Journal of Combat Medicine
2023; 6(1): 11-17
10.30491/JCM.2024.430809.1020
Narrative Review

Cyber Security Challenges of the Health Section: A Review Study

Kourosh Narimani [1*], Mona Ahmadi [1], Parisa Farhangi [1]

[1] *Department of Nursing, Maragheh Branch, Islamic Azad University, Maragheh, Iran*

Received: 16 December 2022 **Accepted:** 27 January 2023

Abstract

Background and Aim: The advancement of technology and the subsequent change in the way of recording and storing medical data have created challenges in terms of privacy and security of people's health information, which is one of the most important controversial topics in this era. Because these data are of special importance for people and the health system, these challenges can affect people's lives sometimes effectively and sometimes ineffectively. The purpose of this article is to identify the challenges of information security in the field of health. The purpose of this paper is to identify the challenges of information security in the field of health.

Methods: This study results from a search in Iran doc, Civilica, MagIran, SID, PubMed, and Google Scholar websites. Articles whose full text was not available and articles that were repeated were also excluded from the study process. Also, articles in Persian and English since 2015 Using cyber security keywords, health domain, cyber security, cyberattack, and finally 30 articles were selected and entered the study process.

Results: Surveys showed that cyber security in the field of health means safe access to clients' information in a confidential manner, which the main challenges are information confidentiality, hackers attack, secure data storage, and secure data sharing.

Conclusion: Using technology to record and store medical data and information, despite safe storage, easy access and many advantages due to the possibility of cyberattacks, can be considered the biggest threat to patients, treatment teams, and policymakers.

Keywords: Cyber Security, Cyber Attack, Health Section.

*** Corresponding Author:** Kourosh Narimani
Address: Department of Nursing, Maragheh Branch, Islamic Azad University, Maragheh, Iran.
E-mail: Narimanyk@yahoo.com

نشریه بهداری رزمی دفاع مقدس و مقاومت
۱۴۰۲: دوره ۶: شماره ۱: صفحات: ۱۷-۱۱
10.30491/JCM.2024.430809.1020
مروری روایتی

چالش‌های امنیت سایبری درحوزه سلامت: مطالعه مروری

کوروش نریمانی[۱*]، مونا احمدی[۱]، پریسا فرهنگی[۱]

[۱] گروه پرستاری، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران

دریافت مقاله: ۱۴۰۱/۰۹/۲۵ **پذیرش مقاله:** ۱۴۰۱/۱۱/۰۷

چکیده

زمینه و هدف: با پیشرفت فن‌آوری و به دنبال آن تغییر در نحوه ثبت و ذخیره داده‌های پزشکی، چالش‌هایی در راستای حریم خصوصی و امنیت اطلاعات سلامت افراد به وجود آمده است که از مهمترین مباحث بحث‌برانگیز در این عصر به شمار می‌رود، زیرا این داده‌ها برای افراد و نظام سلامت از اهمیت خاصی برخوردار است که این چالش‌ها می‌تواند زندگی افراد را گاه به صورت مؤثر و گاه غیر مؤثر تحت تأثیر قرار دهد. هدف مقاله حاضر در ارتباط با شناسایی چالش‌های امنیت اطلاعات در حوزه سلامت است.

روش‌ها: مطالعه انجام شده نتیجه جستوجو در پایگاه‌های Google Scholar, PubMed, SID, MagIran, Civilica, Iran doc است. مقاله‌هایی که متن کامل آن‌ها در دسترس نبود و مقالاتی که تکرار شده بودند و همین‌طور مقالات با ارتباط کمتر از روند مطالعاتی حذف شدند. همچنین مقالات به زبان‌های فارسی و انگلیسی از سال ۲۰۱۵ با استفاده از کلیدواژه‌های امنیت سایبری، حوزه سلامت، Cyber Security، Cyber Attack مورد بررسی قرار گرفتند و در نهایت ۳۱ مقاله انتخاب و وارد روند مطالعه گردیدند.

یافته‌ها: بررسی‌ها نشان داد امنیت سایبری در حوزه سلامت به معنای دسترسی ایمن به اطلاعات مددجویان به‌صورت محرمانه است که چالش‌های اصلی پیش‌رو شامل محرمانه‌بودن اطلاعات، حمله نفوذگران، ذخیره‌سازی ایمن داده‌ها و اشتراک‌گذاری ایمن داده‌ها است.

