مقایسه الگوریتم‌های بیمار محور برای امنیت اطلاعات سلامت در شبکه‌های اجتماعی سلامت و محیط ابر

مهین محمدی [۱] عباس شیخ طاهری [۲*] فرزانه کرمانی [۳]

۱. دانشجوی کارشناسی ارشد، انفورماتیک پزشکی، گروه مدیریت اطلاعات سلامت، دانشگاه علوم پزشکی ایران تهران، ایران. ORCID: 0000-0003-0558-7333
۲. گروه مدیریت اطلاعات سلامت، دانشکده مدیریت و اطلاع‌رسانی پزشکی، دانشگاه علوم پزشکی ایران، تهران، ایران.
۳. دانشجوی دکتری، انفورماتیک پزشکی، گروه مدیریت اطلاعات سلامت، دانشگاه علوم پزشکی ایران تهران، ایران.

مجله اطلاع‌رسانی پزشکی نوین؛ دوره پنجم؛ شماره دوم؛ پاییز و زمستان ۱۳۹۸؛ صفحات ۶۸-۷۹.

چکیده

هدف: *سلامت الکترونیک بیماران را قادر می‌سازد تا اطلاعات پزشکی خود را به اشتراک بگذارند و این موضوع خطر امنیت اطلاعات را در پی دارد. هدف این مطالعه بررسی و مقایسه الگوریتم‌ها و روش‌های حل مشکلات امنیت اطلاعات بیماران در زمان به اشتراک‌گذاری، از جنبه‌های مختلفی مانند لغو کاربر و قابلیت کنترل دسترسی و همچنین شناسایی نقاط قوت و ضعف این الگوریتم‌ها است.*

منابع اطلاعات یا داده‌ها: *این مطالعه مروری، بر اساس جستجوی موضوعی از بانک‌های اطلاعاتی PubMed, Web of Science و Science Direct با کلیدواژه‌های مرتبط انجام شد.*

روش‌های انتخاب برای مطالعه: *جستجوی مقالات با کلمات کلیدی سیستم‌های اطلاعات سلامت، امنیت رایانه‌ای، دسترسی به اطلاعات، رایانش ابری و شبکه‌های اجتماعی انجام شد. مقالات چاپ‌شده در فاصله زمانی ۲۰۰۹- ۲۰۱۹ انتخاب شدند. ۲۹ مقاله برای حل مسئله لغو کاربر و ۷ مقاله برای حل مسئله کنترل دسترسی انتخاب شد.*

ترکیب مطالب و نتایج: *به‌منظور حفظ محرمانگی اطلاعات بیماران، روش رمزنگاری قبل از به اشتراک‌گذاری پیشنهادشده است. این راه‌حل مشکل لغو کاربر را دارد. برای حل این مشکل روش‌های مختلفی ارائه شده است. این راه‌حل‌ها از جنبه‌های مختلف کوتاه بودن زمان لغو، به‌روزرسانی متن رمز شده، آزاد بودن محیط ابر، تناوب در به‌روزرسانی کلید و لغو فوری متفاوت هستند. همچنین، روش‌هایی برای کنترل دسترسی اطلاعات توسط بیمار ارائه شد.*

نتیجه‌گیری: *مسائل مربوط به امنیت اطلاعات سلامت باعث می‌شود بیماران نسبت به ارسال اطلاعات حساس سلامت خود و اشتراک آن با ارائه‌دهندگان خدمات سلامت مردد باشند. در این مقاله الگوریتم‌ها و روش‌های امنیت اطلاعات سلامت مقایسه شدند. اکثر راه‌حل‌های لغو کاربر به رمزنگاری مجدد نیاز دارند. همچنین راه‌حل‌های کنترل دسترسی انعطاف‌پذیری لازم ندارند. ازاین‌رو در آینده باید روش‌های بهتری ارائه شود.*

کلیدواژه‌ها: *سیستم‌های اطلاعات سلامت، امنیت رایانه‌ای، دسترسی به اطلاعات، رایانش ابری، شبکه‌های اجتماعی.*

نوع مقاله: مروری

دریافت مقاله: ۱۳۹۸/۶/۲۳ اصلاح نهایی: ۹۸/۹/۲۹ پذیرش مقاله: ۹۸/۱۰/۱

ارجاع: محمدی مهین، شیخ طاهری عباس، کرمانی فرزانه. مقایسه الگوریتم‌های بیمار محور برای امنیت اطلاعات سلامت در شبکه‌های اجتماعی سلامت و محیط ابر. مجله اطلاع‌رسانی پزشکی نوین. ۱۳۹۸؛ (۲)۵:. ۶۸-۷۹.

مقدمه:

فناوری اطلاعات و ارتباطات [ICT: Information and communications technology] چهره ارائه مراقبت‌های سلامت را از سازمانی به شخصی تبدیل کرده است [۱]. رویکردهای جدید بخصوص فناوری‌های نوین بیماران را قادر می‌سازد که به‌طور فعال در سلامت خود مشارکت داشته باشند [۲،۳]؛ بدیهی است، در این شرایط اطلاعات سلامت بیماران از طرف آن‌ها با اعضای گروه مراقبت از طریق فضای مجازی (برنامه‌های تلفن همراه، شبکه‌های اجتماعی و غیره) به اشتراک گذاشته می‌شوند که درنهایت در سرورهای مختلف ذخیره می‌شوند. این

نویسنده مسئول:
عباس شیخ طاهری
گروه مدیریت اطلاعات سلامت، دانشکده مدیریت و اطلاع‌رسانی پزشکی، دانشگاه علوم پزشکی ایران، تهران، ایران.
تلفن: ۸۸۷۹۴۳۰۱ (۰۲۱) ۹۸+ پست الکترونیکی: Sheikhtaheri.a@iums.ac.ir ORCID: 0000-0002-6879-5415

اطلاعات می‌توانند به پزشکان و مشاوران به‌منظور درک بهتر رفتار و علائم بیمار و ارائه پشتیبانی و یا مشاوره کمک شایانی نمایند [۴]. در این شرایط، امنیت اطلاعات سلامت می‌تواند توسط اشخاص غیرمجاز به خطر بیفتد [۵]. برخی از سازمان‌ها اطلاعات مربوط به بیماران را به خدمات ابری انتقال می‌دهند. ارائه‌دهندگان خدمات ابری نیز به‌طور کامل قابل‌اعتماد نیستند زیرا امکان دارد داده‌ها و اطلاعات ذخیره‌شده در محیط ابر توسط حملات مختلف مورد تهدید قرار بگیرد [۵،۶]. ازآنجاکه داده‌های سلامت حساس و خصوصی هستند، نیاز به محرمانه بودن و امنیت این داده‌ها کاملاً واضح و مشخص است [۷]. ازاین‌رو نگرانی اصلی در مورد امکان کنترل به اشتراک‌گذاری اطلاعات حساس توسط خود بیماران است [۸]، به همین دلیل، حفظ امنیت اطلاعاتی که بیماران با گروه مراقبت (در فضای ابر و شبکه‌های اجتماعی و غیره) به اشتراک می‌گذارند و کنترل دسترسی‌های غیرمجاز به این اطلاعات مهم است [۹]. صاحبان داده (بیماران) باید بتوانند دسترسی، امکان مشاهده، اصلاح و امکان توزیع داده‌های خود را کنترل کنند و از داده‌های خود محافظت نمایند و سیاست حفاظت از داده‌های خود را مشخص کنند [۱۲-۱۰].

