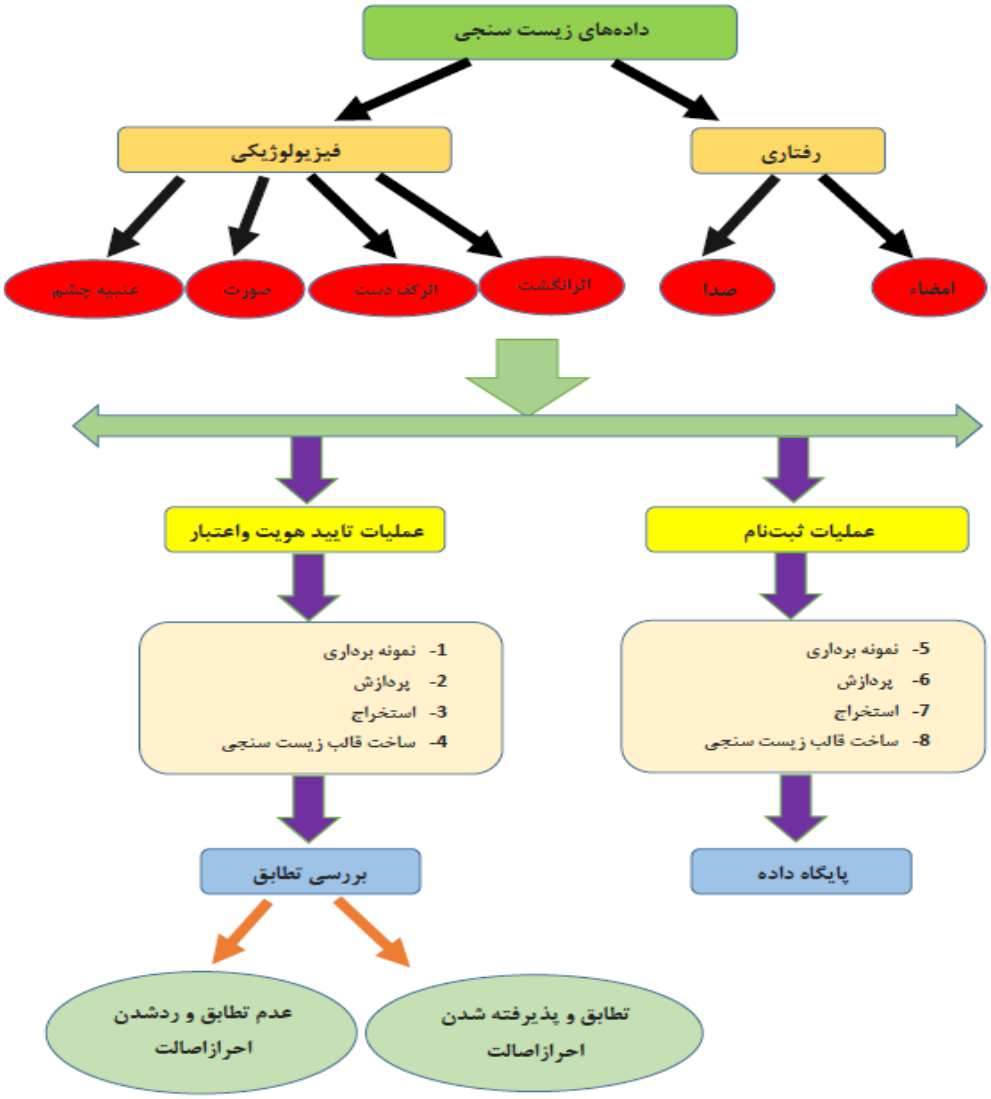
طرح‌های احراز هویت مبتنی بر دو عامل

طرح‌های احراز هویت مبتنی بر سه عامل

بر اساس سیر تکامل پیشرفت‌های اخیر فناوری، در ابتدا روش احراز هویت مبتنی بر یک عامل یعنی گذرواژه‌ی ساده مطرح شد که در نهایت به طرح‌های احراز هویت مبتنی بر دو عامل و سه عامل توسعه پیدا کرد. اولین روش احراز هویت از راه دور توسط لمپورت مطرح شد. این طرح بسیار ساده پیاده‌سازی شد و فقط شامل نام کاربری و گذرواژه‌ی ساده‌ی کاربر برای دسترسی به سامانه بود. مهم‌ترین مسئله‌ای که در پیاده‌سازی این سامانه مطرح است، ذخیره و حفظ گذرواژه کاربران در راستای حفظ حریم خصوصی و ناشناس بودن آن‌ها است. پروتکل‌های احراز هویت مبتنی بر یک عامل، تأیید هویت را آسان کرده‌اند، زیرا در اینگونه طرح‌ها کاربر بایستی تنها گذرواژه خود را برای اهداف تأیید هویت به خاطر داشته باشد. از این‌رو، طرح‌های امن‌تر و پیچیده‌تری مبتنی بر عامل‌های بیش‌تر جهت احراز هویت متقابل پیشنهاد گردید. در سال ۱۹۹۰ اولین طرح احراز هویت مبتنی بر دو عامل توسط هوانگ پیشنهاد شد و در نهایت طرح‌های احراز هویت مبتنی بر سه عامل در اوایل قرن ۲۱ مطرح شدند (۳۰، ۳۶).

در طرح‌های احراز هویت مبتنی بر دو عامل، کاربر علاوه بر شناسه و گذرواژه، به کارت هوشمند نیاز دارد که سطح راحتی کاربر کاهش می‌یابد. با گسترش تهدیدات امنیتی در بستر اینترنت عمومی، در طرح‌های