Sadra Med. Sci. J. 2024; 12(4): 587-598.

Sadra Medical Sciences Journal

https://smsj.sums.ac.ir/

Original Article

Developing a Model for Protecting the Privacy of Internet Customers in the Field of Health

Zahra Sharifi[1*], PhD Candidate; Mohammad Ali Keramati[2], PhD; Mehrzad Minooei[3], PhD

[1]PhD Candidate, Islamic Azad University, Central Tehran branch, Tehran, Iran
[2]Professor, Islamic Azad University, Central Tehran branch, Tehran, Iran
[3]Assistant Professor, Islamic Azad University, Central Tehran branch, Tehran, Iran

Article Information

Article History:
Received: Feb. 26, 2024
Accepted: May 05, 2024

***Corresponding Author:**
Zahra Sharifi, PhD Candidate; PhD Candidate, Islamic Azad University, Central Tehran branch, Tehran, Iran
Email: zahrasharifi22@gmail.com

Abstract

Introduction: Protecting the privacy of internet customers is crucial in the field of health. In this area, there is sensitive and personal information, and privacy can increase customers' trust in companies and create a stronger relationship between them.

Methods: The target sample was chosen using a criterion-oriented purposeful sampling method. The sampling procedure was continued until the theoretical saturation of data was reached. Accordingly, 12 professors and administrators participated in the study. The data collection tool was a semi-structured interview. Nvivo software was used for theme analysis.

Results: Based on the theme analysis method, two constructive themes of level one and 14 themes of level two were identified. Constructive themes of level one were technological infrastructure and obligations of the seller to the consumer. The themes of technological infrastructure were personalization services, social interaction performance, access control, information technology security, security enforcement measures, safety algorithm and data-based planning, and decision making. The constructive themes of the seller's obligations to the consumer were awareness, user and seller education, safety, maintenance and support of information, responsibility, framework and principles, and trust.

Conclusion: The proposed model showed that privacy protection was essential. Medical device businesses should implement a robust privacy policy, closely monitoring access, training employees on privacy protection, and upgrading security systems.

Keywords: Confidentiality, Banking, Personal, Trust, Job security, Internet Use, Health, Electronic health records

Please cite this article as:
Sharifi Z, Keramati MA, Minooei M. Developing a Model for Protecting the Privacy of Internet Customers in the Field of Health. Sadra Med. Sci. J. 2024; 12(4): 587-598.

دوره ۱۲، شماره ۴، پاییز ۱۴۰۳، صفحات ۵۸۷-۵۹۸

مجله علوم پزشکی صدرا

https://smsj.sums.ac.ir/

مقاله پژوهشی

طراحی مدل حفاظت از حریم خصوصی مشتریان اینترنتی حوزه سلامت

زهرا شریفی[۱*]، محمدعلی کرامتی[۲]، مهرزاد مینویی[۳]

[۱]دانشجوی دکتری، گروه مدیریت فناوری اطلاعات، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران
[۲]استاد، گروه مدیریت صنعتی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران
[۳]استادیار، گروه مدیریت مالی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران

اطلاعات مقاله

تاریخچه مقاله:
تاریخ دریافت: ۱۴۰۲/۱۲/۰۷
تاریخ پذیرش: ۱۴۰۳/۰۲/۱۶

***نویسنده مسئول:**
زهرا شریفی
دانشجوی دکتری، گروه مدیریت فناوری اطلاعات، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران
پست الکترونیکی: zahrasharifi22@gmail.com

چکیده

مقدمه: حفظ حریم خصوصی مشتریان اینترنتی در حوزه سلامت از اهمیت بسیار بالایی برخوردار است. حفظ اطلاعات مشتریان می‌تواند اعتماد آن‌ها به شرکت‌ها را افزایش دهد و ارتباط قوی‌تری بین آن‌ها ایجاد کند.

مواد و روش‌ها: ۱۲ نفر از استادان و مدیران از طریق نمونه‌گیری هدفمند از نوع ملاک محور، به عنوان نمونه موردنظر انتخاب شدند و نمونه‌گیری تا رسیدن به حد اشباع نظری داده‌ها ادامه یافت. ابزار گردآوری داده‌ها در این تحقیق، مصاحبه نیمه ساختاریافته بود و در روش تحلیل تم از نرم‌افزار Nvivo نسخه ۲۰ استفاده شد.

یافته‌ها: مدل حفاظت از حریم خصوصی مشتریان اینترنتی در حوزه سلامت نیازمند ترکیب موازی از زیرساخت‌های تکنولوژیکی پیشرفته و تعهدات قوی از سوی فروشندگان است. این ترکیب امکان ارائه خدمات با کیفیت و اطمینان از حفظ حریم خصوصی مشتریان را فراهم می‌سازد. همچنین، نیاز به پایش و ارزیابی مداوم این مدل برای اطمینان از اثربخشی آن و جلوگیری از هرگونه تخلف یا نقض حریم خصوصی وجود دارد. به طور کلی، این مدل می‌تواند به بهبود اعتماد مشتریان به سیستم‌های سلامت دیجیتال کمک کرده و به توسعه پایدار این حوزه کمک نماید.

نتیجه‌گیری: مدل پیشنهادی نشان داد حفاظت از حریم خصوصی در حوزه سلامت ضروری است. ایجاد یک سیاست حریم خصوصی قوی، مدیریت دقیق دسترسی، آموزش کارکنان در زمینه حفاظت از حریم خصوصی و ارتقای فناوری‌های امنیتی ازجمله اقداماتی هستند که شرکت‌های تجهیزات پزشکی باید انجام دهند.

کلمات کلیدی: محرمانه بودن، اعتماد، امنیت شغلی، استفاده از اینترنت، سلامت، پرونده الکترونیک سلامت

لطفاً این مقاله را به این صورت استناد کنید:
شریفی ز، کرامتی م ع، مینویی م. طراحی مدل حفاظت از حریم خصوصی مشتریان اینترنتی حوزه سلامت. مجله علوم پزشکی صدرا. دوره ۱۲، شماره ۴، پاییز ۱۴۰۳، صفحات ۵۸۷-۵۹۸.

مقدمه

در طی همه‌گیری جهانی کرونا، ارگان‌های نظارت بر تجهیزات پزشکی به‌سرعت با شرایط موجود همراه شدند (۱) تا چالش تأمین تجهیزات حفاظت فردی به‌صورت کافی برای ارائه‌دهندگان مراقبت‌های بهداشتی در خط مقدم و تجهیزات نجات‌دهنده زندگی برای افرادی که نیاز پزشکی دارند، برآورده شود (۲، ۳). تولیدکنندگان تجهیزات پزشکی نیز باید با این چالش روبرو می‌شدند و از این فرصت‌ها استفاده می‌کردند تا دستگاه خود را سریع‌تر وارد بازار کنند و به جامعه کمک نمایند تا با خیال راحت از آن‌طرف منحنی کرونایی بیرون بیایند (۴، ۵).