فناوری اطلاعات منجر به کیفیت بالاتر و کاهش هزینه مراقبت شده ولی از سوی دیگر باعث افزایش خطرات امنیت اطلاعات نیز شده است [۱۳]. مبادله اطلاعات میان پزشک و بیمار باید در یک فضای محرمانه و امن باشد و امنیت در تمام مراحل ورود، ذخیره‌سازی، استفاده و انتقال داده موردتوجه قرار گیرد [۱۶-۱۴]. در این راستا روش‌ها و الگوریتم‌های مختلفی برای امنیت به اشتراک‌گذاری داده‌های سلامت در شبکه‌های اجتماعی و سیستم‌های ابری طراحی شده است، بااین‌حال، هریک از این روش‌ها دارای مزایا و محدودیت‌هایی است که قبل از پیاده‌سازی یا بهبود آن‌ها باید این مزایا و محدودیت‌ها را شناخت. هدف اصلی این مقاله مقایسه الگوریتم‌ها و روش‌های ارائه‌شده جهت حفظ امنیت اطلاعات بیماران در زمان به اشتراک‌گذاری این اطلاعات در محیط‌های شخص ثالث مانند ابر و شبکه‌های اجتماعی است.

مواد و روش‌ها:

این مطالعه با داده‌های کاربران در ارتباط نبوده است به همین دلیل نیاز به دریافت رضایت آگاهانه کاربران نداشته است.

در این مقاله رویکردهای به اشتراک‌گذاری، لغو کاربر و کنترل دسترسی به اطلاعات و الگوریتم‌های رمزنگاری مربوطه شناسایی و مقایسه گردید. مطالعه حاضر به‌صورت مرور متون انجام شد. مقالات مرتبط با کلمات کلیدی مناسب و مترادف انگلیسی آن‌ها در فاصله زمانی ۲۰۰۹- ۲۰۱۹ جستجو شدند. بعد از حذف مقالات تکراری، عناوین و چکیده مقالات ازنظر ارتباط موضوعی بررسی شدند و درنهایت، در خصوص حل مسئله لغو کاربر و حل مسئله کنترل دسترسی به ترتیب ۲۹ و ۷ مقاله انتخاب شد (جدول ۱). اطلاعات موردنیاز ازجمله الگوریتم مورداستفاده، رویکرد استفاده‌شده و یافته‌های حاصل از پیاده‌سازی الگوریتم از هر مقاله استخراج و مقایسه شد.

جدول ۱ تعداد مقالات منتخب از پایگاه‌های مختلف

کلمات کلیدی	فاصله زمانی	پایگاه‌های داده	تعداد مقالات دریافت شده	تعداد مقالات استخراج‌شده
“Health Social Networks”,” Information security”,” Health information”,” Cloud storage environments”,” Control access to health information”,” ABE encryption algorithm”” User Revocation”	۲۰۰۹ -۲۰۱۹	Web of Science	۳۰	۲۴
		PubMed	۵	۱
		Science Direct	۱۵	۱۱

یافته‌ها:

یکی از راه‌حل‌ها برای به اشتراک‌گذاری داده‌ها این است که بیماران داده‌های خود را قبل از ذخیره‌سازی در سرورهای ابری یا شبکه‌های اجتماعی رمزگذاری کنند و سپس کلیدهای رمزگذاری را برای کاربر موردنظر توزیع کنند. کاربران مجاز می‌توانند داده‌های رمزگذاری شده را از ابر دانلود و رمزگشایی کنند. مشکل اصلی این راه‌حل، لغو کاربر است. هنگامی‌که صاحب داده خواستار لغو یکی از کاربران است، باید داده‌ها را با کلید جدید رمزگذاری کرده و کلید جدید را برای همه کاربران باقی‌مانده منتشر کند؛ این فرایند بار بزرگی برای مالکین داده‌ها ایجاد می‌کند [۴]. برای حل این مسئله پنج رویکرد زیر ارائه‌شده است. (جدول ۲)

۱- رویکرد به‌روزرسانی کلید برای کاربران غیر لغو شده: در این روش، به‌روزرسانی کلید رمزنگاری برای کاربرانی که لغو نمی‌شوند انجام می‌شود که درنتیجه برای کاربرانی که قرار است لغو شوند کلید رمزنگاری به‌روزرسانی نمی‌شود [۱۷].

۲-رویکرد جاسازی فهرست لغو در متن رمز شده: در این روش، رمزگذاری به‌گونه‌ای است که لیست لغو در متن رمزنگاری وارد می‌شود، به‌این‌ترتیب کاربران در لیست لغو نمی‌توانند متن رمزنگاری را رمزگشایی کنند، حتی اگر ویژگی‌ها / سیاست‌های آن‌ها، ویژگی‌های مربوط به متن رمز شده را برآورده کند. با استفاده از این روش، نیازی به به‌روزرسانی کلید نیست [۳۲].

۳- رویکرد با کمک ابر: در این روش، قابلیت رمزگشایی به دو قسمت تقسیم می‌شود. نیمه اول متعلق به کاربر و نیمه دیگر متعلق به ابر است. اگر کاربر لغو شده است، ابراز انجام رمزگشایی سطح اول اجتناب می‌کند، در این صورت کاربر لغو شده نمی‌تواند متن رمزنگاری را بدون کمک ابر رمزگشایی کند. ابر کنترل لازم برای ممانعت از کاربران لغو شده برای رمزگشایی را دارد [۳۹].

۴- رویکرد لغو کاربر با استفاده از رمزگذاری مجدد پراکسی و الگوریتم رمزنگاری الجمال: رمزگذاری مجدد پراکسی مبتنی بر مفهوم پراکسی نیمه اعتماد است که از کلید رمزگذاری مجدد برای تبدیل متن رمزنگاری تحت کلید عمومی مالک داده به متن دیگری که می‌تواند از طریق کلید خصوصی کاربر رمزگشایی شود، استفاده می‌کند. وقتی صاحب داده خواستار لغو دسترسی کاربری است، به‌سادگی به سرور پراکسی اطلاع می‌دهد که قطعه کلید کاربر را حذف نماید. یکی از مشکلات عمده این طرح این است که از رمزنگاری کلید عمومی الجمال استفاده می‌شود که برای داده‌های زیاد مانند اطلاعات پزشکی مناسب نیست. Tranو همکاران از ایده پراکسی رمزگذاری مجدد استفاده کرده‌اند، در این رویکرد مدیر کاربران کلید خصوصی مالک داده را به دو قسمت تقسیم می‌کند. یک بخش آن در دستگاه مالک داده و بخش دیگر در سرور پراکسی ذخیره می‌گردد. مدیر کاربران برای کاربران دیگر که دارای حقوق دسترسی هستند، همان کلید خصوصی مالک اطلاعات را به بخش‌های مختلف تقسیم می‌کند. یک بخش از آن را به دستگاه کاربر و بخش‌های دیگر در سرور پراکسی ذخیره می‌گردد. وقتی صاحب داده خواستار لغو دسترسی کاربری است، به‌سادگی به سرور پراکسی اطلاع می‌دهد که قطعه کلید کاربر را حذف نماید. این طرح نیازی به رمزگذاری مجدد در زمان لغو کاربر ندارد. درنتیجه هزینه‌های محاسبات کاهش پیدا می‌کند [۱۸].

