ISSN:2821-1588 htpps://www.jadm.khadu.ir

فصلنامه علمی ((مدیریت دفاع هوایی))

دوره ۲، شماره ۲ ،اسفند ۱۴۰۲

مقاله پژوهشی

چالش‌های توسعه امن اینترنت اشیاء پزشکی در ایران

منصور فرزین‌فر[۱]، رسول رمضانی دهقی[۲]

۱. مدیر فناوری اطلاعات دانشگاه علوم پزشکی بقیه الله، تهران، ایران

۲. گروه سایبر، دانشکده برق، دانشگاه پدافند هوایی خاتم الانبیاء(ص)، تهران، ایران

اطلاعات مقاله

تاریخ پذیرش: ۱۴۰۲/۱۱/ ۱۵

تاریخ دریافت: ۱۴۰۲/۰۹/۲۰

کلمات کلیدی:

اینترنت اشیاء پزشکی، چالش، امنیت، حوزه سلامت.

نویسنده مسئول:

رسول رمضانی دهقی

ایمیل:

sepehrramezany@yahoo.com

چکیده

هدف: هدف اصلی این تحقیق احصاء چالش‌های توسعه امن اینترنت اشیاء پزشکی در ایران با در نظر گرفتن حوزه نظامی است.

روش: تحقیق حاضر از نوع کاربردی بوده و روش آن توصیفی- تحلیلی با رویکرد آمیخته (کمی و کیفی) است و داده‌های کیفی این تحقیق از مطالعه منابع و مطالعات پژوهش‌های علمی و با استفاده از روش پژوهش کیفی فراترکیب جمع‌آوری گردیده است.

یافته‌ها: پس از بررسی جوانب مختلف مرتبط با موضوع تحقیق تعداد ۹۲ گویه استخراج شد که پس از مراجعه به نظر خبرگان و کارشناسان تعداد ۲۶ چالش اساسی در حوزه‌های عرضه، تقاضا، حکمرانی و امنیت مشخص گردید. از میان چالش‌های مشخص شده، چالش عدم دسترسی مناسب همه اقشار جامعه به امکانات حوزه سلامت با میزان اهمیت ۸/۵۰ به عنوان مهم‌ترین چالش، عدم راه‌اندازی کامل زیرساخت‌های ملی و حیاتی (شبکه ملی اطلاعات، شبکه شمس) با میزان اهمیت ۸/۴۴ در رتبه دوم و عدم تحقق کامل پرونده الکترونیک سلامت در کشور با میزان اهمیت ۸/۴۱ در رتبه سوم قرار گرفت.

نتیجه‌گیری: توسعه امن اینترنت اشیاء پزشکی مستلزم تکمیل پروژه‌هایی همچون توسعه و یکسان سازی خدمات حوزه سلامت، تشکیل پرونده سلامت الکترونیک برای همه اقشار جامعه، راه‌اندازی کامل شبکه ملی اطلاعات، ایجاد یک پلتفرم قابل اعتماد و تامین امنیت تجهیزات اینترنت اشیاء پزشکی است.

استناد به مقاله: فرزین‌فرد، منصور و رمضانی دهقی، رسول، چالش‌های توسعه امن اینترنت اشیاء پزشکی در ایران، فصلنامه علمی(مدیریت دفاع هوایی) دوره۲، شماره۴، اسفند ۱۴۰۲.

ISSN:2821-1588 htpps://www.jadm.khadu.ir

Journal of Air Defense Management

Vol. 2, No, 4, 1402

Research Paper

Challenges of safe development of medical Internet of Things in Iran

Mansour Farzinfard [1], Rasool Ramezani Dehaghi[2]

1. Director of Information Technology of Baqiyatallah University of Medical Sciences, Tehran, Iran.
2. Corresponding Author, Department of cyber, Faculty of electrical engineering, University of Khatam Al-Anbia Air Defense, Tehran, Iran.

Article Information

Accepted: 1402/11/15

Recceived:1402/09/20

Keywords:

Internet of medical objects, challenge, security , health field

Corresponding anuthor:
Mansour Farzinfard
Email:
sepehrramezany@yahoo.com

Abstract

Objective: The main purpose of this research is to estimate the challenges of the safe development of medical Internet of Things in Iran with considering the military field.

Methodology: The current research is of an applied type and its method is descriptive-analytical with a mixed approach (quantitative and qualitative) and the qualitative data of this research has been collected from the study of sources and studies of scientific research and using the meta-composite qualitative research method.

Findings: After examining various aspects related to the research topic, 92 items were extracted, and after referring to the opinions of experts, 26 basic challenges were identified in the fields of supply, demand, governance and security. Among the identified challenges, the challenge of lack of proper access of all sections of the society to health facilities with an importance of 50.8 as the most important challenge, lack of full launch of national and critical infrastructures (National Information Network, Shams Network) ranked second with an importance of 8.44 and the lack of complete implementation of electronic health records in the country ranked third with an importance of 8.41.

Conclusion: The safe development of the Internet of Medical Objects requires the completion of projects such as the development and standardization of health services, the creation of electronic health records for all sections of the society, the complete launch of the national information network, the creation of a reliable platform and the security of Internet equipment.

HOW TO CITE: Farzinfard, M., & Ramezani Dehaghi,, Challenges of safe development of medical Internet of Things in the country. Journal of Air Defense management, Vol. 2, No, 4, 1402.

۱.مقدمه

مدیریت سلامت و بهداشت به دلیل کمبود خدمات پزشکی، افزایش تقاضا، افزایش جمعیت، بروز پیری و بیماری‌های مزمن، روز به روز دشوارتر می‌شود. یکی از راه‌های برون رفت از مشکلات یاد شده، بهره‌برداری از فناوری‌های جدید و حرکت به سمت مدل‌های نوین پزشکی همچون انتقال وضعیت از کلینیک محوری به سمت بیمار محوری می‌باشیم که در آن هر یک از عوامل مانند بیمار، بیمارستان و ... باید به صورت بی‌سیم به هم متصل گردند. این تغییر وضعیت با بهره‌گیری از زیست‌بوم اینترنت اشیاء میسر خواهد شد.

اینترنت اشیاء یک فناوری نوظهور و برهم‌زن[1] و در حال رشد سریع است و با ورود به عرصه پزشکی، کل زیست‌بوم نظام سلامت را متحول ساخته است (Gabriel, Darwsih, Hassanien; 2021: 97). این فناوری شامل شبکه‌ای از اجزاء فیزیکی (از قبیل ابزارهای پوشیدنی، لوازم برقی خانگی، سامانه‌های امنیتی، نانوتکنولوژی، ابزارهای ساخت و تولید و غیره) است که به اجزاء هوشمندی (از قبیل ریزپردازنده‌ها، حافظه‌های ذخیره‌سازی، حسگرها و غیره) مجهز شده‌اند و بر بستر اینترنت با سایر ابزارها ارتباط برقرار می‌کنند (Quamara, 2018: 293 &Gupta). دستگاه های اینترنت اشیاء به صورت یکپارچه از طریق شبکه اینترنت اشیاء به یک دنیای مجازی پیوند داده می‌شوند و امکان اتصال هر زمان و هر مکان را فراهم می‌کنند (Aref & Tran, 2017). در حال حاضر این فناوری نوظهور، جایگاه ویژه خود را در بخش بهداشت و درمان (سلامت) به دست آورده است و از آن به عنوان یک انقلاب در مراقبت‌های بهداشتی-درمانی می‌توان نام برد.