بسیاری از شرکت‌هایی که در دوران پیش از کرونا، ارتباط حضوری با مشتریان، رکن اصلی استراتژی‌های فروش آن‌ها بود حالا پس از کرونا دو سناریو پیش رو داشتند؛ یا باید مغلوب محدودیت‌های پاندمی می‌شدند و ارتباط خود را به‌طور کامل از دست می‌دادند یا راه‌های مدرن‌تر را جایگزین می‌کردند (۶) . نکته مهم این بود که باوجود قطع ارتباطات مؤثر حضوری در دوران کرونا باهدف قطع زنجیره بیماری، مشتریان نباید فراموش و رها می‌شدند (۷). به‌علاوه بسیاری از الگوهای رفتاری مشتریان در این دوره تغییر کرده بود و نیازهای متفاوتی نیز ایجاد شده بود که رد پای آن در هر فعالیتی در فردای بدون کرونا نیز دیده شد و در استراتژی‌های میان‌مدت و بلندمدت بازاریابی شرکت‌ها گنجانده گردید (۸، ۹). با شیوع ویروس کرونا، چنین انتظار می‌رفت که در بخش فروش تجهیزات پزشکی نوساناتی دیده شود و تعداد خریداران با کاهش یا حتی افزایشی غیرقابل‌انتظار روبرو شود (۱۰، ۱۱). همچنین در این ایام نحوه مراودات خریداران با شرکت‌ها، مشکلات اقتصادی و درآمدزایی فروشندگان، تغییر و تحولات فاکتورهای بازاریابی و فروش شرکت‌های تجهیزات پزشکی نیز ابهامات فراوانی داشت (۱۲).

در این میان بنا به نیاز مبرم بیماران و مشتریان به صنعت تجهیزات پزشکی و پاندمی شدن کرونا و ترس از استفاده و یا خرید و مراجعه حضوری از ترس مبتلا شدن، یکی از روش‌های رفع مشکلات موجود در مسیر توزیع عادلانه، سریع و مناسب و محافظت از مشتریان در مقابل بیماری، ارائه آن‌ها به‌صورت اینترنتی و در معرض قرار دادن عموم این تجهیزات پزشکی بود (۱۳). فروشگاه‌های تجهیزات پزشکی، با راه‌اندازی خرید آنلاین و سایت فروش، دسترسی اینترنتی به فروشگاه‌های خود را برای مردم آسان ساختند تا کسانی که ممکن است فقط به‌دلیل تهیه این اقلام مجبور به خروج از خانه شوند بتوانند تجهیزات موردنیاز خود را از طریق ثبت سفارش باقیمتی منصفانه و درزمانی کوتاه‌تر خریداری کنند (۱۴). البته در دنیای تکنولوژی بدون وجود کرونا نیز، فروش این تجهیزات در بسیاری از اقلام با اینترنت صورت می‌گرفت ولی با شیوع کرونا این روند، تسریع گردید (۱۵، ۱۶) .

شایان ذکر است که مسئله مطرح‌شده در حوزه فناوری، ارائه این محصولات و خدمات بخش حوزه امنیت اطلاعات مشتریان و کاربران این مجموعه است که با حجم وسیع مشتریان باید به دنبال روش‌ها و مدل‌هایی برای داشتن محیطی امن برای کاربران در این حوزه تجهیزات پزشکی و فروش و ارائه امکانات از طریق اینترنت برای مشتریان باشند (۱۷, ۱۸) . شاید یکی از دغدغه‌ها و مشکلات مشتریان در این حوزه، عدم توجه به مسئله امنیت اطلاعات از حریم شخصی آن‌ها باشد (۱۹، ۲۰).

از طرف دیگر، اگرچه تعداد کاربران اینترنت به‌طور چشمگیری افزایش یافته است، اما بسیاری از کاربران خرید آنلاین انجام نمی‌دهند. آن‌ها تمایلی به ارائه اطلاعات شخصی و یا اطلاعات معاملاتی برای پرداخت‌های الکترونیکی آنلاین ندارند، زیرا به تجارت الکترونیک اعتماد کافی ندارند (۲۱). اطلاعاتی که می‌تواند محرمانه یا شخص تلقی شود و امکان افشای آن از طریق اینترنت وجود دارد، شامل علائم تجاری، روابط جنسی، امور مذهبی و سیاسی، اطلاعات پزشکی و مالی یا امنیتی و غیره هستند. این اطلاعات که به دلایل مختلف و برای سهولت دسترسی به آن‌ها و یا انتقال به دیگران از سوی شبکه‌های رایانه‌ای حفظ می‌شود، به‌راحتی می‌تواند در اختیار افراد غیر صالح قرار بگیرد و با افشای آن ضررهای هنگفتی به مال یا آبروی افراد وارد آید (۲۲، ۲۳)؛ بنابراین می‌توان گفت حفظ حریم خصوصی مشتریان اینترنتی برای شرکت‌های تجهیزات پزشکی از اهمیت بسیار بالایی برخوردار است. اطلاعات حساس و شخصی مانند تاریخچه بیماری‌ها، اطلاعات پزشکی و حتی اطلاعات مالی در رابطه با بیماران و مشتریان این شرکت‌ها وجود دارد (۲۴، ۲۵). حفظ حریم خصوصی این اطلاعات می‌تواند اعتماد مشتریان را به شرکت‌ها افزایش دهد و ارتباط قوی‌تری بین آن‌ها ایجاد کند. این اعتماد بسیار

حیاتی است زیرا مشتریان به تجربه‌ای امن و خصوصی در ارتباط با اطلاعات پزشکی خود نیاز دارند (۲۶) .