۵-رویکرد لغو کاربر با استفاده از رمزگذاری مجدد پراکسی [Proxy Re-Encryption]و الگوریتم رمزنگاری ویژگی بنیاد: را ایده استفاده ترکیبی رمزگذاری مجدد پراکسی و الگوریتم رمزنگاری [ABE: Attribute-Based Access]نیز ارائه شده است. الگوریتم رمزنگاری ABEیک الگوریتم رمزگذاری کلید عمومی است [۱۹]. این رویکرد مستلزم این است که یک‌بار کاربر از سیستم لغو شود، صاحب داده باید کلیدهای PRE را به ارائه‌دهندگان خدمات ابر [CSP:Cloud Service Providers] ارسال کند که با آن CSP می‌تواند دوباره رمزنگاری را انجام دهد.CSP توزیع کلیدهای به‌روزرسانی برای کاربران مجاز باقی‌مانده را انجام می‌دهد. بااین‌حال، CSP ابتدا هویت کاربران مجاز را می‌داند و درنهایت زمان مؤثر هر کاربر را می‌داند؛ بنابراین، برای جلوگیری از انتشار اطلاعات اضافی، صاحب داده باید کلیدهای به‌روزرسانی خود را توزیع کند [۲۰ ,۲۱].

طبق مقایسه (جدول ۲) اکثر مطالعات از رویکردهای به‌روزرسانی کلید برای کاربران غیر لغو شده و جاسازی فهرست لغو در متن رمز شده برای حل مسئله لغو کاربر استفاده کرده‌اند. تنها در رویکرد لغو کاربر با استفاده از رمزگذاری مجدد پراکسی و الگوریتم رمزنگاری الجمال از الگوریتم رمزنگاری الجمال استفاده شده بقیه روش‌ها از مزایا و ویژگی‌های الگوریتم رمزنگاری ABE استفاده کرده‌اند. در همه رویکردها به‌جز رویکرد رمزگذاری مجدد پراکسی و الگوریتم رمزنگاری الجمال، به‌روزرسانی متن رمز شده انجام می‌شود.

جدول ۲: مقایسه رویکردهای لغو کاربر

مطالعات	رویکرد به‌روزرسانی کلید برای کاربران غیر لغو شده	رویکرد جاسازی فهرست لغو در متن رمز شده	رویکرد با کمک ابر	لغو کاربر با استفاده از رمزگذاری مجدد پراکسی و	لغو کاربر با استفاده از رمزگذاری مجدد پراکسی و	کوتاه بودن زمان لغو کاربر	به‌روزرسانی متن رز شده	آزاد بدون محیط ابر	بدون تناوب در بروز رسانی کلید	لغو فوری	استفاده از الگوریتم الجمال	استفاده از الگوریتم رمزنگاری ABE

					الگوریتم رمزنگاری ABE	الگوریتم رمزنگاری الجمال						
Boldyreva و همکاران[۲۲]	✓	×	×	×	×	×	✓	✓	✓	×	×	✓
Yu و همکاران [۲۳]	✓	×	×	×	×	×	✓	✓	✓	×	×	✓
Sahai و همکاران [۲۴]	✓	×	×	×	×	×	✓	✓	✓	×	×	✓
Naruse و همکاران [۲۶, ۲۷]	✓	×	×	×	×	×	✓	✓	✓	×	×	✓
Xie وهمکاران[۲۵]،	✓	×	×	×	×	×	✓	✓	✓	×	×	✓
Li و همکاران[۲۸]	✓	×	×	×	×	×	✓	✓	✓	×	×	✓
Qian و همکاران[۲۹]	✓	×	×	×	×	×	✓	✓	✓	×	×	✓
Attrapadung و همکاران [۳۰،۳۱]	×	✓	×	×	×	×	×	✓	✓	✓	×	✓
Wang و همکاران [۳۲]	×	✓	×	×	×	×	×	✓	✓	✓	×	✓
Nieto و همکاران[۳۳]	×	✓	×	×	×	×	×	✓	✓	✓	×	✓
Zhang و همکاران[۳۵]	×	✓	×	×	×	×	×	✓	✓	✓	×	✓
Datta و همکاران[۳۶, ۳۷]	×	✓	×	×	×	×	×	✓	✓	✓	×	✓
Liu و همکاران[۳۸]	×	✓	×	×	×	×	×	✓	✓	✓	×	✓
Hur و همکاران[۳۹]	×	×	✓	×	×	×	×	✓	×	✓	×	✓
Tu و همکاران [۴۰]	×	×	✓	×	×	×	×	✓	×	✓	×	✓
Yu و همکاران[۲۱]	×	×	×	✓	×	×	×	✓	×	×	×	✓
Liu و همکاران [۴۱, ۴۲]	×	×	×	✓	×	×	×	✓	×	×	×	✓
Yang و همکاران[۴۳]	×	×	×	✓	×	×	×	✓	×	×	×	✓
Lin و همکاران[۴۴]	×	×	×	✓	×	×	×	✓	×	×	×	✓
Au و همکاران [۴۵]	×	×	×	✓	×	×	×	✓	×	×	×	✓
Ramu و همکاران[۴۶]	×	×	×	✓	×	×	×	✓	×	×	×	✓
Thilakanathan وهمکاران [۴]	×	×	×	×	✓	✓	×	✓	✓	✓	✓	×
Tran و همکاران [۱۸]	×	×	×	×	✓	✓	×	✓	✓	✓	✓	×
Thilakanathan وهمکاران [۴۷]	×	×	×	×	✓	✓	×	✓	✓	✓	✓	×

کنترل استفاده از داده‌ها در شبکه‌های اجتماعی و محیط ابر هنگامی‌که داده‌ها از سیستم بیمار به‌منظور به اشتراک‌گذاری ارسال می‌گردند، بیمار دیگر بر روی آن‌ها کنترل ندارد. بیمار از جایی که داده‌ها ذخیره می‌شود؛ کسی که به داده‌ها دسترسی دارد و تعداد نسخه‌ای که از داده‌ها تولید می‌شود، هیچ اطلاعی ندارد [۴۸]. کنترل استفاده از داده‌ها رویکردهایی را برای بیماران فراهم می‌کند تا بتوانند در مورد نحوه استفاده از داده‌های خود پس از دسترسی دادن به آن‌ها، کنترل داشته باشند [۴۹]. استفاده غیرمجاز از محتویات می‌تواند شامل دسترسی غیرمجاز و نامحدود، کپی غیرمجاز، اصلاح غیرمجاز و توزیع غیرمجاز اطلاعات باشد [۵۰].