نتیجه‌گیری: استفاده از تکنولوژی برای ثبت و ذخیره داده‌ها و اطلاعات پزشکی علی‌رغم ذخیره‌سازی ایمن، دسترسی آسان و مزایای بسیاری که دارد با توجه به احتمال حملات سایبری می‌تواند خود به‌عنوان بزرگترین تهدید برای بیماران، تیم درمان و سیاست‌گذاران باشد.

کلیدواژه‌ها: امنیت سایبری، حمله سایبری، حوزه سلامت.

* **نویسنده مسئول:** کوروش نریمانی
آدرس: گروه پرستاری، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران.
ایمیل: Narimanyk@yahoo.com

مقدمه

در طول تاریخ بشر، به دلیل نوآوری که آینده بشریت را تشکیل می‌دهند، بسیاری از فن‌آوری‌ها ابداع شده‌اند و در حال حاضر برای تسهیل زندگی مردم استفاده می‌شوند (۱). از آن‌جایی که مهمترین و اولین نیاز مردم سلامتی می‌باشد، بدیهی است که حوزه بهداشت و درمان از حوزه‌های زیرساختی مهم کشور می‌باشد که از این نوآوری‌ها مستثنی نیست (۲). عصری که در آن زندگی می‌کنیم را «عصر سایبری» نام نهاده‌اند (۳). واژه فضای سایبر نخستین بار در سال ۱۹۸۰ توسط ویلیام گیبسون (William Gibson) معرفی شد و از آن زمان تاکنون این مفهوم و عناصر اصلی آن در یک سیر تاریخی توسعه و تکامل یافته و جهان با سرعت و شتاب روزافزون به سمت جامعه سایبری- فیزیکی یا جامعه الحاقی در حرکت است (۴). فضای سایبری چشم‌انداز سیستم مراقبت‌های بهداشتی را در سراسر جهان تغییر داده است و یک تحول تدریجی و سیستماتیک در سیستم‌های مراقبت‌های بهداشتی ایجاد کرده است که رویه مراقبتی را از سوابق کاغذی به سوابق الکترونیکی سوق داده و انقلابی را در صنعت مراقبت‌های بهداشتی به‌وجود آورده‌است (۵)، اما نگرانی در مورد حریم خصوصی و امنیت که به اطلاعات بیمار مربوط می‌شود، باعث پذیرش نسبی توسط تعدادی از مؤسسات بهداشتی شده (۶) و در نتیجه نیازمند ارائه راهکارهای حفاظتی لازم برای نگهداری از آن‌ها است (۴).

ارائه خدمات بهداشتی با استفاده از فن‌آوری دیجیتال به‌عنوان «سلامت الکترونیک» نامگذاری می‌شود (۷). سازمان بهداشت جهانی، سلامت الکترونیک را به این صورت تعریف کرده است: «سلامت الکترونیک به معنای انتقال منابع سلامت و مراقبت‌های بهداشتی از طریق وسایل الکترونیکی است که شامل سه حوزه اصلی است: ارائه اطلاعات پزشکی به فرد متخصص از طریق اینترنت و ارتباطات راه دور، استفاده از فن‌آوری اطلاعات و تجارت الکترونیکی برای بهبود خدمات پزشکی از طریق آموزش افراد مرتبط و استفاده از تجارت الکترونیکی و کسب وکار الکترونیکی در مدیریت سامانه پزشکی» (۸). با این حال، هنگامی که کاربران اطلاعات پرونده الکترونیک سلامت را در سرورهای ابری ذخیره می‌کنند، با انواع تهدیدات امنیتی مانند نقض حریم خصوصی بیماران، یکپارچگی داده‌ها و احراز هویت آن‌ها مواجه می‌شوند. بنابراین، خطرات بسیار زیادی متوجه مدیریت متمرکز داده‌های پزشکی است. داده‌های پزشکی می‌توانند به‌راحتی سرقت، دستکاری و یا حتی به‌طور کامل حذف شوند. در این موارد نمی‌توان داده‌های پزشکی را به‌صورت قابل اعتماد ضبط یا بازیابی کرد، که موجب تأخیر در فرآیند درمان و یا حتی به خطر انداختن زندگی بیمار خواهد شد (۷). در نتیجه امنیت و حریم خصوصی کاربران در سلامت الکترونیک از چالش‌های مهم محسوب می‌شود (۹) و باید به آن توجه ویژه‌ای شود (۱۰). از آن جایی که اطلاعات به‌عنوان یک دارائی مهم و باارزش محسوب می‌شود، ارائه راهکارهای حفاظتی لازم برای نگهداری از آن‌ها در اولویت است. بر این اساس یکی از ضروریات امنیت اطلاعات فضای سایبر، شناخت ابعاد، مؤلفه و شاخص‌های امنیت اطلاعات فضای سایبر و داشتن یک مدل مفهومی کلان می‌باشد (۱۱). باوجود افزایش تمرکز بر امنیت پرونده‌های الکترونیکی سلامت و تلاش شهرهای بزرگ سراسر جهان برای بهبود زیرساخت‌های امنیتی و دسترسی در قالب شهرهای هوشمند، دستبرد و نقض حریم خصوصی اطلاعات بیماران همچنان به‌نحوی فراگیر از دغدغه‌های مهم پیش روی سامانه‌های الکترونیکی سلامت است. استفاده و افشای غیرمجاز داده‌ها منجر به ناامنی‌های جسمی و روانی برای افراد جامعه می‌شود (۸). بنابراین امنیت اطلاعات در محیط‌های مجازی و فضای سایبری به‌عنوان مهمترین الزام در توسعه فن‌آوری اطلاعات و ارتباطات می‌باشد (۱۲).

