مجله دانشکده پیراپزشکی دانشگاه علوم پزشکی تهران (پیاورد سلامت)
دوره ۱۴ شماره ۱ فروردین و اردیبهشت ۱۳۹۹، ۱۰-۱

مقاله پژوهشی

چالش‌های امنیتی رایانش مه در حوزه‌ی سلامت

محمدحسین رونقی[1]، فروغ السادات حسینی[2]

دریافت مقاله : آبان ۱۳۹۸
پذیرش مقاله : اسفند ۱۳۹۸

* نویسنده مسئول :
محمدحسین رونقی؛
دانشکده اقتصاد، مدیریت و علوم اجتماعی دانشگاه شیراز
Email :
mh_ronaghi@shirazu.ac.ir

چکیده

زمینه و هدف: رایانش مه بستری مجازی است که موجبات ذخیره‌سازی، محاسبه و خدمات شبکه‌ای بین مراکز داده ابری و ابزارهای نهایی را فراهم می‌کند. رایانش مه با سیستم‌های نظارت فوری حوزه‌ی پزشکی منطبق است در چنین سیستم‌هایی حجم انبوه داده از حسگرهای محیطی و زیستی متعددی به‌دست می‌آید. از سوی دیگر ساختار باز و توزیع شده‌ی رایانش مه در برابر تهدیدات امنیتی، آسیب پذیر و ضعیف است. از همین رو هدف این پژوهش شناسایی چالش‌های امنیتی رایانش مه در حوزه‌ی سلامت است.

روش بررسی: این پژوهش از نوع آمیخته و کاربردی است که در سه مرحله در بهار ۹۸ انجام گردید. در مرحله‌ی اول با استفاده از روش تحلیل محتوا، کدهای امنیتی فناوری رایانش مه از بین منابع کتابخانه‌ای شناسایی گردید. در مرحله‌ی دوم نظر متخصصان فناوری اطلاعات متشکل از ۱۲ نفر شاغل در حوزه‌ی سلامت با استفاده از روش دلفی ارزیابی گردید. در نهایت با استفاده از تکنیک تحلیل سلسله مراتبی فازی، کدهای امنیت رتبه بندی گردید.

یافته‌ها: با توجه به نتایج حاصل از تحلیل سلسله مراتب فازی حملات شبکه(۰/۳۱)، ارتباطات امن(۰/۲۳)، تشخیص هویت و کنترل دسترسی(۰/۱۹)، اعتماد(۰/۱۵) و حریم خصوصی(۰/۱۲) در عوامل امنیتی رایانش مه دارای بیشترین اهمیت بودند.

نتیجه‌گیری: بر اساس نتایج پژوهش می‌توان اذعان داشت که حملات شبکه و ارتباطات امن، مهمترین چالش‌های به‌کارگیری رایانش مه در حوزه‌ی پزشکی محسوب می‌شوند؛ به‌دلیل اینکه گره‌های شبکه مه معمولاً در نقاط مختلفی با محافظت ضعیف‌تر مستقر می‌شوند؛ از همین رو ممکن است با حمله‌ی بدافزارهای مختلفی روبه‌رو شوند. در نتیجه سیاستگذاران باید به نقش این چالش‌ها در پیاده‌سازی رایانش مه آگاه باشند.

واژه‌های کلیدی: رایانش ابری، امنیت کامپیوتر، تکنیک دلفی، بخش سلامت

۱ استادیار گروه مدیریت، دانشکده اقتصاد، مدیریت و علوم اجتماعی، دانشگاه شیراز، شیراز، ایران

۲ کارشناس ارشد مهندسی کامپیوتر، دانشکده برق و کامپیوتر، دانشگاه آزاد اسلامی، واحد زنجان، زنجان، ایران

مقدمه

تاثیر پیشرفت‌های فناوری اطلاعات بر زندگی انسان و کسب وکارها هر روزه بیشتر می‌شود. از جمله می‌توان به فناوری رایانش ابری و اینترنت اشیا اشاره کرد. رایانش ابری با ارایه برخی از مزایای عمده برای کاربران، از جمله حذف سرمایه‌گذاری اولیه فناوری اطلاعات، مقیاس پذیری و هزینه‌های متناسب تحول عظیمی در شیوه‌ی دسترسی و مدیریت داده‌ها و نرم افزارها ایجاد کرده است(۱). توسعه‌ی فناوری اینترنت اشیا موجب شده است تا بسیاری از اشیا قادر به اتصال به اینترنت برای برقراری ارتباط با یکدیگر بدون دخالت انسان باشند. در اصل اینترنت اشیا، ورود داده‌های انسانی را کاهش داده و از انواع مختلف حسگرها برای جمع آوری داده‌ها از محیط استفاده می‌کند و اجازه‌ی ذخیره‌سازی و پردازش خودکار تمام داده‌ها را ایجاد می‌کند(۲).