برای حل مشکل فوق، روش‌هایی ارائه شده است. Narayan و همکاران شیء داده‌ای را ایجاد کرده‌اند که حاوی اطلاعات و سیاست مالک داده است سرویس نظارت پیگیری عملیاتی مانند ذخیره، چاپ و کپی را که بر روی‌داده‌ها انجام می‌شود را نگهداری می‌کند. همچنین انجام عملیات غیرمجاز توسط کاربر را شناسایی کند. در این پژوهش از عملیاتی که بر روی اطلاعات انجام می‌شود، لاگ گرفته می‌شود و به صاحب اطلاعات هشدار داده می‌شود [۵۰]. Munier و همکاران رویکردی بنام سند خود محافظ ارائه کردند که تنها از محتوای درون سند محافظت می‌کند و به سایر انواع محتوا مانند فایل‌های فیلم اعمال نمی‌شود [۵۱]. Chen و همکاران در مطالعه خود شی خود محافظتی [SPO:Self Protect Object]را معرفی کردند. در این رویکرد، سیاست‌ها به زبان XACML نوشته می‌شوند. زبان سیاست این امکان را می‌دهد تا مالک داده مشخص کند که مثلاً محتوای داده‌ها در یک کشور خاص یا در یک محدوده زمانی خاص مثلاً در یک روز قابل‌دسترسی باشد یا نباشد. روش پیشنهادی نمی‌تواند برحسب نقش کاربران و نوع داده اعمال شود، به همین دلیل انعطاف لازم را ندارد [۵۲]. Chen و همکاران بسته‌بندی داده‌ها با خط‌مشی دسترسی را پیشنهاد کرده‌اند. در این طرح صاحب داده بسته را برای کاربران مجاز و برنامه‌های غیرقابل‌اعتماد ارسال می‌کند. در معماری پیشنهادی، سیاست‌ها به تگ‌های سخت‌افزاری مرتبط با هر بخشی از داده‌ها تبدیل می‌شوند [مانند بخش‌هایی از اسناد، پرونده‌های الکترونیک سلامت و غیره.]

این تگ‌های سخت‌افزاری امکان ارائه کنترل‌های دسترسی را می‌دهند. بااین‌حال، این داده‌ها تنها در دستگاه‌های DataSafe و با سخت‌افزارهای خاصی قابل‌دسترسی هستند که این امر باعث محدود کردن قابلیت دسترسی کاربران می‌شود [۱۲]. Squicciarini و همکاران نیز ایده اشیاء خودکنترل [SCO:Self-Controlling Objects] را ارائه داده‌اند. در این رویکرد سیاست‌های داده‌ها، سیاست‌های ایجادشده توسط کاربر و سیاست‌های مبتنی بر قوانین به همراه داده‌ها در اشیاء خودکنترلی رمز می‌شوند. مجوزهای مربوط با SCO نیز ایجاد می‌شوند؛ بنابراین، شکستن و مهندسی معکوس SCO به‌منظور رمزگشایی کردن و به دست آوردن محتوای داده برای کاربر غیرمجاز امکان‌پذیر نیست. بااین‌حال، در این روش کاربر مجاز می‌تواند داده‌ها را برای کاربران غیرمجاز توزیع کند [۵۳]. Thilakanathanو همکاران اشیاء خودکنترل کننده [SafeShare objects] را معرفی کردند. این اشیا حاوی اطلاعات حساس و همچنین فراداده‌های مربوط به این داده‌ها و هم‌چنین عملیات مجاز بر روی آن‌ها (سیاست‌ها) است. [۱۰،۴۷].

Chen و همکاران اطلاعات ایمن [DataSafe] را به‌منظور جلوگیری از انتشار غیرمستقیم داده‌های محافظت‌شده توسط گیرندگان مجاز پیشنهاد دادند. DataSafe نیاز به سخت‌افزار خاصی دارد و حفاظت از رمز عبور مایکروسافت تنها بر روی محصولات مایکروسافت کار می‌کند.

DataSafe از تگ‌های سخت‌افزاری استفاده می‌کند که هر بار دستورالعمل‌های سخت‌افزاری مربوط به جریان داده‌ها اجرا می‌شود، این تگ‌ها فعال می‌شوند [۵۴، ۱۲]. تغییر مسیر فراخوانی فایل و تنظیم SDCs توسط نرم‌افزار DataSafe ازنظر عملیاتی و محاسباتی سنگین است. به‌طور مشابه، ردیابی جریان اطلاعات توسط سخت‌افزاری‌های DataSafe نیز هزینه‌بر است [۵۵].

جدول ۳ مقایسه مطالعات انجام‌شده بر روی کنترل دسترسی بر اساس ویژگی‌های مختلف را نشان می‌دهد و همان‌گونه که مشخص است اکثر روش‌های پیشنهادی به‌صورت نرم‌افزاری است و بیش‌تر بر روی قابلیت جلوگیری از دسترسی غیرمجاز و نامحدود و جلوگیری از توزیع غیرمجاز تمرکز شده است، بقیه ویژگی‌ها کم‌تر موردتوجه قرارگرفته‌اند.

جدول ۳ مقایسه مطالعات انجام‌شده بر روی کنترل دسترسی

مطالعات	مبتنی بر نوع داده	مبتنی بر نقش	اطلاع‌رسانی به صاحب اطلاعات	جلوگیری از اصلاح غیرمجاز	جلوگیری از کپی غیرمجاز	جلوگیری از دسترسی غیرمجاز و نامحدود	جلوگیری از توزیع غیرمجاز	نرم‌افزاری	سخت‌افزاری
Narayan و همکاران [۵۰]	×	×	✓	×	×	×	×	✓	×
Munier و همکاران [۵۱]	×	×	×	×	×	✓	✓	✓	×
Chen و همکاران [۵۲]	×	×	×	✓	×	✓	✓	✓	×
Thilakanathan و همکاران [۱۰]	×	×	×	×	✓	✓	✓	✓	×
Thilakanathan وهمکاران [۴۷]	×	×	×	×	✓	✓	✓	✓	×
Chen و همکاران [۱۲]	×	×	×	×	×	✓	✓	✓	✓
Chen و همکاران [۵۴]	×	×	×	×	×	✓	✓	✓	✓

بحث و نتیجه‌گیری:

فناوری‌های جدید منجر به افزایش قابلیت‌های تبادل اطلاعات سلامت شده است [۵۹]. با توجه به اهمیت حفظ امنیت اطلاعات بیماران و افراد در زمان به اشتراک‌گذاری با گروه مراقبت در سیستم‌هایی مانند شبکه‌های اجتماعی سلامت و محیط‌های ذخیره‌سازی ابر در مطالعات مختلف الگوریتم‌ها و روش‌هایی برای تأمین امنیت اطلاعات انجام‌شده است. یکی از راه‌حل‌های این است که بیماران داده‌های خود را قبل از ذخیره‌سازی در سرورهای ابری یا شبکه‌های اجتماعی رمزگذاری کنند. مشکل اصلی این راه‌حل لغو کاربراست [۴].