مطالعه حاضر به‌منظور بررسی مفاهیم پایه امنیت فضای سایبری و چالش‌های آن در پیرامون حوزه سلامت انجام شده‌است. مجموع این موضوعات اهمیت ایجاد محیط امن و پایدار در فضای سایبر خصوصاً امنیت اطلاعات را مشخص می‌کند (۱۱).

روش‌ها

این پژوهش یک مطالعه مروری است که با جست‌وجو بر مبنای چالش‌های امنیت سایبری در حوزه سلامت در پایگاه‌های علمی معتبر Google Scholar, PubMed, SID, MagIran, Civilica, Iran doc و با استفاده از کلیدواژه‌های امنیت سایبری، حوزه سلامت، Cyber Security، Cyber Attack انجام گرفته است. ابتدا چکیده مقالات مرتبط با تحقیق را انتخاب نموده و با بررسی متن کامل مقالات، مقالات غیر مرتبط و تکراری و مقالاتی که متن کامل آن‌ها در دسترس نبود از روند مطالعاتی حذف گردیدند. مقالات منتخب به دو زبان فارسی و انگلیسی و با اعمال فیلتر سال (۲۰۲۳-۲۰۱۵) انتخاب گردیدند و در نهایت از میان ۵۱ مقاله‌ای که مورد مطالعه قرار گرفت، ۳۱ مقاله وارد روند مطالعاتی گردید.

نتایج

امروزه با توجه به گسترش استفاده از اینترنت در دو دهه اخیر، بیمارستان‌های سرتاسر دنیا نیز شروع به استفاده از این تکنولوژی کرده‌اند (۲). یکی از نوآوری‌های اخیر فن‌آوری اینترنت اشیاء، اطلاعات است که قصد دارد دنیای فیزیکی و دیجیتال را به هم وصل کند (۱۰) که ادغام دستگاه‌های پزشکی، شبکه، نرم‌افزار و سیستم‌های عامل از جمله آن‌هاست (۳). این ادغام تشخیص بیماران را بهبود می‌بخشد و همچنین امنیت و حریم خصوصی داده‌های مراقبت‌های بهداشتی آن‌ها را تعیین می‌کند (۱۳). این فن‌آوری‌ها رویه‌های کنترل نظارت خود را دیجیتالی کرده و به اینترنت متصل می‌شوند، که بسیاری از مسائل امنیتی و حریم

خصوصی را ایجاد می‌کند و از هم‌اکنون به یک خطر بزرگ تبدیل شده است (۱). علاوه‌بر این، رشد فن‌آوری و ارتباطات منجر به سناریویی شده است که به موجب آن داده‌های سلامت بیماران بر تهدیدات امنیتی و حریم خصوصی تأثیر می‌گذارد (۶). ثبت اطلاعات درمانی بیماران و همچنین ثبت الکترونیکی سوابق درمانی، مواردی هستند که هم‌اکنون به‌طور رایج در مراقبت‌های درمانی استفاده می‌شوند که در مقابل حملات سایبری آسیب‌پذیر هستند (۲).

استفاده از پرونده سلامت الکترونیکی یک رویکرد رایج برای ثبت اطلاعات پزشکی بیماران محسوب می‌شود (۷). مدارک پزشکی الکترونیکی می‌تواند مزایای بسیاری را برای پزشکان، بیماران و خدمات مراقبت‌های بهداشتی فراهم کند (۶). برای مثال دسترسی آسان‌تر و سریع‌تر به داده‌های بالینی، توانایی حفظ جریان کار بالینی مؤثر، کاهش خطاهای پزشکی و پشتیبانی بهتر و قوی‌تر برای تصمیم‌گیری بالینی (۱۴) و بهبود کیفیت مراقبت‌های بهداشتی می‌باشد (۶).