در ایران حق حفاظت از حریم خصوصی را می‌توان در زمره حقوق بنیادین و مسلم بشر دانست و یا به‌عنوان حق شخصیT و ازجمله حقوق مالکیت به‌حساب آورد. به‌خصوص اطلاعات حساس ممکن است از ارتباط مطلق با فرد تا مسائل مهم اجتماعی در جریان باشد. در نهایت مهم‌ترین موضوع در رابطه با حریم خصوصی، ممانعت از استفاده نابجا از اطلاعات شخصی است. متأسفانه در کشور ایران اطلاعات مهم و امنیتی افراد به‌راحتی قابل دسترسی است، اشخاص غیرمجاز می‌توانند بهره‌برداری‌های نادرستی از اطلاعات در جهت جعل یا سرقت هویت، نمایند، از این رو بررسی و تحقیق و توسعه حفظ حریم خصوصی در کشور ایران از ملزومات اصلی توسعه روابط اینترنتی است و ضرورت حفظ حریم خصوصی در زمینه تجهیزات پزشکی به‌دلیل ماهیت بسیار حساس اطلاعات پزشکی روشن‌تر است.

هرگونه نقض یا نادیده گرفتن حریم خصوصی می‌تواند منجر به پیامدهای جدی شود، زیرا نقض حریم شخصی، سوءاستفاده از اطلاعات برای تبلیغات نامطلوب یا حتی دسترسی غیرمجاز به اطلاعات پزشکی، می‌تواند برای بیماران و مشتریان این شرکت‌ها آسیب‌های جدی به همراه داشته باشد. علاوه بر این، رعایت حریم خصوصی مشتریان به‌عنوان یک استاندارد اخلاقی و قانونی در حوزه پزشکی و درمان بسیار حائز اهمیت است. قوانین حفظ حریم خصوصی مانند مقررات عمومی حفاظت از داده‌ها» GDPR[1] در اروپا و قانون قابلیت انتقال و مسئولیت بیمه سلامت HIPAA[2] در ایالات‌متحده، اطمینان می‌دهند که شرکت‌های پزشکی موظف به حفظ حریم خصوصی اطلاعات مشتریان خود هستند. رعایت این قوانین نه‌تنها از دیدگاه اخلاقی بلکه ازلحاظ قانونی نیز ضروری است و عدم رعایت آن‌ها ممکن است منجر به پیامدهای قانونی جدی برای شرکت‌ها شود. بر اساس موارد بیان‌شده این تحقیق به دنبال پاسخی برای این سؤال است که مدل حفاظت از حریم خصوصی مشتریان اینترنتی حوزه سلامت چگونه است؟

مواد و روش‌ها

پژوهش حاضر از نظر رویکرد جزو تحقیقات کیفی و از لحاظ روش، تحلیل تم است.

جامعه آماری

جامعه مورد مطالعه این پژوهش در بخش کیفی، استادان دانشگاه در حوزه مدیریت بازرگانی و مدیران فروشگاه‌های تجهیزات پزشکی بودند.

روش نمونه‌گیری و حجم نمونه

نمونه‌گیری هدفمند و از نوع ملاک محور بود و تا رسیدن به حد اشباع نظری داده‌ها ادامه یافت. مشارکت‌کنندگان در پژوهش ۱۲ نفر از استادان و مدیران فروشگاه‌های تجهیزات پزشکی بودند.

ابزار گردآوری داده‌ها

ابزار گردآوری داده‌ها در این تحقیق، مصاحبه نیمه ساختاریافته بود. فرایند تحلیل داده‌های حاصل از متن مصاحبه‌ها نیز با توجه به اهمیت آن در رویکرد تحلیل تم، هم‌زمان با جمع‌آوری داده‌ها طی سه مرحله کدگذاری باز انجام شد و در قالب مضامین و زیر مقولات طبقه‌بندی گردید (۲۷). درروش تحلیل تم از نرم‌افزار ان وی وو[3] نسخه ۲۰ استفاده‌شده است.

در (جدول ۱) اطلاعات جمعیت شناختی مربوط به مصاحبه‌شوندگان نشان داده شده است. در تحلیل تم، هم‌زمان با گردآوری اطلاعات کدگذاری و تحلیل انجام می‌گیرد. با کدگذاری باز، مضامین زیادی به دست آمد که طی فرایند رفت و برگشتی داده‌ها، مجموع داده‌های کیفی اولیه به مقوله‌های کمتری کاهش یافت. در این مرحله با استفاده از داده‌های خام، مقولات مقدماتی در ارتباط با حریم شخصی مشتریان در فروشگاه‌های تجهیزات پزشکی از طریق مقایسه و واکاوی پدیده‌ها استخراج گردید.

ملاحظات اخلاقی

شرکت‌کنندگان در جریان هدف پژوهش و مراحل اجرای آن قرار گرفتند و از محرمانه بودن اطلاعات خود اطمینان یافتند و به آن‌ها توضیح داده شد که هر زمان که بخواهند، می‌توانند مطالعه را ترک کنند و در صورت تمایل، نتایج پژوهش در اختیار آن‌ها قرار خواهد گرفت، همچنین از شرکت‌کنندگان رضایت‌نامه کتبی اخذ شد.

1. General Data Protection Regulation
2. Health Insurance Portability and Accountability Act
3. Nvivo v20

جدول ۱. اطلاعات جمعیت شناختی

کد مصاحبه شونده	سن (سال)	تحصیلات	جنسیت
۱	۳۷	کارشناسی ارشد	مرد
۲	۴۲	دکتری	مرد
۳	۴۴	دکتری	زن
۴	۴۶	دکتری	مرد
۵	۳۹	کارشناسی ارشد	مرد
۶	۵۱	دکتری	مرد
۷	۴۷	دکتری	زن
۸	۴۸	دکتری	مرد
۹	۵۱	دکتری	مرد
۱۰	۴۸	دکتری	مرد
۱۱	۳۹	کارشناسی ارشد	مرد
۱۲	۵۲	دکتری	مرد

یافته‌ها

تحلیل تم و کدگذاری به روش براون و کلارک[۴]

مرحله اول: آشنایی با داده‌ها

محقق برای آشنایی با عمق و گستره محتوایی داده‌ها باید خود را در آن‌ها غوطه‌ور سازد. این حالت معمولاً شامل بازخوانی مکرر داده‌ها و خواندن داده‌ها به‌صورت فعال (جستجوی معانی و الگوها) است.

مرحله دوم: ایجاد کدهای اولیه

مرحله دوم زمانی شروع می‌شود که محقق داده‌ها را می خواند و با آن‌ها آشنایی پیدا می‌کند. این مرحله شامل ایجاد کدهای اولیه است. از طریق کدها یکی از ویژگی‌های داده‌ها متمایز می شود و به نظر تحلیلگر جالب می‌آید. داده‌های کدگذاری شده متمایز از واحدهای تحلیل (تم‌ها) هستند. کدگذاری را می‌توان به‌صورت دستی یا از طریق برنامه‌های نرم‌افزاری انجام داد. در این پژوهش از روش کدگذاری دستی استفاده شد (جدول ۲).