احراز هویت مبتنی بر سه عامل، علاوه بر گذرواژه، شناسه و کارت هوشمند، به اطلاعات خاص‌تری از جمله اطلاعات زیست‌سنجی کاربر نیز نیاز است. دیده می‌شود هرچه طرح‌های احراز هویت مبتنی بر عامل‌های بیشتری گردند، سطح راحتی کاربر جهت ورود به سامانه کاهش می‌یابد. به طورکلی، تأیید هویت در طرح‌های احراز هویت شامل مراحل زیر است:

مرحله‌ی ثبت‌نام: در این مرحله کاربر با ارائه‌ی اطلاعات هویتی خود، از طریق کانال امن در سرورهای موجود در سامانه‌های اطلاعات



شکل ۳: فرایند طرح‌های احراز هویت مبتنی بر داده‌های زیست‌سنجی (۸).

پزشکی مراقبت از راه دور ثبت‌نام می‌کند. همچنین کاربر می‌تواند گذرواژه خود را در همین مرحله انتخاب کند و پس از اولین ورود به سامانه آن را تغییر دهد.

مرحله‌ی ورود و احراز هویت متقابل: طی این مرحله، کاربر با ارائه‌ی اطلاعات هویتی خود به سرور احراز هویت می‌شود. بعد از تأیید هویت کاربر در سامانه، هویت سرور نیز متقابلاً باید برای کاربر تأیید شود. از این‌رو پس از احراز هویت متقابل کاربر و سرور به یکدیگر، کاربر می‌تواند به خدماتی که توسط سامانه‌های اطلاعات پزشکی مراقبت از راه دور ارائه می‌شود، دسترسی یابد.

مرحله‌ی به‌هنگام‌رسانی گذرواژه: در این مرحله، کاربر می‌تواند گذرواژه خود را به طور مرتب به‌هنگام‌رسانی کند، تا از احتمال حملات مبتنی بر استفاده از گذرواژه مشابه و همچنین ردیابی‌پذیری بکاهد.