دانشمندان علم رایانه و انفورماتیک تلاش می‌کنند تا روش‌های دقیق حفظ حریم خصوصی و امنیتی را توسعه دهند (۶). بنابراین، روش‌های ممکن برای افزایش حفاظت از داده‌ها در طول فرآیند به اشتراک‌گذاری داده‌ها شامل اغتشاش داده‌ها (به‌عنوان مثال اضافه کردن نویز به داده‌ها) برای جلوگیری از نشت اطلاعات حساس (اشتراک‌گذاری داده‌ها با حفظ حریم خصوصی)، رمزگذاری و برون‌سپاری محاسبات به یک شخص ثالث قابل اطمینان، تحلیل ایمن با پشتیبانی سخت‌افزار محافظ نرم‌افزار (۱۵)، نصب نرم‌افزار آنتی‌ویروس، محاسبات ابری، ترتیب‌دهنده‌های ارزیابی اولیه ریسک، استخدام یک کارشناس ارشد امنیت اطلاعات و شناسایی فرکانس است (۶). اگر چه این فضا و به کارگیری فن‌آوری اطلاعات و ارتباطات امکانات بسیاری را فراهم آورده تا بخش قابل توجهی از فعالیت‌های انسانی با سرعت بیشتر و هزینه کمتر انجام گیرد؛ اما همین فن‌آوری اطلاعات با تسهیل زمینه و شیوه ارتکاب جرم و توسعه خسارت مادی و معنوی ناشی از جرم و ایجاد جرایم جدید و پدید آوردن شیوه‌های مجرمانه نوین، فرصت‌های طلایی زیادی را برای مجرمان فراهم کرده است (۱۲) و می‌تواند ایمنی بیمار را در تمامی جهات به‌طور قابل توجهی به‌خطر بیندازد (۳). در نتیجه وابستگی به این فن‌آوری باعث شده است که اگر در ارائه خدمات سیستم‌های اطلاعاتی خللی پیش‌آید سازمان‌ها نتوانند به کار خود ادامه دهند (۱۶).

داده‌های شخصی اطلاعاتی هستند که به یک شخص حقیقی شناسایی شده یا قابل شناسایی مربوط می‌شود (۱۷). داده‌های مربوط به حوزه پزشکی، از جمله موارد پرطرفدار در وب تاریک به‌شمار می‌روند، به‌نحوی که قیمت خرید و فروش آن‌ها حتی از اطلاعات کارت‌های بانکی هم بیشتر است (۱۸). امنیت یکی از نگرانی‌های اصلی مرتبط با نظارت بر مراقبت‌های بهداشتی است، زیرا داده‌های مهم می‌توانند به‌راحتی توسط هکرها خراب شوند؛ بنابراین، حریم خصوصی و حفاظت داده‌ها، ملاحظات مهمی با توجه به انتقال داده‌ها IOT (Internet Of Things) در سیستم‌های مراقبت‌های بهداشتی هستند (۱۹).

فن‌آوری‌های جذاب و فرامتنی توانسته‌اند زمینه جدیدی را برای انواعی از تعاملات اجتماعی، ابراز عقاید و سبک زندگی، ارتباطات و مبادلات تجاری و اطلاع‌رسانی و افزایش تحرک اجتماعی افراد فراهم سازند. این فضا علاوه‌بر مخاطرات و آسیب‌های بررسی شده، در صورت استفاده صحیح و آگاهانه جنبه‌های مثبتی را نیز شامل می‌شود (۲۰).

هم‌زمان با رونق بازار اینترنت اشیاء، امنیت سایبری نیز به یکی از موضوعات تبدیل شده‌است (۳). امنیت سایبری با توجه به دیدگاه حقوقی و اخلاقی داده‌های پزشکی بیمار، یک موضوع اولیه و چالش‌برانگیز در مراقبت‌های بهداشتی است (۲۱). حملات سایبری به اقداماتی گفته می‌شود که جامعه هدف یا گروه هدف را نشانه می‌گیرد و بدون درگیری نظامی و گشوده شدن آتش، رقیب را به شکست وا می‌دارد. بشر از آغازین روزهای حیاتش به فکر امنیت بوده است؛ چرا که همواره در معرض آسیب، تعرض و تهدید قرار داشته‌است. فضای سایبری زمینه را برای حملات متجاوزان فراهم می‌کند (۱۲). نهادهای دولتی، غیر دولتی و تروریست‌ها به این نتیجه رسیده‌اند که بیمارستان‌ها به‌ویژه نسبت به این نوع حملات حساس هستند (۱۸).