مرحله سوم: جستجوی کدهای گزینشی

این مرحله شامل دسته‌بندی کدهای مختلف در قالب کدهای گزینشی و مرتب کردن همه خلاصه داده‌های کدگذاری شده است. در واقع محقق، تحلیل کدهای خود را شروع می‌کند و می‌اندیشد که چگونه کدهای مختلف می‌توانند برای ایجاد یک تم کلی ترکیب شوند. در این مطالعه بعد از حذف کدهای ناقص یا نامرتبط و همچنین کدهای تکراری ۱۴ کد گزینشی به دست آمد.

مرحله چهارم: شکل‌گیری تم‌های فرعی (مؤلفه‌ها)

بعد از اینکه محقق مجموعه‌ای از تم‌ها را ایجاد کرد باید آن‌ها را مورد بازبینی قرار دهد. این مرحله شامل دو مرحله بازبینی و تصفیه و شکل‌دهی به تم‌های فرعی است. مرحله اول شامل بازبینی در سطح خلاصه‌های کدگذاری شده است و مرحله دوم اعتبار تم‌های فرعی در رابطه با مجموعه داده‌ها را در نظر می‌گیرد. نتایج حاصل از تحلیل عاملی در این پژوهش نشان داد که از میان ۹۵ شاخص (گویه) موجود، ۱۴ مضمون سازنده سطح دوم و ۲ دسته مضمون سازنده سطح اول هستند.

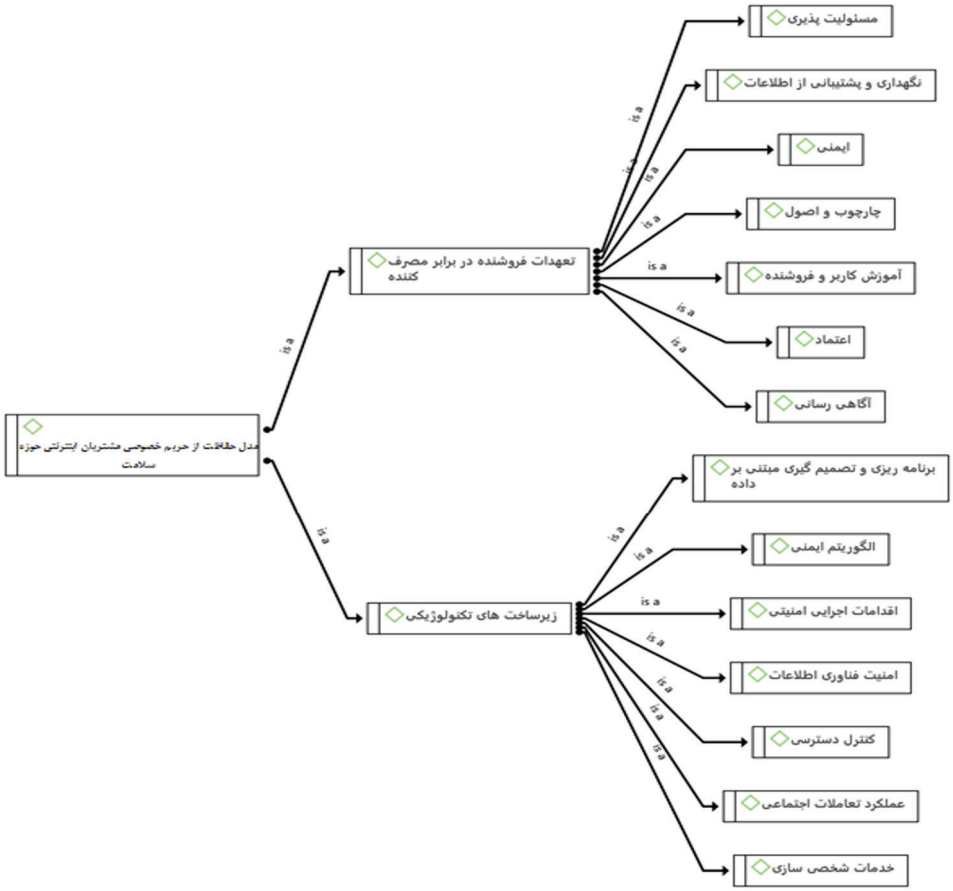
مرحله پنجم: تعریف و نام‌گذاری تم‌های فرعی (بُعدهای اصلی)

مرحله پنجم زمانی شروع می‌شود که یک تصویر رضایت‌بخش از تم‌ها وجود داشته باشد. محقق در این مرحله، تم‌های اصلی را که برای تحلیل ارائه کرده و تعریف نموده بود، بازبینی می‌کند، و داده‌های داخل آن‌ها را تحلیل می‌نماید. به‌وسیله تعریف و بازبینی کردن،

4. Braun & Clarke

جدول ۲. کدهای اولیه مصاحبه با خبرگان

ردیف	نمونه کدهای باز استخراج‌شده	مصاحبه مرتبط
۱	مدیریت مرزهای شخصی	مدیریت مرزهای شخصی به معنای تعیین و مدیریت مرزهای داده‌های شخصی مشتریان است، یعنی اطلاعات حساس به دست کسانی نرسد که نباید به آن‌ها دسترسی داشته باشند.
۲	مدیریت دسترسی	مدیریت دسترسی مرتبط با کنترل دسترسی به اطلاعات و شامل اعطای دسترسی به اطلاعات فقط به کاربران مجاز و مشخص، ازجمله کارکنان مجاز و تأییدشده است.
۳	خدمات دسته‌بندی اطلاعات	خدمات دسته‌بندی اطلاعات که تأکید بر دسته‌بندی و طبقه‌بندی دقیق اطلاعات دارد تا داده‌ها به‌طور صحیح و مطمئن دسته‌بندی شوند و به کاربردهای مشخصی اختصاص یابند.
۴	ترجیح راحتی بر حریم خصوصی	ترجیح راحتی بر حریم خصوصی نشان‌دهنده تمایل به ارائه سرویس‌هایی است که ممکن است به نقض حریم خصوصی منجر شوند و این در تضاد با حریم خصوصی قرار می‌گیرد.
۵	انتخاب راهکارها بر اساس ترجیحات شخصی	انتخاب راهکارها بر اساس ترجیحات شخصی به کاربران اجازه می‌دهد راهکارهای مختلف حفاظت از حریم خصوصی را بر اساس ترجیحات و نیازهای شخصی خود انتخاب کنند که شامل انتخاب سطوح مختلف حفاظتی یا روش‌های مختلف مدیریت حریم خصوصی است.



