Sadra Med. Sci. J. 2026; 14(1): 207-225.

Sadra Medical Sciences Journal

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

Original Article

Developing a Fuzzy Interpretive Structural Model for Customer Privacy Protection in Online Healthcare Businesses

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

[1]Department of Information Technology Management, Faculty of Management, Central Tehran Azad University, Tehran, Iran
[2]Department of Financial Management, Faculty of Management, Central Tehran Azad University, Tehran, Iran
[3]Information Technology Management, Faculty of Management, Central Tehran Azad University, Tehran, Iran

Article Information

Article History:
Received: November 12, 2025
Accepted: February 01, 2026

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

Abstract

Introduction: With the rapid expansion of medical and healthcare services in the virtual space, safeguarding the confidentiality of users' personal information has emerged as a fundamental and critical challenge. This study aimed to design a structured model for protecting consumer privacy in the field of electronic health, utilizing an integrated approach combining interpretive structural modeling and fuzzy logic.

Methods: This research was conducted with a participant pool comprising university professors and managers of medical equipment stores, employing purposive sampling with 12 participants. The research instrument was a researcher-designed questionnaire, and the data were analyzed using the fuzzy Delphi method with the assistance of MATLAB and MICMAC software.

Results: The findings identified 14 key components—including information technology security, access control, personalization services, and trust—which were organized in a seven-level hierarchical model. The results of the fuzzy interpretive structural modeling (FISM) indicated that certain factors acted as drivers and accelerators, while others were more influenced by these driving factors. Consequently, focusing on the driving factors could lead to the improvement of other system indicators.

Conclusion: The research findings indicated that the issue of privacy in the online health space was multidimensional and requires simultaneous attention to technical, managerial, and behavioral aspects. The proposed model could serve as a practical guide for managers of online health stores to increase customer trust by prioritizing security measures. It could also assist policymakers in developing more precise regulations for the protection of healthcare data. The integration of technical strategies with managerial and behavioral approaches could contribute to the enhancement of user privacy and security.

Keywords: Privacy; Equipment and Supplies; Digital Health; Decision Support Techniques; Models, Theoretical

Please cite this article as:
Sharifi Z, Keramati MA, Minooei M. Developing a Fuzzy Interpretive Structural Model for Customer Privacy Protection in Online Healthcare Businesses. Sadra Med. Sci. J. 2026; 14(1): 207-225. doi: 10.30476/smsj.2026.104746.1583.

دوره ۱۴، شماره ۱، بهار ۱۴۰۵، ۲۰۷-۲۲۵.

مجله علوم پزشکی صدرا

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

مقاله پژوهشی

ارائه مدل فازی حفاظت از حریم خصوصی مشتریان در کسب‌وکارهای اینترنتی حوزه سلامت با استفاده از مدلسازی ساختاری تفسیری

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

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

اطلاعات مقاله

تاریخچه مقاله:
تاریخ دریافت: ۱۴۰۳/۰۸/۲۲
تاریخ پذیرش: ۱۴۰۴/۱۱/۱۲

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

چکیده

مقدمه: با گسترش روزافزون خدمات پزشکی و بهداشتی بر بستر فضای مجازی، موضوع حفظ محرمانگی اطلاعات شخصی کاربران به یک چالش اساسی و حیاتی تبدیل شده است. هدف از این پژوهش، طراحی یک الگوی ساختاریافته برای صیانت از حریم خصوصی مصرف‌کنندگان در عرصه سلامت الکترونیک با بهره‌گیری از روش تلفیقی مدل‌سازی تفسیری-ساختاری و منطق فازی است.

مواد و روش‌ها: این پژوهش با جامعه‌ای شامل اساتید دانشگاه و مدیران فروشگاه‌های تجهیزات پزشکی انجام شد و از ۱۲ نفر به‌صورت نمونه‌گیری هدفمند بهره برده است. ابزار تحقیق پرسشنامه محقق‌ساخته است و اطلاعات با استفاده از روش دلفی فازی و نرم‌افزارهای MATLAB و MICMAC تحلیل شده است.

یافته‌ها: بر اساس نتایج به‌دست‌آمده، ۱۴ عامل کلیدی مؤثر شناسایی شد. این عوامل در قالب یک مدل سلسله‌مراتبی ۷ سطحی سازماندهی شدند. خروجی حاصل از مدل‌سازی تفسیری-ساختاری فازی (FISM) نشان داد برخی از عوامل نقش پیشبرنده و محرک داشته در حالی که برخی دیگر بیشتر تحت تأثیر قرار می‌گیرند؛ در نتیجه تمرکز بر عوامل پیشران می‌تواند به ارتقاء سایر شاخص‌های سیستم انجامد.

نتیجه گیری: یافته‌های پژوهش حاکی از آن است که مقوله حریم خصوصی در فضای سلامت آنلاین دارای ابعاد چندگانه بوده و مستلزم توجه همزمان به جنبه‌های فنی، مدیریتی و رفتاری است. الگوی پیشنهادی می‌تواند به عنوان راهنمایی عملی برای مدیران فروشگاه‌های اینترنتی حوزه سلامت مورد استفاده قرار گیرد تا با اولویت‌بندی اقدامات امنیتی، سطح اعتماد مشتریان را افزایش دهند. همچنین این مدل به سیاست‌گذاران کمک می‌کند تا مقررات دقیق‌تری برای حفاظت از داده‌های بهداشتی-درمانی تدوین نمایند. تلفیق راهبردهای فنی با رویکردهای مدیریتی و رفتاری می‌تواند منجر به ارتقاء حریم خصوصی و امنیت کاربران شود.

کلمات کلیدی: حریم خصوصی، تجهیزات و ملزومات، سلامت دیجیتال، تکنیک‌های حمایت از تصمیم‌گیری، مدل‌های نظری

لطفاً این مقاله را به این صورت استناد کنید:
شریفی ز، کرامتی م ع، مینویی م. ارائه مدل فازی حفاظت از حریم خصوصی مشتریان در کسب‌وکارهای اینترنتی حوزه سلامت با استفاده از مدلسازی ساختاری تفسیری. مجله علوم پزشکی صدرا. دوره ۱۴، شماره ۱، بهار ۱۴۰۵، ۲۰۷-۲۲۵.

مقدمه

فناوری‌های سلامت دیجیتال، که می‌توانند به‌عنوان برنامه‌ها و نرم‌افزارهای مورد استفاده در سیستم بهداشت و مراقبت تعریف شوند، به‌طور فزاینده های در حال پیشرفت هستند. این فناوری‌ها، طیف عظیمی از محصولات و خدمات سیستمی بر مبنای فناوری اطلاعات سطح بالا را پشتیبانی می‌کنند (۱).

دستگاه‌های مراقبت‌های بهداشتی (به دستگاه‌های پزشکی اطلاق می‌شوند که علائم حیاتی بیماران را بررسی می‌کنند) قابلیت بهبود تشخیص و درمان آنی و دقیق بیماری را دارند. این دستگاه‌ها به مراقبت‌های پزشکی اجازه میدهند نه‌تنها در محیط های بالینی سنتی، بلکه در خانه‌ها، محل کار و مکان های سفر نیز نفوذ کنند. به این ترتیب، پزشکی مشارکتی، بار مؤسسات مراقبت‌های بهداشتی فیزیکی را کاهش میدهد و در عین حال مراقبت‌هایی را به بیماران ارائه میدهد که با زندگی روزمره آنها ادغام می‌شود. دستگاه‌ها می‌توانند بیماران را برای دفاع از خود، کنترل و مراقبت از خود و تصمیم‌گیری آگاهانه‌تر در مورد سلامتی خود توانمند کنند. مراقبت‌های بهداشتی دیجیتال همچنین راه‌های جدیدی را برای تسهیل پیشگیری و مدیریت بیماری‌های مزمن در سطح جمعیت ارائه می‌دهد (۲).

طبق تعریف سازمان غذا و دارو (FDA) حوزه گسترده سلامت دیجیتال شامل مقوله‌هایی مانند mHealth به معنی استفاده از تکنولوژی‌های موبایل و بی‌سیم (Wireless) و فناوری اطلاعات سلامت، دستگاه‌ها و ابزارهای پوشیدنی، بهداشت از راه دور، پزشکی از راه دور، و پزشکی فردی می‌باشد(۳). در واقع سلامت دیجیتال کاربرد فناوری اطلاعات و ارتباطات (ICT) برای تبادل اطلاعات پزشکی است. این برنامه‌ها به شدت بر داده‌های سلامت انسان تکیه دارند. معمولاً جمع آوری داده‌های بهداشتی توسط دستگاه‌های پزشکی دارای مجوز رسمی، مانند ابزار های تشخیصی یا توالی سنجی ژنوم انجام می‌شود که توسط متخصصان بهداشت در محیط‌های بالینی و تحت شرایط نظارتی سختگیرانه اداره می‌شوند. علاوه بر این، داده‌های بالینی به طور معمول در لیست‌های بهداشت عمومی، در بیمارستان‌ها و یا در آرشیو پزشکان شخصی ذخیره می‌شوند(۴).

حریم خصوصی مشتریان اینترنتی در حوزه سلامت یکی از موضوعات حساس و حیاتی است که با گسترش خدمات آنلاین و دیجیتالی شدن اطلاعات، اهمیت آن به‌طور فزاینده‌ای افزایش یافته است (۵). اطلاعات شخصی بیماران، شامل جزئیات پزشکی، سوابق درمانی، و اطلاعات شناسایی، باید به‌گونه‌ای مدیریت شود، که اطمینان حاصل شود این اطلاعات در برابر دسترسی‌های غیرمجاز، سرقت داده‌ها و سوءاستفاده‌ها محافظت می‌شود. حفظ محرمانگی اطلاعات به معنای رعایت اصول اخلاقی و قانونی در حفظ داده‌های بیمار است (۶). در حوزه سلامت، این موضوع به دلیل ماهیت حساس داده‌ها و اثرات منفی احتمالی ناشی از افشای آن‌ها، به ویژه اهمیت دارد (۷). در زمینه خدمات اینترنتی سلامت، مانند پرونده‌های الکترونیکی و مشاوره‌های آنلاین، وجود سازوکارهای امنیتی از قبیل رمزنگاری داده ها، احراز هویت دو مرحله ای، و محافظت از دسترسی‌های غیر مجاز نقش مهمی در حفاظت از حریم خصوصی دارد. همچنین، سیستم‌های درمانی باید به استانداردهای بین‌المللی مانند HIPAA (در ایالات متحده) و GDPR (در اروپا) پایبند باشند. این مقررات قانونی الزامات مشخصی را برای حفظ حریم خصوصی و امنیت داده‌ها تعیین می‌کنند، که شامل محدودیت در اشتراک‌گذاری داده‌ها، ردیابی هر گونه دسترسی به پرونده‌ها، و اخذ رضایت آگاهانه بیماران قبل از استفاده از اطلاعات شخصی آن‌ها است (۸).