معیارهای عملکرد طرح‌های احراز هویت

میزان عملکرد و کارآیی هر طرح احراز هویت وابسته به مقاومت آن در برابر حملات موجود و شناخته شده، برخورداری از ویژگی‌های حریم‌خصوصی و امنیتی، هزینه‌ی ارتباطات، هزینه‌ی محاسبات، هزینه‌ی ذخیره‌سازی داده و زمان تأخیر است. حمله، یک تهدید امنیتی است که منجر به سوء استفاده، افشای اطلاعات و دستیابی به اطلاعات محرمانه‌ی افراد می‌گردد. یک طرح احراز هویت باید در برابر حملاتی از قبیل حملات جعل هویت، تکرار، جعل هویت با کلید تسخیرشده، داخلی اولویت‌دار، فرد در میانه، افشای مقادیر مخفی توسط مهاجم داخلی غیرفعال و غیره مقاوم باشد. علاوه بر این، پروتکل‌ها باید دارای خواص امنیتی از قبیل رازمانی پیش سوی کامل، رازمانی پس‌روی کامل، رازمانی کامل، گمنامی، ردیابی‌ناپذیری، حفظ

حریم‌خصوصی کاربر، پیوندناپذیری و غیره باشند (۲۹-۳۷).

حملات امنیتی

در انقلاب فناوری، اینترنت، بستر تمامی فناوری‌ها و ارتباطات است. از طرفی اینترنت یک فضای عمومی است که امکان رخداد تمامی اتفاق‌ها در آن وجود دارد. پس می‌توان نتیجه گرفت که خدمات ارائه‌شده تحت هر فناوری در برابر تهدیدات اینترنت باز آسیب‌پذیر است. حفظ حریم خصوصی و گمنامی کاربران بزرگترین چالش در پیاده‌سازی بستر استفاده از خدمات از راه دور در سطح جهانی است (۱۹-۲۴).

- حمله‌ی تکرار

در این نوع از حمله، مهاجم در ابتدا کانال ارتباطی ایجاد شده را شنود نموده و سپس پیام‌های احراز هویت مبادله شده بین کاربر و سرور را ضبط می‌نماید. سپس این پیام‌های ضبط شده را که شامل پاسخ کاربر و سرور است، در جلسات بعدی جهت سوء استفاده از پیام‌ها در برابر چالش‌های سرور برای احراز هویت استفاده می‌نماید. همچنین، مهاجم قادر است با ارسال پیام‌های ضبط شده به صورت یکجا، در دسترسی به سامانه اختلال ایجاد کند. زیرا که سامانه به پردازش همه‌ی پیام‌ها جهت تصمیم‌گیری نیاز دارد.

- حمله‌ی حدس گذرواژه

این حمله به دو صورت حدس گذرواژه‌ی برون خط و برخط انجام می‌پذیرد. در حمله‌ی حدس گذرواژه برون خط، مهاجم چندین گذرواژه را حدس زده و تطابق آن‌ها را با نسخه‌ی شنود شده از کانال بررسی می‌کند. در صورت تطابق این دو مقدار باهم، حمله با موفقیت صورت می‌پذیرد. در حمله‌ی حدس‌زدن گذرواژه برخط میزان تلاش مهاجم محدود شده و پس از چندین تلاش ناموفق در حدس گذرواژه، کاربر به عنوان مزاحم مسدود می‌شود.

- حمله‌ی جعل هویت

در این نوع از حمله، مهاجم هویت یکی از افراد شرکت‌کننده در پروتکل را جهت دست‌یابی به اطلاعات مخفی موجود در سامانه‌های اطلاعات پزشکی مراقبت از راه دور جعل می‌نماید. در جعل هویت سرور، مهاجم هویت سرور را جعل می‌کند تا بتواند به اطلاعات مخفی دیگر کاربران قانونی دسترسی یابد. هم‌چنین در جعل هویت کاربر، مهاجم هویت کاربر قانونی را در برابر سرور جعل نموده تا بتولند از خدمات ارائه‌شده توسط سرور قانونی به صورت غیرمجاز استفاده کند.

- حمله‌ی داخلی اولویت‌دار

این نوع از حمله توسط فردی که دارای دسترسی قانونی و مجاز به سامانه است صورت می‌پذیرد، به‌صورتی‌که حریم‌خصوصی و گمنامی کاربران سامانه می‌تواند توسط این دشمن به مخاطره بیفتد.