برخی از برنامه‌های اینترنت اشیا، ممکن است زمان واکنش بسیار کوتاهی داشته باشند و یا اتصال به اینترنت ضعیف باشد؛ برخی ممکن است دارای داده‌های خصوصی باشند و یا مقدار زیادی داده تولید کنند که بار سنگینی بر شبکه ایجاد کند. با اتصال دستگاه-های بیشتر، شبکه با مشکل تاخیر زیاد مواجه می‌شود. بر این اساس بستر رایانش ابر سنتی دارای تحرک‌پذیری کافی و آگاهی از محل نبوده و برای حمایت از این برنامه‌ها به اندازه کافی کارامد نیست(۳). از همین رو فناوری محاسبات جدیدتری با عنوان رایانش مه در مواجه با فناوری اینترنت اشیا استفاده می‌شود. رایانش مه به‌دلیل توزیع منطقه‌ای دارای امنیت بیشتری نسبت به رایانش ابری است(٤). رایانش‌مه، پارادایم محاسباتی توزیع شده‌ای است که بین حسگرها و ابزارهای اینترنت اشیا و مراکز داده ابری قرار می‌گیرد. از جمله مزایای رایانش مه می‌توان به موارد زیر اشاره کرد(۵):

کاهش تاخیرها: در مقایسه با رایانش‌ابری با نزدیک‌تر شدن پردازشگر به وسیله‌ی اطلاعاتی، سرعت پردازش اطلاعات افزایش می‌یابد و تاخیرها و افت زمانی کاهش می‌یابد.

حریم خصوصی: با پردازش داده‌های حساس در درگاهی نزدیکتر نسبت به سرور مرکزی، امکان کنترل حریم خصوصی داده‌ها بیشتر می‌شود.

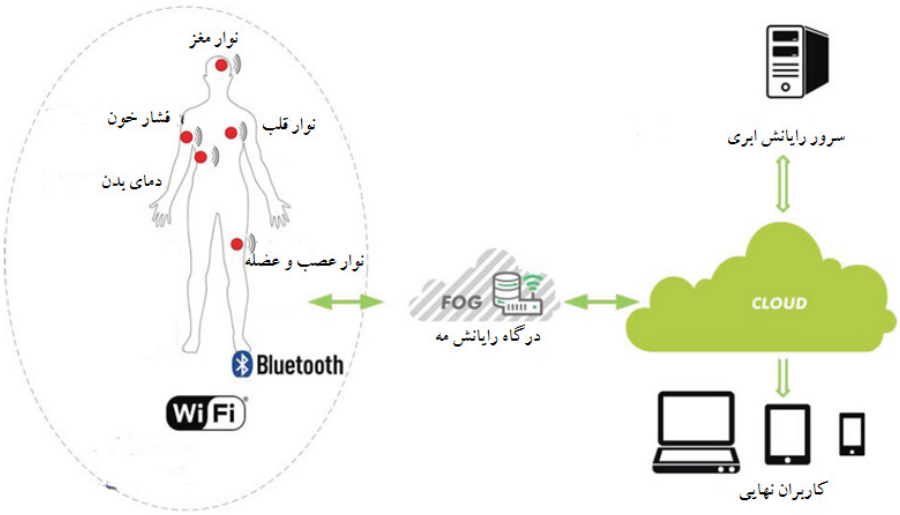
بهره‌وری انرژی: با افزایش درگاه‌های مختلف، زمینه‌ی کنترل انرژی ابزارها و تجهیزات مختلف فراهم می‌شود و می‌توانند زمان بیشتری در حالت خاموش با مصرف انرژی کمتر قرار بگیرند.

پهنای باند: با توجه به فیلترهای مختلفی که در مسیر ارسال داده به سرور مرکزی انجام می‌گیرد، پهنای باند کمتری نسبت به حالت متمرکز استفاده می‌شود.

مقیاس‌پذیری: محاسبات محلی، موجب کاهش بار اطلاعاتی بر سرور مرکزی می‌شوند و از این رو امکان مدیریت حجم داده‌ها در مقیاس مختلف وجود دارد.

قابلیت اطمینان: در رایانش مه با افزایش گره‌های زیادتر در شبکه، موجب کاهش دوباره کاری و عدم وابستگی زیاد به سرور مرکزی می‌شود و از همین رو قابلیت اطمینان به این محاسبات افزایش می‌یابد.