رمزگذاری ABE به‌منظور حفاظت از اطلاعات حساس سلامت، بازسازی پویای داده‌ها، حفظ حریم خصوصی در محیط‌های ذخیره‌سازی خصوصی و عمومی ابر پیشنهاد شده است [۵۶]. در این روش، کلیدهای خصوصی می‌توانند هر ساختار دسترسی را پوشش دهند [۵۷]. جنبه‌های اصلی این الگوریتم انعطاف‌پذیری، مقیاس‌پذیری و کنترل دسترسی دقیق و ممانعت از تبانی کاربران است [۱۹]. با استفاده از این الگوریتم می‌توان داده‌های سلامت را با استفاده از سیاست دسترسی محافظت کرد و تنها افرادی که دارای مجموعه‌ای از ویژگی‌ها هستند و سیاست دسترسی را برآورده می‌کنند، می‌توانند به داده‌ها دسترسی یابند [۵۸]. همان‌گونه که یافته‌ها نشان داد اکثر پژوهشگران این روش را برای امنیت به اشتراک‌گذاری داده‌ها پیشنهاد داده و استفاده کرده‌اند. بااین‌حال، مشکل روش ABE این است که در زمان لغو کاربر مالک اطلاعات (بیمار؛ سیستم بیمار) باید به‌طور مرتب دوباره داده‌ها را رمزگذاری کند و دوباره کلیدهای جدید را برای کاربران مجاز توزیع کند. بنابراین، این رویکرد منجر به بارکاری سنگین در سمت مالک داده‌ها می‌شود و بسیار ناکارآمد است [۴۱]. برای حل مسئله لغو کاربر رویکردهای متفاوتی ارائه شده است.

روش به‌روزرسانی کلید برای کاربران غیر لغو شده در مطالعات [۲۲-۲۹] ارائه‌شده است. این روش داری ویژگی‌های و مزیت‌های کوتاه بودن زمان لغو کاربر، آزاد بودن محیط ابر و استفاده از الگوریتم رمزنگاریABE و داری محدودیت‌های به‌روزرسانی متن رمزشده، تناوب در به‌روزرسانی کلید و عدم لغو فوری است. رویکرد جاسازی فهرست لغو در متن رمز شده در مطالعات ارائه‌شده است [۳۸-۳۰]. در این روش رمزگذار آخرین لیست لغو را به متن رمزگذاری می‌چسباند تا فقط کاربرانی که در فهرست لغو قرار نگرفته‌اند، بتوانند متن رمزنگاری را رمزگشایی کنند [۱۷]. این روش دارای محدودیت‌های کوتاه نبودن زمان لغو کاربر، به‌روزرسانی متن رمزشده و دارای مزیت‌های آزاد بودن محیط ابر، بدون تناوب بودن در به‌روزرسانی کلید، لغو فوری و استفاده از الگوریتم رمزنگاری ABE است. در مطالعات روش لغو کاربر با استفاده از رمزگذاری مجدد پراکسی و الگوریتم رمزنگاری الجمال استفاده شده است [۴۷, ۱۸, ۴]. یکی از مشکلات عمده این طرح این است که از رمزنگاری کلید عمومی الجمال استفاده می‌شود، ازآنجایی‌که این الگوریتم، رمزگشایی داده‌های بسیار زیاد را نخواهد پذیرفت، درنتیجه برای اطلاعات پزشکی مناسب نیست [۴]. این رویکرد دارای ویژگی‌های و مزیت‌های کوتاه بودن زمان لغو کاربر، عدم به‌روزرسانی متن رمزشده، آزاد بودن محیط ابر، بدون تناوب بودن در به‌روزرسانی کلید و لغو فوری است. روش لغو کاربر با کمک ابر در مطالعات پیشنهاد شده است [۴۰, ۳۹]. این روش دارای محدودیت‌های کوتاه نبودن زمان لغو کاربر، به‌روزرسانی متن رمزشده، آزاد نبودن محیط ابر و دارای مزیت‌های متناوب نبودن در

به‌روزرسانی کلید، لغو فوری و استفاده از الگوریتم رمزنگاری ABE است. رویکرد لغو کاربر با استفاده از رمزگذاری مجدد پراکسی و الگوریتم رمزنگاری ABE راه‌حل دیگری برای لغو کاربر با استفاده از ترکیب PRE و ABE است و در مطالعات ارائه شده است [۴۵،۴۶، ۴۳-۲۱،۴۱]. این روش دارای محدودیت‌های کوتاه نبودن زمان لغو کاربر، به‌روزرسانی متن رمزشده، آزاد نبودن محیط ابر، متناوب بودن در به‌روزرسانی کلید و دارای مزیت‌های لغو فوری و استفاده از الگوریتم رمزنگاری ABE است. همان‌گونه که یافته‌ها نشان داد کوتاه نبودن زمان لغو و آزاد نبود سرور (ابر(در بیشتر روش‌های پیشنهادی حل‌نشده باقی مانده است که در روش‌ها و مطالعات آتی باید به آن پرداخته شود .

برای حل مسئله کنترل دسترسی اطلاعات پس از به اشتراک‌گذاری آن توسط بیمار نیز روش‌هایی پیشنهاد شده است که هریک از آن‌ها، ویژگی‌ها و محدودیت‌هایی دارند. Narayan و همکاران به‌منظور کنترل دسترسی اطلاعات توسط صاحب اطلاعات، راه‌حلی نرم‌افزاری و دارای قابلیت اطلاع‌رسانی به صاحب اطلاعات ارائه کرده‌اند. این راه‌حل از فعالیت‌های غیرمجاز بر روی اطلاعات جلوگیری نمی‌کند [۵۰].

Munier و همکاران برای حل این مسئله رویکردی ارائه کردند که تنها از محتوای درون سند محافظت می‌کند و به سایر انواع محتوا مانند فایل‌های فیلم اعمال نمی‌شود. این راه‌حل نرم‌افزاری از دسترسی غیرمجاز و نامحدود و توزیع غیرمجاز جلوگیری می‌کند. در این مطالعه فعالیت‌های مجاز انجام‌شده بر روی اطلاعات به صاحب داده اطلاع‌رسانی نمی‌شود [۵۱]. Chen و همکاران در مطالعه خود راه‌حل نرم‌افزاری ارائه داده‌اند که از اصلاح غیرمجاز، دسترسی غیرمجاز و نامحدود و توزیع غیرمجاز جلوگیری می‌کند. در این مطالعه نیز تغییرات و فعالیت‌های مجاز انجام‌شده بر روی اطلاعات به صاحب داده اطلاع‌رسانی نمی‌شود [۵۲].

Thilakanathanو همکاران روشی نرم‌افزاری ارائه داده‌اند که دارای قابلیت‌های جلوگیری از کپی غیرمجاز، جلوگیری از دسترسی غیرمجاز و نامحدود، جلوگیری از توزیع غیرمجاز است. این روش قابلیت اطلاع‌رسانی به مالک اطلاعات را ندارد [۴۷، ۱۰]. Chen و همکاران راه‌حلی پیشنهاد دادند که نیاز به سخت‌افزار خاصی دارد و تنها بر روی محصولات مایکروسافت کار می‌کند. این روش نیز نرم‌افزاری و سخت‌افزاری بوده و از دسترسی غیرمجاز و نامحدود و توزیع غیرمجاز جلوگیری می‌کند. این مطالعات نتوانستند اطلاع‌رسانی به کاربران را حل کنند [۱۲،۵۴].