در این وضعیت، مسئله مطرح شده در حوزه فناوری ارائه این محصولات و خدمات بخش حوزه امنیت اطلاعات مشتریان و کاربران این مجموعه است که با حجم وسیع مشتریان عنوان‌شده، 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 بود (۹ و ۱۰). چراکه یکی از دغدغه‌ها و مشکلات مشتریان در این حوزه، شاید عدم توجه به مسئله امنیت اطلاعات از بعد حریم شخصی آن‌ها باشد (۱۱ و ۱۲). اگرچه تعداد کاربران اینترنت به‌طور قابل ملاحظه 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 آن‌ها به تجارت الکترونیک اعتماد ندارند (۱۳). به‌طور خاص اطلاعاتی که می‌تواند محرمانه یا شخص تلقی شود و امکان افشای آن از طریق اینترنت هست عبارت‌اند از: علائم تجاری، روابط جنسی، امور مذهبی و سیاسی، اطلاعات پزشکی و

مالی یا امنیتی و غیره، 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 غیرصالح قرار بگیرد و با افشای آن ضررهای هنگفتی به مال یا آبروی افراد وارد آید (۱۴ و ۱۵).

امروزه عرضه فراگیر و عادلانه مراقبت‌ها و خدمات سلامت بخش انکارناپذیر حکمرانی تلقی می‌شود که کما بیش همه کشورها با اولویت بالا به این موضوع می‌پردازند با نفوذ غیر قابل مقاومت ابزارها و شیوه‌های دیجیتالی به ابعاد گوناگون زندگی بشری خدمات مربوط به سلامت هم به اجبار و حتی با اشتیاق از دیجیتالی شدن بهره برده اند. نکته مهم فرایند دیجیتالی شدن آن است که الکترونیکی شدن خدمات سلامت تنها به معنی تغییر شیوه‌های دستی و غیرالکترونیکی به جایگزین دیجیتال آنها نیست. به دنبال نفوذ تدریجی الگوهای دیجیتال به لایه‌های مختلف مدیریت و عرضه خدمات بهداشتی، ضرورت‌ها و راهبردهای نوینی نمایان می‌شوند که پیش از دیجیتالی شدن به ذهن دست اندرکاران خطور نمی کرده است (۱۶).

مدل حفاظت از حریم خصوصی مشتریان اینترنتی در حوزه سلامت با رویکرد مدلسازی ساختاری تفسیری فازی[1] به دنبال شناسایی و اولویت بندی عوامل مؤثر بر حفاظت از حریم خصوصی است. این روش به عنوان یک رویکرد سیستماتیک، با استفاده از تکنیک‌های فازی و ساختار تفسیری، به تبیین روابط میان عوامل مختلف می‌پردازد. در این مدل، ابتدا عوامل کلیدی مانند امنیت اطلاعات، کنترل دسترسی، اعتماد کاربران، سیاست‌های حریم خصوصی، و ایمنی داده‌ها شناسایی می‌شوند. سپس، به کمک تکنیک‌های فازی، میزان عدم قطعیت و ابهامات موجود در قضاوت‌های مربوط به این عوامل مدیریت می‌شود تا ارتباطات پیچیده میان آن‌ها روشن‌تر گردد.

بدین ترتیب با عنایت به مطالب پیشگفت و با توجه به این که استقرار فناوری سلامت دیجیتال مزایای بسیاری را برای بخش سلامت کشور به ارمغان می‌آورد، توجه بدان در زمان حاضر و در سطح ملی ضروری به‌نظر می‌رسد؛ و از آنجایی که یکی از چالش‌های امروزه سازمان‌ها این است که چگونه بتوانند با استفاده از خدمات هوشمند در فروشگاه‌های زنجیره‌ای، مدل‌های کاری جدید و سودمندی را به‌دست آورند، لازم است محققان و مدیران در شناسایی مدل‌ها و استراتژی‌های فوق همکاری نمایند.

علاوه بر آن به منظور بهره‌مندی از فناوری‌های روز و استقرار گسترده‌ی خدمات هوشمند در بخش سلامت کشور و برای این که موضوع مذکور بتواند به‌عنوان فرایندی مهم و مورد توجه، به حرکت رو به جلوی خود ادامه دهد نیازمند الگویی مشخص جهت پیاده‌سازی هستیم، و در این‌راستا به منظور ایجاد یک تحول دیجیتالی در این بخش از کشور لازم است توجهی همه جانبه بر روی تمامی ابعاد سیستم فوق صورت پذیرد.

مدلسازی ساختاری تفسیری فازی به تصمیم‌گیران کمک می‌کند تا سلسله مراتب و روابط میان این عوامل را به‌طور دقیق‌تری درک کنند و بتوانند برای بهبود حریم خصوصی، اقدامات مناسبی اتخاذ کنند. این مدل قابلیت تفسیر روابط علت و معلولی بین عوامل را فراهم می‌کند و با کاهش عدم قطعیت‌ها، به ایجاد چارچوبی کارآمدتر برای سیاست‌گذاری و مدیریت داده‌های پزشکی آنلاین می‌پردازد. به این ترتیب، سازمان‌ها می‌توانند با بهره‌گیری از این رویکرد، راهکارهای مناسبی را برای ارتقای سطح حفاظت از داده‌های کاربران و افزایش اعتماد عمومی در زمینه خدمات پزشکی آنلاین توسعه دهند.

با وجود تلاش‌های محدود و پراکنده‌ای که تاکنون در این راستا در سطح کشور صورت گرفته است، پرداختن به این موضوع در قالب طراحی و تبیین یک مدل در قالب تغییرات ساختاری و فرایندی در لایه‌های مختلف سیستم سلامت کشور، به‌عنوان کمبودی جدی در سطح جامعه کنونی تلقی می‌شود و پژوهش حاضر به دنبال پرکردن این خلأ با ارایه مدلی برای اولین بار در بخش سلامت ایران با توجه به شرایط بومی کشور می‌باشد.

بنابراین این پژوهش به دنبال پاسخی برای این سوال است که مدل حفاظت از حریم خصوصی مشتریان اینترنتی حوزه سلامت با رویکرد مدلسازی ساختاری تفسیری فازی چگونه است؟

سلامت دیجیتال

سلامت دیجیتال، به نوبه خود، مستلزم اتصال داده‌های مرتبط با سلامت، از جمله داده‌های تولید شده توسط خود بیماران، و استفاده از پتانسیل پزشکی ابزارهای فناوری رایج، مانند تلفن‌های هوشمند، نوارهای سلامتی، برنامه‌ها، رسانه‌های اجتماعی و دستگاه‌های حسگر است که در محیط

1. (Fuzzy Interpretive Structural Modeling)

زندگی ما منتشر شده‌اند (۱۷). بیشتر این ابزارها در ابتدا برای استفاده پزشکی طراحی نشده‌اند و به‌عنوان ابزار پزشکی به بازار عرضه نمیشوند. برخی از ابزارهای سلامت دیجیتال ویژگی‌های کاملاً جدیدی دارند، مانند قرص‌های دیجیتالی که به لطف یک ریزمدار فعال در هنگام تماس با مایعات در معده بیمار، می‌توانند به حسگر خارجی بفهماند که آیا بیمار داروی خود را مصرف کرده است یا خیر (۱۸). با این حال، ویژگی تعیین کننده سلامت دیجیتال به‌جای فناوری، به داده‌ها مربوط می‌شود. چیزی که در مورد سلامت دیجیتال از این نظر متمایز است، این است که معمولاً از طریق دستگاه‌های پوشیدنی، قابل حمل، قابل بلع یا کاشتن، جریان یکپارچه داده های پزشکی حیاتی بین بیماران، خانواده‌ها و پزشکان‌شان ایجاد می‌شود (۱۹). بنابراین، سلامت دیجیتال به‌عنوان گردش داده از بیماران (داده‌های تولیدشده توسط بیمار) ، به دستگاه‌ها و یا متخصصان سلامت (که داده‌ها را تجزیه وتحلیل و معنا می‌کنند)، و سپس بازگشت به دستگاه‌های مورد نظر که توصیف کننده داده‌ها می‌باشد معنا می‌شود که در نهایت اطلاعات و درمان‌هایی که مورد نیاز بیمار می‌باشد توصیه و مدیریت می‌شود (۲۰).

شرکت‌های تجهیزات پزشکی

شرکت‌های تجهیزات پزشکی به شرکت‌هایی اشاره دارد که فعالیت خود را در زمینه طراحی، تولید، توسعه، و توزیع تجهیزات، دستگاه‌ها، و محصولات مرتبط با صنعت پزشکی انجام می‌دهند (۲۱). این شرکت‌ها ممکن است به صورت گسترده در زمینه‌های مختلف پزشکی فعالیت داشته باشند ازجمله تجهیزات پزشکی تشخیصی و درمانی، وسایل پزشکی، دستگاه‌های پزشکی تصویربرداری، و تکنولوژی‌های پیشرفته مرتبط با صنعت بهداشت و درمان.

این شرکت‌ها معمولاً با هدف ارائه و توسعه فناوری‌های نوین و بهبود فرآیندهای درمانی و تشخیصی در حوزه پزشکی فعالیت می‌کنند. آن‌ها تلاش می‌کنند تا تجهیزات پزشکی را بهبود بخشند، نوآوری‌های جدیدی ارائه دهند و به پیشرفت‌های علمی و پزشکی کمک کنند. این شرکت‌ها ممکن است به صورت تخصصی در زمینه‌های مختلف مانند جراحی، پزشکی عفونی، تصویربرداری پزشکی، دیالیز، تجهیزات بیهوشی و... فعالیت داشته باشند و محصولات خود را به اساس نیازها و تقاضای بازار به ارمغان بیاورند (۲۲).

حفاظت از حریم خصوصی

حریم خصوصی مشتریان اینترنتی به معنای حفاظت از اطلاعات شخصی و حساس کاربران در برابر سوءاستفاده‌ها (۲۳)، دسترسی‌های غیرمجاز، و افشاهای ناآگاهانه است. این مفهوم در دنیای دیجیتال اهمیت ویژه‌ای یافته است، به‌ویژه زمانی که افراد از اینترنت برای انجام تراکنش‌های مالی، خریدهای آنلاین، و یا حتی دریافت خدمات پزشکی استفاده می‌کنند (۲۴ و ۲۵). اطلاعاتی که در این فرآیندها رد و بدل می‌شوند، شامل داده‌های حساس مانند اطلاعات شناسایی، سوابق خرید، اطلاعات بانکی، و حتی داده‌های مربوط به سلامت است. این داده‌ها در معرض خطرهایی چون هک، نقض امنیتی و استفاده‌های غیرمجاز قرار دارند و نیاز به محافظت جدی دارند. اولین گام در حفظ حریم خصوصی مشتریان اینترنتی، شفافیت در جمع‌آوری و استفاده از داده‌ها است. شرکت‌ها و سرویس‌دهندگان آنلاین باید سیاست‌های روشن و شفافی در خصوص جمع‌آوری، ذخیره سازی و پردازش اطلاعات مشتریان خود داشته باشند (۲۶ و ۲۷).کاربران باید آگاه باشند که چه نوع اطلاعاتی از آنها جمع‌آوری می‌شود، این اطلاعات چگونه استفاده خواهند شد و چه اشخاص یا سازمان‌هایی به آن‌ها دسترسی خواهند داشت. اصولی مانند "رضایت آگاهانه" در این فرآیند کلیدی است، به این معنا که کاربران باید به طور واضح و آگاهانه با جمع‌آوری و استفاده از داده‌هایشان موافقت کنند. این امر از بسیاری از چالش‌های قانونی و اخلاقی جلوگیری می‌کند (۲۸).

