فصلنامهٔ پدافند غیرعامل و امنیت (پژوهشی)
سال دهم: شمارهٔ ۳۷- زمستان ۱۴۰۰
صص: ۵۱ - ۸۴
تاریخ دریافت: ۱۴۰۰/۱۰/۱۷ تاریخ پذیرش: ۱۴۰۰/۱۲/۱

Quarterly of Passive Defense & Security
Vol.10, No.37,Winter 2021
P-P: 51 - 84

سازوکارهای به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی

احمد زوارتربتی[۱]
جمشید نصرت‌آبادی[۲]
اکبر ابدال چگینی[۳]

چکیده:

فناوری رایانش ابری، الگویی جدید در فناوری اطلاعات است که امروزه به دلایلی نظیر مزیت‌های بالقوه آن، سازمان‌ها، گرایش زیادی به سمت بهره‌برداری از خدمات ابری دارند. از آنجایی که رایانش ابری؛ منابع را از طریق شبکه و در محیط باز به اشتراک می‌گذارد، بایستی در به‌کارگیری آن ملاحظات فراوانی مدنظر قرار گیرد. به تبع آن، سازمان‌ها و به‌ویژه سازمان‌های امنیتی که ماهیت، مأموریت‌ها و همچنین اطلاعاتِ در گردش آنها از اهمیت خاصی برخوردار است، در به‌کارگیری فناوری رایانش ابری با چالش‌های عمده مواجه هستند. در این پژوهش کاربردی که با روش آمیخته (کمّی-کیفی) انجام شده، ضمن معرفی مزیت‌های به‌کارگیری فناوری رایانش ابری، ابتدا چالش‌های مختلفی که سازمان‌های امنیتی در به‌کارگیری این فناوری با آن مواجه هستند، جمع‌بندی شد و در ادامه، سازوکارهای به‌کارگیری فناوری رایانش ابری به دو دسته سازوکارهای مدیریتی و فناورانه تقسیم شدند و در مجموع، ۵۶ مؤلفه در قالب یک پرسشنامه محقق‌ساخته استخراج شد که چالش‌ها، ۲۰ مؤلفه، سازوکارهای مدیریتی و فناورانه نیز هر کدام ۱۸ مؤلفه را به‌خود اختصاص دادند. اطلاعات از طریق مصاحبه، پرسشنامه، اسناد و مدارک، منابع الکترونیکی و وبگاه‌های معتبر علمی و نیز از دو روش کتابخانه‌ای و میدانی جمع‌آوری گردیده است. نتایج تجزیه و تحلیل سؤالات پژوهشی نشان داد که پرسش‌شوندگان معتقدند ۷۸/۲% چالش‌های فناوری رایانش ابری، ۸۵/۰۶% سازوکارهای مدیریتی و ۸۸/۲۲% سازوکارهای فناورانهس استخراج شده، در حد زیاد و خیلی زیاد بر به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی مؤثر است. هر کدام از فرضیه‌های پژوهشی نیز؛ با استفاده از آزمون خی‌دو مورد تجزیه‌وتحلیل قرار گرفتند و با استفاده از آزمون فریدمن، مشخص شد که مؤلفه "هزینه‌های بالا برای ایجاد و تأمین امنیت فناوری رایانش ابری در سازمان‌های امنیتی" با اولویت‌ترین چالش و مؤلفه "اتخاذ تدابیر لازم برای تست نفوذ و ارزیابی امنیتی زیرساخت‌های فناوری رایانش ابری در سازمان‌های امنیتی" با اولویت‌ترین سازوکار مدیریتی و مؤلفه "تأمین زیرساخت‌ها، سامانه‌های امنیتی، سامانه‌های کنترلی و ... برای پیاده‌سازی و امن‌سازی فناوری رایانش ابری در سازمان‌های امنیتی" با اولویت‌ترین سازوکار فناورانه در به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی هستند.

واژگان کلیدی: رایانش ابری، سازمان‌های امنیتی، چالش‌ها، سازوکارهای مدیریتی، سازوکارهای فناورانه.

۱. دکتری برق-مخابرات سیستم، پژوهشگر و مدرس دانشکده علوم و فنون فارابی، نویسنده مسئول zavvarahmad@gmail.com
۲. استادیار مدیریت راهبردی فضای سایبر دانشکده علوم فنون فارابی nosratabadi110@chmail.ir
۳. دانش‌آموخته کارشناسی ارشد علوم سیاسی گرایش امنیت ملّی دانشکده علوم فنون فارابی ebdal1378@chmail.ir

جستارگشایی

دنیای فناوری اطلاعات و اینترنت که امروزه به بخشِ حیاتی از زندگی بشر تبدیل شده، روزبه‌روز در حال گسترش است. امروزه نقش فناوری اطلاعات در سازمان‌های نوین به اندازه‌ای پررنگ است که بسیاری از نظریه‌پردازان، مدیران و تصمیم‌گیرندگان سازمان‌ها را به اتخاذ استراتژی مرتبط با این فناوری‌ها در جهت‌گیری‌های آتی سازمان‌ها توصیه می‌کنند (دشمن زیاری، ۱۳۹۵، ۲۸). با ظهور اینترنت و سرویس‌های مبتنی بر وب، تحولی بسیار ارزشمند در زمینه فناوری اطلاعات ایجاد شد (اسمعیلی رنجبر و سلاجقه، ۱۳۹۹، ۱۶، ۶۲). با پیشرفت فناوری اطلاعات، نیاز به انجام کارهای سنگین‌تری در این ارتباط به‌وجود آمد. این که افراد بتوانند کارهای سنگین اطلاعاتی و محاسباتی را بدون صرف هزینه زیاد و سخت‌افزارهای گران، از طریق خدمات انجام دهند. رایانش ابری آخرین پاسخ فناوری به این نیازها بوده است. طبق فهرست گارتنر، رایانش ابری جزء ۱۰ فناوری برتر سال‌های آینده است (حیدری دهویی و همکاران، ۱۳۹۶، ۲، ۴). رایانش ابری یک روش جدید محاسبات برای ارائه خدمات محاسباتی و یک مدل برای ارایه خدمات ویژه در اینترنت است. این خدمات می‌تواند شامل شبکه‌ها، سرورها، محیط‌های ذخیره‌سازی، خدمات نرم‌افزاری باشد. به این ترتیب فناوری رایانش ابری راه‌حلی تازه و پاسخی انعطاف‌پذیر، همیشه در دسترس، به‌صرفه و همگانی، برای برطرف کردن نیازهایی از جنس: پردازش سریع، دسترسی پویا و آنی، ایجاد مشارکت متقابل، قدرت تمرکز روز پروژه‌های سازمانی به‌جای اتلاف وقت برای نگهداری سرورها و از همه مهم‌تر، صرفه‌جویی در هزینه‌ها را به میدان آورد (اسمعیلی رنجبر و سلاجقه، ۱۳۹۹، ۱۶، ۶۲). مدل رایانشی بر پایهٔ شبکه‌های بزرگ کامپیوتری مانند اینترنت است که الگویی تازه برای عرضه، مصرف و تحویل سرویس‌های فناوری اطلاعات (شامل سخت‌افزار، نرم‌افزار، اطلاعات و سایر منابع اشتراکی رایانشی) با بکارگیری اینترنت ارائه می‌کند. رایانش ابری راهکارهایی برای ارائه خدمات فناوری اطلاعات به شیوه‌های مشابه با صنایع همگانی (آب، برق، تلفن و ...) پیشنهاد می‌کند (بهادر و صادقی، ۱۳۹۸، ۵، ۱). این بدین معنی است که دسترسی به منابع فناوری اطلاعات در زمان تقاضا و بر اساس میزان تقاضای کاربر به گونه‌ای انعطاف‌پذیر و مقیاس‌پذیر از راه اینترنت به کاربر تحویل داده می‌شود. واژه "ابر" واژه‌ای است استعاری که به اینترنت اشاره می‌کند و در نمودارهای شبکه‌های رایانه‌ای نیز از شکل ابر برای نشان دادن شبکه اینترنت استفاده می‌شود (مل و گریس[1]، ۲۰۱۱). دلیل تشبیه اینترنت به ابر در این است که اینترنت همچون ابری جزئیات فنی‌اش را از دید کاربران پنهان می‌سازد و لایه‌ای از انتزاع را بین این جزئیات فنی، از دید کاربران به‌وجود می‌آورد. به‌عنوان مثال آنچه یک ارائه دهندهٔ سرویس نرم‌افزاری رایانش ابری ارائه می‌کند، برنامه‌های کاربردی تجاری برخط است که از طریق مرورگر وب یا نرم‌افزارهای دیگر به کاربران ارائه می‌شود. نرم‌افزارهای کاربردی نیازی به تخصص یا کنترل در مورد فناوری زیرساخت ابری که از آن استفاده

1. Mell & Grance

می‌کنند ندارند. رایانش ابری را گروهی تغییر الگو واره‌ای می‌دانند که دنباله‌روی تغییری است که در اوایل دهه ۱۹۸۰ از مدل رایانه بزرگ به مدل کارخواه – کارساز صورت گرفت (بویا و همکاران[1]، ۲۰۱۳). اخیراً سازمان‌های دولتی شروع به استفاده از معماری، بسترها و برنامه‌های رایانش ابری جهت تحویل خدمات و برآورده ساختن نیازهای زیرمجموعه خود کرده‌اند.

سازمان‌های دفاعی در دنیا نیز در حال مهاجرت به‌سوی فناوری نوظهور رایانش ابری هستند تا از این طریق به مزیت‌های فراوانی از جمله چابکی، کارایی و نوآوری دست یابند. پیدایش رایانش ابری مرتبط با توسعه فناوری در حوزه‌های سخت‌افزاری (نظیر مجازی‌سازی و پردازنده‌های چندهسته‌ای)، فناوری اینترنت (نظیر وب سرویس‌ها، معماری سیرویس‌گرا و وب ۲) و رایانش توزیع شده (نظیر رایانش خوشه‌ای[2] و رایانش مشبک[3]) است. می‌توان رایانش ابری را حاصل همگرایی و پیشرفت در حوزه‌های اصلی فناوری دانست (ولوی و همکاران، ۱۳۹۶). اما در کنار مزیت‌های زیادی همچون کاهش هزینه‌های سخت‌افزاری و نرم‌افزاری که در استفاده از یک سامانه مبتنی بر ابر وجود دارد، هنوز این فناوری با مشکلات فراوانی همراه است چراکه رایانش ابری، مراحل اولیه رشد و توسعه خود را طی می‌کند و برای استفاده گسترده، به‌ویژه در سازمان‌های با مأموریت حساس آماده نیست. برخلافِ مدلِ محاسباتِ معمولی که در آن کاربران بر ذخیره داده‌ها و محاسبات، کنترل کامل دارند، در رایانش ابری لازم است که مدیریت فیزیکی داده‌ها و ماشین‌ها (سرورها و...)، به ارائه‌دهندگان خدمات ابری؛ محول شود. بنابراین ممکن است صحت، محرمانگی ذخیره داده‌ها و محاسبات مربوط، به علت اینکه صاحبان داده‌ها بر امنیت آن کنترل ندارند، به خطر بیافتد (*Wei et al, 2013*). مدیران فناوری اطلاعات سازمان‌ها بر این باورند که امنیت به‌عنوان مانعی برای حرکت به سمت مدل خدمات ابری به شمار می‌رود و هرچه بازار جهانی و کسب‌وکارها به سمت سیستم‌های ابری حرکت می‌کنند، مخاطرات مربوط به مباحث محرمانگی داده‌ها و چالش‌های این حوزه، برجسته‌تر می‌شود. توانایی سازمان‌ها برای مدیریت کردن این مخاطرات و چالش‌ها، در موفقیت رایانش ابری تعیین‌کننده خواهد بود. بنابراین قبل از هرگونه اقدام در زمینه بهره‌برداری از فناوری رایانش ابری، باید تهدیدات و فرصت‌های آن نظیر مسائل مربوط به امنیت و محرمانگی داده‌ها، امنیت مجازی‌سازی، پیروی از قوانین و مقررات، کاهش هزینه‌های سخت‌افزاری و نرم‌افزاری، استفاده از تجهیزات به‌روز و افزایش سرعتِ محاسبات را به‌دقت مورد بررسی قرار داد.

در آیندهٔ نزدیک به علل مختلفی سازمان‌های اطلاعاتی نیز مجبور خواهند شد از فناوری رایانش ابری استفاده کنند. بنابراین شایسته است که موضوع استفاده از رایانش ابری توسط سازمان‌های اطلاعاتی از جوانب مختلف مورد بحث و بررسی قرار گیرد و فرصت‌ها و چالش‌ها استخراج و سازوکارهای احتمالی ارائه گردند.

1. *Buyya et al*
2. *cluster computing*
3. *grid computing*

با توجه به مطالب بیان‌شده؛ مهم‌ترین مسأله‌ای که محقق در این پژوهش با آن روبروست، ضعف در شناخت چالش‌های به‌کارگیری این فناوری در سازمان‌های امنیتی و به تبع آن راه‌کارهای مرتفع ساختنِ آن چالش‌ها با سازوکارهای مناسب می‌باشد. به‌گونه‌ای که اصول امنیتِ اطلاعات ازجمله محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات سازمان نیز تحت تأثیر قرار نگیرد.

همان‌طور که بیان شد، فناوری رایانش ابری، یکی از فناوری‌های نوظهوری است که استفاده از آن مزایای بسیاری دارد و امروزه استفاده از رایانش ابری در سازمان‌ها رواج یافته است. مثلا با توجه به غیریکنواخت بودن ساختار و تشکیلات فناوری اطلاعات در سطح جوامع اطلاعاتی و نیاز به برقراری سامانه‌هایی به‌منظور یکپارچه‌سازی و استفاده سودمند از اطلاعات ذخیره شده در پایگاه داده سازمان‌های مختلف، ضروری است تا تدبیری اندیشیده شود که از اطلاعات ذخیره شده، به همراه رعایت ملاحظه‌های امنیتی حفاظتی، استفاده حداکثری صورت گیرد. رایانش ابری کاندیدای بسیار مناسبی برای این مهم است که پیاده‌سازی آن در سطح کلان، باعث سرعت بخشیدن در انجام امور محوله و بالا بردن کارایی جوامع اطلاعاتی شود (لرستانی، ۱۳۹۵، ۴۰).