اینترنت اشیاء پزشکی[2] کاربرد اینترنت اشیاء در صنعت پزشکی و مراقبت‌های بهداشتی است (Saini, 2021:498). در واقع اینترنت اشیاء پزشکی شکل دیگری از محیط ارتباطی اینترنت اشیاء است که شامل دستگاه‌های مراقبت پزشکی هوشمند، مانند ضربان‌ساز هوشمند، قندسنج هوشمند و غیره است (Wazid, et al, 2019: 461). پیش‌بینی می‌شود که با اجرای اینترنت اشیاء پزشکی به لطف نوآوری‌ها در اینترنت اشیاء از جمله توسعه ریزپردازنده‌ها، معماری حسگرهای زیستی و فناوری‌های در حال تکامل 5G، بهبود قابل توجهی در کارایی، اثربخشی و استاندارد درمان حاصل شود (Hameed, et al, 2021: 414). اینترنت اشیاء یک انقلاب در مراقبت‌های بهداشتی است که می‌تواند برای نظارت بر بیمار استفاده شود و به بیماران خدمات ارائه کند و همچنین، به جمع‌آوری و به اشتراک‌گذاری اطلاعات، تجزیه و تحلیل فرآیند و ذخیره اطلاعات دقیق‌تر نیز بپردازد. سیستم مراقبت‌های

1. Disruptive
2. Internet of Medical Things or IoMT

پزشکی اینترنت اشیاء به هنگام است و می‌تواند زندگی میلیون‌ها نفر را نجات دهد. با توجه به اهمیت حوزه سلامت و درمان در سطح جامعه، پیش‌بینی می‌شود تا سال ۲۰۲۵، بخش غالب بازار اینترنت اشیاء مربوط به حوزه سلامت (شامل سلامت همراه، مراقبت‌های از راه دور و ...) خواهد بود (Jain, Choudhary, 2016).

دستگاه‌های پزشکی و حسگرهای زیستی، مسئول ثبت علائم حیاتی بدن و انتقال داده‌های بیولوژیکی خام (مانند ضربان قلب، سیگنال مغز، دمای بدن و گلوکز سطح در خون) در زمان واقعی هستند (Pradhan, Bhattacharyya, 2021). فناوری اینترنت اشیاء منجر به ظهور شکل جدیدی از نظام مراقبت و سلامت تحت عنوان" پزشکی 4P" (پیش‌بینی پذیر، قابل پیشگیری، شخصی[1] و مشارکتی) شده است (Deloitte, 2018).

درخصوص چالش‌های بکارگیری فناوری اینترنت اشیاء در حوزه پزشکی مطالعات مختلفی انجام شده است. ولی در هیچیک از آن‌ها چالش‌های راهبردی این فناوری با نگاه به دو حوزه کشوری و نظامی بررسی و اولویت‌بندی نگردیده است. لالی[2] و همکاران در ارزیابی‌های خود از کاربران اپلیکیشن‌های سلامت، به دسته‌بندی چالش‌ها و دغدغه‌های استفاده از اینترنت اشیاء پزشکی پرداخته و مهم‌ترین آن‌ها را هزینه، امنیت اطلاعات، حریم خصوصی، آموزش استفاده از اینترنت اشیاء پزشکی، اعتماد به داده‌ها و تحلیل‌های ناشی از اینترنت اشیاء پزشکی بیان می‌نمایند(Lallie, et al, 2021). سعیدی و خاطری در مقاله‌ای "بررسی چالش‌های کلیدی استفاده از اینترنت اشیاء" بیان می‌دارد که مشکلات و چالش‌ها در پیاده سازی اینترنت اشیاء عبارتند از: چالش امنیت و حریم خصوصی، چالش قوانین، چالش تکنولوژی، چالش فرهنگ، چالش مدل کسب و کار و چالش مدل نیروی انسانی (سعیدی و خاطری، ۱۴۰۱: ۹). آیلنی و همکاران در مطالعه خود به جنبه‌های مختلفی در مورد آسیب‌پذیری‌های نرم‌افزاری و سخت‌افزاری دستگاه‌های پزشکی پوشیدنی و حملات سایبری و فناوری‌های امنیتی مرتبط با آن‌ها پرداخته‌اند. (Aileni, et al, 2020). جکسون و همکاران در پژوهشی، به بررسی چالش‌های دستگاه‌های مبتنی بر اینترنت اشیاء پرداخته و مهم‌ترین چالش‌ها در این زمینه را، تأثیر رسانه بر آگاهی از امنیت سایبری بیمار، نیاز به تجزیه و تحلیل ریسک/ سود در تمام سطوح تعامل بیمار، فرهنگ عدم ارتباط در صنعت، نظام سلامت و تجهیزات پزشکی، نیاز به همکاری و آموزش بین تولیدکنندگان، ارائه دهندگان مراقبت‌های بهداشتی و بیماران، بیان نموده است (Jackson, Rahman, 2019). همتی نژاد و مقدسی در پژوهش خود با موضوع "الزامات مدیریت امنیت اینترنت اشیاء در

1. Personalized
2. Lallie

بهداشت و درمان" به عدم استقبال عمومی و بی‌اعتمادی به محرمانگی اطلاعات و ارتباطات به عنوان بزرگترین مشکل برای توسعه اینترنت اشیا در صنعت سلامت اشاره نموده است (امتی‌نژاد، مقدسی، ۱۴۰۰). عبدالهی و همکاران در پژوهشی با عنوان "بررسی چالش‌های اینترنت اشیا در حوزه سلامت هوشمند" به بیان چالش‌های موجود در اینترنت اشیاء در حوزه سلامت مانند معماری شبکه، امنیت و روند توسعه نرم‌افزار، پرداخته است (سیدحسینی و همکاران، ۱۳۹۷).

هرچند بکارگیری فناوری اینترنت اشیاء در حوزه سلامت دارای مزیت‌هایی از قبیل ارتقاء وضعیت پیشگیری از بیماری‌ها، تشخیص سریع بیماری‌ها و کاهش آمار مرگ و میر بیماران می‌باشد، بهره‌گیری از این فناوری در حوزه سلامت با چالش‌هایی از قبیل تولید حجم عظیمی از اطلاعات، نیازمندی به ارتباطات دایمی بی‌سیم، پیچیدگی در معماری، گستردگی مقیاس عملکرد، نیازمندی به پهنای باند زیاد، تامین امنیت و حفظ حریم خصوصی بیماران رو برو است که پیش از عملیاتی نمودن این فناوری در بخش‌های بهداشت و درمان بایستی مورد بررسی دقیق قرار گیرد. دستگاه‌های مراقبت پزشکی با مرگ و زندگی انسان‌ها مرتبط‌اند و باید از قابلیت اطمینان بالایی برخوردار باشند. علاوه بر این، توسعه کاربردهای اینترنت اشیاء پزشکی مستلزم حفظ امنیت داده‌ها و حریم خصوصی بیماران است و بیماران و پزشکان باید متقاعد شوند که حفاظت داده‌ها به شکل مناسب و مطابق با قوانین انجام خواهد شد. از طرف دیگر توسعه امن اینترنت اشیاء در حوزه پزشکی نیاز مبرم به فرهنگ‌سازی، استانداردسازی، تأمین امنیت، اعتمادسازی و وضع قوانین و مقررات توسط قانون‌گذاران، سیاست‌گذاران و حاکمیت می‌باشد. از این رو این تحقیق با هدف احصاء، دسته‌بندی و اولویت‌بندی چالش‌های اساسی در توسعه اینترنت اشیاء پزشکی از طریق بررسی و واکاوی ضعف‌ها، آسیب‌پذیری‌ها، فشارها و گلوگاه‌های پیش روی توسعه امن این فناوری انجام و اقدامات پیشگیرانه به منظور کاهش آسیب‌پذیری‌های احتمالی جهت اجرا توصیه گردید.