فناوری اینترنت اشیا در حوزه‌ی سلامت و پزشکی نیز کاربردهای زیادی دارد از آن جمله می‌توان به مدیریت بیماری‌های مزمن، خدمات پزشکی فوری غیرمستقیم، تشخیص زمین خوردن سالمندان، اطلاعات بیماران، ناسازگاری دارو و اطلاعات سلامت کودکان اشاره کرد. اینترنت اشیا امکان نظارت از راه دور بدون وقفه و قابل اعتماد به علت ماهیت فراگیر خود فراهم می‌کند و اجازه‌ی آزادی حرکت و تحرک‌پذیری برای افراد و بیماران را می‌دهد(٦). پیگیری میزان ضربان قلب و مصرف کالری، سیستم اندازه‌گیری فشارخون، سیستم‌های بررسی سلامت، ضربان سازهای مصنوعی، حسگرهای پوشیدنی و سمعک‌ها نمونه‌های ابزارهای فناوری اینترنت اشیاست(۷). با توجه به کاربرد وسیع اینترنت اشیا در حوزه سلامت نیاز به رایانش مه در پیاده‌سازی این فناوری وجود دارد. در شکل ۱ نمونه‌ی ساده‌ی جایگاه رایانش مه در اینترنت اشیا نشان داده شده است.



شکل ۱: ساختار رایانش مه در فناوری اینترنت اشیا در حوزه‌ی سلامت(۸)

همان‌گونه‌که در شکل ۱ نشان داده شده است، برخی از ویژگی‌های خدمات پزشکی، نیاز به استفاده از محاسبات مه، در سیستم‌های نظارت بر سلامت مبتنی بر اینترنت اشیا را بارز می‌سازد. اول حساسیت و ماهیت دستگاه‌های حسگر(به‌ویژه بسیاری از پوشیدنی‌ها) نیاز به بهره‌وری منابع بیش از حوزه‌های دیگر دارد. دوم، نوع انتقال داده، که توسط این حسگرها مورد نیاز است. به‌عنوان مثال، مجموعه‌ی سیگنال نوار قلب (ECG) نیاز به یک ارتباط مداوم با پهنای باند ٤ کیلوبیت در ثانیه در هر کانال دارد. سوم، با توجه به اهمیت کاربرد، پاسخ فوری و پردازش داده‌هایی که توسط گره‌های حسگر جمع آوری شده است، اجباری است. به‌طورکلی اینترنت اشیا در حوزه‌ی پزشکی نیاز به سطح بالایی از قابلیت اطمینان دارد که باید الگوی فیزیولوژیکی در زمان واقعی شناسایی شوند. علاوه بر این، توجه به حریم شخصی از طریق دستگاه‌های اینترنت اشیا، نیز حایز اهمیت است. این توابع می‌تواند توسط لایه محاسبات مه پشتیبانی شود(۷).

در خصوص کاربردهای رایانش مه در حوزه‌ی سلامت در خارج از کشور مطالعات متعددی در چند سال اخیر انجام شده است. در پژوهشی به بررسی نرم افزارهای کاربردی مبتنی بر رایانش مه در خصوص اندازه‌گیری نوار قلب بیمار پرداخته شد و بر اساس تحلیل تاریخچه داده‌ها به اهمیت این فناوری اشاره گردید(۹). در مطالعه‌ی Vilela و همکاران(۱۰) به کاربری رایانش مه در حوزه پزشکی پرداختند و مشخص گردید که سیستم نظارت بر سلامت رایانش مه موجب کاهش ترافیک داده و افزایش امنیت به دلیل تحلیل منطقه‌ای می‌شود. مطالعه‌ی دیگری، پیشرفت‌های حوزه‌ی سلامت در کشور هند را به چهار نسل تقسیم کرد: نسل اول که با کمبود منابع مواجه بودند بین سال‌های ۱۹۷۰ تا ۱۹۹۰ قرار داشت؛ نسل دوم زمان پیدایش اینترنت و به‌کارگیری فناوری اطلاعات در حوزه سلامت بین سال‌های ۲۰۰۵–۱۹۹۱ قرار گرفت؛ نسل سوم زمان استفاده از سیستم‌های اطلاعاتی در حوزه پزشکی و سامانه‌های ثبت اطلاعات در سال‌های ۲۰۱۵–۲۰۰٦ است. نسل چهارم که از سال ۲۰۱٦ آغاز شده است، به استفاده از هوش مصنوعی، اینترنت اشیا و رایانش ابری و مه اشاره دارد. در این مقاله به مزیت رایانش مه در خصوص جمع‌آوری و تحلیل سریع داده‌ی بیماران و داده‌های محیطی اشاره می‌کند(۱۱). در پژوهش دیگر به بررسی ابعاد پیاده سازی رایانش مه در حوزه‌ی سلامت الکترونیک و هوشمندسازی آن می‌پردازد و به چالش‌های حوزه سلامت مبتنی بر اینترنت اشیا از قبیل تحرک‌پذیری، قابلیت اطمینان و امنیت داده اشاره می‌کند(۵). با توجه به چالش امنیت و دسترسی به داده در اینترنت اشیا و به دنبال آن رایانش مه و اهمیت کاربرد رایانش مه در حوزه‌ی سلامت، هدف پژوهش پیش‌رو شناسایی و رتبه‌بندی چالش‌های مرتبط با رایانش مه مطابق نظر متخصصان حوزه‌ی سلامت است. بر اساس جستجوی انجام شده در زمان انجام این پژوهش مطالعه‌ای در داخل کشور در خصوص رایانش مه در