طبق نظر سازمان بین‌المللی استاندارد، پرونده‌های سلامت الکترونیکی، داده‌های بیمار را در قالب دیجیتال ذخیره می‌کنند و داده‌ها به‌صورت ایمن مبادله می‌شوند و تنها توسط افراد مجاز قابل دسترس هستند (۱۰). این اطلاعات شامل طیف گسترده‌ای از داده‌ها، مانند تاریخچه پزشکی، جمعیت‌شناسی، دارو، وضعیت ایمن‌سازی، گزارش تست‌های آزمایشگاهی و سایر اطلاعات حساس بیمار می‌باشد (۱۴). علاوه‌براین، پردازش داده‌های ژنتیکی، بیومتریک و سلامت که پتانسیل اکتشافات پزشکی قابل توجهی را در خود جای داده است، تحت تأثیر داده‌ها در رابطه با داده‌های شخصی، محدودیت‌های بیشتری قرار دارند که از حقوق مختلفی مانند حق اطلاعات، دسترسی، تصحیح و پاک کردن داده‌های خود برخوردار است (۱۷). بدون شک ورود به فضای مجازی بدون آگاهی و دانش کافی قطعاً زندگی اجتماعی بشر را تهدید خواهد کرد (۲۰).

چالش‌های عمده‌ای که سیستم‌های بهداشتی درمانی در حوزه امنیت سایبری پیش رو دارند بسیار وسیع می‌باشد که از جمله می‌توان به موارد زیر اشاره کرد.

محرمانه بودن اطلاعات

حساسیت برای جمع‌آوری جزئیات بیمار بسیار بالاست (۲۱). در حال حاضر اطلاعات پزشکی و سایر موارد محرمانه از طریق سیستم‌های بسیار امن محافظت می‌گردند (۱۷). محرمانگی را می‌توان از طریق ابزارهای تکنولوژیکی مانند رمزگذاری داده‌ها یا

از طریق کنترل دسترسی به سیستم‌ها تأمین کرد (۶).

حمله هکری

رشد سوابق پزشکی دیجیتال، سرقت هویت پزشکی را به آهنربایی برای هکرها تبدیل کرده و فن‌آوری اطلاعات نیز در مراقبت‌های بهداشتی سرمایه‌گذاری کرده‌است (۱۸). اگر سامانه به‌طور مخرب مورد حمله قرار گیرد، تمام گره‌ها از بین می‌روند و قادر به ذخیره و استفاده از داده‌ها نیستند (۷). به‌طور مثال در ایالات متحده آمریکا، هکرها سد مقاومتی را شکستند و با نفوذ به پایگاه داده سیستم‌های سلامت جامعه یک گروه بیمارستانی برجسته، به مقدار زیادی از اطلاعات سلامت شخصی، از جمله شماره تأمین اجتماعی بیش از یک میلیون بیمار دسترسی پیدا کردند (۱۴). این حمله‌های امنیتی به تدریج در حال توسعه هستند (۳).

ذخیره‌سازی ایمن داده‌ها

در بحث امنیت اطلاعات سلامت، سیستم‌های اطلاعات بالینی به‌دلیل اینکه مخزن داده‌ها و اطلاعات بیماران است، از حساسیت ویژه‌ای برخوردار می‌باشد. بنابراین، با توجه به فن‌آوری‌های به کاررفته در سیستم‌های اطلاعات بالینی و نوع اطلاعات ذخیره شده در آن‌ها، باید امنیت آن‌ها توسط سازمان‌ها تأمین گردد (۲۲). به‌منظور مدیریت بهتر پرونده‌های الکترونیکی سلامت، لازم است محل و نحوه ذخیره‌سازی اطلاعات مشخص گردد. پرونده بیمار از فایل‌های متنی و چندرسانه‌ای تشکیل شده است؛ اگر بنا باشد تمام محتویات پرونده بیمار را در بلوک ذخیره کنیم، یک تکنیک غیرایمن برای ذخیره‌سازی صورت گرفته ممکن است منجر به نقص در محافظت از داده‌های مراقبت‌های بهداشتی شود و بدین شکل هکرها می‌توانند به حساب‌های ایمیل، پیام‌ها و گزارش‌های بیماران دسترسی کامل پیدا کنند (۱۳).