حفاظت از حریم خصوصی به مجموعه‌ای از اقدامات، سیاست‌ها، و فرآیندهایی اشاره دارد که به منظور حفظ و محافظت از اطلاعات شخصی و حساس افراد اتخاذ می‌شود سائورا و همکاران (۲۹). این اطلاعات می‌توانند اطلاعات شخصی مانند نام، آدرس، شماره تماس، اطلاعات مالی، اطلاعات پزشکی و هر نوع اطلاعاتی که می‌تواند به‌صورت مستقیم یا غیرمستقیم به یک شخص خاص مرتبط شود، باشند (۳۰).

حفاظت از حریم خصوصی بر اساس احترام به حقوق فردی و اطمینان افراد درباره استفاده صحیح و محافظت از اطلاعات خود انجام می‌شود (۳۱). این مفهوم شامل مجموعه‌ای از استانداردها، سیاست‌ها، و فرآیندهای فنی و سازمانی است که به شرکت‌ها، سازمان‌ها، و دولت‌ها کمک می‌کند تا اطلاعات شخصی

جدول ۱. اطلاعات جمعیت شناختی

کد	سن	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

را محافظت کرده و از دسترسی غیرمجاز، استفاده نادرست، یا انتشار غیرقانونی آن‌ها جلوگیری کنند (۳۲). اهمیت حفاظت از حریم خصوصی به دلیل رشد فناوری و دیجیتالی شدن زندگی روزمره بسیار افزایش یافته است. با ذخیره و پردازش بیشتر اطلاعات در دنیای دیجیتال، تضمین امنیت و محرمانگی اطلاعات شخصی افراد از اهمیت بیشتری برخوردار شده و حفظ این حریم خصوصی ازلحاظ فنی، قانونی و اخلاقی ضروری است (۳۳).

مواد و روش‌ها

این پژوهش از لحاظ هدف‌کاربردی، از لحاظ ماهیت اکتشافی است که بر اساس روش‌آمیخته (کیفی و کمی) انجام شده است. در تهیه مولفه‌های مؤثر بر حریم خصوصی مشتریان اینترنتی حوزه سلامت از روش مطالعات اسنادی و روش دلفی فازی استفاده شده است. انتخاب تیم دلفی، با روش نمونه‌گیری هدفمند از نوع قضاوتی بوده است. در بخش کیفی جامعه مورد مطالعه این پژوهش اساتید دانشگاه در حوزه مدیریت بازرگانی و مدیران فروشگاه‌های تجهیزات پزشکی بودند. از طریق نمونه گیری هدفمند، از نوع ملاک محور، نمونه موردنظر انتخاب و نمونه‌گیری تا رسیدن به حد اشباع نظری داده‌ها ادامه یافت. ازاین رو مشارکت‌کنندگان در پژوهش شامل ۱۲نفر از اساتید و مدیران بود (۳۴). در جدول ۱، اطلاعات جمعیت شناختی مربوط به مصاحبه شوندگان نشان داده شده است. در تحلیل تم، هم زمان با گردآوری اطلاعات کدگذاری و تحلیل انجام می‌گیرد. با کدگذاری باز، مضامین زیادی به دست آمد که طی فرایند رفت و برگشتی داده‌ها، مجموعهٔ 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.

در پردازش اطلاعات از روش تحلیل اثرات متقابل ساختاری در نرم‌افزار MICMAC استفاده‌شده است. درنتیجه پایش متغیرها، ۱۴ مولفه بر مبنای مطالعات کتابخانه‌ای شناسایی و خوشه‌بندی‌شده است (جدول ۲).

در جدول ۳ طیف فازی دلفی مشخص شده است.

یافته ها

در این تحقیق از تکنیک دلفی فازی برای ارزیابی و برازش ۱۴ مولفه شناسایی شده استفاده شده است. دیدگاه ۱۲ خبره پیرامون هر شاخص در جدول ۴ نمایش داده شده است:

در گام بعدی باید دیدگاه خبرگان تجمیع شود.

جدول ۲. نمادگذاری مولفه ها

نماد	مولفه
C01	خدمات شخصی‌سازی
C02	عملکرد تعاملات اجتماعی
C03	کنترل دسترسی
C04	امنیت فناوری اطلاعات
C05	اقدامات اجرایی امنیتی
C06	الگوریتم ایمنی
C07	برنامه‌ریزی و تصمیم‌گیری مبتنی برداده
C08	آگاهی‌رسانی
C09	آموزش کاربر و فروشنده
C10	ایمنی
C11	نگهداری و پشتیبانی از اطلاعات
C12	مسئولیت‌پذیری
C13	اعتماد
C14	چارچوب و اصول

جدول ۳. طیف هفت درجه فازی برای ارزش‌گذاری شاخص‌ها

متغیر زبانی	مقدار فازی	مقیاس عدد فازی
کاملاً بی اهمیت	$\tilde{1}$	(۰/۱ ,۰ ,۰)
خیلی بی اهمیت	$\tilde{2}$	(۰/۳ ,۰/۱ ,۰)
بی اهمیت	$\tilde{3}$	(۰/۵ ,۰/۳ ,۰/۱)
متوسط	$\tilde{4}$	(۰/۷۵ ,۰/۵ ,۰/۳)
بااهمیت	$\tilde{5}$	(۰/۹ ,۰/۷۵ ,۰/۵)
خیلی بااهمیت	$\tilde{6}$	(۱ ,۰/۹ ,۰/۷۵)
کاملاً با اهمیت	$\tilde{7}$	(۱ ,۱ ,۰/۹)

در این مطالعه برای فازی‌زدایی از روش مرکز سطح به صورت زیر استفاده می‌شود:

$$DF_{ij} = \frac{[(u_{ij} - l_{ij}) + (m_{ij} - l_{ij})]}{3} + l_{ij}$$

سه راند دلفی انجام شد. در نهایت در دور سوم هیچ سوالی حذف نشد که این خود نشانه‌ای برای پایان راندهای دلفی است. بطور کلی یک رویکرد برای پایان دلفی آن است که میانگین امتیازات سوالات دو راند آخر با یک‌دیگر مقایسه شوند. در صورتیکه اختلاف بین دو مرحله از حد آستانه خیلی کم (۰/۲) کوچکتر باشد در این صورت فرایند نظرسنجی متوقف می‌شود.

براساس نتایج مندرج در جدول ۵ مشخص گردید که در تمامی موارد اختلاف کوچکتر از ۰/۲ است بنابراین می‌توان راندهای دلفی را به پایان برد.

در ادامه برای تحلیل داده‌ها نیز از روش مدل‌سازی ساختاری تفسیری در نرم‌افزار MICMAC استفاده شده است. طراحی مدل ساختاری تفسیری (ISM) روشی است برای بررسی اثر هر یک از متغیرها بر روی متغیرهای دیگر؛ این طراحی رویکردی فراگیر

جدول ۴. فازی سازی دیدگاه پنل خبرگان برای هریک از شاخص‌های تحقیق

فازی‌سازی	خبره ۱	خبره ۲	خبره ۳	...	خبره ۱۲
C1	(۱ ,۰/۹ ,۰/۷۵)	(۱ ,۰/۹ ,۰/۷۵)	(۰/۷۵ ,۰/۵ ,۰/۳)	...	(۱ ,۱ ,۰/۹)
C2	(۰/۵ ,۰/۳ ,۰/۱)	(۰/۹ ,۰/۷۵ ,۰/۵)	(۱ ,۱ ,۰/۹)	...	(۱ ,۱ ,۰/۹)
C3	(۱ ,۰/۹ ,۰/۷۵)	(۱ ,۱ ,۰/۹)	(۱ ,۱ ,۰/۹)	...	(۱ ,۱ ,۰/۹)
C4	(۰/۹ ,۰/۷۵ ,۰/۵)	(۱ ,۱ ,۰/۹)	(۱ ,۱ ,۰/۹)	...	(۱ ,۱ ,۰/۹)
C5	(۰/۹ ,۰/۷۵ ,۰/۵)	(۱ ,۱ ,۰/۹)	(۰/۹ ,۰/۷۵ ,۰/۵)	...	(۰/۹ ,۰/۷۵ ,۰/۵)
C6	(۰/۵ ,۰/۳ ,۰/۱)	(۰/۹ ,۰/۷۵ ,۰/۵)	(۱ ,۰/۹ ,۰/۷۵)	...	(۱ ,۰/۹ ,۰/۷۵)
C7	(۱ ,۰/۹ ,۰/۷۵)	(۱ ,۱ ,۰/۹)	(۱ ,۱ ,۰/۹)	...	(۱ ,۱ ,۰/۹)
C8	(۰/۱ ,۰ ,۰)	(۰/۹ ,۰/۷۵ ,۰/۵)	(۱ ,۱ ,۰/۹)	...	(۱ ,۰/۹ ,۰/۷۵)
C9	(۱ ,۰/۹ ,۰/۷۵)	(۰/۹ ,۰/۷۵ ,۰/۵)	(۰/۵ ,۰/۳ ,۰/۱)		(۱ ,۰/۹ ,۰/۷۵)
C10	(۱ ,۰/۹ ,۰/۷۵)	(۰/۷۵ ,۰/۵ ,۰/۳)	(۱ ,۱ ,۰/۹)		(۰/۹ ,۰/۷۵ ,۰/۵)
C11	(۱ ,۰/۹ ,۰/۷۵)	(۰/۹ ,۰/۷۵ ,۰/۵)	(۱ ,۰/۹ ,۰/۷۵)		(۱ ,۱ ,۰/۹)
C12	(۱ ,۰/۹ ,۰/۷۵)	(۱ ,۱ ,۰/۹)	(۱ ,۰/۹ ,۰/۷۵)		(۱ ,۱ ,۰/۹)
C13	(۱ ,۱ ,۰/۹)	(۱ ,۰/۹ ,۰/۷۵)	(۱ ,۱ ,۰/۹)		(۱ ,۱ ,۰/۹)
C14	(۱ ,۱ ,۰/۹)	(۱ ,۱ ,۰/۹)	(۱ ,۰/۹ ,۰/۷۵)	...	(۱ ,۱ ,۰/۹)