- حمله‌ی جعل هویت با کلید تسخیرشده

جهت مقاومت در برابر این حمله، اگر مقادیر مخفی بلندمدت یک هستار فاش و توسط مهاجم دریافت شود، دشمن نباید بتواند هویت هستارهای دیگر را جعل و یک کلید نشست مشترک را با هستاری که مقادیر مخفی‌اش فاش شده به توافق برساند.

- حمله‌ی تغییر

در این نوع حمله، هنگامی که کاربر درخواست خود را مبنی بر استفاده از خدمات به سمت سرور ارسال می‌کند، مهاجم به‌راحتی می‌تواند پیام او را دستکاری کند، آن را تغییر دهد و سپس با پیام تغییر داده شده توسط سرور احراز هویت گردد و از خدمات بهره ببرد.

- حمله‌ی فرد در میانه

در این نوع از حمله، مهاجم با قرارگرفتن در ارتباط بین طرفین شرکت‌کننده در پروتکل و شنود پیام‌های مبادله شده، هویت طرفین را جعل نموده و اینطور به‌نظر می‌رسد که یک تبادل اطلاعات عادی برقرار است. لازم به ذکر است، در صورتی‌که احراز هویت متقابل بین طرفین شرکت‌کننده در پروتکل صورت پذیرد و حمله‌ی جعل قابل اعمال نباشد، طرح موردنظر در برابر این حمله مقاوم است.

- حمله‌ی افشای مقادیر مخفی

این حمله به دو صورت فعال و غیرفعال صورت می‌پذیرد. سناریوی حمله در نوع فعال به این صورت است که مهاجم پیام‌های دریافتی را متوقف نموده، تغییر و با استفاده از این پیام‌های دستکاری‌شده با طرفین ارتباط برقرارمی‌کند. در حمله‌ی از نوع غیرفعال، مهاجم تنها پیام‌های مبادله‌شده بین طرفین شرکت‌کننده را استراق‌سمع نموده و سپس با استفاده از این مقادیر شنود شده عملیاتی برون‌خط را جهت یافتن مقادیر مخفی انجام می‌دهد.

خصوصیات امنیتی پروتکل‌های احراز هویت

سه اصل اساسی امنیت موسوم به CIA و برخی از این خصوصیات امنیتی در پروتکل‌های احراز هویت در این‌جا بیان شده است (۱۲).

- محرمانگی داده

در این ویژگی، اطلاعات بایستی از همه‌ی بخش‌های غیرمجاز مخفی نگه‌داشته شود، به‌گونه‌ای‌که فقط صاحب کلید قادر به یافتن اطلاعات است.

- در دسترس‌پذیری داده

در این خصوصیت، بایستی داده‌ها و اطلاعات در زمان نیاز در دسترس کاربر مجاز قرار بگیرند.

- جامعیت داده

در این ویژگی، گیرنده‌ی پیام باید بتواند پیامی را که به وسیله‌ی عامل ناشناس و یا مهاجم تغییر داده شده است، تشخیص دهد.

- رازمانی کامل

اگر کلیدهای طولانی‌مدت موردتوافق بین طرفین مورد سوء استفاده قرار بگیرند، در نتیجه کلیدهای مورداستفاده در نشست‌های

قبلی به خطر نیفتد. در این حالت پروتکل از ویژگی رازمانی پیش سوی کامل برخوردار است. به طور مشابه، اگر کلیدهای طولانی‌مدت موردتوافق بین طرفین مورد سوءاستفاده قرار بگیرند، درنتیجه کلیدهای مورداستفاده در نشست‌های بعدی به خطر نیفتد. در این حالت، پروتکل از ویژگی رازمانی پس روی کامل برخوردار است. درنتیجه، طبق موارد بیان‌شده می‌توان استنتاج کرد که طرح موردنظر از ویژگی رازمانی کامل برخوردار است.