شکل ۱. مدل حفاظت از حریم خصوصی مشتریان اینترنتی حوزه سلامت

ماهیت آن چیزی که یک تم در مورد آن بحث می‌کند مشخص و تعیین می‌گردد که هر تم اصلی کدام جنبه از داده‌ها را در خود دارد. در این مرحله محقق در نهایت پس از رفت و برگشت در میان تم‌های فرعی به ۱ تم اصلی دست یافت، که در زمینه موردنظر تحقیق قابل تبیین است. در ادامه به برخی از تم‌های فرعی که تم‌های اصلی از آن‌ها استخراج‌شده اشاره می‌شود (جدول ۳).

مرحله ششم: تهیه گزارش

مرحله ششم زمانی شروع می‌شود که محقق مجموعه‌ای از تم‌های اصلی کاملاً انتزاعی و منطبق با ساختارهای زمینه‌ای در تحقیق را در اختیار داشته باشد. این مرحله شامل تحلیل پایانی و نگارش گزارش است. در نهایت الگوی این تحقیق مشتمل بر ۱ مضمون فراگیر و ۲ مضمون سازمان دهنده سطح یک و ۱۴ مضمون سازنده سطح دو و ۹۵ مضمون اولیه بود.

جدول ۳. مضامین نهایی شناسایی‌شده جدول کدهای استخراجی تحلیل مضمون مدل حفاظت از حریم خصوصی مشتریان اینترنتی حوزه سلامت

مضمون فراگیر: حفاظت از حریم خصوصی مشتریان اینترنتی حوزه سلامت		
مضمون سازنده (سطح یک)	مضمون سازنده (سطح دو)	مضمون اولیه
زیرساخت‌های تکنولوژیکی	خدمات شخصی‌سازی	مدیریت مرزهای شخصی مدیریت دسترسی خدمات دسته‌بندی اطلاعات ترجیح راحتی بر حریم خصوصی انتخاب راهکارها بر اساس ترجیحات شخصی برآورده سازی نیازها بر اساس حریم شخصی‌سازی‌شده
	عملکرد تعاملات اجتماعی	تعیین کنترل لازم برای دسترسی اجتماعی همکاری بین سازمان‌ها دسترسی مصرف‌کنندگان به فروشندگان پاسخ‌دهی ۷/۲۴ به مصرف‌کنندگان ترکیب اومنی چنلی در ارائه خدمات و محصولات کنترل ارتباطات با افراد قابلیت پنهان کردن مشخصات کاربری تعامل پنهان با مدیران فروش
	کنترل دسترسی	مدیریت دسترسی کاربر تعیین افراد مجاز برای استفاده از تسهیلات پردازش اطلاعات مسئولیت‌های کاربر کنترل دسترسی به شبکه کنترل دسترسی به سیستم عامل کنترل دسترسی به برنامه‌های کاربردی نظارت بر دسترسی و استفاده از سیستم
	امنیت فناوری اطلاعات	امنیت تجارت الکترونیک انجام آزمون نفوذ نیازهای امنیتی سیستم امنیت سسیتم‌های دارای الکترونیکی امنیت در توسعه و پشتیبانی فرآیندها کنترل‌های رمزنگاری تنظیمات سفارشی‌شده در اکثر برنامه‌ها امنیت فایل‌های سیستمی ایجاد فرآیند امنیتی بومی امنیت مبتنی بر ابر نیازهای امنیتی در قراردادهای منعقده با بیرون سازمان در نظر گرفتن ملاحظات امنیتی در عقد قرارداد
	اقدامات اجرایی امنیتی	امنیت تجهیزات رسانه‌ای در هنگام جابه‌جایی امنیت محیطی و فیزیکی امنیت تجهیزات کنترل‌های عمومی مدیریت عملیات و ارتباطات حفاظت در مقابل نرم‌افزارهای ناسالم مدیریت داخلی: تهیه نسخه پشتیبان از اطلاعات، ثبت عملکرد اپراتور، ثبت خطا مدیریت شبکه مدیریت رسانه و امنیت
	الگوریتم ایمنی	ارزیابی ادواری کاهش نقض اطلاعات و داده‌ها ارزیابی ریسک استخراج داده‌های افراد برای شناسایی رفتار رصد و پاسخ به تهدیدات قوانین ایمنی پلتفرم الگوریتم ایمنی دیجیتالی
	برنامه‌ریزی و تصمیم‌گیری مبتنی برداده	آنالیز رفتاری نگهداری سوابق سرمایه‌های سازمان برنامه‌ریزی و پذیرش سیستم برنامه‌ریزی و پذیرش سیستم سازگاری با ملاحظات قانونی

مضمون فراگیر: حفاظت از حریم خصوصی مشتریان اینترنتی حوزه سلامت		
مضمون سازنده (سطح یک)	مضمون سازنده (سطح دو)	مضمون اولیه
تعهدات فروشنده در برابر مصرف‌کننده	آگاهی‌رسانی	اطلاعات سایبری اطلاعاتی اطلاع‌رسانی در زمینه تغییرات اطلاعات و هشدارهای امنیتی اطلاعات دسترسی و وضعیت موجود معرفی خطرهای ناشی از دسترسی شخص ثالث معرفی راهکارهای مقابله با خطرهای ناشی از دسترسی شخص ثالث اطلاع‌رسانی حساسیت اطلاعات در فضای دیجیتالی
	آموزش کاربر و فروشنده	سرمایه‌گذاری در زمینه آموزش کاربر، فروشنده و مصرف‌کننده طراحی مدل یادگیری و آموزشی مناسب با سایت و شبکه‌های اینترنتی آموزش کاربر پاسخ به حوادث و سوء کارکردهای امنیتی شفافیت و سادگی آموزش
	ایمنی	افزایش ایمنی در برابر هکرها افزایش ایمنی در برابر بات‌ها و ربات‌ها بومی‌سازی ایمنی بر اساس هوش مصنوعی مدیریت بحران در شرایط اضطراری مدیریت تغییر در برابر تغییرات پیش‌بینی‌نشده حفاظت فیزیکی
	نگهداری و پشتیبانی از اطلاعات	هماهنگی در امنیت اطلاعات بازبینی از امنیت اطلاعات، تقسیم مسئولیت‌های امنیت اطلاعات کارشناس مشاور امنیت اطلاعات
	مسئولیت‌پذیری	درک رفتار مشتری در شرایط غیرعادی مدیریت تداوم فعالیت‌های سازمانی مسئولیت‌پذیری اخلاقی و رفتاری مسئولیت‌پذیری در برابر مشکلات سایت مسئولیت‌پذیری در برابر خطای انسانی
	چارچوب و اصول	دریافت مجوزهای مرتبط در زمینه تخصصی (اداره کل تجهیزات پزشکی) مطالعه سیاست‌های حفاظت از حریم خصوصی سرویس‌دهنده‌ها توسعه سیاست‌ها و راهنماها گواهی (سازمان غذا و دارو آمریکا*) و نشان سی‌ای** کد استعلام ایران***» تجهیزات پزشکی دریافت نمادهای اعتماد (نماد صنعت و معدن و تجارت، وزارت ارشاد و تجارت الکترونیک) اعمال حریم خصوصی غیرقابل نفوذ اعمال حریم خصوصی در طراحی سایت
	اعتماد	شفاف‌سازی اطلاعات انتخاب سرویس‌دهنده مورد اعتماد جمع‌آوری و ذخیره امن داده‌ها بروز رسانی مداوم ارائه مستندات مبنی بر ایمنی و عملکرد تجهیزات پزشکی توجه به میزان پذیرش کاربر و مصرف‌کننده توجه به نگرش مصرف‌کننده نسبت به شرکت‌های تجهیزات پزشکی اینترنتی