روش تحقیق

پژوهش حاضر از نوع توسعه‌ای/ کاربردی و در زمره تحقیقات آمیخته (کمی وکیفی) دسته‌بندی می‌گردد که به روش توصیفی- تحلیلی و با رویکرد اکتشافی انجام شد. در این پژوهش جهت گردآوری داده‌های کیفی، منابع، مطالعات و پژوهش‌های علمی داخل و خارج از کشور مورد مطالعه قرار گرفت و چالش‌های اینترنت اشیاء در حوزه سلامت احصاء گردید. سپس با برگزاری چندین جلسه خبرگی و انجام مصاحبه عمیق، شیوه دسته‌بندی چالش‌ها و معیارهای کلیدی مورد نظر درحوزه سلامت انتخاب شد. در بخش کمی، با تدوین و انتشار

پرسشنامه محقق ساخته از صاحبنظران خواسته شد که میزان اهمیت و شدت تاثیرگذاری هر یک از چالش‌های احصاء شده در چهار حوزه عرضه، تقاضا، حکمرانی و امنیت را مشخص نمایند.

در این تحقیق برای سنجش روایی پرسشنامه از روایی محتوا، استفاده شده است. روایی محتوا اطمینان می‌دهد که ابزار مورد نظر به تعداد کافی، پرسش مناسب برای اندازه‌گیری مفهوم مورد سنجش را دارد. هر قدر این عناصر، مقیاس گسترده‌تر و قلمرو مفهوم مورد سنجش را بیشتر در برگیرند، روایی محتوا بیشتر خواهد بود (حسینزاده، چوبینه و قائم، ۱۳۹۳: ۲۹۹). در این تحقیق سوال‌های پرسشنامه متناسب با مبانی نظری طراحی شده و سپس با توزیع آن بین صاحبنظران مرتبط با موضوع، معیارهای غیر مرتبط تعدیل یا حذف شد و با پیشنهادهای ارایه شده معیارهایی نیز اضافه و پرسشنامه اصلی با ۹۲ گویه تدوین و توزیع گردید. جامعه آماری پژوهش بر اساس رابطه کوکران و سطح خطای ۵ درصد، شامل تعداد ۲۵ نفر از صاحبنظران، مدیران و اعضای هیات علمی با مدارک کارشناسی ارشد و دکتری، آشنا با مباحث فضای سایبر، فناوری اینترنت اشیاء، حوزه‌های سلامت و سلامت الکترونیک کشور بود که به صورت هدفمند و به روش گلوله برفی تا رسیدن نظرات به اشباع انتخاب گردیدند. جامعه نمونه به صورت تمام شمار انتخاب و پرسشنامه در خصوص آنها اجرا گردید. در این تحقیق داده‌های گردآوری شده با استفاده از روش‌های آمار توصیفی و آمار تحلیلی شامل آزمون آماری T و محاسبه دامنه اطمینان ۹۵ درصد با کمک نرم‌افزار SPSS برای مقایسه چالش‌های اینترنت اشیاء در حوزه سلامت، مورد تجزیه و تحلیل قرار گرفت.

روایی پرسشنامه از دو جنبه روایی ظاهری و محتوایی به جهت روشن و بدون ابهام بودن گویه‌ها و همچنین کفایت کمیت و کیفیت آن‌ها همانطور که توضیح داده شد توسط خبرگان و صاحب‌نظران و اساتید دانشگاه تایید گردید. در این پژوهش برای تعیین پایایی پرسشنامه از ضریب آلفای کرونباخ استفاده شده است که مشهورترین ضریب اعتبار از طریق یکبار اجرای آزمون می‌باشد (محمدبیگی، محمدصالحی و علیگل،۱۳۹۵: ۷۷). با توجه به واریانس هریک از متغیرها، ضریب آلفای کرونباخ با استفاده از نرم افزار SPSS مطابق جدول (۱) محاسبه گردید، با توجه به اینکه در پژوهش‌های علوم انسانی، ضریب آلفای بالاتر از ۰.۷۰ قابل قبول است، مقدار آلفای حاصله بر قابلیت اعتماد پرسشنامه‌ها صحه گذاشت.

جدول(۱) آلفای کرونباخ پرسشنامه

سوالات	حوزه	آلفای کرونباخ	میانگین واریانس	میانگین کوواریانس	میانگین انحراف معیار
۱ تا ۲۷	عرضه	۰.۷۲۸	۰.۳۹۰	۰.۱۶۴	۰.۷۳۱
۲۸ تا ۵۲	تقاضا	۰.۷۲۸	۰.۵۵۹	۰.۱۹۵	۰.۷۴۷
۵۳ تا ۷۵	حکمرانی	۰.۸۲۳	۰.۳۹۰	۰.۱۳۳	۰.۶۲۵
۷۶ تا ۹۲	امنیت	۰.۸۲۹	۰.۵۳۴	۰.۱۶۴	۰.۷۳۱

یافته‌های تحقیق

در این تحقیق، چالش‌ها به مساله‌یابی مشکلات، ضعف، تهدیدها و مسایل عمومی در موضوع بکارگیری اینترنت اشیاء پزشکی اشاره دارد. چالش از تعامل نقاط قوت و ضعف و فرصت و تهدید که ناشی از شناخت محیط داخلی و بیرونی است، به دست می آید. برای شناسایی و احصاء چالش‌های اساسی در این حوزه، پژوهشگر از طریق مطالعه عمیق منابع موجود، بررسی ادبیات تحقیق، بررسی قوت‌ها، ضعف‌ها، فرصت‌ها و تهدیدات و همچنین مصاحبه با خبرگان اقدام نموده است. لذا در ابتدا با استفاده از ادبیات نظری و مصاحبه با خبرگان، مدل اولیه زیست بوم اینترنت اشیاء پزشکی ترسیم و سپس با استفاده از روش پیمایشی (نظرات متخصان این حوزه) و مصاحبه با ۱۱ نفر از خبره‌های حوزه سلامت و نوآوری در چندین مرحله رفت و برگشت، اصلاحات لازم انجام و مدل مفهومی نهایی (شکل-۱) تبیین و در یک جلسه خبرگی مورد تایید قرار گرفت.

شکل (۱) مدل مفهومی زیست بوم اینترنت اشیاء پزشکی

این مدل مفهومی راهنما و مبنای استخراج چالش‌های بکارگیری اینترنت اشیاء پزشکی در چهار حوزه عرضه، تقاضا، حکمرانی و امنیت تدوین و قرارگرفت و مبتنی بر آن به تفکیک هر یک از عوامل اثرگذار، دسته‌بندی و استخراج شد. در ادامه مصادیق استخراج شده در جلسه پانل خبرگان و در گروه کاری مورد بررسی و تجزیه و تحلیل خبرگان قرار گرفت. (در این گام برخی از موارد احصاء شده حذف و یا تغییر نمود و پیشنهادات برخی از اعضا به لیست اضافه گردید). سپس جهت تایید نهایی و تعیین میزان اهمیت و تاثیرگذاری هریک از چالش‌ها، با استفاده از پرسشنامه با طیف لیکرد پنج تایی به جامعه نمونه مراجعه گردید. در جدول (۲) حوزه‌های اصلی مدل مفهومی و تعداد گویه‌های (چالش‌ها) گردآوری شده برای هریک از حوزه‌ها آمده است.