حوزه سلامت یافت نشد. وجه تمایز این پژوهش با مطالعات قبل توجه به بعد امنیتی رایانش مه و نظرسنجی از متخصصان در حوزه سلامت ایران است. نتایج این پژوهش برای سیاستگذاران حوزه‌ی سلامت، جهت پیاده سازی اثربخش فناوری اینترنت اشیا بر بستر رایانش مه کاربرد دارد.

روش بررسی

این پژوهش از منظر هدف کاربردی و از لحاظ روش آمیخته است و در بهار ۱۳۹۸ انجام گردید. در مرحله اول پژوهش با استفاده از روش تحلیل محتوای کیفی چالش‌های حوزه رایانش مه بر اساس مطالعات پیشین استخراج و شناسایی شدند. روش دلفی، روشی است که با مطالعه و بررسی به‌وسیله‌ی یک گروه نظارت‌کننده، رهبری و هدایت می‌شود و شامل چندین دور است؛ که با استفاده از یک گروه متخصص که برای همدیگر ناشناس هستند انجام می‌شود و هدف این روش رسیدن به یک اجماع نظر در بین گروهی از متخصصان، براساس شناخت شهودی و ذهنی آنان است، که پس از هر دور یک بازخورد استاندارد آماری از قضاوت گروه به اعضا ارایه می‌شود(۱۲). در مرحله‌ی دوم پژوهش با استفاده از روش دلفی شاخص‌های استخراج شده از منابع پیشین جهت بومی سازی چالش‌ها مورد نظرسنجی گروه خبرگان پژوهش قرار گرفت. گروه خبرگان پژوهش متشکل از ۱۲ نفر از متخصصان حوزه‌ی فناوری اطلاعات شاغل در دانشگاه علوم پزشکی زنجان بودند. این افراد دارای مدرک تحصیلی کارشناسی و کارشناسی‌ارشد در حوزه کامپیوتر و فناوری اطلاعات و دارای سابقه کار حداقل ۱۰ سال بودند. گروه خبرگان با استفاده از روش نمونه‌گیری در دسترس صورت گرفت. دلیل انتخاب این افراد آشنایی با فناوری رایانش ابر و مه و همچنین سابقه کار در حوزه‌ی سلامت بود. شاخص‌های نهایی مورد توافق گروه خبرگان در مرحله‌ی سوم پژوهش با استفاده از تحلیل سلسله مراتبی فازی رتبه‌بندی گردید تا بر این اساس میزان اهمیت هر یک از چالش‌ها بر اساس نظر خبرگان در حوزه‌ی سلامت مشخص گردد. فرایند تحلیل سلسله مراتبی یک روش تصمیم‌گیری چند معیاره است. این رویکرد به فرد تصمیم گیرنده این امکان را می‌دهد تا مساله را در قالب سلسله مراتبی از هدف، معیارها، زیرمعیارها و گزینه‌ها در نظر بگیرد(۱۳). دلیل استفاده از رویکرد فازی نسبت به مقادیر قطعی، نزدیکی اعداد فازی به واقعیت است. در این مرحله از ماتریس مقایسات زوجی جهت ارزیابی میزان اهمیت چالش‌ها نسبت به یکدیگر استفاده شد.

یافته‌ها

خروجی مرحله اول پژوهش در قالب جدول ۱ نشان‌دهنده‌ی چالش‌های رایانش مه است که در مطالعات پیشین به آنها اشاره شده است.

جدول ۱: چالش‌های امنیتی رایانش مه

منبع	چالش‌های امنیتی
(۳)	• فرایند داده‌های منطقه‌ای • سازگاری داده • ذخیره سازی منطقه‌ای • امنیت داده
(۱٤)	• قابلیت تنظیم مجدد • شناسایی وسایل و موبایل‌ها • تشخیص نفوذ • تشخیص هویت
(۱۵)	• مجازی سازی(استفاده از سخت افزار و منابع سخت افزاری شامل حافظه، پردازنده، دیسک و کارت شبکه در یک سیستم کامپیوتری برای راه اندازی و استفاده(میزبانی) بیش از یک سیستم عامل به‌صورت همزمان را مجازی سازی می‌نامند)