ورود و به‌کارگیری همه جانبهٔ فناوری رایانش ابری می‌تواند موجب تغییرات کمی و کیفی در انجام فعالیت‌ها و خدمات سازمانها شود. بنابراین مسائلی از قبیل استفاده از مزایای و فرصت‌های ناشی از بکارگیری تکنولوژی، جلوگیری از عقب ماندگی ناشی از عدم استفاده از تکنولوژی، سازمان‌ها را ملزم می‌کند که از تکنولوژی استفاده کنند؛ اما بررسی‌ها نشان می‌دهد که در آینده نزدیک، موضوع اجبار استفاده از تکنولوژی جدید نیز مطرح خواهد شد؛ چراکه منافع صاحبان تکنولوژی ایجاب می‌کند با به‌روزرسانی سخت‌افزاری و نرم‌افزاری و عدم پشتیبانی از محصولات قبلی، مصرف‌کنندگان مجبور به خرید محصولات جدید، که از تکنولوژی‌های جدید نظیر رایانش ابری پشتیبانی می‌کنند، شوند. مثلا به احتمال زیاد در آینده نزدیک، رایانه‌های رومیزی تنها شامل صفحه کلید، مانیتور و سخت‌افزار رابط اینترنت، برای اتصال به فضای ابری، خواهند بود. یعنی سخت‌افزارهایی نظیر پردازشگر، حافظه در رایانه‌ها وجود نخواهند داشت یا بسیار ضعیف خواهند بود. یا بسیاری از برنامه‌های کاربردی و خدمات نرم‌افزاری فقط به‌صورت نسخه تحت ابر ارائه خواهند شد و نسخه‌های قبلی که قابل استفاده در رایانه‌های مستقل از فضای ابری بودند؛ پشتیبانی نخواهند شد. بنابراین محدودیت‌های سخت‌افزاری و نرم‌افزاری ناشی از پیشرفت تکنولوژی، افراد و سازمان‌ها را ملزم به استفاده از خدمات ابری خواهد کرد. این موارد، نشان می‌دهد که توجه به چالش‌های استفاده از فناوری نوظهور رایانش ابری از اهمیت بالایی برخوردار است. به خصوص در سازمان‌های اطلاعاتی که داشتن یک ارتباط سریع و سرتاسری می‌تواند یکی از مهم‌ترین فاکتورهای ارتقای عملکرد مأموریت‌ها و سطح مطلوبی از بهره‌وری سازمانی در نظر گرفته شود، به‌کارگیری رایانش ابری با

توجه به ماهیت و مأموریت‌ها و همچنین اهمیت اطلاعات در گردش این سازمان‌ها، از جهت‌های مختلف می‌توانند مورد بررسی قرار گیرد. از این‌رو برنامه‌ریزی و اتخاذ سیاست‌های درست در راستای اهداف و چشم‌اندازهای سازمانی دارای اهمیت خاصی است.

تحقیقات انجام شده نشان می‌دهد که تاکنون به‌صورت منسجم و هدفمند "سازوکارهای به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی " ارائه نشده است. همچنین چالش‌ها و تهدیدات استفاده از تکنولوژی رایانش ابری با نگاه و معیارهای سازمان‌ها امنیتی مورد بررسی قرار نگرفته است. از طرفی نیز، اشراف ناقص و مبهم بودن مفهوم ابر، مانند هر فناوری دیگری می‌تواند سبب ایجاد درک ناصحیح از این فناوری شود که در تصمیم‌سازی مدیران مؤثر واقع می‌گردد. بنابراین می‌توان مدعی شد با بررسی دقیق تمام ابعاد ابر، می‌توان مدیران سازمانی را در زمینهٔ تصمیم‌گیری برای به‌کارگیری و یا به‌کار نگرفتن ابر یاری رساند (رایانش ابری در خدمت سازمانهای اطلاعاتی، تهدید یا فرصت). از این رو در این تحقیق، ضمن معرفی تکنولوزی رایانش ابری و بررسی و دسته‌بندی چالش‌های استفاده از تکنولوژی رایانش ابری در سازمان‌های امنیتی، راه‌کارهای متناظر مطرح و اولویت‌بندی خواهند شد و می‌توان گفت که پیامدهای ناشی از انجام این پژوهش عبارتند از:

- آشنایی با خدمات مورد نیاز و یا قابل ارائه سازمان‌های امنیتی از طریق رایانش ابری.
- شناسایی و تعریف بهینه نیازمندی‌های پژوهشی سازمان‌های امنیتی در زمینه تأمین یا ارائه خدمات از طریق رایانش ابری.
- ایجاد آمادگی و مقدمات (مدیریت و فناورانه) سازمان‌های امنیتی برای پیاده‌سازی، فعالیت و یا اتصال به شبکه‌های مبتنی بر رایانش ابری.
- آشنایی با ماهیت فناوری رایانش ابری و شناسایی مزایا و فرصت‌های مدیریتی، فناورانه ناشی از به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی.
- شناسایی و اولویت‌بندی معایب، خلأها، تهدیدات و چالشهای مدیریتی، فناورانه به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی.
- تبیین ملاحظات و ارائه راهکارهای مدیریتی و فناورانه برای استفاده بهینه از فناوری رایانش ابری در سازمان‌های امنیتی و همچنین تعیین اولویت‌های عملکردی.

اما واقعیت این است که امروزه محیط پیرامونی سازمان‌ها، متناسب با تغییراتِ سریعِ فناوری اطلاعات و ارتباطات، در حال تغییر است و سازمان‌هایی می‌توانند به حیات و حرکت روبه‌جلوی خود ادامه دهند که سازوکارهای لازم را برای رویارویی با این تغییرات را دارا باشند. ساختار باز و توزیع‌شده در فناوری رایانش ابری و سرویس‌های آن موجب می‌شود تا تهدیدات و آسیب‌پذیری‌های بیشتری داشته و هدفی

جذاب برای مهاجمان باشد. در صورتی که کاربران خصوصی و سازمان‌ها با لحاظ نمودن سازوکارهایی بتوانند اطمینان حاصل نمایند که اطلاعات آن‌ها در محیطی ذخیره می‌شود که امکان از بین رفتن آن و دسترسی غیرمجاز کاربران و حتی ارائه‌دهندگان خدمات ابری به داده‌ها وجود ندارد، قطعاً استقبال بیشتری از این فناوری خواهند داشت. شناسایی مخاطرات و چالش‌های بکارگیری فناوری نوظهور در سازمان‌ها و پیش‌بینی سازوکارهای مقابله‌ای می‌تواند در کنار بهره‌برداری حداکثری از مزایا، آسیب‌پذیری را به حداقل برساند. عدم انجام این تحقیق، تبعات مشروحه زیر را در پی خواهد داشت:

- در زمینه به‌کارگیری فناوری‌های نوظهور، نظیر فناوری رایانش ابری، درک لازم برای مدیران تصمیم‌گیر در سازمان‌های امنیتی ایجاد نخواهد شد و به تبع آن در آینده غافلگیری رخ خواهد داد.
- ضعف آشنایی با خدمات قابل ارائه و درخواست و ملاحظات به‌کارگیری فناوری رایانش ابری.
- ضعف آشنایی و تعریف بهینه نیازمندی‌های پژوهشی در زمینه تأمین سازوکارهای مقابله‌ای با تهدیدات به‌کارگیری خدمات ابری.
- عدم شناسایی و تبیین فرصت‌ها، چالش‌ها و تهدیدات مدیریتی، فناورانه و امنیتی – عملیاتی به‌کارگیری فناوری رایانش ابری.
- مغفول واقع شدن الزامات امنیتی و کنترلِ امنیتی در مراحل پیاده‌سازی و بهره‌برداری از این فناوری، در آیین‌نامه‌ها و شیوه‌نامه‌های مربوطه.

موارد بالا بر ضرورت این تحقیق دلالت می‌کنند؛ از این رو " تبیین سازوکارهای به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی " به عنوان هدف اصلی این پژوهش مطرح گریده و فرض شده که سازوکارهای مدیریتی و فناورانه، می‌توانند در به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی مؤثر باشند و تلاش شده با بهره‌گیری از تجارب علمی داخلی و خارجی و در چارچوب نظریه‌ها و الگوهای مرجع رایانش ابری، با در نظر داشتن اسناد بالادستی کشور و سازمان‌های امنیتی در حوزه فناوری اطلاعات و ارتباطات، به اهداف فرعی بدین شرح پرداخته شود: ۱– احصاء چالش‌های به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی. ۲– تعیین سازوکارهای مدیریتی به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی. ۳–تعیین سازوکارهای فناورانه به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی. در رابطه با اهداف فرعی نیز فرض شده ۱– مهم‌ترین چالش‌های به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی عبارتند از پایین بودن تحمل‌پذیری خطا در فناوری ابر، ایجاد تعادل و توازن بین مزایای رایانش ابری و وظایف امنیتی، عدم آشنایی و اعتقاد مدیران ارشد سازمانی به جایگاه راهبردی و اثرگذار فناوری ابری، به خطر افتادن صحت و محرمانگی داده‌ها و محاسبات مربوطه، وجود ساختار باز و توزیع‌شده در رایانش ابری و سرویس‌های آن و همچنین جذاب بودن آن برای مهاجمین و هکرها. ۲–سازوکارهای مدیریتی به‌کارگیری

فناوری رایانش ابری در سازمان‌های امنیتی عبارتند از درک خطرات امنیتی، حفظ حریم خصوصی، تدوین آیین‌نامه‌ها، شیوه‌نامه‌ها، قوانین و مقررات مربوط و ارائه خدمات ابری به‌صورت منعطف. ۳-سازوکارهای فناورانه در به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی عبارتند از استفاده از پراکسی‌ها، پیاده‌سازی ابر خصوصی، طراحی چارچوب معماری امنِ بومی و استفاده از مجازی‌سازی.

برابر بررسی‌های انجام‌گرفته از طریق مراجعه به آثار مکتوب اعم از کتاب‌ها، مقاله‌های علمی و منابع الکترونیکی و وبگاه‌های معتبر علمی، پژوهشی در زمینه "سازوکارهای به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی" صورت نپذیرفته است ولی در پژوهش‌های متعددی، موضوعات مرتبط با فناوری رایانش ابری مطرح شده است که ابر موضوعی پیرامون فناوری رایانش ابری بدین صورت است:

- در برخی از مقالات به موضوع پذیرش فناوری رایانش ابری پرداخته شده است به عنوان مثال نتایج پژوهش حمدی‌پور و همکارانش نشان داده که مزیت نسبی، آزمون پذیری، پیچیدگی، سازگاری، و قابلیت رویت نتایج، مهم‌ترین عوامل اثرگذار بر پذیرش رایانش ابری کتابداران کتابخانه‌های دانشگاه تبریز و علوم پزشکی بر مبنای نظریه اشاعه نوآوری راجرز هستند (حمدی‌پور و همکاران، ۱۳۹۷، ۵۲، ۴). والمحمدی و مظاهری نیز در پژوهشی به تبیین عوامل تأثیرگذار بر پذیرش فناوری توسط کاربران سیستم‌های اطلاعاتی پرداخته‌اند که نتایج این پژوهش نشان داد درک سودمندی بیشترین تأثیر را بر تصمیم به استفاده از فناوری رایانش ابری دارد و پس از درک سودمندی، عوامل نگرش نسبت به استفاده و سهولت در رتبه‌های بعدی قرار می‌گیرند (والمحمدی و مظاهری، ۱۳۹۶، ۵، ۱۹).
- در برخی مقالات نیز به نقش، کاربردها و مزیت‌های استفاده از فناوری رایانش ابری بیشتر توجه شده است. مثلا اسمعیلی رنجبر و سلاجقه در تحقیقی به عنوان " بررسی و نقش رایانش ابری در شرکت‌های دانش بنیان ایران " به تشخیص و ارزیابی و رتبه‌بندی فاکتورهای مختلف تطابق شرکت‌های دانش‌بنیان با ابر پرداختند که نتایج تحقیق آنها نشان داد نوآوری تصمیم‌گیرندگان فناوری اطلاعات و نیاز بیشترین تأثیر را درتطابق شرکت‌های دانش‌بنیان با ابر دارند (اسمعیلی رنجبر و سلاجقه، ۱۳۹۹، ۱۶، ۶۲). فراحی و کاردانی ملکی‌نژاد در پژوهشی به بررسی و ارائه کاربردها، مزیت‌ها و چالش‌های فناوری رایانش ابری در مدیریت منابع انسانی شرکت‌های کوچک و متوسط پرداخته‌اند و الزامات و چگونگی کاربست آن در این سازمان‌ها را ارائه کرده‌اند (فراحی و کاردانی ملکی‌نژاد، ۱۳۹۸، ۶۰). مرعشی و عبدالوند در پژوهشی به پیاده‌سازی و معرفی چارچوب‌های حاکمیتی در حوزه انتقال فناوری رایانش ابری پرداخته‌اند که نتایج حاصل از پژوهش معرفی دو مدل حاکمیتی است (مرعشی و عبدالوند، ۱۳۹۷، ۵۵). دشمن زیاری در پژوهشی به شناسایی عوامل موثر بر کاربرد رایانش ابری در دانشگاه‌های دولتی شهر تهران پرداخته است (دشمن زیاری، ۱۳۹۵، ۲۸).
- برخی مقالات به موضوع برون‌سپاری خدمات فناوری اطلاعات در بستر رایانش ابری پرداخته‌اند. به

عنوان مثال شفایی تنکابنی و همکارانش در پژوهش خود، نیازهای بخش فناوری اطلاعات سازمان‌ها و خدمات ابری را معرفی کرده و به‌منظور موفقیت بیشتر در برون‌سپاری در بستر رایانش ابری، به اولویت‌بندی نیازها و اندازه‌گیری خدمات ابری پرداخته‌اند. که نتایج به‌دست آمده از پیاده‌سازی آن‌ها، نشان داد مهم‌ترین معیارهای برون‌سپاری در بستر رایانش ابری به ترتیب پذیرش، کارایی و تجربه قرارداد است و مدیریت امنیت، مالکیت و تجربه قرارداد، نیز از معیارهای تأثیرگذار هستند (شفایی تنکابنی و همکاران، ۱۳۹۴، ۷، ۲). یکتایی و رنجبر نوشری نیز در تحقیقی به ارائه مدلی برای برون‌سپاری فناوری اطلاعات بر مبنای پذیرش رایانش ابری پرداخته‌اند که بر اساس نتایج این پژوهش، دانش کارکنان، حمایت مدیران و امنیت و حفظ حریم خصوصی از بیشترین اهمیت در پذیرش رایانش ابری در برون‌سپاری فناوری اطلاعات است که می‌تواند کمک شایانی به سازمان‌ها داشته باشد (یکتایی و رنجبر نوشری، ۱۳۹۵، ۲۷، ۱۰۷).