جدول(۲) حوزه‌های اصلی مدل مفهومی و تعداد گویه‌های (چالش ها) پرسشنامه

ردیف	حوزه های اصلی مدل مفهومی	تعداد گویه‌ها
۱	حوزه عرضه	۲۷
۲	حوزه تقاضا	۲۵
۳	حوزه حکمرانی	۲۳
۴	حوزه امنیت	۱۷
	جمع کل گویه‌ها	۹۲

در جدول(۳) به طور خلاصه و اجمالی درصد فراوانی نظرات پاسخگویان درباره حوزه‌های مختلف آمده‌است.

جدول(۳) درصد فراوانی نظرات پاسخگویان چالش‌های توسعه اینترنت اشیاء در حوزه سلامت

ردیف	نظرات پاسخگویان درباره میزان تاثیرگذاری چالش‌ها	تعداد چالش‌ها	درصد فراوانی پاسخ‌ها				
			خیلی زیاد	زیاد	متوسط	کم	خیلی کم
۱	حوزه عرضه	۲۷	۷۳	۱۹	۴	۲	۲
۲	حوزه تقاضا	۲۵	۶۳	۲۲	۹	۳	۳
۳	حوزه حکمرانی	۲۳	۴۶	۳۸	۱۲	۲	۲
۴	حوزه امنیت	۱۷	۶۲	۲۳	۱۰	۳	۲

داده‌های پرسشنامه برای تجزیه و تحلیل وارد نرم افزار SPSS گردید. سپس بر اساس میزان اهمیت، چالش‌ها بر اساس بالاترین نمرات اخذ شده و طبق دسته‌بندی حوزه‌های چهارگانه مرتب وجمع‌بندی گردید. مهمترین چالش‌های احصاء شده بر اساس بالاترین نمرات اخذ شده در جدول(۴) قابل مشاهده است. چالش‌های اساسی توسعه اینترنت اشیاء پزشکی استخراج شده به تفکیک چهار حوزه عرضه، تقاضا، حکمرانی و امنیت در آورده شده است.

جدول (۴) مهمترین چالش‌های توسعه امن اینترنت اشیاء پزشکی

حوزه	چالش‌ها	میزان اهمیت
عرضه	عدم راه‌اندازی کامل زیرساخت‌های ملی و حیاتی (شبکه ملی اطلاعات، شبکه شمس)	۸/۴۴
	فقدان یک سکوی یا پلتفرم ارزیابی شده و قابل اعتماد و سرویس دهنده به متقاضیان سلامت	۸/۳۸
	کمبود شبکه‌های متحرک کم‌مصرف، با توان و برد بالا و کمترین تاخیر ارسال داده	۸/۲۲
	کمبود نیروی انسانی متخصص و متعهد کارآزموده در حوزه زیست بوم اینترنت اشیاء پزشکی	۷/۸۳
	اهمیت ابعاد حقوقی اینترنت اشیاء از منظر حاکمیت، حقوق مصرف، رقابت و کسب وکارها	۷/۶۶
	جایگاه حقوق مالکیت فکری در توسعهٔ اینترنت اشیاء	۷/۵۵
	نبود مشوق‌های مالی دولتی و کمبود منابع مالی جهت تحقیق و توسعه اینترنت اشیاء پزشکی	۷/۳۸
تقاضا	عدم توانمندی همه اقشار جامعه در دسترسی مناسب به امکانات حوزه سلامت	۸/۵۰
	سیستم‌های جزیره‌ای پزشکی و عدم تبادل داده‌های سلامت بین مراکز درمانی کشور	۸/۳۲
	عدم تحقق رویکرد سلامت همه جانبه و ناعدالتی در سلامت کشور	۸/۱۵
	هزینه‌های بالای تجهیزات، زیرساخت‌های توسعه و عملیاتی کردن اینترنت اشیاء در سلامت	۸/۰۵
	محقق نشدن شعار اولویت پیشگیری بر درمان در جامعه	۷/۳۸
	رویکرد اقتصاد محوری حاکم بر نظام سلامت کشور	۷/۷۷
	فراگیر نبودن برنامه‌های سلامت و پزشکی از راه دور	۷/۷۲
حکمرانی	عدم تحقق کامل پرونده الکترونیک سلامت در کشور	۸/۴۱
	وجود چالش‌های ناشی از تحریم‌های بین المللی و عدم تعامل با کشورهای صاحب فناوری	۸/۲۹
	ضعف قوانین، مقررات، استانداردها و سیاست‌گذاری مدون در حوزه‌های سلامت و صنعت	۸/۲۵
	عدم راه اندازی شبکه سلامت بر بستر شبکه ملی اطلاعات	۸/۱۱
	تعامل ضعیف بین دستگاه‌های زیربط در نظام سلامت کشور	۷/۸۸
	نگاه جزیره‌ای حاکم بر داده‌های سلامت	۷/۸۸
	عملکرد جزیره‌ای و مجزا از یکدیگر نهادهای تصمیم‌گیر، مقررات گذار و بهره بردار مرتبط	۷/۸۸
امنیت	امنیت و حریم خصوصی در اینترنت اشیاء پزشکی	۸/۳۷
	امکان سرقت اطلاعات حوزه سلامت و ژنومیک کشور	۸/۳۵
	وجود تهدیدات سایبری متصور در حوزه اینترنت اشیاء پزشکی	۸/۳۴
	نیاز به ارتقای سطح امنیت در زیرساخت‌ها و فناوری‌های بکار رفته در این حوزه	۷/۹۴
	امکان تخریب و یا تغییر داده‌ها با توجه به ضعیف بودن تجهیزات اینترنت اشیاء	۷/۹۴

بحث

در این پژوهش به مطالعه چالش‌های توسعه اینترنت اشیاء در حوزه سلامت پرداخته‌ایم. هرچند مطالعات متعددی در این حوزه انجام شده است ولی مطالعه‌ای که به‌طور ویژه به بررسی کامل چالش‌های توسعه اینترنت اشیاء پزشکی در چهار حوزه عرضه، تقاضا، حکمرانی و امنیت بپردازد، در دسترس نیست. این مطالعه با ارائه مهم‌ترین چالش‌های توسعه اینترنت اشیاء پزشکی، چشم‌انداز مناسبی را در اختیار تصمیم‌گیران حوزه‌های سلامت و فناوری جهت بهره‌گیری در تدوین راهبردهای توسعه و پیاده‌سازی این فناوری در حوزه سلامت قرار می‌دهد.