(۱۶)	• امنیت وب • ارتباطات داخلی و خارجی • امنیت داده • امنیت شبکه بی‌سیم • حفاظت از نرم افزارهای مخرب • امنیت شبکه • امنیت داده • کنترل دسترسی • حریم خصوصی • اعتماد • تشخیص هویت
(۱۷)	• ارتباطات امن در رایانش مه • حریم خصوصی کاربر نهایی • حملات مخرب • حمله فرد میانی (MitM)
(۱۸)	• تشخیص نفوذ • تکنیک تشخیص مخرب • مشکل گره مخرب در رایانش مه
(۱۹)	• حفاظت داده • مدیریت داده • اعتماد • حفظ یکپارچگی • لاگ فایل‌ها در شبکه • قابلیت اطمینان دریافت داده • انطباق • چند اجاره‌ای (Multi-tenancy)(از این فناوری برای به اشتراک گذاشتن منابع فناری اطلاعات به صورت امن و به‌صرفه استفاده می‌کنند. این اشتراک‌گذاری با امنیتی بالا بین چندین برنامه‌ی کاربردی و کاربر که از فضای ابری استفاده می‌کنند انجام می‌شود و چندین کاربر می‌توانند از یک نمونه نرم افزار استفاده کنند) • زنجیره‌ی نگهداری • پزشک قانونی دیجیتالی(استفاده از روش‌های اثبات شده علمی جهت حفاظت، جمع آوری، اعتبارسنجی، شناسایی، تحلیل، تفسیر ، مستندسازی و ارایه شواهد دیجیتالی که از منابع دیجیتالی به‌وجود آمده‌اند با هدف سهولت در بازسازی صحنه‌ی جرم یا کمک به پیش بینی فعالیت‌های مخرب جهت جلوگیری از عملیات طرح‌ریزی شده‌ی قبلی است)
(۲۰)	• تشخیص هویت • حریم خصوصی • کدگذاری • حمله منع سرویس (DoS)

با توجه به اطلاعات استخراج شده در جدول ۱ کدهای شناسایی گردید. مطابق نظر سه تن از استادان هیات علمی دانشگاه متعددی در خصوص چالش‌های رایانش مه و پیاده سازی آن دولتی در بخش فناوری اطلاعات می‌توان این موارد را در شش گروه

اصلی شامل تشخیص هویت و کنترل دسترسی، اعتماد، کدگذاری، انواع حملات به شبکه، حریم خصوصی و ارتباطات امن طبقه‌بندی کرد. جهت بومی‌سازی چالش‌های استخراجی و همچنین استفاده از متخصصان حوزه‌ی سلامت پرسش‌نامه‌ای جهت ارزیابی میزان اهمیت هر دسته از چالش‌ها با استفاده از طیف پنج گزینه‌ای لیکرت در بین گروه خبرگان پژوهش توزیع گردید. پاسخ‌ها شامل گزینه‌های بسیار مخالف، مخالف، بی‌نظر، موافق و بسیار موافق بود. مقادیر نتایج دور اول دلفی خبرگان در جدول ۲ نشان داده شده است.

جدول ۲: نتایج دور اول پنل دلفی خبرگان

مولفه‌ها	میانگین	انحراف	کمینه	بیشینه	درصد توافق	تغییرات کیفی
تشخیص هویت و کنترل دسترسی	٤/٠٩	١/٥٠	٢	٥	٨٣/٣٣	–
اعتماد	٤/٠٠	٠/٤٣	٣	٥	٩١/٦٦	–
کدگذاری	٢/٥١	٠/٩٩	١	٤	٣٣/٣٣	حذف
حملات به شبکه	٤/٢٧	٠/٧٥	٣	٥	٧٥/٠٠	–
حریم خصوصی	٣/٨٢	٠/٣٩	٣	٤	٨٣/٣٣	–
ارتباطات امن	٤/٢٧	٠/٩٦	٣	٥	٦٦/٦٦	–

با توجه به اطلاعات میانگین و درصد توافق‌های به‌دست آمده در جدول ۲ تنها مولفه‌ی کدگذاری، مورد تایید و اجماع خبرگان به‌عنوان چالش مستقل رایانش ابری در حوزه‌ی پزشکی قرار نگرفت و این مورد در دور دوم حذف گردید؛ مجدداً پرسش‌نامه در بین خبرگان توزیع گردید. جهت ارزیابی میزان توافق خبرگان پژوهش در خصوص مولفه‌ها از ضریب کندال استفاده شد. مقادیر ضریب توافق کندال در خصوص مولفه‌ها در جدول ۳ نشان داده شده است و هر پنج دسته‌ی مولفه، مورد اجماع خبرگان حوزه سلامت در دور دوم قرار گرفت.