اشتراک‌گذاری ایمن داده‌ها

اطلاعات موجود در اینترنت به روش‌های مختلفی ذخیره شده و با روش‌های گوناگونی قابل ارائه و انتقال هستند، صفحات وب یکی از راه‌های خاص ذخیره و ارائه اطلاعات در بین روش‌های متعدد ذخیره و ارائه اطلاعات در اینترنت هستند (۲۳). دستگاه‌های اینترنت اشیاء این مسئولیت را دارند که مطمئن شوند پیام‌ها و داده‌های ارسال شده توسط دستگاه به مقصد رسیده‌اند. برنامه‌های کاربردی اینترنت اشیاء تعامل بین دستگاه و دستگاه یا انسان را فعال می‌کنند (۱۰). با این حال داده‌های بیمار به دلیل نگرانی‌های حفظ حریم خصوصی و سیاست‌های اشتراک‌گذاری داده‌های سازمانی مرتبط، برای به اشتراک‌گذاری مستقیم و بدون هیچ گونه محافظتی بسیار حساس هستند (۱۵)؛ زیرا دستگاه‌ها، دارای حافظه و قدرت محدود هستند (۲۴).

تهدیدات

تهدیدات غیر مخرب عبارتند از؛ از دست دادن/ افشای تصادفی اطلاعات حساس، مانند افشای اطلاعات حساس بیمار به دیگران، به اشتراک‌گذاری رمز ورود، نوشتن رمز ورود به سیستم یا پاسخ به پیام‌های فیشینگ (۱۴). از این رو تهدیدات امنیتی و حریم خصوصی چالش‌های بزرگی در این شبکه هستند (۲۴). چه بسا تهدیدات این فضا محدود به امنیت اطلاعات فردی نباشد و می‌تواند در دایره‌های گسترده‌تری مثل دسترسی کشورهای بیگانه به اطلاعات محرمانه و سری کشور پیش برود (۲۰).

منابع انسانی

در شرایط حاضر کارکنان با استعداد، منبع حیاتی برای سازمان‌ها به‌شمار می‌آیند؛ منبعی که سازمان‌ها برای دستیابی به بهروری نیازمند آن می‌باشند. شواهد نشان می‌دهد که نیاز به کارکنان با استعداد در سازمان‌ها افزایش یافته است و این درحالی است که بازار نیروی کار حاکی از نبود منابع با استعداد به میزان کافی است (۲۵). از سویی دیگر با افزایش آگاهی کارمندان یک سازمان از امنیت اطلاعات، رعایت اصول امنیتی به تدریج نهادینه می‌شود و این امر به تغییر فرهنگ و ارزش‌های امنیتی کمک می‌کند (۱۶).

بحث

در سناریوی کنونی، فن‌آوری اطلاعاتی پیشرفته، دریچه جدیدی به روی نوآوری در زندگی روزمره ما گشوده است. از میان این فن‌آوری‌های اطلاعاتی، اینترنت اشیاء یک فن‌آوری نوظهور است که راه‌حل‌های بهبود یافته و بهتری را در زمینه پزشکی ارائه می‌کند، مانند نگهداری صحیح پرونده پزشکی، نتایج نمونه‌برداری و علل بیماری‌ها و حتی ادغام دستگاه‌ها (۲۶). بهداشت و درمان یکی از حوزه‌های کاربردی در اینترنت اشیاء است که توجه زیادی را از صنعت، جامعه تحقیقاتی و بخش عمومی به خود جلب می‌کند. توسعه اینترنت اشیاء و رایانش ابری باعث بهبود ایمنی بیمار رضایت کارکنان و کارآرایی عملیاتی در صنعت پزشکی می‌شود (۲۷).

فضای سایبری در معرض چالش‌ها، آسیب‌ها و تهدیدات الکترونیکی گوناگونی نظیر ارتکاب جرائم سازمان‌یافته، تخریب بانک‌های اطلاعاتی، حملات مختل‌کننده خدمات، جاسوسی، خرابکاری، نقض حریم خصوصی و نقض حق مالکیت معنوی قرار دارد؛ به‌طوری که نپرداختن یا رویکرد نادرست به امنیت این فضا، مانع بزرگی در به‌کارگیری امن فن‌آوری اطلاعات و ارتباطات و ورود به جامعه اطلاعاتی خواهد بود. امنیت فضای تبادل اطلاعات، برقراری شرایط و حالتی است که دارایی‌های این فضا از خطرات مختلف محفوظ بماند و بیم و دغدغه نسبت به تهدید سایر دارایی‌های مادی و معنوی جامعه نیز از این طریق جود نداشته‌باشد (۲۸). در این میان راه‌حل‌هایی برای حفاظت از حریم خصوصی برای کار با دستگاه‌هایی مانند کامپیوتر و تلفن‌های همراه طراحی شده‌اند که بعضی از این راه‌حل‌ها الزامات کم‌هزینه و قدرت پایین اشیاء را در نظر نمی‌گیرند (۲۹).