- گمنامی کاربر

این ویژگی بدین معنا است که کاربر و سرور بتوانند به یکدیگر احراز هویت شوند، بدون اینکه هویت کاربر برای مهاجم شناسایی و افشا شود.

- ردیابی‌ناپذیری

مهاجم نباید بتواند هویت شرکت‌کنندگان را از پیام‌های مبادله شده در کانال عمومی به دست آورد و پیام‌ها را به یک کاربر خاص مرتبط نماید.

- پیوندناپذیری

این ویژگی بیان می‌کند که مهاجم نباید بتواند جلسات متعدد کاربر را به یکدیگر پیوند بدهد.

- مقیاس‌پذیری

یک پروتکل مقیاس‌پذیر نامیده می‌شود اگر برای مقیاس‌های بزرگتر هم بتواند به شیوه مناسب استفاده شود و لازم نباشد برای یافتن کاربری خاص کل جداول پایگاه داده‌ی خود را جست‌وجو کند.

نتیجه‌گیری

در این مقاله، ابتدا مفاهیم و جزئیات سامانه‌های اطلاعات پزشکی مراقبت از راه دور و شبکه‌ی بی‌سیم بدن مورد بررسی قرار گرفت و لزوم ایجاد این سامانه‌ها معرفی گردید. همچنین، طرح‌های احراز هویتی که اخیراً ارائه شده است، معرفی گردید. مشاهده شد که میزان عملکرد هر یک از طرح‌های احراز هویت وابسته به مقاومت هر طرح در برابر حملات موجود، ویژگی‌های امنیتی، هزینه‌های محاسباتی و غیره است. ضمناً هر طرح احراز هویت باید در برابر تمامی حملات مطرح مقاوم باشد. طرح‌های احراز هویت جهت مقاوم بودن در برابر حملات مطرح باید از ویژگی‌های امنیتی و حریم خصوصی برخوردار گردند.

در این مقاله به معرفی و توضیح حملات مطرح در سامانه‌های اطلاعات پزشکی مراقبت از راه دور و خصوصیات امنیتی طرح‌های احراز هویت پرداخته شد. یکی از موضوعات مهم دیگر که مورد مطالعه و تمرکز پژوهشگران در حوزه امنیت بوده است، کاهش سربار محاسباتی با استفاده از سامانه‌های رمزنگاری سبک‌وزن است که این کاهش سربار محاسباتی منجر به کاهش امنیت در پروتکل‌های حاضر نشود. در راستای تأمین هرچه بیش‌تر امنیت و حریم خصوصی، باید همکاری‌های بیشتری بین متخصصان امنیت و طراحان پروتکل‌ها صورت پذیرد، زیرا در صورت حصول یک پروتکل امن استفاده‌کنندگان از سامانه‌های اطلاعات پزشکی مراقبت از راه دور بیش‌تر می‌شود. در نتیجه آن، محدودیت و معیار مسافت و زمان در علوم پزشکی کم‌رنگ می‌گردد و زندگی راحت‌تری حاصل می‌شود. امروزه شاهد ارائه‌ی پروتکل‌های بسیاری در حوزه‌ی سامانه‌های اطلاعات پزشکی مراقبت از راه دور هستیم ولی در کنار توسعه و پیشرفت سریع این پروتکل‌ها باید این نکته در نظر گرفته شود که تهدیدات امنیتی و حملات جدید هم از این سرعت فناوری جدا نیستند. به ندرت اتفاق می‌افتد که یک پروتکل امنیتی مستعد آسیب‌پذیری نباشد. در نتیجه پژوهشگران حوزه‌ی امنیت شبکه باید در پی بررسی پروتکل‌های امنیتی باشند تا در نهایت منجر به اطمینان شود که در بدترین شرایط هیچ تهدید امنیتی بر آن‌ها وارد نیست. امید است که بتوانیم از این تحقیقات در فراهم‌سازی بستری ایمن برای توسعه‌ی فناوری جدید مدارک پزشکی الکترونیکی، تحت عنوان پرونده‌ی سلامت الکترونیک بیمار و بیمارستان که به تازگی در حال اجرا و بهره‌برداری است، در آینده نزدیک و به عنوان کارهای آتی قدمی برداریم.