- برخی دیگر از مقالات، بر پیاده‌سازی، ارائه مدل، معماری و یا بهبود در بکارگیری بستر رایانش ابری متمرکز شده‌اند. به عنوان مثال زهرا سلیمی در پژوهشی، با بررسی نقاط ضعف و قوت معماری‌های مختلف رایانش ابری به ارائه راهکارهایی برای توسعه سازمان‌های امنیتی در راستای بهبود معماری امنیتی رایانش ابری پرداخته است (سلیمی، ۱۳۹۸، ۱، ۸). نوروزی و حداد اسکویی در پژوهشی به شناسایی موانع پیاده‌سازی رایانش ابری از دیدگاه مسئولان پورتال کتابخانه‌های دیجیتالی ایران پرداخته‌اند (نوروزی، حداد اسکویی، ۱۳۹۷، ۲۹، ۲). بزی و همکارانش نیز در پژوهشی به تجزیه و تحلیل پژوهش‌های گذشته در زمینهٔ مدل‌ها و معماری‌های پشتیبان پیاده‌سازی رایانش ابری در مراکز آموزش عالی پرداخته‌اند و در نهایت معماری ابری ترکیبی به نام IUHEC را برای پشتیبانی پیاده‌سازی رایانش ابری در مراکز مذکور ارائه کرده‌اند (بزی و همکاران، ۱۳۹۶، ۹، ۴). محمدی در تحقیق خود، مدلی امن و مقیاس‌پذیر برای دورکاری کاربران و ذینفعان سازمان بر اساس فناوری رایانش ابری ارائه داده است (محمدی، ۱۳۹۶، ۳، ۲). حیدری دهویی و همکارانش در کار خود به تدوین چارچوبی علمی برای انتخاب نرم‌افزار مناسب پیاده‌سازی راهکار رایانش ابری در سطح زیرساخت پرداختند و سپس براساس چارچوب ایجاد شده و با استفاده از رویکرد آراس فازی با مقادیر بازه‌ای، به وزندهی و اولویت‌بندی گزینه‌ها اقدام کردند که نتایج حاکی از آن بود که سیستم رایانش ابری Open Stack برترین گزینه است (حیدری دهویی و همکاران، ۱۳۹۶، ۲، ۴).
- تعدادی زیادی از پژوهش‌ها به چالش‌ها، ریسک‌ها، آسیب‌پذیری‌ها و راهکارهای مقابله‌ای استفاده از رایانش ابری پرداخته‌اند. مثلا غیاثوند و همکارانش در تحقیقی به بررسی چالش‌های امنیتی در رایانش ابری، تهدیدات امنیتی و حفظ حریم خصوصی به همراه ارائه راهکارها پرداخته‌اند

(غیاثوند و همکاران، ۱۳۹۷، ۱۳، ۴۰). سلطانی فر و همکاران در تحقیقی، به استخراج استخراج و رتبه‌بندی ریسک‌های امنیتی فناوری رایانش ابری پرداخته‌اند که بر اساس نتایج رتبه‌بندی آن‌ها، ریسک محرمانگی داده، احراز هویت، و موقعیت داده به‌ترتیب در رتبه اول تا سوم قرار گرفتند و رتبه سایر ریسک‌ها نیز مشخص شد (سلطانی‌فر و زرگر، ۱۴۰۰، ۱۰۵). بهادر و صادقی در تحقیق خود روش‌های هوشمند جهت تشخیص نفوذ در شبکه را بررسی کرده‌اند. بر اساس این پژوهش، مهم‌ترین این روش‌ها عبارتند از درخت تصمیم، الگوریتم ژنتیک، منطق فازی و روش بیزین (بهادر و صادقی، ۱۳۹۸، ۵، ۱). سلطان باغشاهی و همکاران، کنترل دسترسی، وقفه در سرویس‌دهی، قابلیت حمل، چند اجاره‌ای، انتقال اطلاعات، رابط‌های ناامن و رابط مدیریت دسترسی از راه دور را به‌عنوان ریسک‌های امنیتی رایانش ابری معرفی کردند (سلطان باغشاهی و همکاران، ۱۳۹۱). در پژوهش دیگری که توسط یعقوبی و همکاران انجام گرفته، ریسک‌های رایانش ابری در سازمان‌های دولتی، به ریسک‌های محسوس و نامحسوس تقسیم‌بندی شده است. عواملی چون دسترس‌پذیری، جامعیت داده، زیرساخت، فروشنده و پشتیبانی تحقیقاتی در بخش ریسک‌های محسوس و عوامل تداوم خدمات، محرمانگی داده، مکانیزم ذخیره‌سازی، مکان داده و حفاظت از داده در بخش ریسک‌های نامحسوس قرار گرفتند (یعقوبی نورمحمد و همکاران، ۱۳۹۴). به عقیده تبریزچی و کوچکی رفسنجانی، برای دستیابی به امنیت گسترده ابر، داده‌ها و زیرساخت‌های ابری باید در برابر حملات شناخته شده و ناشناخته در تمام اجزای ابر بررسی شوند. آن‌ها در پژوهشی مسائل و مشکلاتی را که رایانش ابری با آن دست و پنجه نرم می‌کند و خطرات و تهدیدات رایانش ابری (دستکاری، کلاه‌برداری، افشای اطلاعات، انکار و اجتناب از خدمت) و حملات رایانش ابری را مورد بررسی قرار داده‌اند (*Tabrizchi & Kuchaki Rafsanjani, 2020*).

- در برخی از مقالات نیز، استفاده سازمان‌ها از فناوری رایانش ابری مطرح شده است. به عنوان نمونه، در پژوهشی که توسط ولوی و همکاران انجام شد، یک الگوی راهبردی برای مهاجرت سازمان‌های دفاعی به محیط رایانش ابری ارائه شد. در این پژوهش عواملی چون کارکرد، امنیت اطلاعات، حریم خصوصی داده‌ها، نظارت، دسترس‌پذیری، قابلیت حمل و یکپارچگی به‌عنوان ملاحظات امنیتی رایانش ابری در حوزه دفاعی معرفی گردید (ولوی، موحدی صفت و کوشالشاه، ۱۳۹۶). والمحمدی و مظاهری نیز در پژوهشی به تبیین عوامل تأثیرگذار بر پذیرش فناوری توسط کاربران سیستم‌های اطلاعاتی پرداخته‌اند (والمحمدی و مظاهری، ۱۳۹۶، ۵، ۱۹). علیرضا لرستانی در تحقیقی ضمن بررسی مزایا و عیوب و زیرساخت‌های مورد نیاز فناوری رایانش ابری، به بررسی موردی در زمینهٔ مزایا و عیوب به‌کارگیری و یا عدم به‌کارگیری این فناوری که متوجه سازمان‌های اطلاعاتی است، پرداخته

است. در نتیجه‌گیری این تحقیق آمده که با توجه به مزایا و عیوب رایانش ابری در سطح جوامع اطلاعاتی، می‌توان نتیجه گرفت که مزایای به‌کارگیری ابر، بسیار بیشتر از عیوب به‌کارگیری آن است و ارائه راهکارهای تخصصی در زمینهٔ امنیت رایانش ابری را می‌توان در سطوح مختلف برای اطلاعات با طبقه‌بندی متفاوت بررسی نمود و با اتخاذ استانداردهای بومی برای تأمین امنیت ابر، می‌توان تهدید اصلی رایانش ابری یعنی امنیت را تا حد قابل قبولی مرتفع ساخت و یک محیط کامل بومی شدهٔ امن را به‌وجود آورد (لرستانی، ۱۳۹۵، ۴۰)

که به نظر می‌آید تحقیقات دو دسته آخر، نزدیک‌ترین پژوهش‌های مرتبط با موضوع این تحقیق هستند. پژوهش حاضر از لحاظ ماهیت آمیخته کیفی مقدم بر کمی است و از نظر روش، موردی- زمینه‌ای است و از نظر هدف، کاربردی بوده چرا که با انجام این پژوهش و تبیین سازوکارهای به‌کارگیری رایانش ابری در سازمان‌های امنیتی، می‌توان دستاوردهای این تحقیق را در پیاده‌سازی امن فناوری رایانش ابری در سازمان‌های امنیتی در راستای متمرکزسازی سامانه‌های کاربردی و بانک‌های اطلاعاتی، مدیریت و استفاده بهینه از منابع سخت‌افزاری و نرم‌افزاری و صرفه‌جویی در هزینه‌های مربوط به فناوری اطلاعات و ارتباطات سازمان‌ها، هم‌افزایی اطلاعاتی بین بخش‌های داخلی سازمان و همچنین بین اعضاء جامعه اطلاعاتی، تسریع و تسهیل در روند خدمات‌رسانی به کاربران سازمانی به‌منظور انجام وظایف و مأموریت‌های محوله و... مدنظر قرار داد و بهره برد. در بخش آمار کیفی، ابتدا جمع‌آوری اطلاعات از طریق مصاحبه با روش گلوله برفی تا رسیدن اشباع انجام شد و سپس بررسی اسناد و مدارک، مقالات و منابع کتابخانه‌ای صورت گرفت. در بخش اسنادی، روش تجزیه وتحلیل اطلاعات کیفی بوده و با کمک تحلیل محتوی انجام شد. یعنی در پژوهش حاضر ضمن به‌کارگیری تجارب پژوهشگران و محققین، محورها و خطوط کلی متون، اسناد و مدارک، مقالات و ... استخراج و جهت تعیین، مؤلفه‌های تأثیرگذار بر موضوع مورد تحقیق در اختیار کارشناسان و متخصصان قرارگرفته است. در بخش آمار کمی، برای تحلیل داده‌های حاصل از پرسش‌نامه و نظرات صاحب نظران از آمار توصیفی جهت تجزیه وتحلیل داده‌ها استفاده شد.

جامعه آماری در این پژوهش را تعداد ۱۰۰ نفر از کارشناسان، صاحب‌نظران و مدیران حوزه سایبری سازمان‌های امنیتی و آشنا با مباحث فضای سایبری و امنیت آن تشکیل دادند. به دلیل محدود بودن جامعه آماری، در این پژوهش از نمونه‌گیری استفاده نشده و به‌صورت تمام شمار همه افراد جامعه هدف درنظر گرفته شدند. گردآوری اطلاعات و داده‌ها در این تحقیق با استفاده از روش کتابخانه‌ای و میدانی و با مصاحبه و پرسشنامه انجام شد. به‌منظور تعیین روایی پرسشنامه از نظر متخصصین و خبرگان حوزه پژوهش (روایی محتوایی) استفاده شد و بعد از اعمال نظرات و اصلاحات لازم و اخذ پایایی درونی (آلفای کرونباخ = ۰/۹۰۹) پرسشنامه در بین اعضای جامعه آماری توزیع گردید. به منظور پاسخگویی، مقیاس

لیکرت ۵ تایی (از کاملا موافق تا کاملا مخالف) درنظر گرفته شده که با توجه به آن پاسخ‌دهندگان وضعیت هر شاخص را مشخص نمودند.

مبانی نظری و مفاهیم:

مفهوم رایانش ابری

امروزه، رایانش ابری توسط بسیاری از سازمان‌ها برای افزایش سودآوری و پایداری مورد استفاده قرار می‌گیرد. در دوران انقلاب فناوری، قدرت محاسبات سازمان به‌عنوان کلیدی برای تولید مزیت رقابتی درنظر گرفته می‌شود. مدل رایانش ابر امکان ذخیره و پردازش داده‌های افراد، شرکت‌ها یا سازمان‌ها را در دستگاه ناشناخته از راه دور که برای کاربران هم شناخته شده نیست، فراهم می‌کند (*Bhadani, 2014*). رایانش ابری یک تعریف واحد ندارد، زیرا این مفهوم در طول زمان با پیشرفت اینترنت تغییر کرده است. در ادبیات هیچ تعریف استاندارد و مورد تأیید مورد استفاده قرار نگرفته است زیرا اکثر اوقات آن به‌عنوان خدمات محاسباتی ارائه شده توسط شخص ثالث از طریق اینترنت تعریف می‌شود. با این حال برخی صاحب‌نظران با تمرکز بر مزایای کلیدی آن از دیدگاه فناورانه و کسب و کار، رایانش ابری را تعریف کردند (*Marston et al, 2011*): رایانش ابری یک مدل خدمات فناوری اطلاعات است که خدمات نرم‌افزاری و سخت‌افزاری را بر اساس تقاضای مصرف‌کنندگان ارائه می‌دهد، سیستم شبکه‌ای که در رایانه‌های ابری استفاده می‌شود، خودخدمتی است، مستقل از مکان و دستگاه می‌باشد و سرورهای از راه دور برای ذخیره، پردازش و مدیریت داده‌های موجود در اینترنت بدون دخالت رایانه‌های شخصی یا سرور محلی استفاده می‌شوند (*Stallings, 2007*). مطابق با تعریف *NIST* رایانش ابری، مدلی است برای دسترسی آسان به نیازهای کاربران نهایی از طریق اینترنت و مجموعه‌ای از منابع ابری (شبکه‌ها، سرورها، برنامه‌ها، ظرفیت‌های ذخیره‌سازی) را با دسترسی سریع بدون نیاز شدید به مدیریت منابع یا دخالت مستقیم ارائه دهنده خدمات فراهم می‌کند (*Mell and Grance, 2011*). در تعریف ساده دیگر از رایانش ابری که توسط بسیاری از نویسندگان پذیرفته شده است آن است که رایانش ابری، نوعی فناوری است که مالکیت، ارتقاء، حفظ و مدیریت منابع، وظیفه اشخاص ثالث است و نیازی به دخالت کاربر نهایی نیست (*Ghaffari et al, 2014*). از جمع‌بندی مجموعه نظرات بیان شده از تعاریف و ویژگی‌های رایانش ابری به‌صورت خلاصه می‌توان رایانش ابری را یک ایده گسترده و به‌سرعت در حال پیشرفت دانست که سازمان‌ها را قادر می‌سازد در هر زمان که نیاز به استفاده از منابع کامپیوتری باشند، با بهره‌گیری از زیرساخت‌های شخص ثالث، بدون نیاز به ساخت و نگهداری زیرساخت‌های فیزیکی بتوانند به خدمات این منابع دسترسی داشته باشند. به زبان ساده‌تر با وجود رایانش ابری کاربران نیازی به مالکیت منابع ضروری

مانند سخت‌افزار و نرم‌افزار ندارند و قادر خواهند بود از طریق اینترنت به این زیرساخت دسترسی داشته باشند.

ویژگی‌های رایانش ابری

برای هر سازمانی به‌ویژه شرکت‌های کوچک و متوسط شناختن ویژگی‌های اولیه رایانش ابری به‌منظور کارآیی خدمات آن مهم است. اساساً رایانش ابری کاربران را قادر می‌سازد ظرفیت خود را با ارائه سرویس‌های خودمحور در سرورهای راه‌دور افزایش دهند. بر اساس ادبیات این حوزه برخی از مهم‌ترین ویژگی‌های رایانش ابری شامل موارد ذیل می‌باشد (khan, 2015):

- خویش خدمتی مبتنی بر تقاضا: رایانش ابری به کاربران خود پورتال‌های خود سرویس را ارائه می‌دهد، جایی که آنها می‌توانند به خدمات پایهٔ فناوری اطلاعات مانند انبار و مخزن ذخیره‌سازی و سرور زمان بدون ارتباط بین انسان‌ها دسترسی یابند (khan, 2015).
- انعطاف‌پذیری سریع: ارائه و تخصیص خدمات رایانش ابری می‌تواند بر اساس تقاضا قابل دسترسی باشد. منابع اختصاص یافته به کاربران نامحدود هستند، چنانکه در هر ظرفیتی و در هر زمانی برای پاسخگویی به نیازهای کاربران در دسترس است (Stallings, 2007).
- جمع‌آوری منابع: ارائه‌دهندگان خدمات، منابع مختلف، منابع مختلف فناوری اطلاعات مانند حافظه، منبع ذخیره‌سازی، پردازش و پهنای باند شبکه را ادغام می‌کنند و این مجموعه از منابع محاسباتی را به چندین مشتری عرضه می‌کنند. با این حال، این منابع برای برآورده ساختن تقاضای پویای چندین مشتری قابلیت اینکه از هم جدا شوند را دارند (khan, 2015).
- دسترسی گسترده به شبکه: کاربران می‌توانند به منابع رایانش ابری از شبکه اصلی یا سرور دسترسی پیدا کنند. به‌طور عمده این منابع توسط بسیاری از دستگاه‌های مختلف مانند تلفن‌های همراه، دستگاه‌های تبلت، ایستگاه‌های کاری، لپ‌تاپ‌ها و رایانه‌ها پشتیبانی می‌شوند (Stallings, 2007).
- خدمات اندازه‌گیری شده: استفاده از منابع به‌طور خودکار توسط سیستم محاسباتی کنترل و بهبود می‌یابد، زیرا که از یک معیار اندازه‌گیری مناسب برای خدمات مختلف مانند پهنای باند، پردازش، ذخیره‌سازی و حساب‌های کاربر پویا استفاده می‌کند (Stallings, 2007).