به‌طور خلاصه نیاز به مراقبت از راه دور بیماران در خانه و خود مراقبتی رو به افزایش است. فن‌آوری‌های تلفن همراه و همچنین، رایانش ابری می‌توانند نظارت بر سلامت را توسعه دهند. از سوی دیگر نگرانی بیماران در مورد دسترسی افراد به اطلاعات شخصی آن‌ها افزایش‌یافته است. در این مقاله به مقایسه الگوریتم‌ها، رویکردها و روش‌های حفظ امنیت اطلاعات بیمار در زمان به اشتراک‌گذاری آن پرداخته‌شده، ویژگی‌ها و قابلیت‌ها موردبررسی قرار گرفت و مشخص شد، مسائلی مانند لغو کاربر هنوز به‌طور کامل حل‌نشده است. برخی از روش‌های ارائه شده همچنان به دوباره رمزگذاری اطلاعات، ارائه کلیدهای مجدد رمزنگاری نیاز دارند. راه‌حل‌های ارائه شده برای کنترل دسترسی اطلاعات نیز مبتنی بر نوع اطلاعات و نوع کاربران نیست. به همین دلیل انعطاف‌پذیری لازم را ندارند؛ ازاین‌رو در آینده باید بر روی آن‌ها مطالعات بیشتر انجام شود و الگوریتم‌های بهتری ارائه شود.

تأییدیه اخلاق:

پروتکل مطالعه در کمیته اخلاق دانشگاه علوم پزشکی ایران با کد IR.IUMS.REC.1397.656 مصوب شده است.

تضاد منافع:

در انجام مطالعه حاضر، هیچ‌گونه تعارض منافع برای نویسندگان مقاله وجود ندارد.

سهم نویسندگان:

مهین محمدی (نویسنده اول) پرسشگر اصلی /روش‌شناسی / مقدمه/ تدوین پیش‌نویس (۴۵٪)؛ دکتر عباس شیخ طاهری (نویسنده دوم و مسئول) پرسشگر اصلی/ روش‌شناسی /ویرایش مقاله (۴۵٪)؛ فرزانه کرمانی(نویسنده سوم) مقدمه /ویرایش (۱۰٪)

حمایت مالی:

این مطالعه بخشی از پایان‌نامه کارشناسی ارشد تحت عنوان «بهینه‌سازی الگوریتم‌های امنیت اطلاعات در به اشتراک‌گذاری اطلاعات سلامت» است که با کد ۱۳۹۷-۲-۳۷-۱۲۳۹۷ توسط دانشگاه علوم پزشکی ایران حمایت شده است.

Reference

1. NaseriBooriAbadi T, Sheikhtaheri A. Information privacy and pervasive health: Frameworks at a glance. J Biomed Phys Eng. 2018. Doi: 10.31661/jbpe.v0i0.398
2. Pharow P, Blobel B, Ruotsalainen P, Petersen F, Hovsto A. Portable devices, sensors and networks: Wireless personalized ehealth services. Stud Health Technol Inform. 2009; 150:1012-6. Doi:10.3233/978-1-60750-044-5-1012
3. Meingast M, Roosta T, Sastry S. Security and privacy issues with health care information technology. In: Engineering in Medicine and Biology Society, 2006 EMBS'06 28th Annual International Conference of the IEEE; 2006 Aug Sept 3-30; New York, NY, USA; 29: IEEE; 2006. Doi:10.1109/IEMBS.2006.260060
4. Thilakanathan D, Calvo RA, Chen S, Nepal S, Glozier N. Facilitating secure sharing of personal health data in the cloud. JMIR Med Inform. 2016; 4(2):e15. Doi:10.2196/medinform.4756.
5. Lokhande AR, Jamgekar RS, Takalikar RA. Improving privacy in healthcare service by using cloud assisted technologies. IJCSIT. 2015; 6(5):4605-10.
6. Rocha F, Abreu S, Correia M. The final frontier: Confidentiality and privacy in the cloud. computer. 2011; 44(9):44-50. Doi:10.1109/MC.2011.223
7. Sheikhtaheri A, Hashemi N, Hashemi N. Performance of hospitals in protecting the confidentiality and information security of patients in health information departments. Stud Health Technol Inform. 2019; 260:202-9. PMID: 31118339
8. ACT A. Health insurance portability and accountability act (hipaa). Gramm. 2003; 239(6):772–8. Doi:10.1097/01.sla.0000128307.98274.dc
9. Zhang G, Poon CC, Li Y, Zhang Y. A biometric method to secure telemedicine systems. In:Conf Proc IEEE Eng Med Biol Soc. 2009; 2009 Sept 3- 6; Minneapolis, MN, USA;22: IEEE; 2009. Doi:10.1109/IEMBS.2009.5332470.
10. Thilakanathan D, Calvo R, Chen S, Nepal S. Secure and controlled sharing of data in distributed computing. In: 2013 IEEE 16th International Conference on Computational Science and Engineering (CSE); 3-5 Dec. 2013; Sydney, NSW, Australia; 6: IEEE; 2014. Doi: 10.1109/CSE.2013.125
11. Li J, Zhao G, Chen X, Xie D, Rong C, Li W, et al. Fine-grained data access control systems with user accountability in cloud computing. In:2nd IEEE International Conference on Cloud Computing Technology and Science; 2010 Nov Dec 3-30. Indianapolis, IN, USA;1: IEEE; 2010. Doi: 10.1109/CloudCom.2010.44
12. Chen Y-Y, Jamkhedkar PA, Lee RB. A software-hardware architecture for self-protecting data. In: Yu T,editors. Proceedings of the 2012 ACM conference on Computer and communications security; 2012 October; Raleigh North Carolina: ACM; 2012. Doi:10.1145/2382196.2382201
13. Hajrahimi N, Dehaghani SMH, Sheikhtaheri A. Health information security: A case study of three selected medical centers in iran. Acta Inform Med. 2013; 21(1):42-5. Doi:10.5455/AIM.2012.21.42-45.
14. Mermelstein HT, Wallack JJ. Confidentiality in the age of hipaa: A challenge for psychosomatic medicine. Psychosomatics. 2008; 49(2):97-103. Doi:10.1176/appi.psy.49.2.97.
15. Ray A, Newell S. Exploring information security risks in healthcare systems. Encyclopedia of healthcare information systems. Pennsylvania: IGI Global. 2008;573-7.
16. Hosseinian V, Ayatollahi H, Haghani H, Mehraeen E. Requirements of information security in a telemedicine network: Review of it managers' opinion. JPSR. 2015; 4(2):31-40. [In Persian] Doi:10.22038/JPSR.2015.4391
17. Liu JK, Yuen TH, Zhang P, Liang K. Time-based direct revocable ciphertext-policy attribute-based encryption with short revocation list. International conference on applied cryptography and network security; 2018: Springer.
18. Tran DH, Nguyen H-L, Zha W, Ng WK. Towards security in sharing data on cloud-based social networks. In:Information, Communications and Signal Processing (ICICS) 2011 8th International Conference on; 2011 Dec 13-16; Singapore, Singapore;6: IEEE; 2011. Doi:10.1109/ICICS.2011.6173582
19. Vahidhunnisha J, Ramasamy S, Balasubramaniam T. Survey on multi authority attribute based encryption for personal health record in cloud computing. IJCSNS. 2014; 14(12):51. Doi:10.15373/22778179/OCT2013/53