یافته‌های این تحقیق (جدول-۴) نشان می‌دهد مهم‌ترین چالش بر سر راه توسعه اینترنت اشیاء پزشکی در میان چالش‌های موجود در چهار حوزه عرضه، تقاضا، حکمرانی و امنیت، مشکل عدم توانمندی همه اقشار جامعه در دسترسی مناسب به امکانات حوزه سلامت با میزان اهمیت ۸/۵۰ می‌باشد. کسب این امتیاز نشان می‌دهد تا زمانی که همه اقشار جامعه توانمندی لازم جهت دسترسی مناسب به امکانات حوزه سلامت را نداشته باشند امکان توسعه فناوری اینترنت اشیاء در حوزه سلامت مقدور نخواهد بود. بنابراین، اینترنت اشیاء پزشکی باید قابلیت امکان دستیابی افراد مجاز (پزشک، پرستار، رادیوژیست و فیزیوتراپ) را به تمامی اطلاعات پزشکی یک بیمار در محل‌های مختلف (بیمارستان‌ها و مطب پزشکان) فراهم نماید (نصیری و همکاران، ۱۳۹۸: ۹۲). براساس بررسی‌های انجام شده در حال حاضر هزینه بالای ملزومات و تجهیزات مرتبط با بکارگیری اینترنت اشیاء در حوزه سلامت موجب مقاومت بیماران در برابر تغییر سبک درمان و استفاده از فناوری‌های جدید می‌باشد (Al-Shargabi & Abuarqoub, 2020) همچنین راه‌اندازی فناوری جدید برای حوزه‌های درمانی بخش سلامت نیز با چالش تامین هزینه‌های مرتبط با طراحی، پیاده سازی و اجرا همراه خواهد بود (قدیانی و همکاران، ۱۳۹۸: ۱۱۵).

چالش عدم راه‌اندازی کامل زیرساخت‌های ملی و حیاتی (شبکه ملی اطلاعات و شبکه شمس) با میزان اهمیت ۸/۴۴ در رتبه دوم چالش‌ها قرار گرفته است. نقایص موجود در زیرساخت‌های فناوری اطلاعات کشور مانع توسعه سلامت الکترونیک است (نقیپور و احمدی، ۱۳۹۷: ۲۴۰) و برای توسعه امن و پایدار فناوری اینترنت اشیاء پزشکی نیاز است زیرساخت‌های فناوری اطلاعات در حوزه سلامت کشور به‌طور کامل راه‌اندازی و مورد بهره-برداری قرار گیرد. و در این راستا ایجاد نظام واحد رگولاتوری سلامت الکترونیک، تضمین سرویس‌های خدمات الکترونیک بین دستگاهی در درگاه یکپارچه اطلاعات دولت و تامین

زیرساخت مراکز داده اصلی، پشتیبان و بحرانی، پیش‌نیاز شکل‌گیری نظام سلامت الکترونیک ایران خواهد بود (نقشه راه سلامت الکترونیک، ۱۳۹۸).

یافته‌های این تحقیق نشان داد که تحقق کامل پرونده الکترونیک سلامت در کشور به منظور تجمیع داده‌های اینترنت اشیاء پزشکی در پرونده الکترونیک سلامت بیماران، از ضروریات توسعه این فناوری در حوزه سلامت می‌باشد. این الزام با نتایج پژوهشی که توسط مرکز پژوهش‌های مجلس در خصوص بررسی پرونده الکترونیک سلامت در ایران در سال گذشته انجام پذیرفت همسو می‌باشد، مجموع نتایج حاصل از بررسی مطالعات انجام شده نشان داد که اگرچه تلاش‌های زیادی برای اجرا و پیاده‌سازی پرونده سلامت الکترونیک در ایران صورت گرفته است، با این حال فقدان نقشه و معماری کلان و یکپارچه، عدم تناسب ساختار اجرایی با ابعاد و گستردگی طرح، تغییرات مکرر مدیریتی، عدم تأمین اعتبارات کافی، عدم تحقق امضای الکترونیک، ضعف برخی زیرساخت ها و عدم پیش‌بینی سازوکارهای تضمین امنیت و محرمانگی اطلاعات، به عنوان مهمترین چالش‌ها و موانع در استقرار کامل پرونده الکترونیک سلامت در کشور نام برده است (بختیاری علی‌آباد، غضنفری و رجبی، ۱۴۰۱).

نتایج حاصل از اولویت‌بندی چالش‌ها در این پژوهش نشان داد که رتبه چهارم چالش-های مرتبط با توسعه اینترنت اشیاء پزشکی با میزان اهمیت ۸/۳۸، فقدان یک سکوی یا پلتفرم ارزیابی شده و قابل اعتماد و سرویس دهنده به متقاضیان سلامت بوده است. براساس پژوهش‌های صورت گرفته توسعه اینترنت اشیاء پزشکی در حال حاضر با چالش بزرگی تحت عنوان عدم وجود اپلیکیشن‌های استاندارد شده حوزه سلامت، زمان پیاده‌سازی و پذیرش این اپلیکیشن‌ها، دشواری‌های فنی و پیاده‌سازی‌های کوچک با تعداد بیماران محدود در سازمان‌های مربوط به سلامت، مواجه است (آیت الهی، میرانی و حقانی، ۱۳۹۴: ۷). به دلیل وجود تعداد بسیار زیادی شیء ناهمگن که هر کدام به پلتفرم متفاوتی تعلق دارند قابلیت همکاری بین این تجهیزات یکی دیگر از چالش‌های موجود اینترنت اشیاء پزشکی است. این چالش هم باید توسط تولیدکنندگان تجهیزات و هم توسعه‌دهندگان برنامه‌های کاربردی در نظر گرفته شود تا ارایه خدمت را برای همه افراد بدون در نظر گرفتن نوع پلتفرم آن‌ها تضمین کند (Al-Fuqaha, et al, 2015: 57). در نتیجه برای برآورده‌کردن نیاز مصرف‌کنندگان و اجرای سناریوهای مختلف بر اساس شرایط خاص، قابلیت همکاری یک معیار خیلی مهم در طراحی و ساخت خدمات اینترنت اشیاء است.

بر اساس یافته‌های پژوهش حاضر در حوزه امنیت، ۵ چالش عمده وجود دارد که امنیت و حریم خصوصی مهم‌ترین آنها در توسعه اینترنت اشیاء پزشکی در کشور می‌باشد. مسأله

حریم خصوصی و اطمینان از امنیت داده‌های سلامت در آینده، در گزارش سال ۲۰۱۶ شرکت فیلیپس تحت عنوان «شاخص آینده سلامت فیلیپس»، به عنوان مهم‌ترین دغدغه عمومی مشترک تمامی کاربران، آمده است (Philips future health index, 2016). واژه امنیت در اینترنت اشیاء گستره بزرگی از مفاهیم، مولفه‌ها و الزامات امنیتی همچون محرمانگی، تصدیق یا احراز هویت، تمامیت، عدم انکار، اعطای مجوز و کنترل دسترسی را در بر می‌گیرد که این الزامات با استفاده از مکانیسم‌های مختلف امنیتی فراهم می‌شود (فرزینفرد و موحدی صفت، ۱۳۹۹: ۴۶). محرمانه بودن اطمینان می‌دهد که سیستم اینترنت اشیاء از انتشار اطلاعات پزشکی توسط اشخاص غیر مجاز (کاربران و دستگاه‌ها) ممانعت به عمل می‌آورد (Farahani, et al, 2018: 659). حریم خصوصی به این معنی است که اسرار و داده‌های شخصی بیماران بدون رضایت نباید فاش شود. سیستم اینترنت اشیاء باید مطابق با سیاست‌های حفظ حریم خصوصی باشد که به کاربران اجازه می‌دهد داده‌های خصوصی خود را کنترل کنند (Mosenia & Jha, 2017: 586). یکی دیگر از چالش‌های امنیتی موجود، نیاز به ارتقای سطح امنیت در زیرساخت‌ها و فناوری‌های بکار رفته در اینترنت اشیاء پزشکی می‌باشد که در این خصوص افزایش امنیت سایبری و تاب آوری سایبری در زیرساخت‌ها و دستگاه‌ها برای غلبه بر مخاطرات و رسیدن به بالاترین سطح اعتمادپذیری از الزامات آن می‌باشد. از مهمترین نیازمندی‌های تاب‌آوری اینترنت اشیاء پزشکی می‌توان به قابلیت اطمینان، قابلیت نگهداری، ایمنی، تمایل به بقاء و کارایی، اشاره نمود (Nasiri, et al, 2019: 253).

