رایانش ابری[1]، ابزاری برای همکاری در محیط مجازی[2]:
نگرانی کاربران، امنیت اطلاعات و حفظ حریم خصوصی

مهناز قنبرزاده[3]

عاطفه زارعی[4]

تاریخ دریافت: ۹۵/۰۷/۲۶

تاریخ پذیرش: ۹۵/۱۰/۱۴

چکیده

هدف: در این پژوهش، میزان استفاده از رایانش ابری در محیط مجازی، امنیت اطلاعات و حفظ حریم خصوصی در محیط ابری از نظر کاربران موردبررسی قرار گرفته شده است.

روش‌شناسی:روش پژوهشی، پیمایش- توصیفی است و با استفاده از پرسشنامهٔ محقق‌ساخته، دیدگاه و نظرات ٦٧ نفر ازدانشجوی تحصیلات تکمیلی مقطع دکتری علوم پایه پژوهشگاه ملی مهندسی ژنتیک و زیست‌فناوری گردآوری شده است. با استفاده از نرم‌افزار اس.پی.اس.اس. نسخهٔ ۲۲ به سؤالات و آزمون‌های پژوهش پاسخ داده شده است و پاسخ‌ها نیز با آمار توصیفی و استنباطی تجزیه‌وتحلیل شده‌اند.

یافته‌ها: یافته‌ها نشان می‌دهد که وفاداری نسبت به داده‌ها و اطلاعات کاربران از طرف سرویس‌گرها از اهمیت بالایی برخوردار بوده است؛ همچنین سرویس‌گرها، تلاش‌هایی در جهت کاهش نگرانی‌های کاربران خود و جذب اعتماد آن‌ها انجام می‌دهند؛ درصورتی‌که اطلاعات و حفظ حریم خصوصی در محیط ابری، امنیت کمتری دارد.

نتیجه‌گیری: با توجه به نگرانی و دغدغه‌های کاربران در مورد حفظ حریم خصوصی و امنیت اطلاعات نتایج نشان می دهد که کاربران با اطلاعات کم از مزایای این فناوری، استفاده بسیار کمی از خدمات ارائه شده توسط سرویس‌گرهای ابری می کنند.

کلیدواژه‌ها: امنیت اطلاعات، حریم خصوصی، رایانش ابری، محیط مجازی

---

[1] Cloud Computing

[2] Virtual Environment

[3]. دانشجوی دکترای علم اطلاعات و دانش‌شناسی، مدیریت اطلاعات، دانشگاه آزاد اسلامی واحد همدان (نویسنده مسئول) mahnazgh61@gmail.com

[4]. استادیار علم اطلاعات و دانش شناسی، دانشگاه آزاد اسلامی واحد همدان Atefehzarei@gmail.com

مقدمه

فناوری رایانش ابری اخیراً به منزلهٔ یکی از مهم‌ترین مباحث حوزهٔ توسعهٔ نظام‌های اطلاعات مطرح شده است (لاین و دیگران[1]، ۲۰۱٤)؛ به‌طوری‌که آورام[2] در سال ۲۰۱٤ میلادی، رایانش ابری را به‌صورت مدل جدیدی برای میزبانی و ارائهٔ خدمات در اینترنت مطرح کرده است. این فناوری نوین نظام‌های اطلاعات، مدلی است که به ارائهٔ دسترسی آسان توزیع‌شده و فراگیر به منابع محاسباتی تجمیعی و مشترک قابلِ‌پیکربندی می‌پردازد. در رایانش ابری، قابلیت‌های مبتنی بر فناوری اطلاعات به‌منزلهٔ خدماتی که بدون نیاز به دانش دقیق از فناوری‌های زیرساختی و کمترین تلاش مدیریتی در دسترس قرار می‌گیرد، عرضه می‌شود (صدرالساداتی و کارگر، ۱۳۹۱). با توجه به قابلیت‌ها و خدمات فناوری رایانش ابری، آن را به‌منزلهٔ یک نوآوری در تبادل اطلاعات و حوزه‌ای که در آن، سرمایه‌گذاری گسترده‌ای انجام‌گرفته، شناخته‌اند (آرمبراست[3] و دیگران، ۲۰۱۰).