مدل‌های خدمات و گسترش رایانش ابری

چندین مدل در خدمات رایانش ابری ارائه شده است (Rimal et al, 2011). از جمله این‌ها می‌توان به مدل‌های ذخیره‌سازی به‌عنوان یک سرویس، پایگاه داده به‌عنوان یک سرویس، امنیت به‌عنوان یک سرویس، اطلاعات به‌عنوان یک سرویس، مدیریت به‌عنوان یک سرویس، فرآیند کسب و کار به‌عنوان یک سرویس و برنامه کاربردی به‌عنوان یک سرویس اشاره نمود. در ادامه به تشریح هر یک از این مدل پرداخته می‌شود.

- ذخیره‌سازی به‌عنوان یک سرویس، قابلیت نفوذ به منبع ذخیره‌سازی به‌صورت فیزیکی از راه دور و همچین به‌صورت منطقی یک منبع ذخیره‌سازی محلی برای هر برنامه‌ای کاربردی که نیاز به ذخیره‌سازی دارد را فراهم می‌کند. این مؤلفه، ابتدایی‌ترین مؤلفه رایانش ابری است که توسط بسیاری از دیگر مؤلفه‌های رایانش ابر استفاده می‌شود.
- پایگاه داده به‌عنوان یک سرویس، قابلیت استفاده از خدمات پایگاه داده میزبان از راه دور، به اشتراک‌گذاری آن با دیگر کاربران، و داشتن عملکردی همانند پایگاه داده محلی را فراهم کند.
- امنیت به‌عنوان یک سرویس، قابلیت ارائه خدمات امنیتی از راه دور را از طریق اینترنت فراهم می‌کند. در حالی که معمولاً خدمات امنیتی ارائه شده ابتدایی هستند، سرویس‌های پیچیده‌ای مانند مدیریت هویت در دسترس هستند.
- اطلاعات به‌عنوان یک سرویس، امکان دسترسی و استفاده از هر نوع اطلاعاتی از راه دور از طریق یک رابط کاملاً تعریف‌شده را فراهم می‌کند. مدیریت/ حکومت به‌عنوان یک سرویس، سرویس مبتنی بر تقاضا است که قابلیت مدیریت یک یا چند سرویس ابر دیگر را فراهم می‌کند.
- فرآیند به‌عنوان یک سرویس، به یک منبع از راه دور اشاره دارد که می‌تواند با استفاده از منابع رایانه‌ای مشابه از راه دور، منابع زیادی را برای ایجاد فرآیندهای تجاری به هم متصل کند.
- برنامه کاربردی به‌عنوان یک سرویس، هر برنامه‌ای که بر روی پلت فرم وب به کاربر نهایی تحویل داده شود، و به‌طور معمول کابرد آن از طریق یک مرورگر باشد. برنامه‌های کاربردی اتوماسیون اداری در واقع نمونه‌ای از برنامه‌های کاربردی به‌عنوان یک سرویس نیز هستند.

با مرور و جمع‌بندی انواع مدل‌های خدمات و گسترش رایانش ابری این مدل‌ها در قالب سه مدل گسترش ابر شامل ابر عمومی، خصوصی و ترکیبی[1] و ۳ مدل خدمات ابر شامل نرم‌افزار به‌عنوان خدمت[2]، پلتفرم به‌عنوان خدمت[3] و زیرساخت به‌عنوان خدمت[4] ارائه می‌گردد (*Fazli et al,2015*). جدول زیر خلاصه‌ای از مدل‌های مذکور را معرفی می‌نماید.

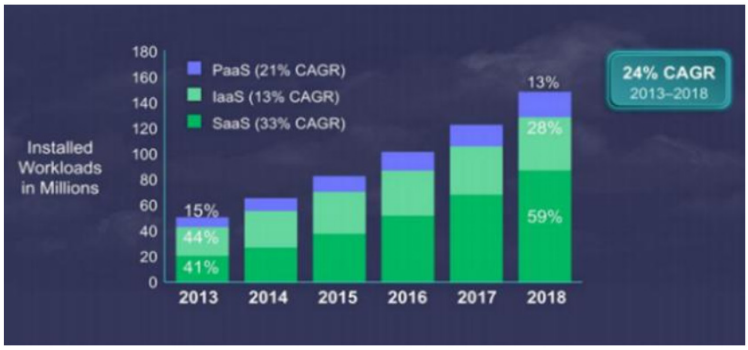
1. *Public, Private, Hybrid Cloud*
2. *Software as a Service (SaaS)*
3. *Platform as a Service (PaaS)*
4. *Infrastructure as a Service (IaaS)*

جدول ۱– انواع مدل‌های خدمات و گسترش رایانش ابری (*Fazli et al,2015*)

مدل‌های گسترش ابرها	ابر عمومی	مالکیت آن به ارائه‌دهنده خدمات داده شده است و تمام منابع به‌صورت در دسترس هستند. کاربران نهایی گزینه اجاره تنظیم منابع را بر اساس الگوی مصرف خود دارند.
	ابر خصوصی	مالک یا اجاره شده توسط یک سازمان برای استفاده شخصی است.
	ابر ترکیبی	ترکیبی از دو یا بیشتر از دو زیرساخت‌های ابر (که می‌تواند عمومی، خصوصی و یا جامعه) باشد و ارائه منابع اضافی در موارد تقاضای بالا برای کاربران را فراهم می‌کند.
مدل‌های خدمات ابر	نرم‌افزار به‌عنوان خدمت	نرم‌افزارها به‌عنوان خدمت یک نمونه سرویسی است که در نرم‌افزار و سایر راهکارها به کاربر نهایی به‌عنوان یک محصول قابل نصب بر روی رایانه کاربر تحویل داده نمی‌شود بلکه از طریق اینترنت به واسطه یک ابر قابل دسترس می‌باشد.
	پلتفرم به‌عنوان خدمت	پلتفرم به‌عنوان خدمت یک نمونه سرویسی است که در آن خدمت ارائه شده به مشتری به‌صورت یک بستر آماده با امکان استقرار خدمات مورد نیاز توسط مشتری می‌باشد و مشتری کنترل کامل را بر روی برنامه‌های مستقر دارد.
	زیرساخت به‌عنوان خدمت	زیرساخت به‌عنوان خدمت یک نمونه سرویسی است که در آن قابلیت ذخیره‌سازی و محاسبات در یک ابر ارائه می‌شود. ابرهای محاسبه و ابرهای منبع، دو نوع زیرساخت به‌عنوان خدمت هستند. ابرهای محاسبه دارای منابع محاسباتی هستند، درحالی که ابرهای منابع دارای منابع مدیریت شده و مقیاس‌پذیر هستند.

رشد ابر

با رشد و توسعه مدل‌های مختلف برای ابر بسیار سودمند خواهد بود که بدانیم چگونه این نرخ رشد در رابطه با مدل‌های ابر ساختار یافته است. پیش‌بینی شده است که تا سال ۲۰۱۸، ۵۹ درصد کل مصرف ابر، نرم‌افزار به‌عنوان سرویس خواهد شد در مقایسه با این‌که در سال ۲۰۱۳، ۴۱ درصد را در بر داشت. از سوی دیگر، سیسکو پیش‌بینی می‌کند که ۲۸ درصد از کل مصرف ابر در سال ۲۰۱۸ به زیرساخت به‌عنوان یک خدمت در مقایسه با ۴۴ درصد در سال ۲۰۱۳ می‌باشد. در نهایت، ۱۳ درصد از کل استفاده از ابر به پلتفرم به‌عنوان خدمت در مقایسه با مقیاس ۱۵ درصدی در سال ۲۰۱۳ اختصاص می‌یابد. شکل ذیل، خلاصه الگوهای رشد *SaaS*، *PaaS* و *IaaS* را از سال ۲۰۱۳ تا ۲۰۱۸ نشان می‌دهد (Cisco, 2015).



شکل ۱– رشد خدمات ابر از سال ۲۰۱۳ تا ۲۰۱۸ (Cisco, 2015)

در پژوهش جعفرنژاد و همکاران، از داده‌های روند جستجوی اینترنتی کلیدواژه فناوری رایانش ابری به‌عنوان نماینده‌ای برای روند انتشار این فناوری برای پیش‌بینی آینده انتشار این فناوری استفاده شد و اثرات روند انتشار در سایر کشورها روی ایران بررسی شد. با توجه به نتایج حاصله از پژوهش، ایران در حدود سال ۲۰۱۸ میلادی به اشباع بازار در زمینه فناوری رایانش ابری خواهد رسید که این مهم بیانگر فرصتی برای کسب و کار و بنگاه‌های فعال در این زمینه است که می‌توانند هنوز به رشد بازار این حوزه در ایران امیدوار باشند. همچنین یافته‌ها حاکی از آن است که تأخیر بالای ایران در شروع انتشار این فناوری در سال ۲۰۱۲، منجر به سرعت بالاتر انتشار این فناوری در ایران نگشته است (جعفرنژاد چقوشی و همکاران، ۱۳۹۵، ۴).

ذینفعان در رایانش ابری

به رغم رویکرد سنتی که فقط دارای دو گروه عمده از ذینفعان شامل ارائه‌دهندگان خدمت و مصرف‌کنندگان است، ذینفعان رایانش ابری علاوه بر موارد سنتی شامل دو گروه دیگر، تنظیم‌کننده‌ها و توانمندسازها هستند که در رایانش ابری نقش ذینفعان مختلف سنتی تغییر خواهد کرد. در رویکرد سنتی، مصرف‌کننده مسئول نگهداری و ارتقاء فرآیندها است در حالی که در رویکرد رایانش ابری، این فرآیندها بخشی از وظایف ارائه‌دهنده است (*Ghaffari et al, 2014*). این ذینفعان در جدول ذیل خلاصه شده‌اند:

جدول ۲– ذینفعان جدید رایانش ابری (*Fazli et al,2015*)

تأمین‌کنندگان	فروشندگانی که تعمیر و ارتقاء سیستم را انجام می‌دهند و مسئول حفاظت از اطلاعات مصرف‌کننده هستند. ارائه‌دهندگان شامل شرکت‌هایی همچون گوگل، مایکروسافت، آی‌بی‌ام، اوراکل، آمازون و غیره هستند.
مصرف‌کنندگان	مشتریانی که سیستم را خریداری و استفاده می‌کنند.
تنظیم‌کنندگان	موجودیت‌های بین‌المللی که در میان ذینفعان دیگر نفوذ می‌کنند.
توانمندسازها	سازمان‌هایی که مسئول فروش خدمات، تسهیل تحویل، پذیرش و استفاده از رایانش ابری هستند.

مزایا و نقاط قوت رایانش ابری

مانند هر فناوری نوظهور، رایانش ابری هم دارای مزایا و عیوبی است؛ اما با توجه به تجربهٔ سازمان‌های مختلف در بهره‌مندی از ابر، می‌توان گفت که مزایای آن بر عیب‌های آن دارای رجحان هستند. این مزایا دارای مصداق‌هایی در فناوری اطلاعات و ارتباطات جوامع اطلاعاتی می‌باشد (احمدی و همکاران، ۱۳۹۳).

۱- هزینه‌های رایانه‌ای کمتر

شما برای اجرای برنامه‌های کاربردی مبتنی بر وب، نیازی به استفاده از یک رایانه قدرتمند و گران‌قیمت ندارید. از آنجایی که برنامه‌های کاربردی بر روی ابر اجرا می‌شوند (نه بر روی یک رایانه رومیزی)، رایانه رومیزی شما نیازی به توان پردازشی زیاد یا فضای دیسک سخت که نرم‌افزارهای *Desktop* محتاج آن هستند ندارد. وقتی شما یک برنامه کاربردی تحت وب را اجرا می‌کنید، رایانه شما می‌تواند ارزان‌تر، با یک دیسک سخت کوچک‌تر، با حافظه کمتر و دارای پردازنده کارآمدتر باشد. در واقع، رایانه شما حتی نیازی به یک درایو CD یا *DVD* هم ندارد؛ زیرا هیچ نوع برنامه نرم‌افزاری بار نمی‌شود و هیچ سندی نیاز به ذخیره شدن بر روی رایانه ندارد.

۲- هزینه‌های نرم‌افزاری کمتر و ارتقای نرم‌افزاری سریع و دائم

به‌جای خرید برنامه‌های نرم‌افزاری گران‌قیمت برای هر رایانه، شما می‌توانید تمام نیازهای خود را به‌صورت سرتاسری برطرف کنید. با نصب یک نسخه واحد در مراکز و سوئیچ کردن کاربران برای بهره‌مندی از این برنامه‌ها، می‌توانید نیازهای خود را برطرف کنید. یکی دیگر از مزایای مربوط به نرم‌افزار در رایانش ابری این است که شما دیگر نیازی به، به‌روز رسانی نرم‌افزارها و یا اجبار به استفاده از نرم‌افزارهای قدیمی ندارید. وقتی برنامه‌های کاربردی، مبتنی بر وب باشند ارتقاءها به‌صورت خودکار رخ می‌دهد. وقتی شما به یک برنامهٔ کاربردی مبتنی بر وب دسترسی پیدا می‌کنید، بدون نیاز به پرداخت پول برای دانلود یا ارتقای نرم‌افزار، از آخرین نسخه آن بهره‌مند می‌شوید.

۳- سازگاری بیشتر شکل اسناد و دستگاه‌های مختلف

نیازی نیست که شما نگران مسئلهٔ سازگاری اسنادی که بر روی رایانه خود ایجاد می‌کنید با سایر سیستم‌عامل‌ها یا سایر برنامه‌های کاربردی دیگران باشید. در دنیایی که اسناد *2007WORD* نمی‌توانند بر روی رایانه‌ای که *WORD 2003* را اجرا می‌کند باز شوند، تمام اسنادی که با استفاده از برنامه‌های کاربردی مبتنی بر وب ایجاد می‌شوند، می‌توانند توسط سایر کاربرانی که به آن برنامهٔ کاربردی دسترسی دارند خوانده شوند. وقتی همه کاربران اسناد و برنامه‌های کاربردی خود را بر روی ابر به اشتراک می‌گذارند، هیچ نوع ناسازگاری بین شکل‌ها به‌وجود نخواهد آمد؛ و با هر دستگاهی نظیر تبلت، گجت‌های هوشمند و سایر موارد می‌توان بدون کوچک‌ترین مشکلی به اطلاعات طبقه‌بندی مربوط دست یافت.