*Food and Drug Administration of America، **CE marking، ***Iran registration code

بر اساس جدول فوق، الگوی تحقیق مشتمل بر یک مضمون فراگیر و ۲ مضمون سازمان دهنده و ۱۴ مضمون پایه ای بود و در نهایت براساس مقوله های نهایی، مدل پژوهش ارائه شد (شکل ۱):

برای بررسی قابلیت اعتبار، قابلیت انتقال، قابلیت تأیید و اطمینان‌پذیری از چهار معیار کمی استفاده‌شده است: ضریب هولستی[5]، ضریب پی اسکات[6]، شاخص کاپای کوهن[7] و آلفای کریپیندروف[8].

میزان همبستگی دیدگاه خبرگان با محاسبه ضریب هولستی یا «درصد توافق مشاهده‌شده» ۰/۸۲۷ به دست آمده است که مقدار قابل توجهی است. با توجه به ایراداتی که به روش هولستی وارد است شاخص پی-اسکات نیز محاسبه شد و میزان آن ۰/۷۳۳ به دست آمد. چهارمین شاخص برآورد اعتبار

5. Holstie
6. Scott's pi
7. Capai kohen
8. Kerpindrof

تحقیقات کیفی شاخص کاپای کوهن است. شاخص کاپای کوهن در این مطالعه ۰/۷۵۴ به دست آمد و در نهایت نیز از آلفای کرپیندروف استفاده شد و میزان آن ۰/۸۲۶ برآورد گردید.

بحث

در عصر مجازی و دهکدهٔ جهانی، تبادلات و ارتباطات الکترونیکی شروع به جایگزین شدن کرده‌اند و ما را وارد شبکه جدید و گسترده‌ای از روابط مجازی ساخته‌اند که چالش‌ها و امکانات و احتمالات جدیدی را با خود به همراه دارد. یکی از مسائل مهمی که در حوزه عصر مجازی مطرح می‌شود، بحث حریم خصوصی است.

تحقیقات زیادی برای اطمینان از حریم شخصی انجام شده‌اند که همگی در بعد علمی (فناوری) و رفتاری قرار می‌گیرند. معروف‌ترین آن‌ها پژوهش وانگ[9] و همکاران (۲۰۰۹) است که در آن پشتیبانی داده‌ها به‌صورت پویا و صریح (واضح-روشن) مطرح‌شده است و در رایانش ابر[10] قابل انجام است. در کنار ایجاد حریم شخصی در این روش، کاهش سربار ذخیره‌سازی در مقایسه با تکنیک‌های توزیع مبتنی بر تکرار سنتی نیز دیده می‌شود (۲۸). مدل دیگری با نام اثبات بازیابی است که برای حصول اطمینان از یکپارچگی داده‌ها از راه دور توسط جولز و کالیسکی [11] (۲۰۰۷) مطرح شده است. طرح آن‌ها ترکیبی از دو روش (تست) چک کردن نقطه و کد تصحیح خطا برای اطمینان از هر دو مالکیت (در اختیار داشتن) و بازیابی فایل‌ها در آرشیو (بایگانی) یا سیستم‌های خدمات پشتیبان است، و یک تابع خطی تصادفی مبتنی بر تأییدکننده اتبار، آن را قادر می‌سازد تا به تعداد نامحدودی از پرس‌وجوها دسترسی داشته باشد و در نتیجه نیاز به سربار ارتباطاتی کمتری باشد (۲۹) که تاکنون طرحی کارآمد و انعطاف‌پذیر بوده است. همچنین، برای اطمینان از حفظ حریم خصوصی، استانداردهای مختلف برای رمزگذاری داده‌ها و کلید رمزنگاری وجود دارد. برای داده‌ها، سیستم متکی بر قدرت طرح رمزگذاری (پروتکل پاسخ چالش) و خاصیت دانش صفر است که پروتکلی برای حسابرسی کلید رمزنگاری محسوب می‌شود (۳۰). در بعد رفتاری یا الگوهای رفتاری حفاظت از حریم شخصی، جهت‌گیری حریم خصوصی (۳۱) با چهار مقیاس حریم خصوصی تحت عناوین حق قانونی، نگرانی در مورد حریم اطلاعات شخصی، حریم ارتباط با دیگران، و نگرانی در مورد حریم خصوصی دیگران مطرح‌شده است، که در کل به معنای تعاریف حریم خصوصی در اینترنت و موارد مشابه با آن بحث می‌شوند. در موارد دیگر شفافیت و یکپارچگی به‌عنوان الگوهای رفتاری حفاظت از حریم خصوصی در نظر گرفته شده‌اند که در آن هر فرد باید امکان واقعی دانستن اینکه چه کسی، چگونه، و برای چه هدفی به اطلاعات دسترسی دارد را داشته باشد، علاوه بر این، فرد باید از افرادی که به داده‌ها دسترسی دارند و داده‌ها برای آن‌ها فاش می‌شود، اطلاعات داشته باشد (۱۶).