تشکر و قدردانی

بدین‌وسیله از تمام کسانی که در اجرای این مطالعه همکاری داشتند تشکر و قدردانی به عمل می‌آید.

References

۱. Safkhan, M, Camara C, Peris-Lopez P. Bagheri N. RSEAP۲: An enhanced version of RSEAP, an RFID based authentication protocol for vehicular cloud computing. Vehicular Communications ۲۰۲۱; ۲۸: ۱۰۰۳۱۱.
۲. Safkhani M, Bagheri M. Passive secret disclosure attack on an ultralightweight authentication protocol for internet of things. Journal of Supercomputing ۲۰۱۷; ۷۳: ۳۵۷۹-۸۵.
۳. Amintoosi H, Nikooghadam M, Shojafar M, Kumari S, Alazab M. Slight: A lighweight authentication scheme for smart healthcare services. Computers and Electrical Engineering ۲۰۲۲; ۹۹: ۱۰۷۸۰۳.
٤. Dadkhah P, Dakhilalian M, Rastegari P. Security analysis and improvement of an access control scheme for wireless body area networks. ISeCure ۲۰۲۳; ۱۵(۳): ۳۵-٤۲.

۵. Safkhani M, Servati MR. ECCbAS: An ECC based authentication scheme for healthcare IoT systems. Pervasive and Mobile Computing ۲۰۲۳; ۹۰: ۱۰۱۷۵۳.
۶. Meshram Ch, Obaidat MS, Ibrahim RW, Meshram SG, Raikwar AV. An efficient privacy-preserved authentication technique based on conformable fractional chaotic map for TMIS under smart homes environments. J Supercomput ۲۰۲٤; ۸۰: ۲۵۱٤–۳۷.
۷. Nikkhah F. Improving the privacy security of telecare medical information systems [in Persian]. [MSc Thesis]. Tehran, Iran: Shahid Rajaee University; ۲۰۲۰.
۸. Pirmoradian F. Design and security analysis of authentication protocols used in Telecare Medicine Information Systems (TMIS) [in Persian]. [Thesis]. Isfahan, Iran: University of Technology; ۲۰۲۳.
۹. Sowjanya K, Dasgupta M, Ray S. An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems. Int J Inf Secur ۲۰۲۰; ۱۹: ۱۲۹-٤٦.
۱۰. Xiong H, Tao J, Yuan C. Enabling telecare medical information systems with strong authentication and anonymity. IEEE Access ۲۰۱۷; ۵: ٥٦٤٨-٦١.
۱۱. Mehmood Z, Ghani A, Chen G, Alghamdi AS. Authentication and secure key management in e-health services: a robust and efficient protocol using biometrics. IEEE Access ۲۰۱۹; ۷: ۱۱۳۳۸۵-۹۷.
۱۲. Liu J, Zhang L, Sun R. ۱- RAAP: an efficient ۱-round anonymous authentication protocol for wireless body area networks. Sensors ۲۰۱٦; ۱٦(۵): ۷۲۸.
۱۳. Li X, Peng J, Kumari S, Wu F, Karuppiah M, Raymond Choo KK. An enhanced ۱-round authentication protocol for wireless body area networks with user anonymity Computers and Electrical Engineering ۲۰۱۷; ٦۱: ۲۳۸–٤۹.
۱٤. Chiou SY, Chang SY. An enhanced authentication scheme in mobile RFID system. Ad Hoc Networks ۲۰۱۸; ۷۱: ۱-۱۳.
۱۵. Deebak BD, Al-Turjman F. Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical thing. IEEE Journal on Selected Areas in Communications ۲۰۲۰; ۳۹(۲): ۳٤٦-٦۰.
۱٦. Chandrakar P, Om H. Cryptanalysis and improvement of a biometric-based remote user authentication protocol usable in a multiserver environment. Transactions on Emerging Telecommunication Technologies ۲۰۱۷; ۲۸(۱۲): e۳۲۰۰.
۱۷. Yessad N, Bouchelaghem S, Ouada FS, Omar M. Secure and reliable patient body motion based authentication approach for medical body area networks. Passive and Mobile Computing ۲۰۱۷; ٤۲: ۳۵۱-۷۰.
۱۸. Wu F, Li X, Kumari S, Karuppiah M, Shen J. A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server. Computer and Electrical Engineering ۲۰۱۷; ٦۳: ۱٦۸–۸۱.