چالش بعدی توسعه اینترنت اشیاء پزشکی در کشور، نبود قوانین و مقررات، استانداردها و سیاست‌های مدون و یکپارچه در حوزه امنیت می‌باشد. نهاد انجمن استانداردهای ارتباطاتی اروپا[1]، که یک سازمان استانداردسازی غیرانتفاعی و مستقل اروپایی در صنعت مخابرات است در ابتدای سال ۲۰۱۹ سندی با عنوان "امنیت سایبری برای مصرف‌کننده اینترنت اشیاء" با هدف حمایت از همه سازمان‌ها و شرکت‌های درگیر در تولید و توسعه شبکه اینترنت اشیاء از طریق محفوظ نگه داشتن محصولات تولیدی، منتشر کرده است که می‌تواند راهنمای مناسبی جهت توسعه امنیت برای تولید کنندگان محصولات اینترنت اشیاء پزشکی در داخل کشور باشد (ETSI, 2019).

از طرفی در حوزه امنیت با چالش امکان سرقت اطلاعات حوزه سلامت و ژنومیک کشور مواجه می‌باشیم. در حوزه پزشکی برنامه‌های کنترل و پایش سلامت و خدمات عملیاتی مبتنی بر اینترنت اشیاء به طور فزاینده‌ای در برابر هرگونه اختلال و یا سرقت اطلاعات

1. ETSI

آسیب‌پذیر هستند (فرزینفرد و موحدی صفت، ۱۳۹۹: ۴۶). چالش بعدی حوزه امنیت به وجود تهدیدات سایبری مرتبط با اینترنت اشیاء پزشکی اشاره می‌نماید. یکی از خطرناک‌ترین اهداف حملات سایبری، بخش بهداشت و درمان است دستگاه‌های پزشکی نیز مانند سایر سیستم‌های رایانه‌ای می‌توانند در برابر حملات امنیتی آسیب‌پذیر باشند و این حملات می‌تواند بر روی امنیت و کارایی دستگاه تأثیرگذار باشد. این آسیب‌پذیری با افزایش اتصال دستگاه‌های پزشکی و شبکه‌های بیمارستانی به اینترنت افزایش می‌یابد (Conti, et al, 2018: 544). از آن جایی که نمی‌توان حملات امنیتی سایبری را به طور کامل حذف نمود سازندگان دستگاه‌های پزشکی، بیمارستان‌ها و ... باید این حملات را مدیریت نمایند. در واقع لازم است بین افزایش کارایی دستگاه‌های پزشکی و توسعه فناوری‌های نو و تضمین امنیت بیماران تعادل مناسبی را برقرار نمود (Burns, et al., 2016). سازمان غذا و داروی آمریکا برای کاهش و یا مدیریت حملات امنیتی سایبری به سازندگان دستگاه‌های پزشکی و ابزارهای سلامتی توصیه می‌کند همواره در مورد خطرات امنیتی مربوط به این دستگاه‌ها در حالت آماده باش کامل باشند و خطرات امنیتی که متوجه بیماران است را به حد کافی کاهش داده و از عملکرد مناسب دستگاه اطمینان حاصل نمایند. همچنین بیمارستان‌ها و ارائه‌دهندگان خدمات سلامت را مسئول می‌داند تا امنیت شبکه خود را ارزیابی نموده و سیستم‌های بیمارستانی خود را در مقابل حملات سایبری محافظت نمایند (FDA, 2018).

رتبه هشتم چالش‌های مهم توسعه اینترنت اشیاء پزشکی، سیستم‌های جزیره‌ای پزشکی و عدم تبادل داده‌های سلامت بین مراکز درمانی کشور است که در حوزه تقاضا قرار دارد. این چالش به عملکرد جزیره‌ای و مجزا از یکدیگر نهادهای تصمیم‌گیر، مقررات‌گذار و بهره‌بردار، نهادها و دستگاه‌های حاکمیتی اشاره دارد (فروم اینترنت اشیاء ایران، ۱۳۹۵). بررسی‌ها نشان می‌دهد در حال حاضر از مجموع حدوداً ۱۷۰ هزار مراکز ارائه خدمت سلامت در کل کشور، کمتر از ۳۰ هزار مرکز به مرکز تبادل اطلاعات سلامت کشور اتصال یافته‌اند. (بختیاری علی‌آباد، غضنفری و رجبی، ۱۴۰۱). از طرفی در سطح کشور در حوزه نظام سلامت بین ساختارها و کارکردهای سازمان‌ها، نهادها و بخش‌های مسئول، هماهنگی مناسبی وجود ندارد (حکمرانی اینترنت اشیاء، ۱۳۹۷). در راستای رفع این چالش توجه به اسناد بالادستی و سیاست‌های کلی نظام سلامت و همچنین الزام بخش‌های مختلف به رعایت سیاست‌ها، رویه‌ها و دستورالعمل‌های ابلاغی می‌تواند راه‌گشا باشد.

از منظر دولت آمریکا مهمترین چالش‌های پیشرفت اینترنت اشیاء در زمینه مسائل میان حوزه‌ای مانند امنیت سایبری، حفظ حریم خصوصی، نوآوری و مالکیت معنوی، حاکمیت داده‌ها، توسعه استانداردها، مشارکت عمومی و خصوصی در سطوح مختلف محلی، ملی و

بین‌المللی می‌باشد (World Bank Group, 2017). که با چالش‌های احصاء شده دراین پژوهش حاضر، کاملا مطابقت دارد.

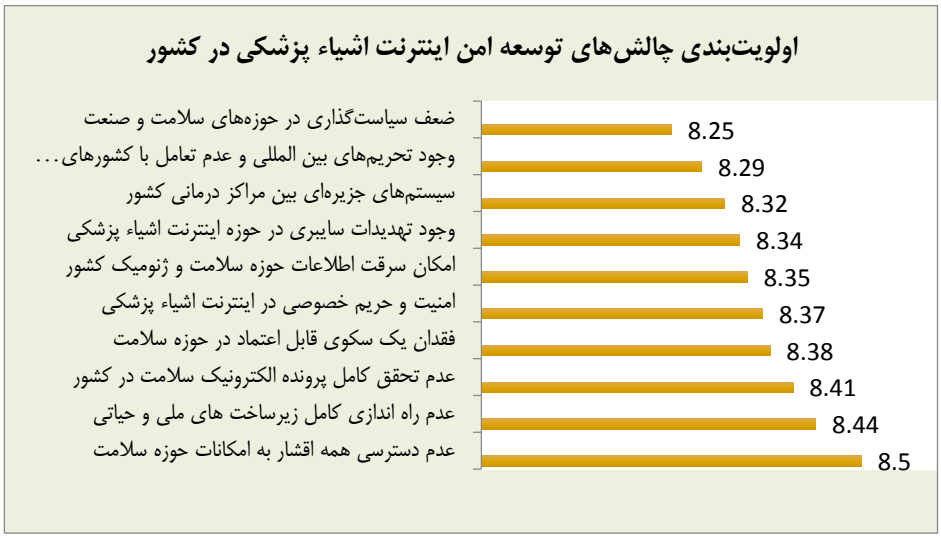
یافته‌های این پژوهش نشان داد که به چالش کمبود نیروی انسانی متخصص و متعهد کارآزموده در حوزه زیست بوم اینترنت اشیاء پزشکی و مقوله آموزش و آگاهی کاربران کمتر توجه شده است. این چالش در کنار فرهنگ، در پژوهش سعیدی و خاطری به عنوان یکی از مشکلات و چالش‌های کلیدی در پیاده‌سازی اینترنت اشیاء در نظر گرفته شد (Unbehagen & Miller, 2016). این در حالی است که می‌بایست به نیروی انسانی بسان سرمایه «سرمایه انسانی» نگریسته شود که می‌تواند به عنوان نیروی محرکه دانشگاه‌ها، مراکز تحقیقاتی و صنعتی نقش ایفا کند (Jackson, Rahman, 2019).