۴- ظرفیت نامحدود ذخیره‌سازی

رایانش ابری ظرفیت نامحدودی برای ذخیره‌سازی در اختیار شما قرار می‌دهد. دیسک سخت ۲۰۰ گیگابایتی فعلی رایانه رومیزی شما در مقایسه با صدها پتابایت (یک میلیون گیگابایت) که از طریق ابر در دسترس شما قرار می‌گیرد چیزی به‌حساب نمی‌آید. شما هر چیزی را که نیاز به ذخیره کردن آن داشته باشید می‌توانید ذخیره کنید.

۵- قابلیت اطمینان بیشتر به داده

برخلاف پردازشگر که در آن یک دیسک سخت می‌تواند آسیب ببیند و تمام داده‌های ارزشمند شما را از بین ببرد، رایانه‌ای که بر روی ابر آسیب ببیند، نمی‌تواند بر داده‌های شما تأثیر بگذارد. این همچنین بدان معنا است که اگر رایانه‌های شخصی شما نیز آسیب ببیند، تمام داده‌ها هنوز هم آنجا و بر روی ابر وجود دارند و کماکان در دسترس شما هستند. در دنیایی که تنها تعداد اندکی از کاربران به‌طور مرتب و منظم از داده‌های مهم و حساس خود نسخهٔ پشتیبان تهیه می‌کنند، رایانش ابری حرف آخر در زمینهٔ محافظت از داده‌ها به‌شمار می‌رود.

۶- دسترسی سراسری به اسناد

آیا تا به‌حال کارهای مهم خود را از محیط کار به منزل برده‌اید و یا تاکنون به همراه بردن یک یا چند فایل مهم را فراموش کرده‌اید، این موضوع در رایانش رخ نمی‌دهد؛ زیرا شما اسناد مهم خود را همراهتان حمل نمی‌کنید. در عوض، این اسناد بر روی ابر می‌مانند و شما می‌توانید از هر جایی که یک رایانه و اتصال اینترنتی وجود داشته باشد به آن دسترسی پیدا کنید. شما در هر کجا که باشید به‌سرعت می‌توانید به اسناد خود دسترسی پیدا کنید و به همین دلیل، نیازی به همراه داشتن آنها نخواهید داشت. با توجه به شکل مأموریت‌ها که در موقعیت‌های جغرافیایی مختلف است و در برخی موارد دسترسی به یک رایانه با تشکیلات آن غیرممکن و یا سخت است، ابر می‌تواند با ارائه خدمات در هر مکان و یا زمانی این مشکل را حل نماید. با توجه به تنوع دستگاه‌ها و سیستم‌های عامل (ویندوز، اندروید و یا ios) در ابر محدودیت دسترسی به اطلاعات و اسناد مرتفع می‌گردد.

۷- همکاری گروهی ساده‌تر

به اشتراک گذاشتن اسناد، شما را به‌طور مستقیم به همکاری بر روی اسناد رهنمون می‌شود. برای بسیاری از کاربران، این یکی از مهم‌ترین مزایای استفاده از رایانش ابری محسوب می‌شود؛ زیرا چندین کاربر به‌طور هم‌زمان می‌توانند بر روی اسناد و پروژه‌ها کار کنند، به‌دلیل اینکه اسناد بر روی ابر میزبانی می‌شوند، نه بر روی رایانه‌های منفرد؛ تمام چیزی که شما نیاز دارید یک رایانه با قابلیت دسترسی به شبکه است.

۸- مستقل از سخت‌افزار

در اینجا به آخرین و بهترین مزیت رایانش ابری اشاره می‌کنیم. شما دیگر مجبور نیستید به یک شبکه یا یک

رایانه خاص محدود باشید. کافی است رایانهٔ خود را تغییر دهید تا ببینید برنامه‌های کاربردی و اسناد شما کماکان و به همان شکل قبلی، بر روی ابر در اختیار شما هستند. حتی دیگر نیازی به خرید یک نسخه خاص از یک برنامه برای یک وسیله خاص، یا ذخیره کردن اسناد با یک شکل مبتنی بر یک ابزار ویژه ندارید. فرقی نمی‌کند که شما از چه نوع سخت‌افزاری استفاده می‌کنید؛ زیرا اسناد و برنامه‌های کاربردی شما در همه حال به یک شکل هستند که مصداق موارد دسترسی همیشگی به اسناد در هر زمان و مکان با هر وسیله‌ای است.

نقاط ضعف رایانش ابری

رایانش ابری نیز مانند هر فناوری نوپا، دارای نقاط ضعفی است که ممکن است با استناد به آنها شما نخواهید از رایانش ابری استفاده کنید. در اینجا به نقطه ضعف‌های رایانش ابری اشاره می‌کنیم:

۱) نیاز به اتصال دائمی به بستر ارتباطی

درصورتی‌که شما نتوانید به اینترنت متصل شوید، رایانش ابری غیرممکن خواهد بود. از آنجایی که شما باید برای ارتباط با برنامه‌های کاربردی و اسناد خود به اینترنت متصل باشید، اگر یک ارتباط اینترنتی نداشته باشید نمی‌توانید به هیچ چیزی، حتی اسناد خودتان دسترسی پیدا کنید. نبود یک ارتباط اینترنتی، به معنای نبود کار است. وقتی شما آفلاین هستید، رایانش ابری کار نمی‌کند.

۲) عملکرد ضعیف با بستر کم سرعت

به همان شکلی که در بالا اشاره شد، یک ارتباط اینترنتی کم سرعت نظیر نمونه‌ای که در سرویس‌های Dial-up دیده می‌شود در بهترین حالت، استفاده از رایانش ابری را با دردسرهای زیادی همراه می‌کند و اغلب وقت‌ها، استفاده از آن را غیرممکن می‌سازد. برنامه‌های کاربردی تحت وب و همچنین اسنادی که بر روی ابر ذخیره شده‌اند برای دانلود شدن به پهنای باند بسیار زیادی نیاز دارند. اگر شما از یک اینترنت Dial-up استفاده می‌کنید اعمال تغییر در یک سند یا رفتن از یک صفحه به صفحهٔ دیگر همان سند، ممکن است برای همیشه به طول بیانجامد؛ و البته در مورد بار شدن یک سرویس غنی از امکانات حرفی نمی‌زنیم. به‌عبارت دیگر، رایانش ابری برای افرادی که از بستر مناسب (باند پهن) استفاده نمی‌کنند، نیست.

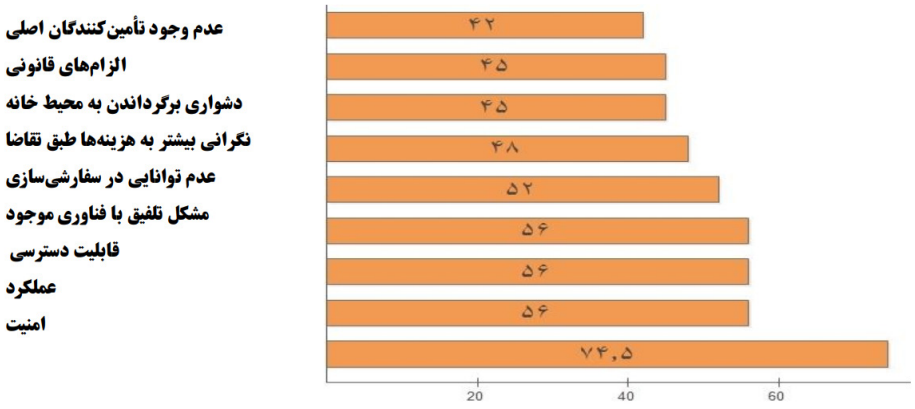
۳) امنیت

با استفاده از رایانش ابری، تمام داده‌های شما بر روی ابر ذخیره می‌شوند؛ اما این سؤالها مطرح می‌شود که مکان و تعیین نحوهٔ دسترسی به این داده‌ها تا چه حد قابل اطمینان و ایمن هست؟ آیا کاربران غیرمجاز می‌توانند به داده‌های مهم و محرمانهٔ ذخیره شده در ابر دسترسی پیدا کنند؟ کمپانی رایانش ابری اظهار می‌کند که داده‌ها امن هستند اما هنوز برای اطمینان کامل از این موضوع خیلی زود است. از نظر تئوری، داده‌های ذخیره شده بر روی ابر ایمن هستند و بین چندین ماشین توزیع شده‌اند؛ اما در صورتی که داده‌های

شما مفقود شوند، شما هیچ نسخهٔ پشتیبان فیزیکی یا محلی در اختیار نخواهید داشت (مگر اینکه تمام اسناد ذخیره شده بر روی ابر را بر روی Desktop خود دانلود کنید که کمتر کاربری چنین کاری می کند). به‌سادگی بگوییم، اتکا به ابر، شما را در معرض خطر قرار می‌دهد. مبنای وضع قواعد و هنجارهای عمومی در فناوری اطلاعات و ارتباطات، امنیت آن است. به بیان دیگر، حقوق فناوری اطلاعات و ارتباطات، بر امنیت استوار است و ارکان امنیت، ارکان نظام حقوقی این حوزه را تشکیل می‌دهند. به‌طور کلی امنیت اطلاعات بر سه شاخهٔ دسترس‌پذیری، صحت و تمامیت و محرمانگی استوار است. همین ارکان می‌توانند مبنای وضع قواعد حقوقی، قانونی و مقرراتی این حوزه قرار گیرد و به‌ویژه هم‌آوردسازی قواعد دسترس‌پذیری و محرمانگی و تعدیل و توازن آنها با یکدیگر، پویایی و همچنین امنیت پایدار این حوزه را رقم بزنند. این موضوع به‌ویژه از آن جهت اهمیت دارد که قواعد دسترس‌پذیری و محرمانگی در برابر یکدیگر قرار می گیرند و چنانچه احکام آنها به‌طور شفاف و مشخص تعریف نشود، خود بر ناامنی این حوزه دامن خواهد زد (احمدی، ۱۳۹۳)

تهدیدهای فراروی رایانش ابری

به‌دلیل فراهم آوردن امکانات مختلف برای سازمان‌ها، رایانش ابری در آیندهای متصل به حال، دارای یک رشد سریع خواهد بود؛ و اکثر سازمان‌ها ناچار به استفاده از خدمات ارائه شده در ابر در غالب سرویس‌های ابری می‌باشند؛ اما در این بین تهدید اصلی، بحث امنیت در محیط ابری است که ممکن است سبب تردید در مهاجرت به ابر گردد. نتایج حاصل از تحقیق و نظرسنجی شرکت IDC[1] از ۲۴۴ مدیر فناوری اطلاعات مطابق با شکل ۲ است که نشان می‌دهد در بین ۹ تهدید اساسی مطرح در حوزهٔ رایانش ابری، امنیت بزرگ‌ترین تهدید است و با کسب ۷۴/۵ درصد در مقام نخست دغدغه‌های ابری قرار (Velte,2010).



شکل ۲– تهدیدهای اصلی رایانش ابری (Velte, 2010)

1. International Data Corporation

از منظر حقوقی و قواعد جاری در شوراهای فناوری اطلاعات و ارتباطات، ابر دارای تهدیدهایی است. در جدول ۳ ضمن بررسی این تهدیدها، در مورد وضعیت این تهدیدها در جوامع اطلاعاتی پرداخته می‌شود. به‌دلیل اختصاصی بودن محیط و زیرساخت‌ها، ممکن است بعضی از این تهدیدها در ابر خصوصی مصداق نداشته باشند.

جدول ۳ – تهدیدهای رایانش ابری و آثار آن در جوامع اطلاعاتی (لرستانی، ۱۳۹۵، ۴۰)

شرح تهدید	توصیف در جوامع اطلاعاتی
چندکاربره و اشتراک منابع	این حالت زمانی رخ می‌دهد که اطلاعات هم‌ٔردهها در یک مکان واحد ذخیره گردند و اگر جداسازی منطقی انجام نگیرد ممکن است اطلاعات یک کاربر در اطلاعات دیگری نشت کند. این مشکل نیازمند اتخاذ تدابیری سخت‌گیرانه برای اعمال در محل ذخیره داده‌ها می‌باشد.
محل قرارگیری داده‌ها	این تهدید در حالت‌هایی برقرار است که مشتریان از خدمات ابری بین‌المللی استفاده نمایند. در مواردی که ابر خصوصی استفاده گردد مطرح نیست اما می‌توان گفت بنا بر طبقه‌بندی و ارزش اطلاعات، تنها اطلاعاتی در ابر مستقر گردند که اکنون در سامانه‌های ارتباطی جاری می‌باشند (بنا بر تشخیص مدیران تا سطح خیلی محرمانه در شبکه قرار دارد و بالاتر ممنوع است).
حریم خصوصی و محافظت از داده‌ها	در مواردی که داده‌ها دارای طبقه‌بندی می‌باشند باید ضوابطی برای حفظ محرمانگی آنها در نظر گرفته شود. هرچند نقض حریم خصوصی ممکن است در هر سامانه‌ای غیر از سامانه‌های رایانش ابری رخ دهد.
شفافیت	با توجه به مفهوم شفافیت در فناوری اطلاعات، این مورد به‌خوبی در ابرهای اختصاصی ارائه می‌گردد.
فرآیند حذف داده‌ها	حذف داده‌ها درصورتی‌که با توافق باشد رخ می‌دهد و حتی این داده‌ها از سرور پشتیبان نیز باید حذف گردند.
از دست دادن داده‌ها	در زمان انتقال به ابر ممکن است از دست رفتن داده‌ها رخ دهد، در این حالت لازم است سازوکار به نحوی اندیشیده شود تا اطمینان حاصل گردد که اطلاعات به‌طور کامل منتقل گردند و تدابیری همچون پشتیبانگیری لحظه‌ای هم قادر است گره‌گشای کار باشد.
محدود شدن به یک فراهم کننده (انحصار شرکتی)	این محدودیت با توجه به مستقل عمل نمودن جوامع اطلاعاتی و دارا بود تشکیلات فناوری اطلاعات و الزام به تربیت نیروی بومی تا حد زیادی مرتبط نمی‌باشد.

یافته‌های پژوهش

تجزیه و تحلیل توصیفی و استنباطی سؤالات پرسشنامه:

در جداول ۱،۲ و ۳ با استفاده از داده‌های حاصل از پرسش‌نامه و نظرات صاحب نظران، آمار توصیفی

(میانگین، انحراف معیار، ماکزیمم و مینیمم) و آمار استنباطی اولیه (مقدار خی دو به همراه درجه آزادی) آورده شده است. شرح سؤالات پرسشنامه‌ها به علت محدودیت فضا، در این جداول آورده نشده و فقط شماره سؤالات در پرسشنامه درج گردیده و برای اطلاع از شرح سؤالات پرسشنامه‌ها بایستی به جداول ۸، ۹ و ۱۰ مراجعه شود.