از نظر لیویس و کافمن[12] (۲۰۱۰) گسترش ارائه خدمات و محصولات به‌صورت اینترنتی به شکل‌های مختلف، منجر به شکل‌گیری مطالعاتی گشته است که عمده نگرانی آن‌ها به حفظ امنیت اطلاعاتی برمی‌گردد (۴). امروزه، مطالعات در مورد نگرش‌ها و رفتار حفظ حریم خصوصی در شبکه‌های اجتماعی، اساساً بر تفاوت‌های فردی در حفظ حریم خصوصی و افشای اطلاعات متمرکز است. نظر به اینکه در عصر جدید، اینترنت باعث برقراری پیوندهای مختلفی در سراسر دنیا شده است، طبیعتاً نوعی نگرانی در مورد مداخله در فضای خصوصی افراد از طریق همین پیوند اینترنتی به وجود می‌آید و این امر دغدغه ما را برای ساختن ابزارهایی در جهت بررسی و حفظ این حریم خصوصی اینترنتی بیشتر می‌کند (۳۲)، در این میان جامعهٔ ما از این دنیای اینترنتی گسترده مستثنی نیست و باید خود را با آن همگام سازد، اما متاسفانه تابه‌حال ابزاری جهت سنجش ابعاد حریم خصوصی اینترنتی در ایران وجود نداشته و نیاز به هنجاریابی چنین ابزاری به‌شدت حس می‌شود. ابراز عقیده محققان و صاحب‌نظران بر وجود شکاف علمی در زمینه حفاظت از اطلاعات شخصی در بخش بازاریابی، فروش و ارائه محصولات و خدمات، مؤید این سخن است (۳۱).

محدودیت‌های پژوهش

- از آنجا که اکثر خبرگان در پاسخگویی و مصاحبه‌ها نسبت به مسائل امنیتی و سیاسی و داخلی صنعت سلامت نگاه محتاطانه‌ای دارند، به نظر می‌رسد که در بسیاری از پاسخ‌ها در مقوله عوامل محیطی به‌عنوان عوامل مداخله‌گر یا در مقوله صنعت سلامت در بخش عوامل زمینه‌ای جواب شخصی نداده و بیشتر بر اساس سنجش جوانب مختلف، ارائه پاسخ

9. Wang
10. Cloud computing
11. Jolse, kaliscy
12. Loise, kafman

داشته‌اند.

- دسترسی کامل به فروشندگان محصولات پزشکی با توجه به پراکندگی مکان آن‌ها وجود نداشت.

پیشنهادات پژوهش

بر اساس مدل ارائه‌شده، پیشنهاد می‌شود در طراحی اپلیکیشن و سایت با توجه به حریم خصوصی، در مرحله طراحی و توسعه نرم‌افزار یا وب‌سایت، احترام به حریم خصوصی کاربران حتماً در نظر گرفته شود. بهبود روابط کاربری و توضیحات واضح در خصوص جمع‌آوری داده‌ها می‌تواند اعتماد کاربران را افزایش دهد. همچنین با توجه به حساسیت بالای اطلاعات پزشکی، ضروری است که داده‌ها به‌طور کامل و امن ذخیره شوند. ایجاد سیستم‌های پشتیبانی قوی و استفاده از روش‌های رمزنگاری مناسب ازجمله اقداماتی است که می‌تواند در این بخش کمک کند. همچنین پیشنهاد می‌شود افرادی که با داده‌های حساس کار می‌کنند، در زمینه حریم خصوصی و تدابیر امنیتی آموزش داده شوند. آگاهی کارکنان از رویه‌ها و استفاده صحیح از سیستم‌های حفاظتی، می‌تواند خطرات ناشی از نقض حریم خصوصی را کاهش دهد. با رعایت این نکات و توجه به جوانب حساس حریم خصوصی، شرکت‌های ارائه‌دهنده خدمات حوزه سلامت می‌توانند راهکارهای مؤثری برای حفاظت از حریم خصوصی مشتریان اینترنتی ارائه کنند و اعتماد آنان را جلب نمایند.

نتیجه‌گیری

هدف تحقیق طراحی مدل حفاظت از حریم خصوصی مشتریان اینترنتی حوزه سلامت بود. بر اساس روش تحلیل تم، ۲ مضمون سازنده سطح یک و ۱۴ مضمون سطح دو شناسایی شد. مضمون‌های سازنده سطح یک عبارت‌اند از زیرساخت‌های تکنولوژیکی و تعهدات فروشنده در برابر مصرف‌کننده. استفاده از فناوری‌های پیشرفته و امنیتی، ازجمله رمزنگاری داده‌ها، سیستم‌های دسترسی ورودی، مکانیسم‌های شناسایی دقیق و حفاظت از داده‌های حساس بسیار حیاتی است، این زیرساخت‌های تکنولوژیکی باید توانایی مقابله با تهدیدات امنیتی را داشته باشند و حریم خصوصی را حفظ کنند، تعهدات فروشنده به مصرف‌کننده نیز اهمیت بالایی دارد. شرکت‌های ارائه‌دهنده خدمات حوزه سلامت باید تعهداتی نسبت به حفظ حریم خصوصی مشتریان خود داشته باشند. این تعهدات شامل استفاده از داده‌ها با اجازه مشتری، عدم انتقال داده‌های حساس به شخص ثالث بدون رضایت و اطمینان از حفظ محرمانگی و امنیت اطلاعات می‌شود.

برای اطمینان از حفظ اطلاعات حساس مشتریان اینترنتی در حوزه سلامت، زیرساخت‌های تکنولوژیکی در مدل حفاظت از حریم خصوصی مشتریان، نقش کلیدی دارند. این زیرساخت‌ها شامل استفاده از رمزنگاری قوی، سرورهای امن، نرم‌افزارهای ضد هک و سایر فناوری‌های مرتبط است که امکان دسترسی غیرمجاز به اطلاعات را به حداقل می‌رسانند. همچنین، تعهدات فروشندگان نقش بسیار مهمی در این مدل دارند. این تعهدات شامل حفظ محرمانگی اطلاعات مشتری، استفاده معقولانه از داده‌ها، اطمینان از امنیت سیستم‌های خود و پیروی از استانداردهای حریم خصوصی می‌شود، ازاین‌رو، همکاری مؤثر بین فناوران و فروشندگان با مشتریان و ارائه خدمات با رعایت حریم خصوصی، به‌عنوان پایه اصلی موفقیت در این مدل محسوب می‌شود. در نتیجه، مدل حفاظت از حریم خصوصی مشتریان اینترنتی در حوزه سلامت نیازمند ترکیب موازی از زیرساخت‌های تکنولوژیکی پیشرفته و تعهدات قوی فروشندگان است. این ترکیب امکان ارائه خدمات با کیفیت و اطمینان از حفظ حریم خصوصی مشتریان را فراهم می‌سازد، همچنین نیاز به پایش و ارزیابی مداوم این مدل برای اطمینان از اثربخشی آن و جلوگیری از هرگونه تخلف یا نقض حریم خصوصی به شکل جدی احساس می‌شود؛ به‌طورکلی، این مدل می‌تواند به بهبود اعتماد مشتریان به سیستم‌های سلامت دیجیتال و توسعه پایدار این حوزه، کمک نماید.