به‌طور کلی کاربردهای اینترنت اشیاء در حوزه سلامت، برای محیط‌های خاص طراحی شده‌اند و انتظار می‌رود بدون دخالت

دست یا با حداقل دخالت اپراتور انسانی، بسیار سریع و قابل اطمینان کار کنند؛ به‌عبارت دیگر شبکه‌های اینترنت اشیاء در حوزه پزشکی باید به اندازه کافی هوشمند باشند تا در شرایط مختلف بتوانند خود را با محیط تطبیق دهند و به اصطلاح خودتطبیق باشند و لزوم این قابلیت، داشتن سیستم تشخیص نفوذ و حمله در این شبکه‌ها است (۳۰). این موضوع بیانگر این نکته است که مؤسسات پزشکی باید به حفاظت از حریم خصوصی داده‌ها توجه ویژه‌ای داشته باشند (۳۱).

نتیجه‌گیری

پیشرفت فن‌آوری و ورود اینترنت اشیاء به زندگی انسان‌ها باعث تسهیل امور زندگی و بهبود روند ارتباطی در همه حوزه‌ها به خصوص حوزه بهداشت و درمان شده‌است، که با ورود آن به خدمات پزشکی و بیمارستانی، تحولی بزرگ در این زمینه فراهم آورده‌است. این فن‌آوری علاوه‌بر مزایای بسیاری که برای تیم درمان و بیماران دارد می‌تواند خود به‌عنوان تهدیدی برای افراد و جامعه باشد، افراد را با چالش‌هایی روبه‌رو کند و جامعه بشری را تحت تأثیر خود قرار دهد. به‌طور کلی، اینترنت اشیاء می‌تواند باعث بهبود و افزایش سرعت در خدمات بهداشتی و درمانی شود، اما لازم است مدیران خبره و مسئولیت پذیر به صورت ویژه امنیت اینترنت اشیاء را که حاوی اطلاعات شخصی افراد است، زیر نظر داشته و به‌صورت ویژه به آن بپردازند.

تضاد منافع: بدین وسیله نویسندگان تصریح می‌نمایند که هیچ‌گونه تضاد منافعی در مطالعه حاضر وجود ندارد.