جدول ۵. اختلاف نتایج راند دوم و سوم

	نتیجه راند سوم	نتیجه راند دوم	اختلاف	نتیجه
C1	۰/۷۴۴	۰/۷۷۶	۰/۰۳۲	پذیرش
C2	۰/۷۹۴	۰/۹۰۴	۰/۱۱	پذیرش
C3	۰/۹۲۵	۰/۷۳۸	۰/۱۸۷	پذیرش
C4	۰/۸۷۵	۰/۹۲۸	۰/۰۵۳	پذیرش
C5	۰/۷۷۶	۰/۷۷۷	۰/۰۰۱	پذیرش
C6	۰/۹۰۴	۰/۸۰۳	۰/۱۰۱	پذیرش
C7	۰/۷۳۸	۰/۸۴۷	۰/۱۰۹	پذیرش
C8	۰/۹۲۸	۰/۸۲۷	۰/۱۰۱	پذیرش
C9	۰/۷۷۷	۰/۸۹۶	۰/۱۱۹	پذیرش
C10	۰/۸۰۳	۰/۷۵۲	۰/۰۵۱	پذیرش
C11	۰/۸۹۰	۰/۹۳۲	۰/۰۴۲	پذیرش
C12	۰/۹۱۸	۰/۸۷۲	۰/۰۴۶	پذیرش
C13	۰/۸۶۶	۰/۸۹۲	۰/۰۲۶	پذیرش
C14	۰/۹۳۲	۰/۹۲۸	۰/۰۰۴	پذیرش

برای سنجش ارتباط است و این طراحی برای توسعهٔ چارچوب مدل به‌کار می‌رود تا اهداف کلی تحقیق امکان‌پذیر شود.

نخستین گام در مدل‌سازی ساختاری-تفسیری محاسبه روابط درونی شاخص‌ها است. جهت انعکاس روابط درونی میان شاخص‌ها از دیدگاه خبرگان استفاده می‌شود.

جدول ۶. حالت‌ها و علائم مورد استفاده در بیان رابطه متغیرها

نماد	AR	SR	FR	LR	UN
رابطه	کاملا مرتبط	به شدت مرتبط	نسبتا مرتبط	ارتباط کم	بی ارتباط
عدد مثلثی	(۱، ۱، ۰/۷۵)	(۱، ۰/۷۵، ۰/۵)	(۰/۷۵، ۰/۵، ۰/۲۵)	(۰/۵، ۰/۲۵، ۰)	(۰/۲۵، ۰، ۰)

جدول ۷. ماتریس دریافتی متغیرهای پژوهش

SSIM	C01	C02	C03	C04	C05	C06	C07	C08	C09	C10	C11	C12	C13	C14
C01	AR	SR	SR	LR	LR	AR	SR	SR	SR	SR	LR	LR	SR	AR
C02	UN	AR	LR	LR	LR	LR	LR	SR	AR	SR	LR	LR	SR	LR
C03	UN	FR	AR	LR	LR	LR	AR	SR	SR	SR	LR	LR	SR	LR
C04	FR	FR	FR	AR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR
C05	FR	FR	FR	UN	AR	SR	SR	SR	SR	SR	AR	AR	SR	SR
C06	FR	FR	FR	UN	UN	AR	SR	SR	SR	SR	SR	LR	SR	AR
C07	UN	FR	FR	UN	UN	UN	AR	SR	SR	SR	LR	LR	SR	LR
C08	UN	UN	UN	UN	UN	UN	UN	AR	LR	SR	LR	LR	SR	LR
C09	FR	UN	UN	UN	UN	UN	UN	UN	AR	SR	LR	LR	SR	LR
C10	UN	UN	UN	UN	UN	UN	UN	UN	UN	AR	AR	LR	LR	AR
C11	FR	FR	FR	UN	FR	FR	FR	FR	FR	FR	FR	AR	AR	SR
C12	FR	FR	FR	UN	FR	FR	FR	FR	FR	FR	FR	FR	AR	SR
C13	UN	UN	UN	UN	UN	UN	UN	UN	UN	UN	UN	UN	AR	LR
C14	FR	FR	FR	UN	UN	FR	FR	FR	FR	FR	FR	UN	FR	AR

ماتریس بدست آمده در این گام نشان می‌دهد یک متغیر بر کدام متغیرها تأثیر دارد و از کدام متغیرها تأثیر می‌پذیرد. بطور مرسوم برای شناسایی الگوی روابط عناصر از نمادهایی مانند جدول ۶ استفاده می‌شود.

ماتریس خودتعاملی ساختاری از ابعاد و شاخص‌های مطالعه و مقایسه آنها با استفاده از چهار حالت روابط مفهومی تشکیل می‌شود. اطلاعات حاصله بر اساس متد مدل‌سازی ساختاری تفسیری جمع بندی و ماتریس خودتعاملی ساختاری نهایی تشکیل می‌گردد. با توجه به علائم مندرج در جدول ۶ ماتریس خودتعاملی ساختاری بصورت جدول ۷ خواهد بود.

ماتریس دریافتی از تبدیل ماتریس خود تعاملی ساختاری به یک ماتریس دو ارزشی صفر و یک بدست می‌آید. در ماتریس دریافتی درایه‌های قطر اصلی برابر یک قرار می‌گیرد. بنابراین ماتریس دریافتی تکنیک ISM در جدول ۸ ارائه شده است.

در این قسمت ابتدا به فازی زدایی کردن ماتریس پرداخته می‌شود. در این تحقیق مانند قسمت دلفی از تکنیک مرکز ثقل استفاده شده است. اندیس i به فرد خبره اشاره دارد. به طوری که

- X_{ij}: مقدار ارزیابی خبره i ام از معیار j ام
- L_j: حداقل مقدار ارزیابی‌ها برای معیار j ام
- M_j: میانگین هندسی مقدار ارزیابی‌خبرگان از عملکرد معیار j ام
- U_j: حداکثر مقدار ارزیابی‌ها برای معیار j ام

در این مطالعه از روش میانگین فازی استفاده شده است. معمولا می‌توان تجمیع میانگین اعداد فازی مثلثی و ذوزنقه‌ای را توسط یک مقدار قطعی که بهترین میانگین مربوطه است، خلاصه کرد. این عملیات را فازی‌زدایی گویند. روش‌های متعددی برای فازی زدایی وجود دارد. در بیشتر موارد برای فازی‌زدایی از روش ساده زیر استفاده می‌شود:

$$\pi_{ij} = \frac{L_j + M_j + U_j}{3}$$

$$if\ \pi_{ij} \geq t \rightarrow \pi_{ij} = 1, \pi_{ji} = 0$$

$$if\ \pi_{ij} < t \rightarrow \pi_{ij} = 0, \pi_{ji} = 1$$

بنابراین ماتریس دریافتی متغیرهای پژوهش در جدول ۹ ارائه شده است.

$$M = (A + I)^n \qquad A + I$$

جدول ۸. ماتریس خودتعاملی ساختاری SSIM

SSIM	C01	C02	C03	C04	C05	C06	C07	C08	C09	C10	C11	C12	C13	C14
C01	(۱، ۱، ۱) (۰/۷۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۰/۵) ۰/۲۵، (۰)	(۰/۵) ۰/۲۵، (۰)	(۱، ۱) (۰/۷۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۰/۵) ۰/۲۵، (۰)	(۰/۵) ۰/۲۵، (۰)	(۱) ۰/۷۵، (۰/۵)	(۱، ۱، ۱) (۰/۷۵)
C02	(۰/۲۵) ۰، ۰)	(۱، ۱) (۰/۷۵)	(۰/۵) ۰/۲۵، (۰)	(۰/۵) ۰/۲۵، (۰)	(۰/۵) ۰/۲۵، (۰)	(۰/۵) ۰/۲۵، (۰)	(۰/۵) ۰/۲۵، (۰)	(۱) ۰/۷۵، (۰/۵)	(۱، ۱) (۰/۷۵)	(۱) ۰/۷۵، (۰/۵)	(۰/۵) ۰/۲۵، (۰)	(۰/۵) ۰/۲۵، (۰)	(۱) ۰/۷۵، (۰/۵)	(۰/۵) ۰/۲۵، (۰)
C03	(۰/۲۵) ۰، ۰)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۱، ۱) (۰/۷۵)	(۰/۵) ۰/۲۵، (۰)	(۰/۵) ۰/۲۵، (۰)	(۰/۵) ۰/۲۵، (۰)	(۱، ۱) (۰/۷۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۰/۵) ۰/۲۵، (۰)	(۰/۵) ۰/۲۵، (۰)	(۱) ۰/۷۵، (۰/۵)	(۰/۵) ۰/۲۵، (۰)
C04	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۱، ۱) (۰/۷۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)
C05	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۲۵) ۰، ۰)	(۱، ۱) (۰/۷۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱، ۱) (۰/۷۵)	(۱، ۱) (۰/۷۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)
C06	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۱، ۱) (۰/۷۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۰/۵) ۰/۲۵، (۰)	(۰/۵) ۰/۲۵، (۰)	(۱) ۰/۷۵، (۰/۵)	(۱، ۱، ۱) (۰/۷۵)
C07	(۰/۲۵) ۰، ۰)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۱، ۱) (۰/۷۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۰/۵) ۰/۲۵، (۰)	(۰/۵) ۰/۲۵، (۰)	(۱) ۰/۷۵، (۰/۵)	(۰/۵) ۰/۲۵، (۰)
C08	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۱، ۱) (۰/۷۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)	(۰/۵) ۰/۲۵، (۰)	(۰/۵) ۰/۲۵، (۰)	(۱) ۰/۷۵، (۰/۵)	(۰/۵) ۰/۲۵، (۰)
C09	(۰/۲۵) ۰، ۰)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۱، ۱) (۰/۷۵)	(۱) ۰/۷۵، (۰/۵)	(۰/۵) ۰/۲۵، (۰)	(۰/۵) ۰/۲۵، (۰)	(۱) ۰/۷۵، (۰/۵)	(۰/۵) ۰/۲۵، (۰)
C10	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۱، ۱) (۰/۷۵)	(۰/۵) ۰/۲۵، (۰)	(۰/۵) ۰/۲۵، (۰)	(۰/۵) ۰/۲۵، (۰)	(۱، ۱، ۱) (۰/۷۵)
C11	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۲۵) ۰، ۰)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۱، ۱) (۰/۷۵)	(۱، ۱) (۰/۷۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)
C12	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۲۵) ۰، ۰)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۱، ۱) (۰/۷۵)	(۱) ۰/۷۵، (۰/۵)	(۱) ۰/۷۵، (۰/۵)
C13	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۱، ۱) (۰/۷۵)	(۰/۵) ۰/۲۵، (۰)
C14	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۲۵) ۰، ۰)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۰/۲۵) ۰، ۰)	(۰/۲۵) ۰، ۰)	(۰/۷۵) ۰/۵، (۰/۲۵)	(۱، ۱، ۱) (۰/۷۵)