تضاد منافع

هیچ‌گونه تضاد منافعی وجود ندارد.

منابع

1. Degerli M. Privacy issues in data-driven health care. Data-Driven Approach for Biomedical and Healthcare. 2022:23-37.
2. Iadanza E, Cerofolini S, Lombardo C, Satta F, Gherardelli M. Medical devices nomenclature systems: a scoping review. Health and Technology. 2021;11:681-92.
3. Hutchings E, Loomes M, Butow P, Boyle FM. A systematic literature review of health consumer attitudes towards secondary use and sharing of health administrative and clinical trial data: a focus on privacy, trust, and transparency. Syst Rev. 2020;9(1):235.
4. Labaf A, Jalili M, Jaafari Pooyan E, Mazinani M. Management of Covid-19 Crisis in Tehran University of Medical Sciences Hospitals: Challenges and Strategies. Journal of School of Public Health and Institute of Public Health Research. 2021;18(4):355-72. [Persian].
5. Maher A, Malmir R, Toghyani R, Safari MS. COVID-19 Crisis Management: Reengineering the Health Care System in Iran. Journal of Medical Council of Islamic Republic of Iran. Medical Research Organization. 2020;38(1):11-8. [Persian].
6. Motti VGBS. Healthcare Privacy. In: Knijnenburg BP, Page X, Wisniewski P, Lipford HR, Proferes N, Romano J, editors. Modern Socio-Technical Perspectives on Privacy. Cham: Springer: 2022. p. 203-31.
7. Löhr H, Sadeghi A-R, Winandy M, editors. Securing the e-health cloud. Proceedings of the 1st acm international health informatics symposium; 2010.
8. Mehdi B. Presenting and analyzing the methods of connecting light users to the blockchain network with privacy protection: Sharif University of Technology; 2021. [Persian].
9. Boerman SC, Kruikemeier S, Zuiderveen Borgesius FJ. Exploring motivations for online privacy protection behavior: Insights from panel data. Communication Research. 2021;48(7):953-77.
10. Dey N, Ashour AS, Bhatt C. Internet of things driven connected healthcare. Internet of things and big data technologies for next generation healthcare. 2017:3-12.
11. Hartigan L, Cussen L, Meaney S, O'Donoghue K. Patients' perception of privacy and confidentiality in the emergency department of a busy obstetric unit. BMC health services research. 2018;18:1-6.
12. Degerli M, Ozkan Yildirim S. Identifying critical success factors for wearable medical devices: a comprehensive exploration. Universal Access in the Information Society. 2022;21(1):121-43.
13. Batarseh FA, Ghassib I, Chong D, Su P-H. Preventive healthcare policies in the US: solutions for disease management using Big Data Analytics. Journal of big Data. 2020;7(1):38.
14. Hwang H-G, Lin Y. Evaluating people's concern about their health information privacy based on power-responsibility equilibrium model: A case of Taiwan. Journal of Medical Systems. 2020;44(6):112.
15. Khalajzadeh MR, Vatankhah Yazdi K, Malekpoor Z, Moosavi A, Ebadnezami R, Movahed M. The challenges of supervising medical laboratories in Corona pandemy. Laboratory & Diagnosis. 2022;14(56):13-22. [Persian].
16. Knijnenburg BP, Page X, Wisniewski P, Lipford HR, Proferes N, Romano J. Modern socio-technical perspectives on privacy: Springer Nature; 2022.
17. Alghanim AA, Rahman SMM, Hossain MA, editors. Privacy analysis of smart city healthcare services. 2017 IEEE International Symposium on Multimedia (ISM); 2017:394-8.
18. Dhasarathan C, Shanmugam M, Kumar M, Tripathi D, Khapre S, Shankar A. A nomadic multi-agent based privacy metrics for e-health care: a deep learning approach. Multimedia Tools and Applications. 2024;83(3):7249-72.
19. Hahanov V, Miz V, editors. Big data driven healthcare services and wearables. Lviv: The Experience of Designing and Application of CAD Systems in Microelectronics; 2015.
20. Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big healthcare data: preserving security and privacy. Journal of big data. 2018;5(1):1-18.
21. Mekovec R. Online privacy: overview and preliminary research. Journal of information and organizational sciences. 2010;34(2):195-209.

22. Kuacharoen P, editor A practical customer privacy protection on shared servers. Beijing: 2010 IEEE International Conference on Information Theory and Information Security; 2010
23. Gupta B, Chennamaneni A. Understanding Online Privacy Protection Behavior of the Older Adults: An Empirical Investigation. J Inf Technol Manag. 2018;29(3):1-13.
24. Lorenzen-Huber L, Boutain M, Camp LJ, Shankar K, Connelly KH. Privacy, technology, and aging: A proposed framework. Ageing International. 2011;36:232-52.
25. Meingast M, Roosta T, Sastry S, editors. Security and privacy issues with health care information technology. 2006 international conference of the IEEE engineering in medicine and biology society; 2006: p. 5453–8.
26. Chaki J. Introduction to digital future of healthcare. Digital Future of Healthcare: CRC Press; 2021. p. 1-10.
27. Khaki G. Research method with an approach to thesis writing. Tehran: Fujan Publications; 2020. [Persian].
28. Ganjavi R. Privacy Preserving Cloud Assisted Crowdsensed Data Analysis. Tehran: Tarbiat Modares Faculty; 2023. [Persian].
29. Modirnia Y, Vazifehdoust H, Abdolvand MA. Presenting the behavioral model of customers in the level of acceptance and the way of using electronic banking services with the development and analysis of the UTAUT theory. Journal of Development and Transformation Management. 2021;12(43):1-18. [Persian].
30. O T. Presenting a cooperative learning-based privacy-preserving method for indoor localization. Tehran: Shahid Beheshti University; 2020. [Persian].
31. Nasiri S, Sadoughi F, Tadayon MH, Dehnad A. Security and privacy mechanisms of internet of things in healthcare and non-healthcare industry. Journal of Health Administration. 2020;22(4):86-105. [Persian].
32. F N. Providing an end-to-end encrypted structure in smart city systems to protect users' privacy and security. Kashan: Kashan University; 2023. [Persian].