20. Wang G, Liu Q, Wu J, Guo M. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers. Comput Secur. 2011; 30(5):320-31. Doi:10.1016/j.cose.2011.05.006
21. Yu S, Wang C, Ren K, Lou W. Achieving secure, scalable, and fine-grained data access control in cloud computing. In:2010 Proceedings IEEE INFOCOM; 2010 March14-19; San Diego, CA, USA;23: IEEE; 2010. Doi:10.1109/INFCOM.2010.5462174
22. Boldyreva A, Goyal V, Kumar V. Identity-based encryption with efficient revocation. In: Ning P,editors. Proceedings of the 15th ACM conference on Computer and communications security; 2008 October; Alexandria Virginia USA: ACM; 2008. Doi:10.1145/1455770.1455823
23. Yu S, Wang C, Ren K, Lou W.: Attribute based data sharing with attribute revocation. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security; 2010 April; Beijing China: ACM; 2010. Doi:10.1145/1755688.1755720
24. Sahai A, Seyalioglu H, Waters B. Dynamic credentials and ciphertext delegation for attribute-based encryption. Advances In: Safavi-Naini R, Canetti R. Editors.Advances in Cryptology – CRYPTO 2012. CRYPTO 2012. Lecture Notes in Computer Science; 2012,August, 19-23; Santa Barbara, CA, USA, Springer, 2012. P199-217. Doi:10.1007/978-3-642-32009-5_13
25. Xie X, Ma H, Li J, Chen X. An efficient ciphertext-policy attribute-based access control towards revocation in cloud computing. JUCS. 2013; 19(16):2349-67. Doi:10.3217/jucs-019-16-2349
26. Naruse T, Mohri M, Shiraishi Y. Provably secure attribute-based encryption with attribute revocation and grant function using proxy re-encryption and attribute key for updating. Human-centric Computing and Information Sciences. 2015;5(1):8. Doi:10.1186/s13673-015-0027-0
27. Naruse T, Mohri M, Shiraishi Y. Attribute-based encryption with attribute revocation and grant function using proxy re-encryption and attribute key for updating. Future information technology. 2014; 5(8):119-25. Doi:10.1186/s13673-015-0027-0
28. Li M, Yu S, Zheng Y, Ren K, Lou W. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans Parallel Distrib Syst. 2013; 24(1):131-43. Doi:10.1109/TPDS.2012.97
29. Qian H, Li J, Zhang Y, Han J. Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation. Int J Inf Secur. 2015; 14(6):487-97. Doi:10.1007/s10207-014-0270-9
30. Attrapadung N, Imai H. Conjunctive broadcast and attribute-based encryption. In: Shacham H, Waters B,editors. Pairing-Based Cryptography – Pairing 2009. Pairing 2009. Lecture Notes in Computer Science International Conference on Pairing-Based Cryptography; 2009,August,12-14; Palo Alto, CA, USA: Springer, 2009. p248-265. Doi:10.1007/978-3-642-03298-1_16
31. Attrapadung N, Libert B, De Panafieu E. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In: Catalano D, Fazio N, Gennaro R, Nicolosi A.,editors. Public Key Cryptography – PKC 2011. PKC 2011. Lecture Notes in Computer Science; 2011, March, 6-9; Taormina, Italy: Springer, 2011.p 90-108.
32. Wang P, Feng D, Zhang L. Towards attribute revocation In: Lin D, Tsudik G, Wang X,editors. Cryptology and Network Security. CANS 2011. Lecture Notes in Computer Science Security; 2011, December, 10-12; Sanya, China: Springer,2011. p 272-291. Doi:10.1007/978-3-642-25513-7_19
33. González-Nieto JM, Manulis M, Sun D. Fully private revocable predicate encryption. In: Susilo W, Mu Y, Seberry J,editors. Information Security and Privacy. ACISP 2012. Lecture Notes in Computer Science; 2012, July, 9-11, ollongong, NSW, Australia: Springer,2012. p 350-363. Doi:10.1007/978-3-642-31448-3_26
34. Balu A, Kuppusamy K. Ciphertext-policy attribute-based encryption with user revocation support. In: Singh K, Awasthi A.K, editors.Quality, Reliability, Security and Robustness in Heterogeneous Networks. QShine 2013. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; 2013, January, 11-12; Greader Noida, India: Springer; 2013. P696-705. Doi:10.1007/978-3-642-37949-9_61.
35. Zhang M. New model and construction of abe: Achieving key resilient-leakage and attribute direct-revocation. In: Susilo W, Mu Y, editors. Information Security and Privacy. ACISP 2014. Lecture Notes in Computer Science;2014, July, 7-9; Wollongong, NSW, Australia: Springer;2014. p192-208. Doi:10.1007/978-3-319-08344-5_13.
36. Datta P, Dutta R, Mukhopadhyay S. General circuit realizing compact revocable attribute-based encryption from multilinear maps. In: Lopez J, Mitchell C, editors. Information Security. ISC 2015. Lecture Notes in Computer Science; 2015, September,9-11; Trondheim,