۱۹. Pirmoradian F, Dakhilalian SM, Safkhani M. ECKCI: An ECC-based Authenticated Key Agreement (AKA) scheme resistant to Key Compromise Impersonation Attack for TMIS. The ISC International Journal of Information Security ۲۰۲٤; ۱٦(۲): ۱۱۵-۳٦.
۲۰. Li C, Shih DH, Wang CC. Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems. Comput Methods Programs Biomed ۲۰۱۸; ۱۵۷: ۱۹۱-۲۰۳.
۲۱. Mohit P, Amin R, Karati A, Biswas GP. A standard mutual authentication protocol for cloud computing based health care systems. J Med Syst ۲۰۱۷; ۱(٤): ۵۰.
۲۲. Qi M, Chen J, Chen Y. A secure biometrics-based authentication key exchange protocol for multi-server TMIS using ECC. Comput Methods Programs Biomed ۲۰۱۸; ۱٦٤: ۱۰۱-۹.
۲۳. Amin R, Hafizul Islam SK, Biswas GP, Khurram Khan M, Kumar N. A robust and anonymous patient monitoring systme using wireless medical sensor networks. Future Generation Computer Systems ۲۰۱۸; ۸۰: ٤۸۳-۹۵.
۲٤. Ravanbakhsh N, Nazari N. An efficient improvement remote user mutual authentication and session key agreement scheme for e-healthcare systems. Multimed Tools Appl ۲۰۱۹; ۷۷: ۵۵-۸۸.
۲۵. Ostad-Sharif A, Abbasinezhad-Mood D, Nikooghadam M. An enhanced anonymous and unlinkable user authentication and key agreement proocol for TMIS by utilization of ECC. International Journal of Communication Systems ۲۰۱۹; ۳۲(۵): e۳۹۱۳.
۲٦. Nikooghadam M, Amintoosi H. An improved secure authentication and key agreement scheme for healthcare applications. Proceedings of the ۲۵th International Computer Conference, Computer Society of Iran (CSISS), Tehran, Iran: IEEE; ۲۰۲۰.
۲۷. Karthigaiveni M, Indrani B. An efficient two-factor authentication scheme with key agreement for IoT based E-health care application using smart card. J Ambient Intell Human Comput ۲۰۱۹.
۲۸. Alzahrani BA. Secure and efficient cloud-based iot authenticated key agreement scheme for e-health wireless sensor network. Arabian Journal for Science and Engineering ۲۰۲۰; ٤٦: ۳۰۱۷-۳۲.
۲۹. Jia X, He D, Kumar N, Choo KKR. Authenticated key agreement scheme for fog-driven IoT healthcare system. Wireless Networks ۲۰۱۹; ۲۵: ٤۷۳۷-۵۰.
۳۰. Li X, Chen T, Cheng Q, Ma J. An efficient and authenticated key establishment scheme based on fog computing for healthcare system. Front Comput Sci ۲۰۱۲; ۱٦: ۱٦٤۸۱۵.
۳۱. Pirmoradian F, Safkhani M, Dakhilalian SM. ECCPWS:An ECC-based protocol for WBAN systems. Computer Networks ۲۰۲۳; ۲۲٤: ۱۰۹۵۹۸.
۳۲. Mehmood Z, Ghani A, Chen G, Alghamdi AS. Authentication and secure key management in e-health services: a robust and efficient protocol using biometrics. IEEE Access ۲۰۱۹; ۷: ۱۱۳۳۸۵-۹۷.
۳۳. Alzahrani BA, Chaudhry SA, Barnawi A, Al-Barakati A, Shon M. An anonymous device to device authentication protocol using ecc and self certified public keys usable in internet of thingd based autonomous devices. Electronics ۲۰۲۰; *9*(۳): ۵۲۰.
۳٤. Hajian R, Haghighat A, Erfani SH. A secure anonymous D۲D mutual authentication and key agreement protocol for IoT. Internet of Things ۲۰۲۲; ۱۸: ۱۰۰٤۹۳.
۳۵. Son S, Park Y, Park Y. A secure, lightweight, and anonymous user authentication protocol for IoT environments. Sustainability ۲۰۲۱; *13*(۱٦): ۹۲٤۱.

