بهینه‌سازی الگوریتم‌های امنیت اطلاعات در به اشتراک‌گذاری اطلاعات سلامت

چکیده

مقدمه: امنیت اطلاعات بیماران در زمان به‌کارگیری فناوری‌های نوین و همچنین در زمان به اشتراک‌گذاری اطلاعات سلامت و ذخیره‌سازی آن‌ها در محیط ابر عمومی یکی از مهم‌ترین مسائل متخصصین حوزه سلامت است. تامین امنیت اطلاعات سلامت موجب اعتماد بیماران و افزایش مشارکت بیماران در برنامه‌های شبکه‌های مجازی سلامت می شود. هدف این مطالعه طراحی و پیاده‌سازی چارچوبی بهینه برای تامین امنیت اطلاعات بیماران در محیط‌های ذخیره سازی و شبکه‌های مجازی است.

روش پژوهش: این پژوهش از نوع توسعه‌ای – کاربردی بود. به منظور شناسایی و تعیین و ویژگی‌های چارچوب بهینه امنیت اطلاعات بیماران، مطالعات انجام‌شده با استفاده از مرور متون بررسی و ویژگی‌ها موردنیاز استخراج شد. در مرحله بعد چارچوب و پروتکل های موردنیاز ارائه و با استفاده از زبان برنامه‌نویسی جاوا پیاده‌سازی شد. چارچوب پیاده‌سازی شده با استفاده از سه آزمون سطح امنیت، عملکرد و مقیاس‌پذیری ارزیابی شد. آزمون امنیت در نرم افزار تحلیل خودکار پرتکل Scyther v1.1.3 انجام شد. آزمون عملکرد و آزمون مقیاس پذیری در محیط نرم افزار IntelliJ IDEA انجام شد.

یافته ها: برای حل مسئله لغو کاربر با استفاده از مرور متون مطالعات انجام‌شده، رویکرد لغو کاربر با استفاده از رمزگذاری مجدد پراکسی و الگوریتم رمزنگاری الجمال و استفاده از الگوریتم CP-ABE در نظر گرفته شد. این رویکرد شامل ویژگی‌های کوتاه بودن زمان لغو کاربر، عدم به‌روزرسانی متن رمزشده، آزاد بودن محیط ابر، بدون تناوب در به‌روزرسانی کلید، لغو فوری، استفاده از الگوریتم الجمال و استفاده از الگوریتم رمزنگاری CP-ABE است. به‌منظور حل مسئله کنترل دسترسی اطلاعات توسط بیمار با استفاده از مرور متون مطالعات انجام‌شده راه‌حلی نرم‌افزاری و مبتنی بر نقش و مبتنی بر نوع اطلاعات پیشنهاد شد که از توزیع غیرمجاز اطلاعات، دسترسی غیرمجاز و نامحدود و کپی غیرمجاز جلوگیری می‌کند. در این راه‌حل صاحب اطلاعات از فعالیت‌های مجاز بر روی‌داده‌ها مطلع می‌گردد. نتایج ارزیابی سطح امنیت نشان داد که در چهار نقش بیمار، پزشک، سرور ابر و سرور پراکسی پروتکل ارائه‌شده در برابر ادعاهای امنیتی Secret x، Alive، WeakAgree، Niagree و Nisynch تائید می‌گردد. نتایج آزمون عملکرد نشان داد به‌طور میانگین برای ۱۶۱۷/۱۰۱۵۶۲۵ کیلوبایت داده ورودی ۱۰/۲۸۲۹۶۰۸۱۴۹ ثانیه موردنیاز است. همچنین، به‌طور متوسط برای ۰۷۴۲۱۸۷۵/ ۱۶۱۷ کیلوبایت داده مصرف‌شده ۰/۷۹۷۴۹۲۱۶۲۲ ثانیه موردنیاز است. نتایج آزمون مقیاس پذیری نشان داد، پراکسی سرور در ۶۰ ثانیه به ۲۸۸۵ درخواست هم‌زمان و سرور ابر نیز در ۶۰ ثانیه می تواند به ۷۷۷ درخواست هم‌زمان پاسخ دهد.

نتیجه گیری: با استفاده از ویژگی ها و نتایج ارزیابی چارچوب ارائه شده می توان به این نتیجه دست یافت که چارچوب پیشنهاد شده بخش عمده ای از نیازها و مشکلات امنیت اطلاعات بیماران را بطور بهینه حل می کند و می تواند در یک سناریو واقعی مورد استفاده قرار گیرد.

کلید واژه ها: امینت اطلاعات سلامت، بهینه سازی، شبکه های اجتماعی سلامت، محیط ابر