جدول ۴– تحلیل اولیه داده‌های پرسشنامه فرضیه اول (چالش‌های به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی)

ردیف	شماره سؤالات در پرسشنامه	میانگین	انحراف معیار	ماکزیمم	مینیمم	دیدگاه خبرگان (درجات ارزیابی (درصد))					Chi-square آزمون خی دو	
						خیلی زیاد	زیاد	متوسط	کم	خیلی کم	مقدار	درجه آزادی
۱	۱	۳,۹۷	۱,۳۲۹	۵	۱	٤٥	۳۶	۲	۵	۱۲	۷٤,۷	٤
۲	۲	٤,۰۶	۰,۹۳	۵	۲	٤۱	۲۹	۲۵	۵	۰	۲۶,۸۸	۳
۳	۳	٤,۲۷	۰,۹۳	۵	۲	٤۹	٤۰	۰	۱۱	۰	۲۳,۶۶	۲
٤	٤	٤,۳۵	۰,۸۹۲	۵	۱	۵٤	۳۳	۱۰	۰	۳	۶٤,۵۶	۳
۵	۵	۳,۵۵	۰,۸۹۲	۵	۱	۱۱	٤۶	۳۳	۷	۳	۶۹,۲	٤
۶	۶	۳,۵۹	۱,۰۳۶	۵	۲	۵۶	۲۲	۱۳	۵	٤	۲۱,۱٤	۳
۷	۷	۳,۶۲	۰,۸۲۶	۵	۲	۱٤	٤۲	۳۶	۸	۰	۳۲,۸	۳
۸	۸	٤,٤	۰,۷۲۵	۵	۲	۵۲	۳۸	۸	۲	۰	۶۸,۶٤	۳
۹	۹	٤,۰٤	۰,۷۵۱	۵	۲	۲۸	۵۰	۲۰	۲	۰	٤۷,۵۲	۳
۱۰	۱۰	٤,۲۲	۰,۹۳۸	۵	۱	٤۶	۳۸	۱۱	۲	۳	۸٤,۷	٤
۱۱	۱۱	٤,۳۵	۰,۸٤۵	۵	۲	۵۵	۲۹	۱۲	٤	۰	۶۱,۰٤	۳
۱۲	۱۲	٤,۱۲	۰,۹۵۶	۵	۱	۳۸	٤۶	۱۰	۲	٤	۸٤	٤
۱۳	۱۳	۳,۹۶	۰,۹۲	۵	۲	۲۹	٤۹	۱۱	۱۱	۰	۳۹,۳۶	۳
۱٤	۱٤	٤,۰۹	۰,۹۵٤	۵	۱	۳۹	۳۹	۱۷	۲	۳	۶۲,۲	٤
۱۵	۱۵	٤,۳۷	۰,۷۰۶	۵	۳	۵۰	۳۷	۱۳	۰	۰	۲۱,۱٤	۲
۱۶	۱۶	٤,۲۶	۰,۷۳۳	۵	۲	٤۰	٤۹	۸	۳	۰	۶۲,۹۶	۳
۱۷	۱۷	٤,۳۳	۰,۸۸۸	۵	۲	۵۶	۲۶	۱۳	۵	۰	۶۰,۲٤	۳
۱۸	۱۸	٤,۳	۰,۷۸۵	۵	۳	۵۰	۳۰	۲۰	۰	۰	۱٤	۲
۱۹	۱۹	٤,۱۹	۰,۸	۵	۲	٤۰	٤۲	۱۵	۳	۰	٤۳,۹۲	۳
۲۰	۲۰	۳,۹۶	۱,۰٤٤	۵	۱	۳۷	۳۵	۱۷	۹	۲	٤۸,٤	٤

جدول ۵– تحلیل اولیه داده‌های پرسشنامه فرضیه دوم (سازوکارهای مدیریتی به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی)

ردیف	شماره سؤالات در پرسشنامه	میانگین	انحراف معیار	ماکزیمم	مینیمم	دیدگاه خبرگان					Chi-square آزمون خی دو	
						درجات ارزیابی (درصد)						
						خیلی زیاد	زیاد	متوسط	کم	خیلی کم	مقدار	درجه آزادی
۱	۱	٤,٤٤	۰,۷۷	۵	۱	۵٤	٤۱	۲	۱	۲	۱۳۰,۳	٤
۲	۲	٤,۳۱	۰,۷۲	۵	۳	٤۶	۳۹	۱۵	۰	۰	۱۵,۸۶	۲
۳	۳	٤,۲۲	۰,۷٤۶	۵	۲	۳۹	٤۶	۱۳	۲	۰	۵۲,٤	۳
٤	٤	٤,۲۱	۰,۸۰۸	۵	۱	۳۷	۵۳	۶	۲	۲	۱۱۱,۱	٤
۵	۵	٤,۲	۰,۷۹۱	۵	۱	۳۷	۵۰	۱۱	۰	۲	۵۹,۷۶	۳
۶	۶	٤,۱۲	۰,۸۶۸	۵	۱	۳۸	٤۰	۲۰	۰	۲	۳۷,۹۲	۳
۷	۷	٤,۳۶	۰,۸۳۵	۵	۱	۵۳	۳٤	۱۱	۰	۲	۶۳,۶	۳
۸	۸	٤,۳٤	۰,۸۵۵	۵	۲	۵٤	۳۱	۱۰	۵	۰	۶۰,۰۸	۳
۹	۹	٤,۳۲	۰,۹٤۲	۵	۱	۵۳	۳۶	۳	۶	۲	۱۰۷,۷	٤
۱۰	۱۰	٤,۵	۰,۸٤۷	۵	۱	۶٤	۲۹	۲	۳	۲	۱٤۷,۷	٤
۱۱	۱۱	٤,٤	۰,۹۲۱	۵	۱	۵۹	۳۱	۳	۵	۲	۱۲٤	٤
۱۲	۱۲	٤,۱۳	۰,۹۶	۵	۱	٤۷	۲۳	۲۸	۰	۲	٤۱,۰٤	۳
۱۳	۱۳	٤,۱۹	۰,۷۶۱	۵	۲	۳۸	٤۵	۱۵	۲	۰	٤۷,۹۲	۳
۱٤	۱٤	٤,۵۵	۰,۷۳	۵	۲	۶۷	۲۳	۸	۲	۰	۱۰۳,٤٤	۳
۱۵	۱۵	٤,۵	۰,۸۲۳	۵	۲	۶۶	۲۳	۶	۵	۰	۹۷,۸٤	۳
۱۶	۱۶	٤,۰٤	۰,۹۰۹	۵	۲	۳۶	۳۹	۱۸	۷	۰	۲۷,۶	۳
۱۷	۱۷	٤,۰۳	۰,۸۸۱	۵	۲	۳۵	۳۸	۲۲	۵	۰	۲۷,۱۲	۳
۱۸	۱۸	٤,٤۷	۰,۷۱۷	۵	۳	۶۰	۲۷	۱۳	۰	۰	۳٤,۹٤	۲

جدول ۶– تحلیل اولیه داده‌های پرسشنامه فرضیه دوم (سازوکارهای فناورانه به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی)

ردیف	شماره سؤالات در پرسشنامه	میانگین	انحراف معیار	ماکزیمم	مینیمم	دیدگاه خبرگان					Chi-square آزمون خی دو	
						درجات ارزیابی (درصد)						
						خیلی زیاد	زیاد	متوسط	کم	خیلی کم	مقدار	درجه آزادی
۱	۱	٤,۶۱	۰,۶۸	۵	۲	۶۹	۲۶	۲	۳	۰	۱۱۸	۳

ردیف	شماره سؤالات در پرسشنامه	میانگین	انحراف معیار	ماکزیمم	مینیمم	دیدگاه خبرگان (درجات ارزیابی (درصد))					Chi-square آزمون خی دو	
						خیلی زیاد	زیاد	متوسط	کم	خیلی کم	مقدار	درجه آزادی
۲	۲	٤,۰۹	۰,۷۸۰	۵	۲	۳۳	٤۵	۲۰	۲	۰	٤۰,۷۲۰	۳
۳	۳	٤,۲۲	۰,۸۱۱	۵	۲	٤۳	۳۹	۱۵	۳	۰	٤٤,۱۶	۳
٤	٤	٤,۵۵	۰,۵۷۵	۵	۳	۵۹	۳۷	٤	۰	۰	٤۵,۹۸	۲
۵	۵	٤,۱۱	۰,۹٤۲	۵	۲	۳۹	٤٤	۶	۱۱	۰	٤٤,۵۶۰	۳
۶	۶	٤,۳۳	۰,۹۲۲	۵	۱	۵۵	۲۹	۱۳	۰	۳	۶۱,۷۶۰	۳
۷	۷	٤,۳۵	۰,۸۰۹	۵	۲	۵۲	۳۵	۹	٤	۰	۶۱,۰٤	۳
۸	۸	٤,۵۱	۰,۶۸۹	۵	۲	۵۹	۳۶	۲	۳	۰	۹۱,۶	۳
۹	۹	٤,۳۵	۰,۶۰۹	۵	۳	٤۲	۵۱	۷	۰	۰	۳۲,٤۲	۲
۱۰	۱۰	٤,۱۹	۰,۸۲۵	۵	۲	٤۰	٤٤	۱۱	۵	۰	٤۷,۲۸	۳
۱۱	۱۱	٤,۳۲	۰,۷۰۹	۵	۳	٤۶	٤۰	۱٤	۰	۰	۱۷,۳۶۰	۲
۱۲	۱۲	٤,۳	۰,۸۸۲	۵	۲	۵۰	۳۸	٤	۸	۰	۶۰,۹۶	۳
۱۳	۱۳	٤,٤۵	۰,۷۹۶	۵	۲	۶۲	۲۳	۱۳	۲	۰	۸۱,۸٤	۳
۱٤	۱٤	٤,۵۳	۰,۶۵۸	۵	۳	۶۲	۲۹	۹	۰	۰	٤۲,۹۸	۲
۱۵	۱۵	٤,۵٤	۰,۷٤٤	۵	۲	۶۶	۲۵	۶	۳	۰	۱۰۱,۰٤	۳
۱۶	۱۶	٤,۵۷	۰,۸۳۲	۵	۱	۷۰	۲۳	٤	۰	۳	۱۱۸,۱۶۰	۳
۱۷	۱۷	٤,٤۵	۰,۷۸۳	۵	۲	۶۱	۲۵	۱۲	۲	۰	۷۹,۷۶	۳
۱۸	۱۸	٤,۵٤	۰,۷۱۷	۵	۲	۶۵	۲۶	۷	۲	۰	۹۸,۱۶	۳

داده‌های سه جدول بالا حاکی از آن است که ارزش خی‌دوی مشاهده‌شده در درجه آزادی مربوطه، معنی‌دار است. در نتیجه تفاوت بین فراوانی‌های مشاهده‌شده تأیید می‌شود. روایی پرسشنامه صوری و با تأئید خبرگان حوزه پژوهش تحصیل شد و پایایی پرسشنامه بر اساس آلفای کرونباخ محاسبه شد و ضریب آلفای کرونباخ، مقدار ۰/۹۰۹ را به خود اختصاص داد که بسیار مطلوب است.

تجزیه و تحلیل استنباطی فرضیه‌ها:

در این قسمت فرضیه‌های پژوهشی به‌ترتیب مورد تجزیه و تحلیل توصیفی و استنباطی قرار می‌گیرد. به این منظور برای هر کدام از فرضیه‌ها پس از تبدیل فرضیه پژوهشی به فرضیه آماری، فرضیه با استفاده از آزمون خی دو مورد تجزیه و تحلیل قرار گرفته و در نهایت به رتبه‌بندی عوامل مؤثر فرضیه با استفاده از آزمون فریدمن پرداخته شده است.

جدول ۷– تحلیل اولیه داده‌های فرضیه‌ها

ردیف	عنوان فرضیه	Chi-square آزمون خی دو	Chi-square آزمون فریدمن	میانگین رتبه‌های فریدمن
		درجه آزادی	درجه آزادی	
۱	مهم‌ترین چالش‌های به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی عبارتند از ۱- هزینه‌های بالا برای ایجاد و تأمین امنیت فناوری رایانش ابری در سازمان‌های امنیتی...، ۲۰- پایین بودن تحمل‌پذیری خطا در فناوری رایانش ابری	۶۸,۷۸۰	۲۰۱,۹۸٤	۱,۶۲
		۲	۱۹	
۲	سازوکارهای مدیریتی به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی عبارتند از ۱- افزایش دانش و آگاهی تصمیم‌سازان و تصمیم‌گیران سازمان...، ۱۸- بررسی رویکرد سازمان‌های اطلاعاتی- امنیتی حریف در حوزه به‌کارگیری فناوری رایانش ابری.	۶۸,۵۶۰	۱۲۹,۹۱۲	۲,۰۹
		۳	۱۷	
۳	سازوکارهای فناورانه در به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی عبارتند ۱- تأمین زیرساخت‌ها، سامانه‌های امنیتی، سامانه‌های کنترلی و ... برای پیاده‌سازی و امن‌سازی فناوری رایانش ابری در سازمان‌های امنیتی...، ۱۸- تدوین و اجرای روش‌های تهیه نسخه پشتیبان از اطلاعات و آزمایش صحت آن.	۶۸,۵۶۰	۱۵۰,۶۹۳	۲,۳۰
		۳	۱۷	

با توجه به اینکه در هر مورد، ارزش خی دوی مشاهده شده در درجه آزادی مربوطه معنی‌دار است، در نتیجه استنباط می‌شود که بین فراوانی‌های مشاهده شده تفاوت معنی‌داری وجود دارد، یعنی فرضیه مربوطه پذیرفته می‌شود و فرضیه مقابل آن رد می‌گردد. با توجه به اینکه در هر مورد، داده‌های جدول آزمون فریدمن نیز نشان می‌دهد که ارزش خی دوی مشاهده شده در درجه آزادی مربوطه معنی‌دار است، در نتیجه استنباط می‌شود که تفاوت بین میانگین‌های رتبه‌ای متغیرهای مربوطه در هر مورد معنی‌دار است.

تجزیه و تحلیل فرضیه اصلی:

با توجه به تأئید فرضیه‌های فرعی نتیجه می‌گیریم که فرضیه اصلی تأئید و مورد پذیرش قرار می‌گیرد یعنی اینکه "سازوکارهای مدیریتی و فناورانه، می‌توانند در به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی مؤثر واقع گردند". با محاسبه میانگین رتبه‌های فریدمن نیز مشخص شد که ترتیب تأثیر فرضیه‌های فرعی بر موضوع پژوهش بدین صورت است که فرضیه سوم با نمره میانگین ۲/۳۰ در رتبه اول و سپس فرضیه دوم و اول به ترتیب با نمره میانگین ۲/۰۹ و ۱/۶۲ در رتبه‌های بعدی قرار دارند.