جدول ۳: نتایج شاخص‌های اجماع دور دوم پنل دلفی خبرگان

مولفه	مقادیر آزمون فرض	میزان کندال
تشخیص هویت و کنترل دسترسی	٠/٠٨٠	٠/٧٩٥
اعتماد	٠/٠٧٨	٠/٨٧٢
حملات به شبکه	٠/٠٩٣	٠/٧٢٦
حریم خصوصی	٠/٠٧٥	٠/٧٣٧
ارتباطات امن	٠/١١٧	٠/٧٠٦

با توجه به نتایج به‌دست آمده از جدول ۳ می‌توان نتیجه گرفت که پنج مولفه‌ی تشخیص هویت، اعتماد، حملات به شبکه، حریم خصوصی و ارتباطات امن به‌عنوان اصلی‌ترین چالش‌های رایانش مه در حوزه سلامت شناسایی می‌گردد. جهت رتبه‌بندی این مولفه‌ها و مقایسه‌ی دو به دو آنها یا یکدیگر از تکنیک تحلیل سلسله مراتبی فازی استفاده گردید. لذا در قالب پرسش‌نامه ماتریسی از خبرگان پژوهش خواسته شد تا میزان اهمیت مولفه‌ها را در قالب متغیرهای زبانی فازی نسبت به یکدیگر مشخص کنند. نمونه‌ی یکی از ماتریس‌های مقایسه زوجی و مقادیر فازی آنها در جدول ٤ نشان داده شده است.

جدول ۴: ماتریس مقایسات زوجی یکی از خبرگان پژوهش

	تشخیص هویت و دسترسی	اعتماد	حملات به شبکه	حریم خصوصی	ارتباطات امن
تشخیص هویت و دسترسی	(١، ١، ١)	(١، ٠/٦، ٠/٥)	(١/٥، ٢، ٢/٥)	(٢، ١/٥، ١)	(٣، ٢/٥، ٢)
اعتماد	(٢، ١/٥، ١)	(١، ١، ١)	(١/٥، ٢، ٢/٥)	(٢، ١/٥، ١)	(٣، ٢/٥، ٢)

حملات به شبکه	(۰/٦، ۰/٥، ۰/٤)	(۰/٦، ۰/٥، ۰/٤)	(۱، ۱، ۱)	(۱، ۰/٦، ۰/٥)	(۱/٥، ۱، ۰/٥)
حریم خصوصی	(۱، ۰/٦، ۰/٥)	(۱، ۰/٦، ۰/٥)	(۲، ۱/٥، ۱)	(۱، ۱، ۱)	(۲/٥، ۲، ۱/٥)
ارتباطات امن	(۰/٥، ۰/٤، ۰/۳)	(۰/٥، ۰/٤، ۰/۳)	(۲، ۱، ۰/٦)	(۰/٦، ۰/٥، ۰/٤)	(۱، ۱، ۱)

مطابق جدول ٤، با استفاده از روابط تحلیل سلسله مراتبی فازی مقادیر وزن‌های هر یک از مولفه‌ها محاسبه گردید و مقادیر نرمال‌سازی شده مطابق زیر به‌دست آمد. بر این اساس چالش‌های حملات به شبکه(۰/۳۱) و ارتباطات امن(۰/۲۳) دارای بالاترین میزان اهمیت و در ادامه تشخیص هویت(۰/۱۹)، اعتماد(۰/۱۵) و حریم خصوصی(۰/۱۲) در جایگاه‌های بعدی قرار دارند.

W=(۰/۱۹، ۰/۱۵، ۰/۳۱، ۰/۱۲، ۰/۲۳)

بحث

بر اساس نتایج به‌دست آمده در قسمت اول پژوهش، عواملی همچون حریم خصوصی، اعتماد، انواع حملات به شبکه(حمله منع سرویس و حمله فرد میانی)، امنیت داده، کنترل دسترسی، ارتباطات امن، مجازی سازی و تشخیص هویت به‌عنوان چالش‌های پیش روی به‌کارگیری فناوری رایانش مه شناسایی گردید. این نتایج منطبق با خروجی پژوهش‌های Stojmenovic و همکاران(١٤)، Khan و همکاران(١٥)، Kumar و همکاران(١٦) و Mukherjee و همکاران(١٧) است و بر اساس تحلیل محتوای این مطالعات استخراج گردید. حملات منع سرویس به عنوان یکی از حملات شبکه به‌عنوان عامل مهم امنیتی رایانش مه، مطابق نظر متخصصان حوزه‌ی سلامت شناخته شد. این یافته با نتایج پژوهش Mukherjee و همکاران(١٧)، Lee و همکاران(١٨) و Li و همکاران(٢٠) مطابقت دارد. این حملات باعث از کارافتادن یا مشغول شدن بیش از اندازه سیستم می‌شود، تاحدی‌که شبکه غیرقابل استفاده شود. در اکثر مواقع، حفره‌های امنیتی محل انجام این حملات است، بنابراین نصب به روزترین برنامه‌های امنیتی از حمله جلوگیری خواهند کرد. یکی از راه‌های مقابله با حملات سایبری استفاده از تجربه و تخصص متخصصان امنیتی است. شرکت‌های امنیتی تامین امنیت با استفاده از راه‌حل‌های مبتنی بر فناوری‌های جدید را تضمین می‌کنند. از همین رو استفاده از افراد متخصص در این حوزه در زمان راه‌اندازی رایانش مه پیشنهاد می‌شود. گاهی اوقات هکرها به‌راحتی می‌توانند کنترل یک شبکه را به‌دست بگیرند و به اطلاعات حساس آن شبکه دست پیدا کنند. این کار می‌تواند از طریق دستیابی به نام کاربری و رمز عبور حساب‌های کاربری کاربران انجام پذیرد. حفاظت از سرور DNS و به‌کارگیری الگوریتم‌های قوی رمزنگاری در دسترسی هکرها اختلال ایجاد می‌کند. خروجی نهایی پژوهش، مشخص ساخت که مطابق نظر خبرگان علوم پزشکی حملات شبکه و ارتباطات امن بالاترین اهمیت را در پیاده‌سازی رایانش مه دارد. این یافته‌ی پژوهش همراستا با مدل ارایه شده‌ی مطالعه‌ی Rahmani و همکاران(٣) است که در آن نیز به ایجاد امنیت فناوری رایانش مه تاکید شده است. از همین رو بزرگ‌ترین چالش مواجه با این فناوری نوین، ایجاد امنیت شبکه و اطمینان از عدم نفوذ بدافزارها و هکرهاست. از جمله محدودیت‌های این پژوهش، می‌توان به تنها بررسی ابعاد امنیتی رایانش مه و عدم بررسی سایر عوامل زیرساختی و انسانی آن اشاره کرد.