۳۶. Hosseinzadeh M, Hussain M, Safkhani M, Bagheri N, Hoang Le Q, Taghtiz L, Mosavi AH. Toward designing a secure authentication protocol for IoT environments. *Sustainability* ۲۰۲۳; *15*(۷): ۵۹۳٤.

۳۷. Guo Y, Guo Y. CS-LAKA: A lightweight authenticated key agreement protocol with critical security properties for iot environments. IEEE Transactions on Services Computing ۲۰۱۹; ۱٦(٦): ٤۱۰۲-۱٤.

DOI: 10.48305/jims.v42.i783.0813

Journal of Isfahan Medical School Vol. ٤٢, No. ٧٨٣, ٣rd Week, November ٢٠٢٤

Received: ٠٩,٠٣٠٢٠٢٤ Accepted: ٢٤,١٠,٢٠٢٤ Published: ١٢,١١,٢٠٢٤

Investigation of Authentication Schemes in Telecare Medicine Information Systems

Seyed Mohammad Dakhilalian[١], Masoumeh Safkhani[٢], Fatemeh Pirmoradian[٣], Behzad Nazari[٤]

Review Article

Abstract

Background: Technological advancements based on the Internet of Things have revolutionized human life, and remote monitoring of patient health is no exception. Telecare medicine information systems are systems between home healthcare organizations and patients at home that allow doctors and patients to view medical data electronically. The development of a wireless body network plays a key role in health monitoring. The body's wireless network includes medical sensors that can be embedded in the patient's body, measure the patient vital signs, and send them to medical servers through a wireless channel. Therefore, security in telemedicine has always been a challenge. As cyber-attacks proliferate, we should expect users to take strict measures to protect their information. Thus, the design of lightweight authentication security protocols with the lowest cost has become a major challenge. In this article, we have limited our focus to reviewing the types of authentication protocols presented recently.

Conclusion: In this article, the concepts of TMIS were first examined, and the necessity of creating these systems is introduced. Also, the recently presented authentication schemes were introduced. It was observed that the performance of each authentication scheme depends on the resistance against existing attacks, security features, computing costs, etc. Today, we see the presentation of many protocols in the field of TMIS. However, in addition to the rapid development and progress of these protocols, it should be taken into account that security threats and new attacks are not separated from this speed of technology. As a result, researchers in network security should investigate security protocols to ensure that there is no security threat to them in the worst case.

Keywords: Internet of Things; System; Privacy

Citation: Dakhilalian SM, Safkhani M, Pirmoradian F, Nazari B. **Investigation of Authentication Schemes in Telecare Medicine Information Systems.** J Isfahan Med Sch ٢٠٢٤; ٤٢(٧٨٣): ٨١٣-٢٤.

١- Associate Professor, Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran

٢- Associate professor, Department of Computer Engineering, Shahid Rajaee Teacher Training University Tehran, Iran

٣- PhD, Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran

٤- Assistant Professor, Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan. Iran

Corresponding Author: Seyed Mohammad Dakhilalian, Associate Professor, Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran; Email: mdalian@iut.ac.ir