جدول ۹. ماتریس دسترسی نهایی متغیرهای پژوهش

SSIM	C01	C02	C03	C04	C05	C06	C07	C08	C09	C10	C11	C12	C13	C14
C01	۱	۱	۱	۰	۰	۱	۱	۱	۱	۱	۰	۰	۱	۱
C02	۰	۱	۰	۰	۰	۰	۰	۱	۱	۱	۰	۰	۱	۰
C03	۰	۱	۱	۰	۰	۰	۱	۱	۱	۱	۰	۰	۱	۰
C04	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱
C05	۱	۱	۱	۰	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱
C06	۱	۱	۱	۰	۰	۱	۱	۱	۱	۱	۰	۰	۱	۱
C07	۰	۱	۱	۰	۰	۰	۱	۱	۱	۱	۰	۰	۱	۰
C08	۰	۰	۰	۰	۰	۰	۰	۱	۰	۱	۰	۰	۱	۰
C09	۰	۱	۰	۰	۰	۰	۰	۱	۱	۱	۰	۰	۱	۰
C10	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۱
C11	۱	۱	۱	۰	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱
C12	۱	۱	۱	۰	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱
C13	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۱	۰
C14	۱	۱	۱	۰	۰	۱	۱	۱	۰	۱	۰	۰	۱	۱

ماتریس A ماتریس دسترسی اولیه ماتریس همانی و ماتریس دسترسی نهایی است. عملیات به توان رساندن ماتریس طبق قوانین بولین[۲] صورت می‌گیرد.
1×1=1; 1+1=1

بنابراین برای اطمینان باید روابط ثانویه کنترل شود. به این معنا که اگر A منجر به B شود و B منجر به C شود در این صورت باید A منجر به C شود. یعنی اگر براساس روابط ثانویه باید اثرات مستقیم لحاظ شده باشد اما در عمل رخ نداده باشد باید جدول ۸ تصحیح شود و رابطه ثانویه را نیز نشان داد. ماتریس دسترسی نهایی متغیرهای پژوهش در جدول ۹ ارائه شده است.

تعیین روابط و سطح‌بندی ابعاد و شاخص‌ها

برای تعیین روابط و سطح‌بندی معیارها باید مجموعه خروجی‌ها و مجموعه ورودی‌ها برای هر معیار از ماتریس دریافتی استخراج شود.

❖ مجموعه دستیابی (عناصر سطر، خروجی یا اثرگذاری‌ها): متغیرهایی که از طریق این متغیر می‌توان به آنها رسید.

❖ مجموعه پیش‌نیاز (عناصر ستون، ورودی یا اثرپذیری‌ها): متغیرهایی که از طریق آنها می‌توان به این متغیر رسید.

مجموعه خروجی‌ها شامل خود معیار و معیارهایی است که از آن تأثیر می‌پذیرد. مجموعه ورودی‌ها شامل خود معیار و معیارهایی است که بر آن تأثیر می‌گذارند. سپس مجموعه روابط دو طرفه معیارها مشخص می‌شود (جدول ۱۰).

براساس سطح بندی انجام شده در نرم افزار میک مک، ۷ سطح برای مولفه‌های شناسایی شده مشخص شده است. در شکل خروجی نرم افزار میک مک نشان داده شده است. براساس در شکل سطح بندی مرتب شده، مدل ساختاری تفسیری بیان شده است (شکل ۱).

بنابراین (C10-C13) سطح آخر یا وابسته است. پس از شناسایی متغیرها سطح اول این متغیرها حذف می‌شوند و مجموعه ورودی‌ها و خروجی‌ها بدون درنظر گرفتن متغیرهای سطح اول محاسبه می‌شود. مجموعه مشترک شناسایی و متغیرهایی که اشتراک آنها برابر مجموعه ورودی‌ها باشد به عنوان متغیرهای سطح دوم انتخاب می‌شوند.

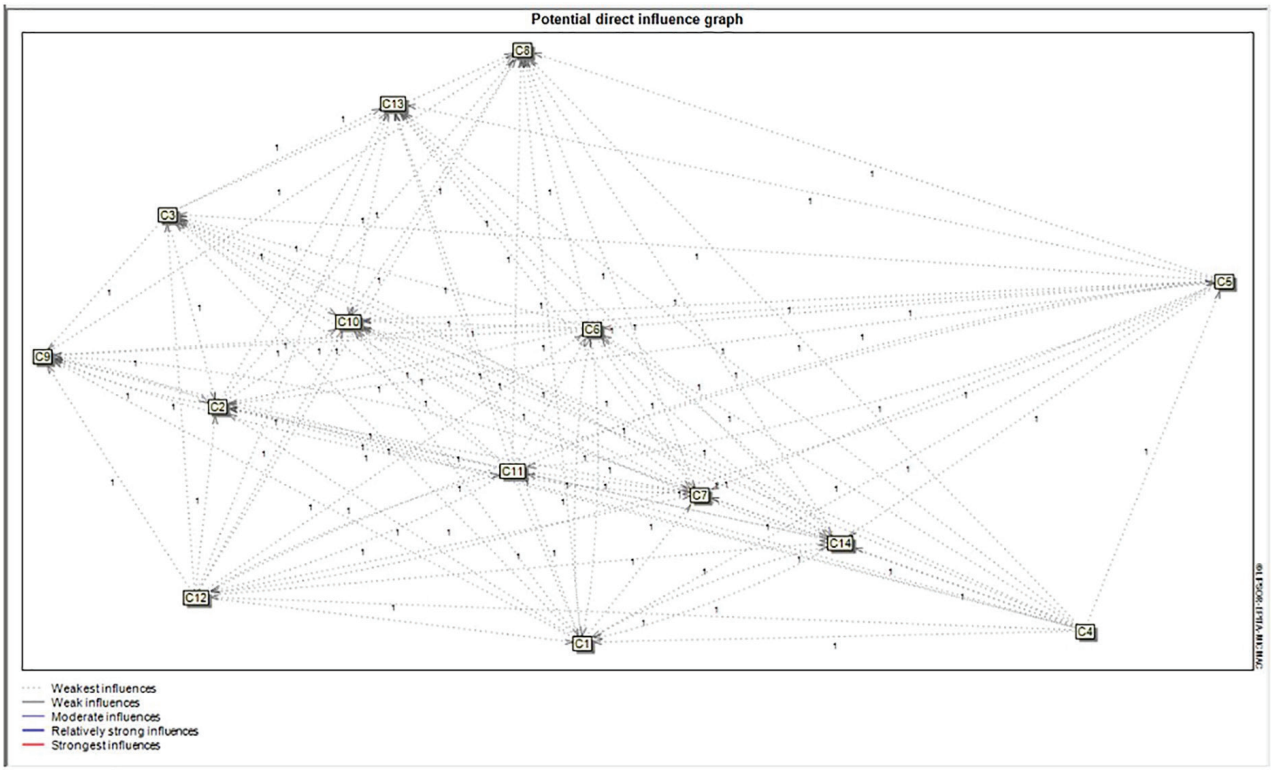
با توجه به خروجی محاسبات ISM متغیر در قالب (C8) سطح ششم است. برای تعیین عناصر سطح سوم، متغیرهای سطح دوم حذف می‌شوند و یکبار دیگر مجموعه ورودی‌ها و خروجی‌ها بدون درنظر گرفتن متغیرهای سطح دوم محاسبه می‌شود.

21. Boolean rule

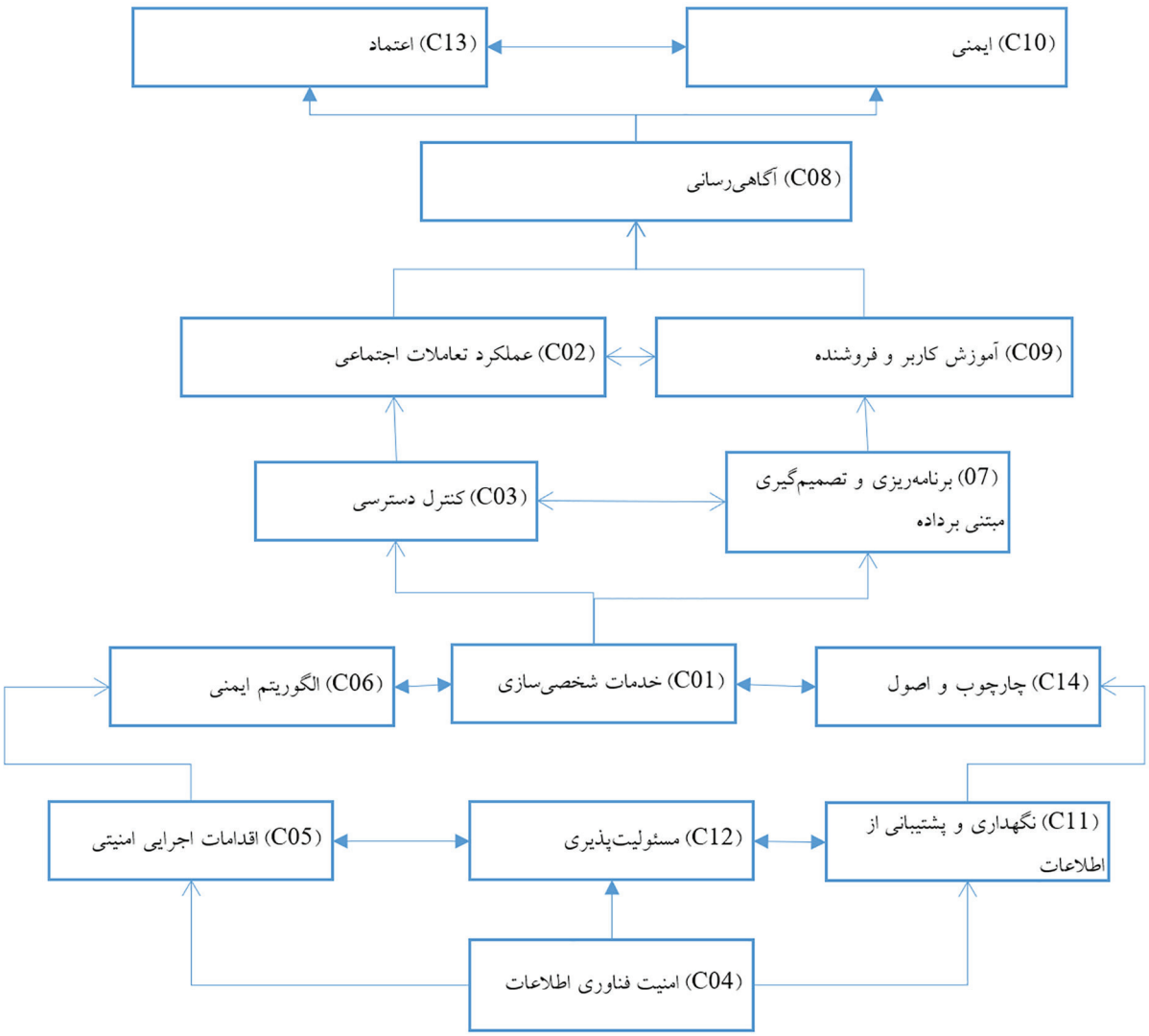
جدول ۱۰. مجموعه ورودی‌ها و خروجی‌ها برای تعیین سطح