مؤسسهٔ ملی فناوری و استانداردهای آمریکا[4]، رایانش ابری را این‌گونه تعریف می‌کند: رایانش ابری، مدلی برای فراهم‌کردن دسترسی آسان بر اساس تقاضای کاربر از طریق شبکه به مجموعه‌ای از منابع رایانشی قابل‌تغییر و قابلِ‌پیکربندی (مثل شبکه‌ها، سرورها، فضای ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها) است که این دسترسی باید بتواند با کمترین نیاز به مدیریت منابع و یا نیاز به دخالت مستقیم فراهم‌کنندهٔ خدمات به سرعت فراهم‌شده یا آزاد (رها) شود. رایانش ابری به معنی توسعه و به‌کارگیری فناوری رایانه بر مبنای اینترنت است؛ درواقع، قابلیت‌های رایانه‌ای به‌صورت یک خدمت اینترنتی، به کاربر عرضه می‌شود.رایانش ابری به خاطر مزایای زیاد، اخیراً در شرکت‌های بزرگی از قبیل گوگل، یاهو، آمازون و فیس‌بوک، کاربرد فراوانی داشته است؛ همچنین رایانش ابری برای صرفه‌جویی در هزینه‌های سرمایه‌گذاری اولیه نیز مورداستفاده قرار گرفته است. دراپ‌باکس[5] و گروپ‌آن[6]، نمونه‌هایی هستند که برای کاربردهای روزمره از رایانش ابری استفاده می‌شوند. شرکت‌های دیگر نیز تمایل دارند که نرم‌افزارهای کاربردی خود را به سمت رایانش ابری انتقال دهند تا هزینه‌ها را کاهش و بازدهی تجاری خود را افزایش دهند (لی هونگ جو[7]،۲۰۱۱).

در این فناوری، کاربران می‌توانند از طریق سرویس‌های عرضه‌شدهٔ رایانش ابری و ابزارهای مختلف به برنامه‌ها، فضاهای ذخیره‌سازی، پردازش و حتی سکوهای توسعهٔ برنامه‌های کاربردی در اینترنت دسترسی

---

1. Lan et al
2. Avram
3. Armbrust et al
4. National Institute of Standard Technology (NIST)
5. Dropbox
6. Groupon
7. Lee Hong Joo

داشته باشند. خدمات فراهم‌شده از طریق رایانش ابری از نوع ابـزار محاسـباتی[1] اسـت و بـه ایـن معناسـت کـه خدمات مورداستفادهٔ مشتریان در سرورها عرضه می‌شود و پرداخت‌ها در آن، همانند سایر خدمات عمومی (مثل برق و آب) بر اساس سطح استفادهٔ افراد انجام می‌شود (فتوتی، ۱۳۹۳).

امروزه سه مدل اصلی تحویل خدمت در محاسبات ابری استفاده می‌شود که عبارتند از:

سس[2]: نرم‌افزاری به‌منزلهٔ خدمت، تمامی برنامه‌های کاربردی که بر روی ابر کار می‌کنند و یک خدمت مستقیم را به مشتریان عرضه می‌کنند، در این لایه قرار می‌گیرند. نرم‌افزار به‌منزلهٔ خدمت، این امکان را می‌دهد تا نیازی بـه نصب و راه‌اندازی برنامه روی سیستم کاربر نباشد. مشخصهٔ اصلی این برنامه، دسترسی بر پایـهٔ شـبکه بـه‌منظـور مدیریت متمرکز و از راه دور است (جادیجا، مؤدی[3]، ۲۰۱۲). در این لایه، عرضه‌کننـدهٔ خـدمت، مسـئول امنیـت فیزیکی است. در این لایه، مشتری قادر به مدیریت زیرساخت‌های ابر مانند شبکه، سرورها، فضاهای ذخیره‌سازی، سیستم‌عامل و حتی برنامه‌های کاربردی با اختیارات محدود است (وینکلر[4]، ۲۰۱۱)؛ در این سـطح، عرضـه‌کننـدهٔ خدمت به‌منظور عرضهٔ خدمات بهتر به مشتریان باید اجزای امنیتی زیر را فـراهم کنـد (تیانفیلـد[5]، ۲۰۱۱): امنیـت داده‌ها، امنیت شبکه، یکپارچگی داده‌ها، تجزیه‌کردن داده‌ها، دسترسی به داده‌ها، مکان‌یابی داده‌ها، احراز هویـت و اصالت، محرمانه‌بودن داده‌ها، امنیت نرم‌افزار، نقض داده، مجازی‌سازی، دسترس‌پذیری، پشتیبان‌گیـری، مـدیریت هویت و روند ثبت‌نام (ملکشاهی، حقانی و حقانی، ۱۳۹۲).