با توجه به چالش‌های پیش گفته، پیشنهاد می‌شود در راستای توسعه امن اینترنت اشیاء پزشکی در کشور و مراکز نظامی و با هدف ارتقاء سلامت و خدمات‌دهی به بیماران، جانبازان، معلولین و سالمندان، طبق اولویت‌های تعیین شده، نسبت یکسان‌سازی نحوه خدمات دهی در مراکز درمانی، راه‌اندازی کامل زیرساخت‌های ملی و حیاتی (شبکه ملی اطلاعات)، تکمیل پرونده الکترونیک سلامت در کشور، ایجاد یک سکوی قابل اعتماد و سرویس دهنده به متقاضیان سلامت، تامین امنیت و حریم خصوصی در اینترنت اشیاء پزشکی و یکسان‌سازی سیستم‌های پزشکی جهت تبادل داده‌های سلامت بین مراکز درمانی کشور اقدام شود و با انجام اصلاحات لازم و ضروری شرایط توسعه امن اینترنت اشیاء پزشکی، فراهم شود.

نتیجه‌گیری

در این تحقیق چالش‌های توسعه امن اینترنت اشیاء پزشکی در کشور مورد بررسی و اولویت‌بندی قرار گرفت. در نمودار (۱) تعداد ده مورد از مهم‌ترین چالش‌های توسعه امن اینترنت اشیاء پزشکی کشور نشان داده شده است. نتایج این تحقیق که برای اولین بار در سطح کشور به ارزیابی چالش‌های توسعه امن اینترنت اشیاء پزشکی از چهار منظر عرضه، تقاضا، حکمرانی و امنیت پرداخته است نشان داد، بهره‌گیری از فناوری اینترنت اشیاء در حوزه سلامت نیازمند دست‌یابی به پیش‌نیازهایی همچون ارایه خدمات درمانی یکپارچه با شفاف سازی فرآیندها و فعالیت‌های مرتبط با اینترنت اشیاء پزشکی و توسعه پرونده الکترونیک برای همه افراد جامعه، یکپارچه کردن و به اشتراک گذاشتن پایگاه اطلاعات و داده‌های سلامت بین نهادهای مختلف مرتبط با بخش سلامت و ایجاد رگولاتوری واحد (قواعد، قوانین و مقررات) می‌باشد. با عنایت به اینکه توسعه فناوری نوین اینترنت اشیاء پزشکی نیازمند در اختیار داشتن زیرساخت‌های فناوری اطلاعات در سطح کشور است لذا

بایستی به راه‌اندازی کامل زیرساخت‌های ملی و حیاتی (شبکه ملی اطلاعات و شمس) و ابر اختصاصی سلامت، ایجاد یک سکوی اینترنت اشیاء قابل اعتماد و پایدار و همچنین ذاتی نمودن ملاحظات امنیت اطلاعات در چرخه اکتساب تجهیزات اینترنت اشیاء به‌طور ویژه توجه گردد. همچنین دولت و مسئولین مربوطه می‌توانند از طریق سیاست‌گذاری صحیح، انجام حمایت‌های مالی و غیرمالی، استفاده از ظرفیت شرکت‌های دانش بنیان، رفع نواقص و مشکلات موجود، بخش‌های مختلف حوزه سلامت را برای بهره‌گیری از امکانات و توانمندی-های بی‌شمار اینترنت اشیاء پزشکی، آماده و مجهز نمایند.



نمودار(۱) اولویت‌بندی چالش‌های توسعه امن اینترنت اشیاء پزشکی در کشور

تشکر و قدردانی: بدین‌وسیله از تمامی اساتیدی که با بذل توجه و ارایه نظرات ارزشمند خود در غنا بخشیدن به مقاله حاضر نویسندگان را یاری نمودند سپاسگزاری می‌شود.

منابع:

- آیت الهی حسین، میرانی ناهید، حقانی حمید (۱۳۹۳). پرونده الکترونیک سلامت: مهمترین موانع چیست؟، چشم انداز مدیریت اطلاعات سلامت.
- بختیاری علی آباد، محمد، غضنفری، صادق و رجبی، ابوالقاسم(۱۴۰۱)، بررسی پرونده الکترونیک سلامت در ایران: الزامات قانونی و چالش‌های اجرا، معاونت پژوهش‌های اجتماعی و فرهنگی مجلس شورای اسلامی

- حسین زاده، کیامرث، چوبینه، علیرضا، و قائم، هاله. (۱۳۹۲). مطالعه روایی و پایایی نسخه فارسی چک لیست توانایی فردی در جمعیت کاری ایران. ارمغان دانش، ۱۸(۴ (پی در پی ۷۶))، ۲۹۵-۳۰۴. SID. https://sid.ir/paper/78093/fa
- دبیرخانه فروم اینترنت اشیاء ایران (IIF). (۱۳۹۵)، پیش نویس طرح جامع اینترنت اشیاء ایران چشم انداز، راهبردها و اقدامات اجرایی ۲۰۲۵، نسخه ۱، بهمن ۱۳۹۵
- سعیدی، فرحناز. خاطری، امیرحسین.(۱۴۰۰)، "بررسی چالش های کلیدی استفاده ازاینترنت اشیاء"، فصلنامه رویکردهای پژوهش نوین در مدیریت و حسابداری، سال پنجم، شماره ۸۳، پاییز۱۴۰۰. ص ۱۶-۱
- سیدحسینی پدرام، عبدالهی کامبیز، میرزا اقاخان مریم، فرهنگ ادیب سارا. (۱۳۹۷)"بررسی چالش های اینترنت اشیا در حوزه سلامت هوشمند". چهارمین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات
- غدیانی قراقانی، علیرضا. (۱۳۹۷). ارائه الگوی راهبردی اداره امور نظام سلامت از طریق تدوین تجارب نظام ج .ا.ا . بر اساس گفتمان ولایت فقیه و قانون اساسی. رساله دکتری، تهران: دانشگاه عالی دفاع ملی.
- فرزین فرد، منصور. موحدی صفت، محمدرضا. (۱۳۹۹) مدل معماری امنیت پایه برای صحنه نبرد مبتنی بر اینترنت اشیاء. فصلنامه علمی پژوهشی، پژوهش های حفاظتی امنیتی، شماره ۳۳، بهار۱۳۹۹
- محمدبیگی، ابوالفضل، محمدصالحیف نرگس، علی گل، محمد (۱۳۹۳). روایی و پایایی ابزارها و روش‌های مختلف اندازه‌گیری آنها در پژوهش‌های کاربردی در سلامت . مجله دانشگاه علوم پزشکی رفسنجان. ۱۳۹۳; ۱۳ (۱۲) :۱۱۵۳-۱۱۷۰
- مرکز ملی فضای مجازی (۱۳۹۸). اینترنت اشیاء
- نصیری، سمیه، صدوقی، فرحناز، تدین، محمدحسام و دهناد، افسانه (۱۳۹۷)، مکانیسم های امنیت و حریم خصوصی اینترنت اشیا در صنعت بهداشت و درمان غیربهداشتی، فصلنامه علمی پژوهشی مدیریت سلامت، دوره ۲۲، شماره ۷۳، صص. ۱۰۵-۸۶.
- نقشه راه سلامت الکترونیک ۱۴۰۰- ۱۳۹۸ (۱۳۹۸)، مرکز مدیریت آمار و فناوری اطلاعات، وزارت بهداشت درمان و آموزش پزشکی، تهران، ۱۳۹۸
- نقی پور، مجید. احمدی، مریم. (۱۳۹۶). بررسی برنامه ریزی استراتژیک سلامت الکترونیک و مروری بر موانع و چالش های موجود در کشور ایران، مجله علوم پزشکی دانشگاه آزاد اسلامی. دوره ۲۷، شماره ۴، زمستان ۱۳۹۶، صفحات ۲۴۳ -۲۳۷
- همتی نژاد فرزاد، مقدسی علی.(۱۳۹۹)، "الزامات مدیریت امنیت اینترنت اشیاء در بهداشت و درمان". چهارمین همایش ملی تحقیقات کاربردی در علوم اقتصاد، مدیریت و حسابداری