نتیجه‌گیری

با توجه به کاربردهای متعدد فناوری اینترنت اشیا در حوزه پزشکی، رایانش مه می‌تواند به خوبی مشکلات محدودیت پهنای باند و تاخیر زمانی رایانش ابری را در به‌کارگیری اینترنت اشیا حل کند. ساختار باز و توزیع شده‌ی رایانش مه، به‌کارگیری این فناوری را با چالش‌هایی مواجه کرده است. نتایج پژوهش مشخص ساخت که چالش‌های حملات به شبکه و ارتباطات امن، تشخیص هویت، اعتماد و حریم خصوصی به‌ترتیب دارای بالاترین اهمیت در حوزه‌ی پزشکی هستند. از همین رو پیشنهاد می‌گردد که فایروال‌های سخت و نرم‌افزاری به‌گونه‌ای تنظیم شوند و مسیریاب‌ها طوری پیکربندی شوند که بتوانند از با فیلترکردن پروتکل‌های غیرضروری از حملات ساده جلوگیری و آدرس‌های IP نامعتبر را نیز متوقف کنند. همچنین پیکربندی مناسب برنامه‌های کاربردی سرویس دهنده، جهت ارتباط اینترنت اشیا در به حداقل رساندن تأثیر حمله منبع سرویس تأثیر بسیار مهمی دارند. مدیر سرور می‌تواند تعیین کند که برنامه کاربردی از چه منابعی استفاده کند و چگونه به درخواست‌های کاربران پاسخ

دهد. با توجه به فراگیر بودن شبکه‌ی مورد استفاده‌ی اینترنت اشیا و نیاز به رایانش مه سیاستگذاری امنیت شبکه در سطح ملی و تعامل وزارت بهداشت با وزارت فناوری اطلاعات باید صورت گیرد. جهت پژوهش‌های آتی نیز پیشنهاد می‌گردد که در خصوص ارزیابی زیرساخت‌های سخت افزاری و مخابراتی پیاده‌سازی رایانش مه در حوزه‌ی پزشکی ایران مطالعه شود و همچنین توانایی دانشی افراد و پذیرش این فناوری جدید توسط کاربران ارزیابی گردد.

منابع

1. Zhang P, Zhou M & Fortino G. Security and trust issues in Fog computing: A survey. Future Generation Computer Systems 2018; 88(1): 16-27.

2. Atlam HF, Walters RJ & Wills G. Fog computing and the internet of things: A review. Big Data and Cognitive 2018; 2(2): 10.

3. Rahmani AM, Gia TN, Negash B, Anzanpour A, Azimi I, Jiang M, et al. Exploiting smart e-Health gateways at the edge of healthcare internet-of-Things: A fog computing approach. Future Generation Computer Systems 2018; 78(2): 641-58.

4. Al-Khafajiy M, Baker T, Asim M, Guo Z, Ranjan R, Longo A, et al. Commitment: A fog computing trust management approach. Journal of Parallel and Distributed Computing 2019; 137(1): 1-16.

5. Kraemer FA, Braten AE, Tamkittikhun N & Palma D. Fog computing in healthcare: A review and discussion. IEEE Access 2017; 5(1): 9206-23.