جدول ۸– ترتیب و توالی شاخص‌های اثرگذار در فرضیه فرعی اول از دیدگاه جامعه آماری

ردیف	شماره سؤالات در پرسشنامه	سؤالات پرسشنامه	میانگین	میانگین رتبه‌های فریدمن
۱	۱۱	هزینه‌های بالا برای ایجاد و تأمین امنیت فناوری رایانش ابری در سازمان‌های امنیتی به دلیل ماهیت ویژه مأموریت و اطلاعات این سازمان‌ها.	٤,۳۵	۱۲,۲۲
۲	۸	عدم آشنایی و اعتقاد مدیران ارشد سازمانی به جایگاه راهبردی و اثرگذار فناوری رایانش ابری.	٤,٤۰	۱۲,۲۱
۳	۱۷	نبود/ کمبود سامانه‌های امنیت و کنترل امنیت بومی در حوزه فاوا.	٤,۳۳	۱۲,۲۰
٤	۱۵	مغایرت با اسناد بالادستی در حوزه نیروهای مسلح و سازمان‌های امنیتی برای به‌کارگیری فناوری رایانش ابری.	٤,۳۷	۱۲,۱۷
۵	٤	احتمال سوءاستفاده شرکت‌های ارائه‌دهنده فناوری رایانش ابری از اطلاعات سازمانی.	٤,۳۵	۱۲,۱۰
۶	۳	نداشتن اطمینان از حفظ حریم خصوصی، صحت و محرمانگی داده‌ها و محاسبات.	٤,۲۷	۱۱,۹۳
۷	۱۸	نبود آزمایشگاه‌های مرجع به‌منظور ارزیابی امنیتی سامانه‌های سخت‌افزاری و نرم‌افزاری در سطح جامعه اطلاعاتی و نیروهای مسلح.	٤,۳۰	۱۱,۹۱
۸	۱۶	نبود استانداردهای حقوقی و قانونی در به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی و نیروهای مسلح.	٤,۲۶	۱۱,۱٤
۹	۱۰	جذاب بودن فناوری رایانش ابری برای مهاجمین و هکرها.	٤,۲۲	۱۱,۱۲
۱۰	۱۹	ضعف در ارزیابی امنیتی زیرساخت‌ها و شبکه‌ها در سطح جامعه اطلاعاتی و نیروهای مسلح.	٤,۱۹	۱۱,۰۱
۱۱	۱	اتصال به اینترنت برای استفاده از ابر عمومی.	۳,۹۷	۱۰,۹۶
۱۲	۱۲	پهنای باند، سرعت تبادل و پردازش بالا برای به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی.	٤,۱۲	۱۰,۶۳
۱۳	۱٤	ضعف آگاهی و دانش کارکنان سازمان‌های امنیتی در مورد فناوری رایانش ابری.	٤,۰۹	۱۰,۲۳
۱٤	۲	عدم اعتماد به شرکت‌های ارائه‌دهنده خدمات فناوری رایانش ابری.	٤,۰۶	۱۰,۱۱
۱۵	۹	وجود ساختار باز و توزیع‌شده در رایانش ابری و خدمات آن.	٤,۰٤	۹,۶۸
۱۶	۲۰	دشواری در ایجاد بسترها و مراکز داده پشتیبان و جایگزین.	۳,۹۶	۹,۶۵
۱۷	۱۳	دشواری در مهاجرت از سامانه‌های کاربردی موجود به سامانه‌های مبتنی بر شبکه (وب بیس).	۳,۹۶	۹,۳٤
۱۸	۶	نداشتن اطمینان از دسترسی دائمی به خدمات ارائه‌شده در فناوری رایانش ابری ناشی از قطع/ اخلال در دسترسی.	۳,۵۹	۷,۳۷
۱۹	۷	ایجاد تعادل و توازن بین مزایای فناوری رایانش ابری و مأموریت‌های امنیتی.	۳,۶۲	۷,۲٤
۲۰	۵	پایین بودن تحمل‌پذیری خطا در فناوری رایانش ابری.	۳,۵۵	۶,۸۱

جدول ۹– ترتیب و توالی شاخص‌های اثرگذار در فرضیه فرعی دوم از دیدگاه جامعه آماری

ردیف	شماره سؤالات در پرسشنامه	سؤالات پرسشنامه	میانگین	میانگین رتبه‌های فریدمن
۱	۱٤	اتخاذ تدابیر لازم برای تست نفوذ و ارزیابی امنیتی زیرساخت‌های فناوری رایانش ابری در سازمان‌های امنیتی.	٤,٥٥	۱۱,٤۱
۲	۱۵	طراحی ساختار سازمانی برای تیم‌های رصد و پایش مستمر و مداوم تهدیدات و آسیب‌پذیری‌های فناوری رایانش ابری در قالب بخش‌های SOC، NOC و Cert به‌منظور واکنش به‌موقع.	٤,۵۰	۱۱,۱۷
۳	۱۰	ایجاد ساختار و جذب نیروی انسانی متخصص برای راه‌اندازی، توسعه، پشتیبانی، امنیت و کنترل امنیت فناوری رایانش ابری در سازمان‌های امنیتی.	٤,۵۰	۱۰,۸۲
٤	۱۸	بررسی رویکرد سازمان‌های اطلاعاتی- امنیتی حریف در حوزه به‌کارگیری فناوری رایانش ابری.	٤,٤۷	۱۰,۷۶
۵	۱	افزایش دانش و آگاهی تصمیم‌سازان و تصمیم‌گیران سازمان در خصوص مزایا و چالش‌های به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی.	٤,٤٤	۱۰,٤۷
۶	۱۱	اعزام کارکنان فاوای سازمان‌های امنیتی به دوره‌های تخصصی در خصوص فناوری رایانش ابری.	٤,٤۰	۱۰,۲۷
۷	۸	تدوین آیین‌نامه‌ها، شیوه‌نامه‌های، الگوهای امنیت و کنترل امنیت مربوط به پیاده‌سازی فناوری رایانش ابری در سازمان‌های امنیتی.	٤,۳٤	۱۰,۰۹
۸	۷	بازنگری در اسناد بالادستی موجود (آیین‌نامه‌ها و شیوه‌نامه‌ها) پیرامون به‌کارگیری فناوری‌های نوین نظیر رایانش ابری در سازمان‌های امنیتی از سوی مراجع ذی‌صلاح.	٤,۳۶	۹,۸۲
۹	۲	درک خطرات امنیتی در به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی.	٤,۳۱	۹,۷٤
۱۰	۹	تأمین اعتبارات مالی موردنیاز برای راه‌اندازی، توسعه، پشتیبانی و امن‌سازی فناوری رایانش ابری سازمان‌های امنیتی.	٤,۳۲	۹,۶۹
۱۱	۳	تبیین حفظ حریم خصوصی در به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی.	٤,۲۲	۸,۸٤
۱۲	٤	تبیین ارائه خدمات فناوری رایانش ابری به‌صورت منعطف.	٤,۲۱	۸,۸۳
۱۳	۵	افزایش حمایت‌های مسئولین سازمان در خصوص به‌کارگیری فناوری رایانش ابری.	٤,۲۰	۸,۶۸
۱٤	۱۳	اتخاذ تدابیر لازم برای فرهنگ‌سازی استفاده از فناوری رایانش ابری در سازمان‌های امنیتی.	٤,۱۹	۸,٤٤
۱۵	۶	نیازسنجی پیرامون یکپارچه‌سازی شبکه‌ها، سامانه‌های کاربردی و بانک‌های اطلاعاتی برای تسریع و تسهیل در اجرای مأموریت‌ها؛ در سازمان‌های امنیتی.	٤,۱۲	۸,۳۱
۱۶	۱۲	آگاه‌سازی فنی و طراحی دوره‌های آموزشی کوتاه‌مدت و بلندمدت برای ارتقاء دانش و آگاهی کاربران سازمان پیرامون فناوری‌های نوین نظیر رایانش ابری.	٤,۱۳	۸,۲۶
۱۷	۱۶	اطلاع‌رسانی مستمر پیرامون سیاست‌های امنیتی که بایستی توسط کاربران مراعات گردد و برخورد قانونی با تخلفات و شکست‌های احتمالی.	٤,۰٤	۷,۷۶
۱۸	۱۷	بررسی تجارب و اقدامات اعضاء جامعه اطلاعاتی و نیروهای مسلح در به‌کارگیری فناوری رایانش ابری.	٤,۰۳	۷,۶۶

جدول ۱۰– ترتیب و توالی شاخص‌های اثرگذار در فرضیه فرعی سوم از دیدگاه جامعه آماری

ردیف	شماره سؤالات در پرسشنامه	سؤالات پرسشنامه	میانگین	میانگین رتبه‌های فریدمن
۱	۱	تأمین زیرساخت‌ها، سامانه‌های امنیتی، سامانه‌های کنترلی و ... برای پیاده‌سازی و امن‌سازی فناوری رایانش ابری در سازمان‌های امنیتی	٤,٦١	۱۱,۱۱
۲	۱۶	پیش‌بینی مرکز/ مراکز داده (دیتاسنتر) و زیرساخت‌های جایگزین برای پایداری شبکه در شرایط بحرانی.	٤,٥٧	۱۰,۹۲
۳	۱۸	تدوین و اجرای روش‌های تهیه نسخه پشتیبان از اطلاعات و آزمایش صحت آن.	٤,٥٤	۱۰,٥۸
٤	۱۵	راه‌اندازی سامانه‌های کنترلی و مانیتورینگ شامل کنترل امنیت، کنترل ترافیک و NOC.	٤,٥٤	۱۰,٥۷
٥	٤	تشکیل تیم‌های کاری طراحی، اجرا، پشتیبانی و رفع اشکال، رصد، پایش و واکنش به تهدیدات احصاءِ شده، تست نفوذ و ارزیابی امنیتی، ارائه گزارش کار به مسئولین سازمان و	٤,٥٥	۱۰,٥٥
۶	۱٤	ایجاد تیم‌های رصد مستمر و مداوم تهدیدات و آسیب‌های رایانش ابری در قالب بخش‌های SOC و Cert به‌منظور واکنش به‌موقع.	٤,٥۳	۱۰,٤۷
۷	۸	پیاده‌سازی مدل ابرِ خصوصی در به‌کارگیری فناوری رایانش ابری.	٤,٥۱	۱۰,۳۷
۸	۱۳	تدبیر و اجرای سازوکارهای امنیتی متناسب با سطوح زیرساخت، شبکه، سرور، سامانه‌های کاربردی و کاربران.	٤,٤٥	۱۰,۱٥
۹	۱۷	ارزیابی امنیتی مستمر زیرساخت‌ها، شبکه‌ها و سامانه‌های کاربردی و ارائه گزارش به مسئولین سازمان‌های امنیتی.	٤,٤٥	۹,۸۷
۱۰	۷	تعیین مدل مفهومی برای معماری و پیاده‌سازی امن فناوری رایانش ابری و بومی‌سازی آن متناسب با کارویژه‌ها و اطلاعات سازمان‌های امنیتی.	٤,۳٥	۹,۱۹
۱۱	۶	دریافت مشاوره از شرکت‌ها و مراکز علمی- دانشگاهی فعال در حوزه فناوری رایانش ابری.	٤,۳۳	۹,۱٥
۱۲	۱۲	اجرای آزمایشی به‌کارگیری فناوری رایانش ابری در قسمت‌های با حساسیت پایین‌تر در سازمان‌های امنیتی.	٤,۳۰	۹,۰۹
۱۳	۹	استفاده از مجازی‌سازی در پیاده‌سازی فناوری رایانش ابری.	٤,۳٥	۹,۰٤
۱٤	۱۱	مهاجرت از سامانه‌های کاربردی فعلی به سامانه‌های مبتنی بر شبکه (وب بیس).	٤,۳۲	۸,۸۷
۱٥	۳	برنامه‌ریزی، اولویت‌بندی و زمان‌بندی مراحل پیاده‌سازی فناوری رایانش ابری.	٤,۲۲	۸,۱٥
۱۶	۱۰	استفاده از پراکسی‌ها در پیاده‌سازی فناوری رایانش ابری.	٤,۱۹	۸,۰۶
۱۷	٥	هم‌افزایی تخصصی فی‌مابین اعضاءِ جامعه اطلاعاتی برای به‌کارگیری فناوری رایانش ابری.	٤,۱۱	۷,٤۳
۱۸	۲	شناسایی شرکت‌های داخلی و خارجی ارائه‌دهنده خدمات فناوری رایانش ابری.	٤,۰۹	۷,٤۲

نتیجه‌گیری

بررسی‌های انجام شده نشان داد که به سه علت عمده ۱- مزیت‌های استفاده از رایانش ابری و ۲- جبر ناشی از محدودیت‌های پیشرفت تکنولوژی (سخت‌افزاری و نرم‌افزاری) و ۳- جلوگیری از عقب افتادگی ناشی از عدم استفاده از تکنولوژی، استفاده از فناوری رایانش ابری در آیندهٔ نزدیک، همه‌گیر خواهد شد. از این رو، در این تحقیق برای تعیین " سازوکارهای به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی"، ابتدا چالش‌های بکارگیری فناوری رایانش ابری (۲۰ مؤلفه) استخراج شدند و در ادامه، سازوکارهای بکارگیری فناوری رایانش ابری نیز در دو دسته ۱- سازوکارهای مدیریتی (۱۸ مؤلفه) و ۲- سازوکارهای فناورانه (۱۸ مؤلفه) مطرح و مورد بررسی قرار گرفتند.

تجزیه و تحلیل فرضیه‌ها با استفاده از آزمون خی‌دو نشان داد که بین فراوانی‌های مشاهده‌شده برای مؤلفه‌های هر سه حوزه مذکور، تفاوت معنی‌داری وجود دارد و می‌توان گفت مؤلفه‌های مطرح شده برای هر حوزه ایفای نقش می‌کنند. رتبه‌بندی عوامل مؤثر بر فرضیه‌ها با استفاده از آزمون فریدمن نیز نشان داد که تفاوت بین میانگین‌های رتبه‌ای مؤلفه‌های هر حوزه معنی‌دار است. میانگین رتبه‌های آزمون فریدمن که ترتیب و توالی اهمیت مؤلفه‌های اثرگذار در فرضیه‌ها را از دیدگاه جامعه آماری مشخص می‌کند، نشان داد که:

۱) از میان مؤلفه‌های مربوط به چالش‌های به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی (۲۰ مؤلفه)، سه مؤلفهٔ زیر به ترتیب بالاترین رتبه‌ها را به خود اختصاص داده‌اند:

۱- هزینه‌های بالا برای ایجاد و تأمین امنیت فناوری رایانش ابری در سازمان‌های امنیتی به دلیل ماهیت ویژه مأموریت و اطلاعات این سازمان‌ها (با میانگین رتبه‌ای فریدمن ۱۲/۲۲)

۲- عدم آشنایی و اعتقاد مدیران ارشد سازمانی به جایگاه راهبردی و اثرگذار فناوری رایانش ابری (با میانگین رتبه‌ای فریدمن ۱۲/۲۱).

۳- نبود/کمبود سامانه‌های امنیت و کنترل امنیت بومی در حوزه فاوا (با میانگین رتبه‌ای فریدمن ۱۲/۲۰).

۲) از میان مؤلفه‌های مربوط به سازوکارهای مدیریتی به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی (۱۸ مؤلفه)، سه مؤلفهٔ زیر به ترتیب بالاترین رتبه‌ها را به خود اختصاص داده‌اند:

۱- اتخاذ تدابیر لازم برای تست نفوذ و ارزیابی امنیتی زیرساخت‌های فناوری رایانش ابری در سازمان‌های امنیتی (با میانگین رتبه‌ای فریدمن ۱۱/۴۱).

۲- طراحی ساختار سازمانی برای تیم‌های رصد و پایش مستمر و مداوم تهدیدات و آسیب‌های فناوری رایانش ابری در قالب بخش‌های SOC، NOC و Cert به‌منظور واکنش به‌موقع (با میانگین رتبه‌ای فریدمن ۱۱/۱۷).