- Aileni RM, Suciu G, Valderrama Sukuyama CA, Pasca S, Maheswar R.; Cybersecurity technologies for the internet of medical wearable devices (iomwd). (2020). Advances in Cyber Security Analytics and Decision Systems: Springer; 2020. https://doi.org/10.1007/978-3-030-19353-9_6
- Al-Fuqaha, A. Guizani, M. Mohammadi, M. Aledhari, M & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols and Applications. IEEE Communications Surveys & Tutorials, vol. 17. pp. 2347-2376. https://doi.org/10.1109/COMST.2015.2444095
- Al-Shargabi, Bassam & Abuarqoub, Simak, (2020), IoT-Enabled Healthcare: Benefits, Issues and Challenges, ICFNDS '20, November 26, 27, 2020, St.Petersburg, Russian Federation, DOI:10.1145/3440749.3442596
- Aref, A. & Tran, T. (2017). Multi-criteria trust establishment for Internet.
- Bashir S, Dahlman CJ, Kanehira N, Tilmes K. The Converging Technology Revolution and Human Capital: Potential and Implications for South Asia. Washington, DC. South Asia Development Forum. 2021;
- Burns AJ et al. A brief chronology of medical device security. Communications of the ACM, 2016. Available from: https://cacm.acm.org/magazines/2016/10/207766-a-brief-chronology-of-medical-device-security/fulltext.
- Conti M, Dehghantanha A, Franke K, Watson S. (2018). Internet of Things security and forensics Challenges and Opportunities. Future Generation Computer Systems, 78(3): 544–546. DOI:10.1016/j.future.2017.07.060
- Deloitte (2018), Medtech and the Internet of Medical Things: How connected medical devices are transforming health care, Deloitte Development LLC, July 2018.
- ETSI (2019), Cyber Security for Consumer Internet of Things, ETSI Technical Specification, TS 103 645 v1.1.1, 2019.
- Farahani B, Firouzi F, Chang V, Badaroglu M, Constant N, Mankodiya K. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Generation Computer Systems. 2018; 78: 659-76. https://doi.org/10.1016/j.future.2017.04.036
- FDA (2018), Overview of Device Regulation, FDA, 2018, Available from: https://www.fda.gov/medicaldevices/device regulation and guidance/overview/default.htm.
- Gabriel AJ, Darwsih A, Hassanien AE. Cyber Security in the Age of COVID-19. Digital Transformation and Emerging Technologies for Fighting COVID-19 Pandemic: Innovative Approaches: Springer; 2021. p. 275-95. DOI: 10.1007/978-3-030-63307-3_18
- Gupta, B. and Quamara, M."An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," Concurrency and Computation: Practice and Experience, pp. 291-319, 2018. DOI:10.1002/cpe.4946.
- Hameed SS, Hassan WH, Latiff LA, Ghabban F. A systematic review of security and privacy issues in the internet of medical things; the role of

machine learning approaches. PeerJ Computer Science. 2021; 7:e414. DOI:10.7717/peerj-cs.414

- Jackson Jr GW, Rahman SS. Exploring Challenges and Opportunities in Cybersecurity Risk and Threat Communications Related To The Medical Internet Of Things (MIoT). International Journal of Network Security & Its Applications (IJNSA) Vol. 11; 2019. https://doi.org/10.48550/arXiv.1908.00666
- Jain, A.K. G, Choudhary. (2016). "Internet of Things: A Survey on Architecture, Technologies, Protocols and Challenges". IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2016), December 23-25, 2016, Jaipur, India. DOI:10.1109/ICRAIE.2016.7939537
- Lallie HS, Shepherd LA, Nurse JR, Erola A, Epiphaniou G, Maple C, et al. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security. 2021; 10 5:102248 https://doi.org/10.1016/j.cose.2021.102248.
- Mosenia A, Jha NK. A Comprehensive Study of Security of Internet- of-Things. IEEE Trans Emerg Top Comput. 2017; 5(4): 586- 602. https://doi.org/10.1109/TETC.2016.2606384
- Nasiri S, Sadoughi F, Tadayon MH, Dehnad A. Security requirements of internet of things-based healthcare system: A survey study. ACTA INFORM MED. 2019 DEC 27(4): 253-258. doi:10.5455/aim.2019.27.253-258
- Philips future health index (2016). The capacity to care: Measuring perceptions of accessibility and integration of healthcare systems, and adoption of connected healthcare. Philips future health index, 2016.
- Pradhan B, Bhattacharyya S, Pal K. IoT-Based Applications in Healthcare Devices. Journal of Healthcare Engineering. 2021;2021. https://doi.org/10.1155/2021/6632599
- Saini G. Security Vulnerabilities And Mitigation Challenges In IOT Based Healthcare Systems. International Journal of Modern Agriculture. 2021; 10(2):495-508.
- Sweta Anmulwar, Anil Kumar Gupta, and Mohammad Derawi, (2020), Challenges of IoT in Healthcare, Centre for Development of Advanced Computing (C-DAC) R&D, Springer Nature Switzerland AG, DOI:10.1007/978-3-030-42934-8_2
- Unbehagen Paul, Miller Eric. "The Internet of Things for Healthcare", Las Vegas, 2016.
- Wazid M, Das AK, Rodrigues JJ, Shetty S, Park Y. IoMT malware detection approaches: analysis and research challenges. IEEE Access. 2019; 7:182459-182476. DOI:10.1109/ACCESS.2019.2960412
- World Bank Group (2017). "Internet of things the new government to business platform", Available at: http://documents.worldbank.org/curated/en/610081509689089303/Internet-of-things-the-new-government-to-business-platform-a-review-of-opportunities-practices-and-challenge.