6. Ronaghi MH & Hosseini F. Identifying and ranking internet of things services in healthcare sector. Journal of Health Administration 2018; 21(73): 106-17[Article in Persian].

7. Rahmani A, Liljeberg P, Preden JS & Jantsch A. Fog computing in the internet of things. Switzerland: Springer International Publishing; 2018: 3-13.

8. Gia T, Jiang M, Rahmani A, Westerlund T, Liljeberg P & Tenhunen H. Fog computing in healthcare internet of things: A case study on ECG feature extraction, Liverpool, UK: IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, 2015.

9. Akrivopoulos O, Chatzigiannakis I, Tselios C & Antoniou A. On the deployment of healthcare applications over fog computing infrastructure. Turin, Italy: IEEE 41st Annual Computer Software and Applications Conference, 2017.

10. Vilela PH, Rodrigues JJ, Solic P, Saleem K & Furtado V. Performance evaluation of a fog-assisted IoT solution for e-Health applications. Future Generation Computer Systems 2019; 97(1): 379-86.

11. Kumari A, Tanwar S, Tyagi S & Kumar N. Fog computing for healthcare 4.0 environment: Opportunities and challenges. Computers and Electrical Engineering 2018; 72(1): 1-13.

12. Pashaeizad H. Delphi method: A comprehensive approach. Peyk Noor-Human Sciences 2008; 6(2): 63-79[Article in Persian].

13. Ly PT, Lai WH, Hsu CW & Shih FY. Fuzzy AHP analysis of internet of things in enterprises. Technological Forecasting and Social Change 2018; 136(1): 1-13.

14. Stojmenovic I, Wen S, Huang X & Luan H. An overview of fog computing and its security issues. Concurrency and Computation: Practice and Experience 2015; 28(10): 2991-3005.

15. Khan S, Parkinson S & Qin Y. Fog computing security: A review of current applications and security solutions. Journal of Cloud Computing: Advances, Systems and Applications 2017; 6(19): 3-22.

16. Kumar P, Zaidi N & Choudhur T. Fog computing: Common security issues and proposed countermeasures. India: International Conference System Modeling & Advancement in Research Trends (SMART), 2016.

17. Mukherjee M, Matam R, Shu L, Maglaras L, Ferrag M, Choudhury N, et al. Security and privacy in fog computing: Challenges. IEEE Access 2017; 5(1): 19293-304.

18. Lee K, Kim D, Ha D, Rajput U & Oh H. On security and privacy issues of fog computing supported internet of things environment, Montreal: 6th International Conference on the Network of the Future (NOF), IEEE, 2015.

19.Wang Y, Uehara T & Sasaki R. Fog computing: issues and challenges in security and forensics, Taiwan: IEEE 39th Annual Computer Software and Applications Conference, 2015.

20. Li Z, Zhou X, Liu Y, Xu H & Miao L. A non-cooperative differential game-based security model in fog computing. China communications 2017; 14(1): 180-9.

Security Challenges in Fog Computing in Healthcare

Mohammad Hossein Ronaghi[1] (Ph.D.) - Foroughosadat Hosseini[2] (M.S.)

1 Assistant Professor, Department of Management, Faculty of Economics, Management and Social Sciences, Shiraz University, Shiraz, Iran

2 Master of Science in Computer Engineering, Faculty of Electrical & Computer Engineering, Islamic Azad University, Zanjan Branch, Zanjan, Iran

Abstract

Received: Oct 2019

Accepted: Feb 2020

Background and Aim: The Fog Computing is a highly virtualized platform that provides storage, computing and networking services between the Cloud data centers and end devices. Fog computing fits the characteristics of real-time health monitoring systems. In such systems, a large amount of data is acquired from a multitude of biological and environmental sensors. On the other hand, its distribution and open structure makes it vulnerable and weak to security threats. Therefore, the aim of this paper was to identify the security challenges in healthcare.

Materials and Methods: This applied research has been done in three phases using mixed-method approach in 2019. In the first phase, security codes from library resources by content analysis was identified. In the second phase interpretation of experts by Delphi method, Panel of IT experts consists of twelve members who work on healthcare sector was evaluated. Finally, we used Analytic Hierarchy Process(AHP) method for ranking security codes.

Results: According to fuzzy AHP results, attacks(0.31), secure communications (0.23), authentication and access control(0.19), trust(0.15) and privacy preservation (0.12) are the most important issues in security challenges of fog computing.

Conclusion: According to the results of this study, secure communications and network attacks are the major challenges in fog computing, because fog nodes are usually deployed in some places with relatively weak protection. They may encounter various malicious attacks. As a result, policymakers should be aware of the role of secure communications and network attacks in fog computing implementation.

Keywords: Cloud Computing, Computer Security, Delphi Technique, Healthcare Sector

*** Corresponding Author:**
Ronaghi MH
Email :
mh_ronaghi@shirazu.ac.ir