ردیف	مولفه	خروجی	ورودی	اشتراک	سطح
۱	C01	C1-C2-C3-- C6-C7-C8-C9-C10- --C13-C14	C4-C5-C6-C11 -C12-C14	C1-C6-C14	۳
۲	C02	C2-- -C8-C9-C10- --C13-	C1-C2-C3- C4-C5-C6-C7 -C9-C11 -C12-C14	C2-C9	۵
۳	C03	C2-C3-- -C7-C8-C9-C10- --C13-	C1-C3- C4-C5-C6-C7-C11 -C12-C14	C3-C7	۴
۴	C04	C1-C2-C3-C4-C5 C6-C7-C8-C9-C10- C11-C12-C13-C14	C4	C4	۱
۵	C05	C1-C2-C3--C5 C6-C7-C8-C9-C10- C11-C12-C13-C14	C4-C5-C11-C12	C5-C11-C12	۲
۶	C06	C1-C2-C3-- C6-C7-C8-C9-C10- --C13-C14	C4-C5-C6-C11 -C12-C14	C1-C6-C14	۳
۷	C07	C2-C3-- -C7-C8-C9-C10- --C13-	C1-C3- C4-C5-C6-C7-C11 -C12-C14	C3-C7	۴
۸	C08	-C8--C10- --C13-	C1-C2-C3- C4-C5-C6- C7-C8 -C9-C11 -C12-C14	C8	۶
۹	C09	C2-- -C8-C9-C10- --C13-	C1-C2-C3- C4-C5-C6-C7 -C9-C11 -C12-C14	C2-C9	۵
۱۰	C10	- C10- --C13-	C1-C2-C3-C4-C5 C6-C7-C8-C9-C10- C11-C12-C13-C14	C10-C13	۷
۱۱	C11	C1-C2-C3--C5 C6-C7-C8-C9-C10- C11-C12-C13-C14	C4-C5-C11-C12	C5-C11-C12	۲
۱۲	C12	C1-C2-C3--C5 C6-C7-C8-C9-C10- C11-C12-C13-C14	C4-C5-C11-C12	C5-C11-C12	۲
۱۳	C13	- C10- --C13-	C1-C2-C3-C4-C5 C6-C7-C8-C9-C10- C11-C12-C13-C14	C10-C13	۷
۱۴	C14	C1-C2-C3-- C6-C7-C8-C9-C10- --C13-C14	C4-C5-C6-C11 -C12-C14	C1-C6-C14	۳

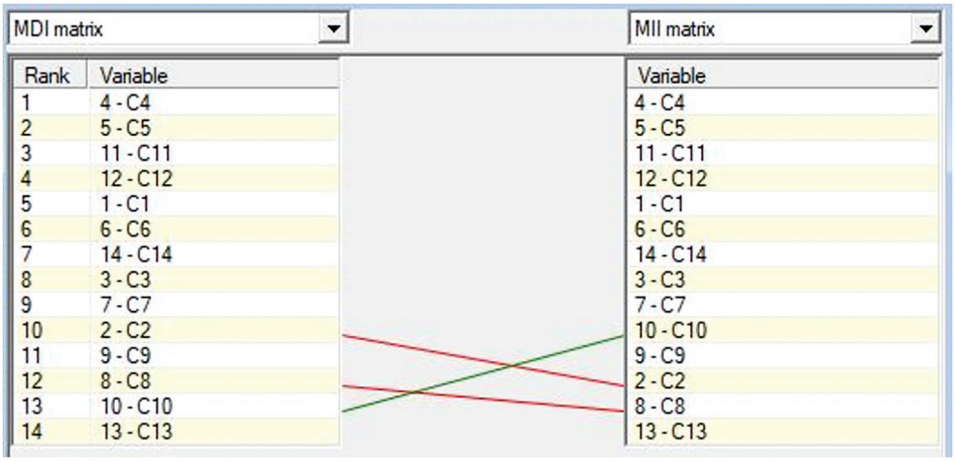
براساس مجموعه مشترک شناسایی و متغیرهایی که اشتراک آنها برابر مجموعه ورودی‌ها باشد به عنوان متغیرهای سطح سوم انتخاب می‌شوند. با توجه به خروجی محاسبات ISM متغیرهای (C03) و (C07) سطح پنجم هستند. همچنین متغیرهای (C02) و (C09) در سطح چهارم قرار گرفتند. متغیرهای (C01) و (C06) و (C10)در سطح سوم قرار دارند و متغیرهای (C11) و (۱۲) و (C05) در سطح دوم قرار دارد. در نهایت نیز (C04) زیربنایی‌ترین عنصر مدل است. الگوی نهایی سطوح متغیرهای شناسایی شده در شکل زیر نمایش داده شده است (شکل ۲).



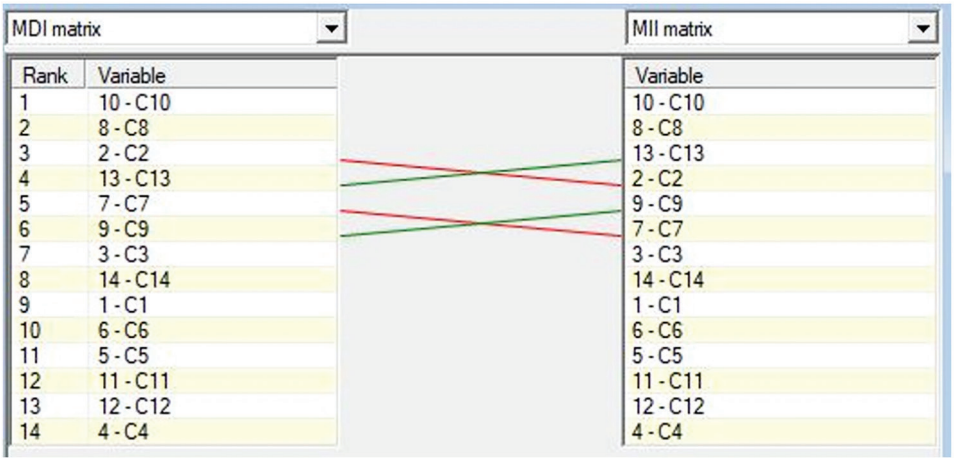
شکل ۱. مدل ساختاری تفسیری خروجی میک مک



شکل ۲. الگوی جامع مدل



شکل ۳. اولویت مولفه‌ها براساس میزان نفوذ



شکل ۴. اولویت مولفه‌ها براساس میزان تاثیرپذیری

در این نگاره فقط روابط معنادار عناصر هر سطح بر عناصر سطح زیرین و همچنین روابط درونی معنادار عناصر هر سطر در نظر گرفته شده است.

عنصر سطح پایین (C04) بیشترین تأثیر را در مدل دارد و به همین ترتیب از میزان تأثیرگذاری در سطوح بعد کاسته می‌شود و متغیرهای هم سطح یعنی تعامل متقابل با هم دارند.

تحلیل قدرت نفوذ-وابستگی (نمودار MICMAC)

در مدل (ISM) روابط متقابل و تأثیرگذاری بین معیارها و ارتباط معیارهای سطوح مختلف به خوبی نشان داده شده است که موجب درک بهتر فضای تصمیم گیری به وسیله مدیران مربوطه می‌شود. برای تعیین معیارهای کلیدی قدرت نفوذ و وابستگی معیارها در ماتریس دسترسی نهایی تشکیل می‌شود. نمودار قدرت-وابستگی برای متغیرهای مورد مطالعه در شکل‌های ۳ و ۴ را نشان می‌دهد. براساس تحلیل میک مک انجام شده در شکل اولویت مولفه‌ها براساس میزان نفوذشان در مدل مشخص شده است.

براساس تحلیل میک مک انجام شده در شکل ۵ اولویت مولفه‌ها براساس میزان تاثیرپذیری شان در مدل مشخص شده است.

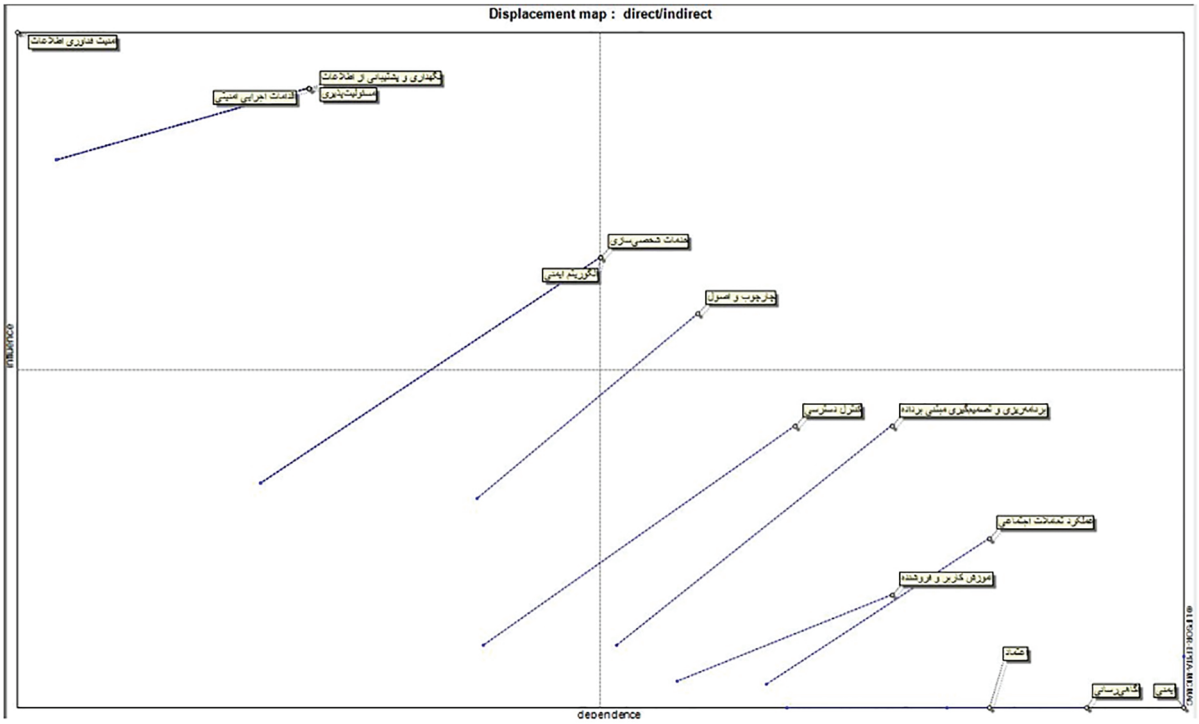
در جدول ۱۱ قدرت نفوذ و میزان وابستگی مولفه‌های تحقیق بیان شده است

بر اساس قدرت وابستگی و نفوذ متغیرها، می توان دستگاه مختصاتی تعریف کرد و آن را به چهار قسمت مساوی تقسیم نمود. در این پژوهش، گروهی از متغیرها در زیرگروه محرک قرار گرفتند،این متغیرها قدرت نفوذ زیاد و وابستگی کمی دارند. در دسته‌ی بعدی متغیرهای وابسته قرار دارند که به گونه ای نتایج فرایند توسعهٔ محصول‌اند و کمتر می توانند زمینه ساز متغیرهای دیگر شوند.