Norway: Springer, 2015. p336-354. Doi:10.1007/978-3-319-23318-5_19.
37. Datta P, Dutta R, Mukhopadhyay S. Adaptively secure unrestricted attribute-based encryption with subset difference revocation in bilinear groups of prime order In: Pointcheval D, Nitaj A, Rachidi T, editors.Progress in Cryptology – AFRICACRYPT 2016. AFRICACRYPT 2016. Lecture Notes in Computer Science;2016, April,13-15; Fes, Morocco:Springer, 2016. p325-345. Doi:10.1007/978-3-319-31517-1_17.
38. Liu Z, Wong DS. Practical ciphertext-policy attribute-based encryption: Traitor tracing, revocation, and large universe. In: Malkin T, Kolesnikov V, Lewko A, Polychronakis M, editors. Applied Cryptography and Network Security. ACNS 2015. Lecture Notes in Computer Science;2015, June,2-5; New York, USA: Springer, 2015. p127-146. Doi:10.1007/978-3-319-28166-7_7
39. Hur J, Noh DK. Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Transactions on Parallel and Distributed Systems. 2011; 22(7):1214-21. Doi:10.1109/TPDS.2010.203
40. Tu S-s, Niu S-z, Li H, Xiao-ming Y, Li M-j. Fine-grained access control and revocation for sharing data on clouds. In: Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), 2012 IEEE 26th International; 2012 May 21-25; Shanghai, China;3: IEEE; 2012. Doi:10.1109/IPDPSW.2012.265
41. Liu Q, Wang G, Wu J. Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. Information sciences. 2014; 258:355-70. Doi:10.1016/j.ins.2012.09.034
42. Liu Q, Wang G, Wu J. Clock-based proxy re-encryption scheme in unreliable clouds. In: Parallel Processing Workshops (ICPPW), 2012 41st International Conference on; 2012 Sept 10-13; Pittsburgh, PA, USA: IEEE; 2012. Doi:10.1109/ICPPW.2012.45
43. Yang Y, Zhang Y. A generic scheme for secure data sharing in cloud. In: Parallel Processing Workshops (ICPPW), 2011 40th International Conference on; 2011 Sept 13-16; aipei City, Taiwan: IEEE; 2011. Doi:10.1109/ICPPW.2011.51
44. Lin G, Ying C, Tan S, Xia Y, Sun Z. Arp-cp-abe: Toward efficient, secure and flexible access control for personal health record systems. In:2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech); 2018 Aug 12-15; Athens, Greece: IEEE; 2018. Doi:10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00024
45. Au MH, Yuen TH, Liu JK, Susilo W, Huang X, Xiang Y, et al. A general framework for secure sharing of personal health records in cloud system. Journal of Computer and System Sciences. 2017; 90:46-62.
46. Ramu G, Reddy BE, Jayanthi A, Prasad LN. Fine-grained access control of ehrs in cloud using cp-abe with user revocation. Health and Technology. 2019; 9:1-10. Doi:10.1007/s12553-019-00304-9
47. Thilakanathan D, Chen S, Nepal S, Calvo R, Alem L. A platform for secure monitoring and sharing of generic health data in the cloud. Future Generation Computer Systems. 2014;35:102-13. Doi:10.1016/j.future.2013.09.011
48. Thilakanathan D. Secure data sharing and collaboration in the cloud [PhD thesis]. Sidney. University of Sydney;2015.
49. Kelbert F, Pretschner A. Data usage control for distributed systems. ACM Transactions on Privacy and Security (TOPS). 2018; 21(3):12. Doi:10.1145/3183342.
50. Pramod N, Narayan R, Rahul A, Ranjan H, Chandrakala B. Secure data control: Privacy and security based on abe for access control over cloud. International Journal of Research and Engineering. 2017; 4(5):156-60.
51. Munier M, Lalanne V, Ricarde M. Self-protecting documents for cloud storage security.In: Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on; 2012 June 25-27; Liverpool, UK;2:IEEE;2012. Doi:10.1109/TrustCom.2012.261
52. Chen S, Thilakanathan D, Xu D, Nepal S, Calvo R. Self protecting data sharing using generic policies. In:Cluster, Cloud and Grid Computing (CCGrid), 2015 15th IEEE/ACM International Symposium on; 2015 May 4-7; Shenzhen, China;15: IEEE; 2015. Doi:10.1109/CCGrid.2015.84
53. Squicciarini AC, Petracca G, Bertino E In:Bertino E,Sandhu R,editors. Adaptive data protection in distributed systems. Proceedings of the third ACM conference on Data and application security and privacy; 2013 February New York NY United States: ACM;2013. Doi:10.1145/2435349.2435401
54. Chen Y-Y, Lee RB. Hardware-assisted application-level access control. In: Samarati P, Yung M, Martinelli F, Ardagna C.A, editors Information Security. ISC 2009. Lecture Notes in Computer Science;2009 September 7-9;

Pisa, Italy: Springer, 2009.p363-78. Doi:10.1007/978-3-642-04474-8_29
55. Ullah F, Edwards M, Ramdhany R, Chitchyan R, Babar MA, Rashid A. Data exfiltration: A review of external attack vectors and countermeasures. Journal of Network and Computer Applications. 2018; 101:18-54. Doi:10.1007/s10916-018-0966-x
56. Alshiky AM, Buhari SM, Barnawi A. Attribute-based access control (abac) for ehr in fog computing environment. International Journal on Cloud Computing: Services and Architecture (IJCCSA). 2017; 7(1):27-34.
57. Zhao Y, Fan P, Cai H, Qin Z, Xiong H. Attribute-based encryption with non-monotonic access structures supporting fine-grained attribute revocation in m-healthcare. IJ Network Security. 2017; 19(6):1044-52. Doi:0.6633/IJNS.201711.19(6).21.
58. Huang Q, Wang L, Yang Y. Secure and privacy-preserving data sharing and collaboration in mobile healthcare social networks of smart cities. Security and Communication Networks. 2017; 2017. Doi:10.1155/2017/6426495
59. Sheikhtaheri A, Kermani F. Use of mobile apps among medical and nursing students in iran. Stud Health Technol Inform. 2018; 248:33-39. Doi:10.3233/978-1-61499-858-7-33.

Comparison of patient-centric algorithms for health information security in health social networks and cloud environments

Mahin Mohammadi [1] Abbas Sheikhtaheri [2*] Farzaneh Kermani [3]

1. MSc Student, Medical Informatics, Department of Health Information Management, School of Health Management and Information Sciences, Iran University of Medical Sciences. ORCID: 0000-0003-0558-7333
2. Department of Health Information Management, School of Health Management and Information Sciences, Iran University of Medical Sciences.
3. PhD student, Medical Informatics, Department of Health Information Management, School of Health Management and Information Sciences, Iran University of Medical Sciences.

(Received 14 Sep, 2019 Accepted 22 Dec, 2019)

Original Article

Abstract

Aim: Electronic health enables patients share their own medical information and this sharing poses security risks. The purpose of this research is to review, and compare algorithms and methods for solving patient information security, from different aspects, including user revocation, and access control capabilities. The strengths and weaknesses of these algorithms are identified.

Information sources or data: This review conducted using online databases including PubMed, Web of Science, and Science Direct.

Selection methods for study: Keywords including health information systems, computer security, access to information, cloud computing and social networking was used to search. Articles published in 2009 to 2019 were selected. 29 articles related to solving the problem of user revocation and 7 articles related to solving the problem of access control were selected. Related articles were reviewed, then the access control and user revocation solutions were compared.

Combine content and results: To protect the confidentiality of patient information, a cryptographic method is suggested before data sharing. This solution has the problem of revocation of the users. To solve this problem, various methods have been proposed. In this paper, these solutions are compared in different respects. The features of these methods have been compared in terms of instant revocation, key update, cloud free, encrypted text updates, and short revocation. Finally, methods for access control by the patients were also compared.

Conclusion: Security issues associated with health data make patients hesitant to post sensitive health information and share it with health providers. In this paper, algorithms and health information security methods were compared. Most of the solutions to revocation of users need re-encryption methods, also, access control solutions do not have the required flexibility. In the future, better methods should be presented.

Key Words: Health Information Systems, Computer Security, Access to Information, Cloud Computing, Social Networking.

Citation: Mohammadi M, Sheikhtaheri A, Kermani F. Comparison of patient-centric algorithms for health information security in health social networks and cloud environments. J Mod Med Info Sci. 2020; 5(2):68-79.

Correspondence:
Abbas Sheikhtaheri
F Department of Health Information Management, School of Health Management and Information Sciences, Iran University of Medical Sciences.
Tel: +98(021) 88794301 *Email: Sheikhtaheri.a@iums.ac.ir*
ORCID :0000-0002-6879-5415