۳- ایجاد ساختار و جذب نیروی انسانی متخصص برای راه‌اندازی، توسعه، پشتیبانی، امنیت و کنترل امنیت فناوری رایانش ابری در سازمان‌های امنیتی (با میانگین رتبه‌ای فریدمن ۱۰/۸۲).

۳) از میان مؤلفه‌های مربوط به سازوکارهای فناورانه به‌کارگیری فناوری رایانش ابری در سازمان‌های امنیتی (۱۸ مؤلفه)، سه مؤلفهٔ زیر به ترتیب بالاترین رتبه‌ها را به خود اختصاص داده‌اند:

۱- تأمین زیرساخت‌ها، سامانه‌های امنیتی، سامانه‌های کنترلی و ... برای پیاده‌سازی و امن‌سازی فناوری رایانش ابری در سازمان‌های امنیتی (با میانگین رتبه‌ای فریدمن ۱۱/۱۱).

۲- پیش‌بینی مرکز/ مراکز داده (دیتاسنتر) و زیرساخت‌های جایگزین برای پایداری شبکه در شرایط بحرانی (با میانگین رتبه‌ای فریدمن ۱۰/۹۲).

۳- تدوین و اجرای روش‌های تهیه نسخه پشتیبان از اطلاعات و آزمایش صحت آن (با میانگین رتبه‌ای فریدمن ۱۰/۵۸).

منابع:

- سلطانی‌فر، مهدی و زرگر،(۱۴۰۰) **سید محمد، ارزیابی و رتبه‌بندی ریسک‌های امنیتی رایانش‌ابری بر اساس یک رویکرد ترکیبی مبتنی بر مقایسه‌های زوجی**، نشریه پردازش و مدیریت اطلاعات، شماره ۱۰۵، صفحه ۲۷-۵.
- سلیمی، زهرا،(۱۳۹۸) **بررسی و مقایسهٔ معماریهای امنیتی رایانش ابری در راستای ارائه راهکارهایی جهت توسعه سازمان‌های امنیتی**، مجله پژوهش‌های معاصر در علوم و تحقیقات، سال اول، شماره ۸، اسفند.
- بهادر، عیسی و صادقی، آیسا،(۱۳۹۸) **امنیت در رایانش ابری با تکیه بر امنیت شبکه مبتنی بر روش‌های هوشمند**، مطالعات علوم کاربردی در مهندسی، ۵، ۱،، صفحه ۷۴-۶۵.
- شفایی تنکابنی، میرسعید و شیخ، رضا و جلالی، محمد مهدی،(۱۳۹۴) **پیمایشی درباره اولویت‌بندی عوامل مؤثر بر برون‌سپاری فناوری اطلاعات در بستر رایانش ابری، در دانشگاه‌های استان سمنان با بهره‌مندی از روش دیمتل فازی**، مدیریت فناوری اطلاعات، دوره ۷، شماره ۲، صفحه ۳۲۵-۳۴۴.
- نوروزی، یعقوب و حداد اسکویی، علیرضا،(۱۳۹۷) **موانع پیاده‌سازی رایانش ابری (نمونه پژوهشی: پورتال کتابخانه‌های دیجیتالی ایران)**، فصلنامه مطالعات ملی کتابداری و سازماندهی اطلاعات، دوره ۲۹، شماره ۲.
- بزی، حمیدرضا و معینی، علی و حسن‌زاده، علیرضا، (۱۳۹۶) **ارائه معماری ترکیبی برای پشتیبانی پیاده‌سازی رایانش ابری در مراکز آموزش عالی با استفاده از رویکرد فراترکیب، مدیریت فناوری اطلاعات**، دانشکده مدیریت دانشگاه تهران، دوره ۹، شماره ۴، صفحه ۷۲۸ -۷۰۱.
- محمدی، عباس،(۱۳۹۶) **ارائه مدلی امن و مقیاس‌پذیر برای دورکاری کاربران و ذینفعان سازمان بر اساس فناوری رایانش ابری**، نشریه صنعت حمل و نقل دریایی، سال سوم، شماره ۲، ۱۳۹۶.
- ولوی، محمدرضا و محمدرضا موحدی صفت و باقری کوشالشاه، ایمان، **ارائه الگوی راهبردی مهاجرت سازمان‌های دفاعی به محیط رایانش ابری**، فصلنامه مدیریت نظامی، ۱۷ (۶۵)،، صفحه ۱۳۰-۱۰۶.
- دشمن زیاری، اسفندیار، (۱۳۹۵) **شناسایی عوامل موثر بر کاربرد رایانش ابری در دانشگاه‌های دولتی به روش تحلیل عاملی**، فصلنامه علمی-پژوهشی رهیافتی نو در مدیریت آموزشی، سال ۷، شماره ۴، پیاپی ۲۸.
- حیدری دهویی، جلیل و محمدی، نوید و ونکی، امیرسالار و جمالی، محسن،(۱۳۹۶) **ارائه چارچوبی**

به‌منظور انتخاب سامانه مناسب برای پیاده‌سازی رایانش ابری (مورد مطالعه: دانشکدهٔ علوم و فنون نوین دانشگاه تهران)، مدیریت فناوری اطلاعات، دوره ۹، شماره ۴، صفحه ۷۸۶-۷۵۹.

- والمحمدی، چنگیز و مظاهری، مریم السادات،(۱۳۹۶) **تبیین عوامل تأثیرگذار بر تصمیم به استفاده از رایانش ابری در میان کارکنان سازمان صدا و سیما بر مبنای مدل پذیرش فناوری**، فصلنامه مطالعات مدیریت فناوری اطلاعات، ۵، ۱۹، صفحه ۱۰۵-۱۲۴.
- غیاثوند، میلاد و محمدزاده، جواد و ملامطلبی، مهدی،(۱۳۹۷) **مروری بر چالش‌های امنیتی در رایانش ابری (با رویکرد حفظ حریم خصوصی افراد در سازمان و ارائه راهکار)**، فصلنامه مطالعات حفاظت و امنیت انتظامی، سال ۱۳، شماره ۴۰).
- حمدی‌پور، افشین و نجاری، تراب و فرمانلو لیلاب، اکبر،(۱۳۹۷) **تحلیل عوامل اثرگذار بر پذیرش رایانش ابری کتابداران کتابخانه‌های دانشگاه تبریز و علوم پزشکی بر مبنای نظریه اشاعه نوآوری راجرز**، تحقیقات کتابداری و اطلاع رسانی دانشگاهی، دوره ۵۲، شماره ۴، صفحه ۳۹-۵۸.
- فراحی، محمدمهدی و کاردانی ملکی‌نژاد، مونا،(۱۳۹۸) **فناوری رایانش ابری در مدیریت منابع انسانی شرکت‌های کوچک و متوسط-کاربردها، مزیت‌ها و چالش‌ها**، فصلنامه رشد فناوری، سال پانزدهم، شماره ۶۰.
- مرعشی، مژگان و عبدالوند، ندا، (۱۳۹۷) **ارائه یک مدل برای حاکمیت انتقال فناوری رایانش ابری**، فصلنامه رشد فناوری، سال چهاردهم، شماره ۵۵.
- اسمعیلی رنجبر، خاطره و سلاجقه، مژده، (۱۳۹۹) **بررسی و نقش رایانش ابری در شرکت‌های دانش بنیان ایران**، فصلنامه رشد فناوری، سال شانزدهم، شماره ۶۲، بهار.
- حیدری دهویی، جلیل و محمدی، نوید و ونکی، امیرسالار و جمالی، محسن، (۱۳۹۶) **ارائه چارچوبی به‌منظور انتخاب سامانهٔ مناسب برای پیاده‌سازی رایانش ابری (مورد مطالعه: دانشکدهٔ علوم و فنون نوین دانشگاه تهران)**، مدیریت فناوری اطلاعات، دوره ۹، شماره ۴، صفحه ۷۸۶-۷۵۹.
- لرستانی، علیرضا، **رایانش ابری در خدمت سازمان‌های اطلاعاتی، تهدید یا فرصت**،(۱۳۹۵) فصلنامه علمی - ترویجی مطالعات حفاظت و امنیت انتظامی، سال یازدهم، شماره چهلم، پاییز.
- کتایی، محمد و رنجبر نوشری، اعظم، (۱۳۹۵) **ارائه مدل پذیرش رایانش ابری در برون‌سپاری فناوری اطلاعات**، فصلنامه آینده‌پژوهی مدیریت، ۲۷، ۱۰۷، ۱۳۹۵.
- سلطان باغشاهی، سمیه و سلطان باغشاهی، لیلا و خادمزاده، احمد و جبه‌داری، سام، **تحلیل چالش‌های امنیتی و تأثیر آن بر رایانش ابری**، اولین کارگاه ملی رایانش ابری ایران، تهران، ۱۳۹۱.
- یعقوبی، نورمحمد و جعفری، حمیدرضا و شکوهی، جواد، **شناسایی و رتبه‌بندی عوامل ریسک**

رایانش ابری در سازمان‌های دولتی، پژوهش‌نامه پردازش و مدیریت اطلاعات، ۳۰ (۳)،، صفحه ۷۵۹-۷۸۴.

- جعفرنژاد چقوشی، احمد و مجتوبی دلویی، احسان و مختارزاده گروسی، نیما،(۱۳۹۵) **پیش‌بینی انتشار فناوری رایانش ابری در ایران به‌وسیله منحنی‌های رشد و اثرات روند انتشار سایر کشورها**، فصلنامه مدیریت توسعه فناوری، شماره ۴، صفحه ۱۲۵-۹۷، بهار.
- احمدی، محمدرضا و آریانپور، احسان،(۱۳۹۲) **استانداردهای فنی و ابعاد حقوقی رایانش ابری در ایران**، تهران: انتشارات نیاز دانش.
- احمدی، محمدرضا و آریانپور، احسان و ملکی، داود،(۱۳۹۳) **اصول مجازی‌سازی و رایانش ابری**، تهران: انتشارات نیاز دانش.
- سلطان‌باغشاهی، سمیه و سلطان‌باغشاهی، لیلا و خادمزاده، احمد و جبه‌داری، سام، (۱۳۹۱) **تحلیل تهدیدهای امنیتی و تأثیر آن بر رایانش ابری**، نخستین کارگاه ملی رایانش ابری ایران، تهران: دانشگاه امیرکبیر.
- لرستانی، علیرضا و فراهی، احمد،(۱۳۹۴) **مروری بر تهدیدها و آسیب‌پذیری‌های ماشین مجازی در رایانش ابری و راهکارهای مقابله با تهدیدها**، سومین کنگره فناوریهای نوین ایران، تهران.
- نقیان فشارکی، مهدی و تمتاجی، مصطفی و طباطبایی، سید غلامحسن، (۱۳۹۳) **ارائه معماری مرجع امنیتی محیط رایانش ابر خصوصی سازمانی**، فصلنامه علمی- پژوهشی امنیت پژوهی، سال سیزدهم، شماره ۴۷.

- *Mell, P., & Grance, T*(2013). ***The NIST definition of cloud computing***, 2011.
- *Buyya, R., Vecchiola, C., & Selvi, S. T.* **Cloud Computing *Architecture. Mastering Cloud Computing***, *R. Buyya, C. Vecchiola, and ST Selvi, eds., Morgan Kaufmann, Boston, MA.*
- *Avram, M. G*(2014). ***Advantages and challenges of adopting cloud computing from an enterprise perspective***. *Procedia Technology, 12*, 529-534.
- *Wei, L, H.Zhu, Z. Cao, X. Dong, W.Jia, Y.Chen, and A.Vasilakos,*(2013) ***Security and privacy for storage and computation in cloud computing***. *Information Sciences 258: 371-386.*
- *Lian, J. W., Yen, D. C., & Wang, Y. T.*(2014) ***An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital***. *International Journal of Information Management, 34*(1), 28-36.

- *Tabrizchi, H., and M. Kuchaki Rafsanjani*(2020). ***A survey on security challenges in cloud computing***: issues, threats, and solutions. *The Journal of Supercomputing* 79: 9493- 9532.
- *Tadapaneni, N. R*(2020). **Cloud computing Security challenges**. *International journal of Innovations in Engineering research and Technology* 7 (6): 1-5.
- *Rupra, S., and A. Omamo*(2020). ***A Cloud Computing Security Assessment Framework for Small and Medium Enterprises***. *Journal of Information Security. 11*: 201-224, .
- *Almorsy, M., J. Grundy, and I. Muller*(2010). ***An analysis of the cloud computing security problem***. *In Proceedings ofthe APSEC 2010 Cloud Workshop, Sydney, Australia,* 30 November; pp. 1–6.
- *Bhadani.R,*(2014)" *A New Dimension in HRM*: **Cloud Computing**," *International Journal of Business and Management Invention, pp* 13-15.
- *Marston. S, Li. Z, Bandyopadhyay. S, Zhang. J, and Ghalsasi.*(2011) *A*, "**Cloud computing: the business perspective**," *Decision Support Systems, pp.*176–189.
- *Stallings. W*(2007)," **Data and computer communications**," *Pearson/Prentice Hall, pp.* 202-245.
- *Mell. P, and Grance. T,*(2011) *The NIST Definition of Cloud Computing, NIST Special Publication* 800-145*[online], http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.*
- *Ghaffari.K, Soltani Delgosha.M and Abdolvand.N,*(2014) "**Towards cloud computing: *A SWOT analysis on ITS adoption in SMES***," *International Journal of Information Technology Convergence and Services* (IJITCS), *pp.*13-20.
- *Khan.I,*(2015)" ***Why Businesses (SMEs) should adopt Cloud Computing***", *M.S thesis, Facalty of graduate school of Oulu University of Applied Sciences.*
- *Rimal, B. P., Jukan, A., Katsaros, D., and Goeleven,*(2011) *Y.*, ***Architectural requirements for cloud computing systems: an enterprise cloud approach***. *Journal of Grid Computing.9: pp.* 3– 26.
- *Fazli. S, Shirdastian.H and Laroche. M*(2015), "***Effective factors of successful cloud marketing adoption by SMEs: the case of Iran***," *Int. J. Business*

Environment, pp.415-434.

- Cisco,(2016) Cisco Global Cloud Index: **Forecast and Methodology**, 2014–2019. Retrieved 3 9, from: http://www.cisco.com/c/en/us/solutions/collateral/serviceprovid er/global-cloud indexgci/Cloud_Index_White_Paper.pdf.
- Florin OGIGAU-NEAMTIU,"**Cloud Computing Security Issues**", Issue no. 2(5). Huber Thomas Introduction to virtualization Vmware. Norman Wilde and ,Virtualization and Cloud Computing, 2012.
- Velte, Toby, Anthony & Elsenpeter, Robert. **Cloud computing, a practical approach**: McGraw-Hill, Inc, 2010.
- Kotecha S, Bhise M, Chaudhary S.(2011) "**Query Translation for Cloud Database**s". In: International Conference On Current Trends In Technology, Ahmedabad, Gujarat.
- Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez (2013):**An analysis of security issues for cloud computing**: Hashizume et al. Journal of Internet Services and Applications, 4:5.
- Mell, Peter and Grance, Tim.(2011) SP-800- 145: **The NIST definition of cloud computing**. National Institute of Standards and Technology (NIST) Special Publication September.