در این تحلیل متغیرها به چهار گروه خودمختار، وابسته، پیوندی (رابط) و مستقل تقسیم می‌شوند.

خودمختار[3]: متغیرهای خودمختار میزان وابستگی و قدرت هدایت کمی دارند این معیارها عموما از سیستم جدا می‌شوند زیرا دارای اتصالات ضعیف با سیستم هستند. تغییری در این متغیرها باعث تغییر جدی در سیستم نمی‌شود.

3. Autonomous variables



شکل ۵. نمودار قدرت نفوذ و میزان وابستگی (خروجی میک-مک)

جدول ۱۱. قدرت نفوذ و میزان وابستگی مولفه‌های تحقیق

ردیف	مولفه	سطر	ستون
۱	خدمات شخصی‌سازی	۹	۶
۲	عملکرد تعاملات اجتماعی	۴	۱۰
۳	کنترل دسترسی	۶	۸
۴	امنیت فناوری اطلاعات	۱۳	۰
۵	اقدامات اجرایی امنیتی	۱۲	۳
۶	الگوریتم ایمنی	۹	۶
۷	برنامه‌ریزی و تصمیم‌گیری مبتنی برداده	۶	۹
۸	آگاهی‌رسانی	۱	۱۱
۹	آموزش کاربر و فروشنده	۳	۹
۱۰	ایمنی	۱	۱۲
۱۱	نگهداری و پشتیبانی از اطلاعات	۱۲	۳
۱۲	مسئولیت‌پذیری	۱۲	۳
۱۳	اعتماد	۱	۱۰
۱۴	چارچوب و اصول	۸	۷
	مجموع	۹۷	۹۷

براساس نمودار قدرت نفوذ و میزان وابستگی متغیر خودمختار در این مدل وجود ندارد.

وابسته[۴]: متغیرهای وابسته دارای وابستگی قوی و هدایت ضعیف هستند این متغیرها اصولا تاثیرپذیری بالا و تاثیرگذاری کمی روی سیستم دارند. براساس نمودار قدرت نفوذ و میزان وابستگی ایمنی، آگاهی، اعتماد، آموزش کاربر و تعامل اجتماعی متغیرهای

4. Dependent variables

وابسته هستند.

مستقل[5]: متغیرهای مستقل دارای وابستگی کم و هدایت بالا می‌باشند به عبارتی دیگر تاثیرگذاری بالا و تاثیرپذیری کم از ویژگی‌های این متغیرها است. براساس نمودار قدرت نفوذ و میزان وابستگی، امنیت فناوری اطلاعات، اقدامات اجرایی امنیتی، نگهداری و پشتیبانی از اطلاعات و مسئولیت پذیری تاثیرگذار ترین متغیرها هستند و مستقل هستند

پیوندی[6]: متغیرهای رابط یا پیوندی از وابستگی بالا و قدرت هدایت بالا برخوردارند به عبارتی تاثیرگذاری و تاثیرپذیری این معیارها بسیار بالاست و هر تغییر کوچکی بر روی این متغیرها باعث تغییرات اساسی در سیستم می‌شود. براساس نمودار قدرت نفوذ و میزان وابستگی الگوریتم ایمنی، اقدامات شخصی سازی و چارچوب و اصول متغیرهای پیوندی هستند.

بحث

در عصر تحول دیجیتال و گسترش خدمات سلامت الکترونیک، حفاظت از حریم خصوصی مشتریان اینترنتی به یکی از چالش‌های حیاتی تبدیل شده است. با افزایش استفاده از بسترهای آنلاین برای ارائه خدمات پزشکی، تبادل اطلاعات حساس و شخصی بیماران از طریق سیستم‌های دیجیتال، نگرانی‌ها درباره سوء استفاده از داده‌ها، دسترسی غیرمجاز و نقض حریم خصوصی نیز افزایش یافته است. اهمیت حفاظت از داده‌های بیماران نه تنها از منظر اخلاقی و حقوقی بلکه از دیدگاه اعتماد مشتریان و پایداری سیستم‌های سلامت دیجیتال، اهمیت فزاینده‌ای یافته است. در این راستا، شناسایی و تحلیل عوامل مؤثر بر حفاظت از حریم خصوصی، گامی بنیادین برای طراحی سیاست‌ها و زیرساخت‌های ایمن محسوب می‌شود. یکی از رویکردهای مناسب برای مدل‌سازی روابط میان این عوامل، روش مدلسازی ساختاری تفسیری فازی است که با بهره‌گیری از منطق فازی و تحلیل‌های ساختاری، امکان ترسیم شبکه‌ای از ارتباطات علت و معلولی بین متغیرها را فراهم می‌سازد (۳۵). این رویکرد به‌ویژه زمانی مؤثر است که با متغیرهای کیفی و پیچیده مواجه باشیم و نیاز به استخراج ساختار سلسله‌مراتبی از مؤلفه‌ها وجود داشته باشد. با استفاده از FISM می‌توان عواملی نظیر آگاهی کاربران از حقوق حریم خصوصی، سیاست‌های شفاف حاکمیتی، اعتماد به ارائه‌دهندگان خدمات، امنیت فنی زیرساخت‌ها، و عوامل فرهنگی و اجتماعی را شناسایی و نقش هرکدام را در حفاظت از حریم خصوصی تحلیل نمود.یافته‌های حاصل از این مدل‌سازی می‌تواند راهنمای مناسبی برای سیاست‌گذاران، طراحان سامانه‌های سلامت الکترونیک و فعالان حوزه فناوری اطلاعات سلامت باشد تا با اولویت‌بندی مؤلفه‌ها، راهکارهای مؤثر و اجرایی برای بهبود سطح اعتماد کاربران و ارتقاء امنیت داده‌ها طراحی کنند. در نهایت، بهره‌گیری از رویکردهای سیستماتیک مانند FISM، درک عمیق‌تری از پویایی‌های حاکم بر حفظ حریم خصوصی در بستر دیجیتال فراهم کرده و زمینه‌ساز تصمیم‌گیری‌های آگاهانه‌تر در این حوزه خواهد بود (۳۶) مطالعه حاضر به ارائه مدل حفاظت از حریم خصوصی مشتریان اینترنتی حوزه سلامت پرداخته است. مطالعه‌ی ادبیات و پیشینه‌ی تحقیق و مصاحبه‌های انجام شده با خبرگان و مطابق یافته‌های تحلیل ساختاری ۱۴ مولفه شناسایی شده عبارتند از خدمات شخصی‌سازی، عملکرد تعاملات اجتماعی، کنترل دسترسی، امنیت فناوری اطلاعات، اقدامات اجرایی امنیتی، الگوریتم ایمنی، برنامه‌ریزی و تصمیم‌گیری مبتنی برداده، آگاهی‌رسانی، آموزش کاربر و فروشنده، ایمنی، نگهداری و پشتیبانی از اطلاعات، مسئولیت‌پذیری، اعتماد و چارچوب و اصول. این ۱۴ مولفه در یک مدل ۷ سطحی طراحی شد.

استفاده از منطق و دانش متخصصان در زمان طراحی سیستم‌های هوشمند سلامت در فروشگاه‌های تجهیزات پزشکی و آشنایی کافی مشتریان اینترنتی فعال در حوزه سلامت با موضوعات و چالش‌های نظام سلامت، که با ایجاد رشته‌های بین رشته‌ای کمک شایانی به این موضوع خواهد کرد. نقایص موجود در زیر ساخت ارتباطی کشور اعم از عدم پوشش و دسترسی اینترنتی با سرعت نامناسب برخی نقاط کشور از دیگر چالش‌ها می‌باشد که وزارت ارتباطات و فناوری اطلاعات و فروشگاه‌های تجهیزات پزشکی به عنوان متولی توسعه زیرساخت‌های ارتباطی، مکلف است که زیرساخت ارتباطی مناسب را در اختیار نظام سلامت قراردهد.

تعاملات اجتماعی در حوزه پزشکی شامل اشتراک‌گذاری اطلاعات و ارتباط با دیگر بیماران و پزشکان است. اگرچه این تعاملات می‌تواند به بهبود تجربیات درمانی کمک کند، باید سازوکارهایی برای اطمینان از امنیت این تبادلات وجود داشته باشد. عدم

5. Independent variables
6. Linkage variables

کنترل صحیح بر این تعاملات می‌تواند به خطر افتادن حریم خصوصی افراد منجر شود. استفاده از پلتفرم‌هایی با مکانیزم‌های رمزگذاری و احراز هویت می‌تواند این مشکلات را کاهش دهد. کنترل دسترسی به داده‌های بیماران یکی دیگر از جنبه‌های کلیدی حفظ حریم خصوصی است. مدیریت دقیق اینکه چه کسانی و تحت چه شرایطی به اطلاعات دسترسی داشته باشند، از اهمیت بالایی برخوردار است. استفاده از سیستم‌های دسترسی چند سطحی و احراز هویت دو عاملی، به افزایش امنیت و کاهش ریسک‌های احتمالی کمک می‌کند. امنیت فناوری اطلاعات باید به‌عنوان ستون فقرات حفظ حریم خصوصی در نظر گرفته شود. بکارگیری زیرساخت‌های IT قوی و مطمئن، شامل فایروال‌ها، سیستم‌های جلوگیری از نفوذ و رمزگذاری اطلاعات، برای جلوگیری از دسترسی‌های غیرمجاز به داده‌های پزشکی الزامی است. به‌روز رسانی مداوم سیستم‌ها و پروتکل‌های امنیتی از اهمیت بسیاری برخوردار است تا از تهدیدات جدید محافظت شود.