منابع

1. Alabdulatif A, Thilakarathne NN, Lawal ZK, Fahim KE, Zakari RY. Internet of nano-things (iont): A comprehensive review from architecture to security and privacy challenges. Sensors. 2023;23(5):2807. doi:10.3390/s23052807
2. Narimani K, Ghani A. Cyber Security in hospitals. 3rd National Conference on Cyber Defens, 2022.
3. Narimani K, Farnoozi A. Cyber security of medical equipment. 3rd National Conference on Cyber Defens, 2022.
4. Karami Ghohroudi MR, Moeinazad S, Karimi E. Typology of the concept and main elements of cyberspace in national cyber security strategy of selected countries. Journal of National Security. 2023;47(13):9-36. [In Persian]
5. Chenthara S, Ahmed K, Wang H, Whittaker F. Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE Access. 2019;7:74361-82.
6. Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal. 2021;22(2):177-83. doi:10.1016/j.eij.2020.07.003
7. Pournaghi SM, Bayat M, Farjami Y. A novel and secure model for sharing protected health record (PHR) based on blockchain and attribute based encryption. Electronic and Cyber Defense. 2020;8(1): 101-24. [In Persian]
8. Rezaei M, Dorri Nogoorani S. Management of Electronic Health Records with Preservation of Privacy using the Blockchain Technology. Biannual Journal Monadi for Cyberspace Security. 2022;11(1): 48-58. [In Persian]
9. Mayabi Joghal M, Doostari MA. A Scheme for Improvement of Security and Privacy in Mobile Health Systems by Using SIM Card. Electronic and Cyber Defense. 2019;7(1):11-24. [In Persian]
10. Ratta P, Kaur A, Sharma S, Shabaz M, Dhiman G. Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives. Journal of Food Quality. 2021;2021:1-20. doi:10.1155/2021/7608296
11. Ghorbani V, Saghafi K. Designing a Conceptual Model for the Information Security of the Islamic Republic of Iran's Cyberspace. National Security. 2019;9(33):315-53. [In Persian]
12. Narimani K, Jafari B. Cyberattacks and threats in the field of health and hygiene. 3rd National Conference on Cyber Defens, 2022.
13. Hathaliya JJ, Tanwar S. An exhaustive survey on security and privacy issues in Healthcare 4.0. Computer Communications. 2020;153:311-35. doi:10.1016/j.comcom.2020.02.018
14. Chenthara S, Ahmed K, Wang H, Whittaker F. Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access. 2019;7:74361-82. doi:10.1109/ACCESS.2019.2919982
15. Kuo TT, Jiang X, Tang H, Wang X, Harmanci A, Kim M, et al. The evolving privacy and security concerns for genomic data analysis and sharing as observed from the iDASH competition. Journal of the American Medical Informatics Association. 2022;29 (12):2182-90. doi:10.1093/jamia/ocac165
16. Kahouei M, Abbasi Z. The prioritization of effective factors on electronic health information security in medical centers. Health Information Management. 2015;12(2):162-170. [In Persian]
17. Brauneck A, Schmalhorst L, Kazemi Majdabadi MM, Bakhtiari M, Völker U, Baumbach J, et al. Federated machine learning, privacy-enhancing technologies, and data protection laws in medical research: Scoping review. Journal of Medical Internet Research. 2023;25:e41588. doi:10.2196/41588
18. Narimani K, Shojaei S, Mohammadzadeh M. The impact of cyberattacks on medical centers. Cyberattacks and threats in the field of health and hygiene. 3rd National Conference on Cyber Defens, 2022.
19. Upadhyay S, Kumar M, Upadhyay A, Verma S, Kavita, Kaur M, et al. Challenges and Limitation Analysis of an IoT-Dependent System for Deployment in Smart Healthcare Using Communication Standards Features. Sensors. 2023;23(11):5155. doi:10.3390/

s23115155
20. Narimani K, Nalbandy N. Cyber threats and their effects on individual and family health. Cyberattacks and threats in the field of health and hygiene. 3rd National Conference on Cyber Defens, 2022.
21. Nguyen GN, Le Viet NH, Elhoseny M, Shankar K, Gupta BB, Abd El-Latif AA. Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. Journal of parallel and Distributed Computing. 2021;153:150-60. doi:10.1016/j.jpdc.2021.03.011
22. Dehghani M, Rahmatpasand-Fatideh Z, Arasteh Z, Shokrizadeh-Bezenjani K. Knowledge, attitude, and performance of health information management staff of Iranian hospitals about health information security. Health Information Management. 2019;16 (1):3-9. doi:10.22122/him.v16i1.3727
23. Bloordi T, Tayyari Pourahmadi M. Government actions in creating cyber security. New Achievements in Public Law. 2022;1(4):64-76.
24. Chaudhary RR, Chatterjee K. A lightweight security framework for electronic healthcare system. International Journal of Information Technology. 2022;14(6):3109-21. doi:10.1007/s41870-022-01034-4
25. Abedini S, Sayadi S, Shokooh Z, Fatehi RN, Mollaei HR. Designing a Branding Model of Human Resources in the Field of Health with an Islamic Approach. Journal of Research on Religion and Health. 2023;9(1):107-21. [In Persian]
26. Javaid M, Khan IH. Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. Journal of Oral Biology and Craniofacial Research. 2021;11(2):209-14. doi:10.1016/j.jobcr.2021.01.015
27. Dang LM, Piran MJ, Han D, Min K, Moon H. A survey on internet of things and cloud computing for healthcare. Electronics. 2019;8(7):768. doi:10.3390/electronics8070768
28. Karimi Ghohroudi M, Moeinazad Sh, Karimi E. Typology of the concept and main elements of cyberspace innational cyber security strategy of selected countries. National Security. 2023;13(47):9-36. [In Persian]
29. Mirvahabi N. A method to protect location privacy using semantic technology in the Internet of Things. Master thesis in computer engineering-software. Payam Noor University of Tehran Province, 2021.
30. Mozdoriane Mehdiabad F. Improving the accuracy of the network intrusion detection systems in medical internet of things systems through the combined algorithm of salp collective intelligence and sine cosine. Master thesis in computer Engineering – Secure Computing. Imam Reza International University, College of Technology and Engineering, 2021.
31. Lv Z, Qiao L. Analysis of healthcare big data. Future Generation Computer Systems. 2020;109: 103-10. doi:10.1016/j.future.2020.03.039