اقدامات اجرایی امنیتی شامل فرآیندها و سیاست‌هایی است که برای اطمینان از محافظت از داده‌ها در برابر تهدیدات داخلی و خارجی تدوین می‌شود. این اقدامات باید شامل آموزش پرسنل، تست‌های امنیتی منظم و پیاده‌سازی سیاست‌های سختگیرانه در استفاده از داده‌های پزشکی باشد. ایجاد فرهنگ امنیتی در محیط‌های کاری می‌تواند تأثیر زیادی در کاهش خطرات مربوط به حریم خصوصی داشته باشد. الگوریتم‌های ایمنی نقش حیاتی در حفظ حریم خصوصی مشتریان ایفا می‌کنند. استفاده از الگوریتم‌های پیشرفته رمزگذاری و هوش مصنوعی برای تشخیص و پیشگیری از تهدیدات، می‌تواند به افزایش امنیت کمک کند. الگوریتم‌ها باید به گونه‌ای طراحی شوند که علاوه بر حفظ حریم خصوصی، امکان مدیریت و پردازش داده‌های پزشکی را به صورت امن فراهم کنند. در نهایت، برنامه‌ریزی و تصمیم‌گیری مبتنی بر داده نقش مهمی در حفظ حریم خصوصی دارد. استفاده از داده‌ها برای بهبود خدمات پزشکی باید با رعایت کامل حریم خصوصی انجام شود. تحلیل دقیق و استفاده از داده‌ها بدون افشای هویت مشتریان می‌تواند به بهبود کیفیت خدمات و در عین حال حفظ حریم خصوصی منجر شود. به همین دلیل، پیاده‌سازی پروتکل‌هایی برای ناشناس‌سازی داده‌ها و استفاده از روش‌های امن تجزیه‌وتحلیل داده از اهمیت بالایی برخوردار است. در مجموع، حفظ حریم خصوصی مشتریان در حوزه پزشکی نیازمند یک رویکرد جامع است که از خدمات شخصی‌سازی تا الگوریتم‌های ایمنی را شامل می‌شود. هماهنگی بین این عناصر و اجرای صحیح اقدامات امنیتی، از اهمیت بالایی برخوردار است تا اطمینان حاصل شود که اطلاعات حساس پزشکی به طور ایمن مدیریت و محافظت می‌شوند.

محدودیت‌ها پژوهشی

قابل ذکر است با توجه به این امر که در پژوهش حاضر اسناد با توجه به محدودیت برخی دسترسی‌ها از برخی پایگاه‌های منتخب انجام گرفت توصیه می‌شود در مطالعات آتی به صورت تطبیقی مستندات حوزه سلامت دیجیتال در دیگر منابع اطلاعاتی داخلی و خارج مورد بررسی قرار گیرد.

پیشنهادات پژوهشی

پیشنهاد می‌گردد با توجه به نقش بسیار مهم دولت در ایجاد این تحول دیجیتالی، تلاشی هماهنگ میان کلیه ذی‌نفعان در این حوزه با بهره‌گیری از یک مدل یکپارچه برنامه‌ریزی و اجرا گردد، و ذینفعان میتوانند با سرمایه‌گذاری بر روی مهارت‌های مورد نیاز فناوری فوق، در تسریع و پایداری این تحول بزرگ به‌صورت طولانی مدت اثرگذار باشند. همچنین به منظور تسریع در توسعه ارایه خدمات فوق مهم است که محققان و مدیران در راستای پیاده‌سازی این سیستم با یکدیگر همکاری نمایند.

نتیجه گیری

این پژوهش به شناسایی و تحلیل مولفه‌های مؤثر بر حریم خصوصی مشتریان اینترنتی در حوزه سلامت پرداخته و از رویکرد ترکیبی کیفی و کمی استفاده کرده است. ۱۴ مولفه کلیدی شناسایی و ارزیابی شده‌اند که شامل امنیت فناوری اطلاعات، کنترل دسترسی، مسئولیت‌پذیری و اعتماد هستند. همچنین، برنامه‌ریزی مبتنی بر داده و آموزش کاربران و فروشندگان به عنوان عوامل مهم در بهبود حریم خصوصی معرفی شده‌اند. نتایج این تحقیق می‌تواند به مدیران و سیاست‌گذاران کمک کند تا سیاست‌های مؤثرتری برای حفظ حریم خصوصی تدوین کنند و اهمیت ارتقاء آموزش و آگاهی در این زمینه را

برجسته می‌سازد. در نهایت، این مطالعه پایه‌ای برای پژوهش‌های آتی در این حوزه فراهم کرده و می‌تواند به توسعه راهکارهای نوین منجر شود.

تضاد منافع

هیچ‌گونه تعارض منافعی وجود ندارد.

منابع

1. Jørgensen CS, SA S, Katt B. Digital twins in healthcare: security, privacy, trust and safety challenges. In: European Symposium on Research in Computer Security. Cham: Springer Nature Switzerland; 2023. p. 140-53.
2. Armeni P, PI P, De Rossi LM, Diaferia L, Meregalli S, Gatti A. Digital twins in healthcare: is it the beginning of a new era of evidence-based medicine? A critical review. J Pers Med. 2022;12(8):1255.
3. Blasiak A, SY S, Leitman D, Ng WY, De Nicola R, Lee VV, et al. Omnichannel communication to boost patient engagement and behavioral change with digital health interventions. J Med Internet Res. 2022;24(11):e32789.
4. Winter PD, CT C. Using the non-adoption, abandonment, scale-up, spread, and sustainability (NASSS) framework to identify barriers and facilitators for the implementation of digital twins in cardiovascular medicine. Sensors. 2023;23(14):6333.
5. Esha NHT, Huq S, Mahmud M, Kaiser MS. Trust IoHT: a trust management model for Internet of Healthcare Things. In: Proceedings of the International Conference on Data Science and Applications; Kolkata; 2021. p. 47-57.
6. Lydahl D. Standard tools for non-standard care: the values and scripts of a person-centred assessment protocol. Health. 2021;25(1):103-20.
7. Zhou W, Y Z, Peng A, Zhang Y, Liu P. The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. IEEE Internet Things J. 2018;6(2):1606-16.
8. Shahid JA, R S, Kiani AK, Ahmad T, Saeed S, Almuhaideb AM. Data protection and privacy of the Internet of Healthcare Things (IoHTs). Appl Sci. 2022;12(4):1927.
9. Alghanim AR, SMM S, Hossain MA. Privacy analysis of smart city healthcare services. In: 2017 IEEE International Symposium on Multimedia (ISM). Piscataway: IEEE; 2017. p. 394-8.
10. Dhasarathan C, Shanmugam M, Kumar M. A nomadic multi-agent based privacy metrics for e-health care: a deep learning approach. Multimed Tools Appl. 2023;82(15):21045-67.
11. Hahanov V, Miz V. Big data driven healthcare services and wearables. In: The experience of designing and application of CAD systems in microelectronics. Piscataway: IEEE; 2015. p. 310-2.
12. Abouelmehdi KB, Khaloufi H, Benhaddou A. Big healthcare data: preserving security and privacy. J Big Data. 2018;5(1):1.
13. Makovee R. Online privacy, overview and preliminary research. J Inf Technol Policy. 2010;34(2):1-15.
14. Kuacharoen P. Practical customer privacy protection on shared servers. Res Pract Inf Technol. 2014;2:1-6.
15. Gupta B, Chennamaneni A. Understanding online privacy protection behavior on the older adults: an empirical investigation. J Inf Technol Manag. 2018;3:1-13.
16. Mohamed NA, Jawhar I, Kesserwan N. Leveraging digital twins for healthcare systems engineering. IEEE Access. 2023;11:69841-53.
17. Hwang H, GL H, Y L. Evaluating people's concern about their health information privacy based on power-responsibility equilibrium model: a case of Taiwan. J Med Syst. 2022;46(2):46.
18. Vidovszky AA, FC F, Loukianov AD, Smith AM, Tramel EW, Walsh JR, et al. Increasing acceptance of AI-generated digital twins through clinical trial applications. Clin Transl Sci. 2024;17(7):e13897.
19. Nourani AH. Artificial intelligence in healthcare. Health Biomed Inform. 2022;9(3):193-5.
20. Sun T, HX H, Song X, Shu L, Li Z. The digital twin in medicine: a key to the future of healthcare? Front Med (Lausanne). 2022;9:907066.
21. Iadanza E, Cerofolini S, Lombardo C. Medical devices nomenclature systems: a scoping review. Health Technol. 2021;11(4):681-92.

22. Ishida K, Fujioka T, Endo T. Evaluation of electromagnetic fields in a hospital for safe use of electronic medical equipment. J Med Syst. 2016;40(2):46.
23. Degerli M. Privacy issues in data-driven health care. In: Dey N, editor. Data-driven approach for bio-medical and healthcare. Singapore: Springer; 2023. p. 23-7.
24. Lazar A, Dixon EE. Safe enough to share: setting the dementia agenda online. Proc ACM Hum Comput Interact. 2019;3(CSCW):1-23.
25. Hutchings E, Loomes M, Butow P. 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.
26. Labbaf A, JM J, Jafaripouyan E, Mazinani M. Challenges and solutions for managing the COVID-19 crisis in hospitals at Tehran University of Medical Sciences. J Sch Public Health Inst Public Health Res. 2020;18(4):255-72. Persian.
27. Malmir R, MA M, Toghyani R, Sfari MS. COVID-19 crisis management: reengineering the health service delivery system in Iran. Sci Res Med Syst Organ. 2020;39(1):11-8. Persian.
28. Motti VG, Berkovsky S. 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.
29. Saura JR, Ribeiro-Soriano D, Palacios-Marqués D. Evaluating security and privacy issues of social networks based information systems in Industry 4.0. Enterp Inf Syst. 2021;15(8):1235-51.
30. Iraj N. Examining the status and scope of individuals' privacy in cyberspace with emphasis on transnational documents [PhD dissertation]. Tehran: Resalat Institute of Higher Education; 2022.
31. Nasirian A, PH P. Privacy for secure cloud storage. In: The Second International Conference on Research in Science and Technology; Istanbul; 2015.
32. Wang EST. Role of privacy legislations and online business brand image in consumer perceptions of online privacy risk. J Consum Aff. 2019;14(2):59-69.
33. Ramin G. Privacy in analyzing data from massive sources in the cloud. J Cloud Comput. 2022;11(1):45.
34. Sharifi Z, Keramati MA, Minouei M. Customers internet of privacy the protecting for model a developing health of field the in. Sadra Med Sci J. 2024;12(4):587-98. Persian.
35. Juanli L, Lei H, Yubo W, Ye L, Sleiman KA, Suliman MA. An empirical investigation of e-loyalty formation for online shopping in China. Acta Psychol (Amst). 2025;258:105135.
36. Datta A, Dey BK, Bhuniya S, Sangal I, Mandal B, Sarkar M, et al. Adaptation of e-commerce retailing to enhance customer satisfaction within a dynamical system under transfer of risk. J Retail Consum Serv. 2025;84:104129.