پاس[6]: سکو به‌منزلهٔ خدمت که اگر یک لایه بالاتر بیاییم، با این بخش روبه‌رو خواهیم شد. چیزی که با عنـوان سکو در اینجا از آن یادشده، به دو محیط متفاوت برمی‌گردد: محیط توسعهٔ نظام و محیط اجرای آن. این لایه میزبان محیط‌های مختلف برای عرضهٔ خدمات است. سکو بـه‌منزلـهٔ خـدمت، فـراهم‌کننـدهٔ بسـتری بـرای پیـاده‌سـازی نرم‌افزارهای موردنیاز و درواقع پشتیبانی از چرخهٔ حیات نرم‌افزار برای کاربر است (زیسایس و لیکـاس[7]، ۲۰۱۱). در این لایه، هم کاربر و هم عرضه‌کنندهٔ خدمت، هر دو در برقراری امنیت سهیم هستند. کـاربر، برنامـهٔ کـاربردی تحت زیرساخت ابر را تهیه می‌کند؛ اما قادر به مدیریت زیرساخت‌های ابر با کنترل نرم‌افـزار بـر روی شـبکه‌هـا و سرورها و فضاهای ذخیره‌سازی نیست (وینکلر، ۲۰۱۱)؛ کاربر قادر به کنترل و مدیریت برنامهٔ کـاربردی اسـت و هرگونه تدابیر امنیتی برای میزبان و جلوگیری از نفوذ و تضمین دردسترس‌نبودن داده‌های برنامهٔ کاربردی بر عهدهٔ عرضه‌کنندهٔ خدمت است (ملکشاهی، حقانی و حقانی، ۱۳۹۲).

---

[1] Utility Computing
[2] SaaS
[3] Jadeja & Modi
[4] Winkler
[5] Tianfield
[6] PaaS
[7] Zissis & Lekkas

ایس[1]: ساختار به‌منزلهٔ خدمت، در فضای ابری، استفاده از منابع محاسباتی زیرساختی از قبیل تجهیزات ذخیره‌سازی، شبکه‌ها و سرورها به‌منظور عرضهٔ خدمات به کاربران نهایی استفاده می‌شود. کاربران نهایی می‌توانند نرم‌افزارهای دلخواه از قبیل سیستم‌های عامل و نرم‌افزارهای کاربردی را پیاده‌سازی و اجرا کنند؛ آمازون یی. سی.[2]، نمونه‌ای از آن‌ها به شمار می‌رود. مشتری، زیرساخت پایه‌ای را کنترل نمی‌کند؛ اما معمولاً می‌تواند ماشین‌های مجازی را با سیستم‌عامل‌های انتخابی که وی مدیریت می‌کند، راه‌اندازی نماید (صدرالساداتی و کارگر، ۱۳۹۱).

این فناوری، شانس بزرگی برای سازمان‌های بزرگ و شرکت‌های فناوری اطلاعات در کشورهای توسعه‌یافته است؛ اما این فرصت‌ها با چالش‌هایی مانند امنیت روبه‌رو است (منسف و گیگادو[3]، ۲۰۱۱). درواقع سازمان‌ها برای پیشبرد اهداف خود به استفاده از چنین فناوری‌هایی تمایل دارند؛ ولی اغلب نمی‌توانند هیچ تضمینی در خصوص امنیت اطلاعات و برنامه‌های کاربردی خود که نزد عرضه‌کنندگان خدمات ابر است، داشته باشند؛ بنابراین امنیت، عنصر مهمی در پذیرش محاسبات ابری می‌باشد که اگر عرضه‌کنندگان خدمات ابر بتوانند امنیت لازم را فراهم کنند، کاربران بسیاری به استفاده از این فناوری روی می‌آورند (ملکشاهی، حقانی و حقانی، ۱۳۹۲).

نتایج حاصل از نظرسنجی شرکت آی.دی.سی.[4] از ۲٤٤ مدیر فناوری اطلاعات نشان می‌دهد که در بین ۹ چالش اساسی مطرح در حوزهٔ رایانش ابری، امنیت بزرگ‌ترین چالش است که با کسب ۷٤/۵ درصد، مقام نخست دغدغه‌های مدیران سازمان‌ها را به خود اختصاص داده است.

مهم‌ترین عامل موفقیت یک نظام در صنعت فناوری اطلاعات، حفظ امنیت اطلاعات است (ساچدوا[5]، ۲۰۱۰). یک نظام محاسبات ابری باید در تمامی جنبه‌ها امنیت داشته باشد که بسیاری از این جنبه‌ها به تنظیمات ابر مربوط می‌شود (رایان[6]، ۲۰۱۳)؛ بنابراین برای ساخت یک نظام امن باید موضوعاتی ازجمله طراحی معماری امن، به‌حداقل‌رساندن سطوح حمله، جلوگیری از نفوذ هکرها و کنترل دسترسی به داده‌ها در نظر گرفته شود (ملکشاهی، حقانی و حقانی، ۱۳۹۲)؛ بنابراین مدل‌های امنیتی در خدمات محاسبات ابری باید با قوانین و مقررات ملی مطابقت داشته باشند؛ این مقررات و قواعد در ابتدا به‌منظور محافظت از اطلاعات است که می‌تواند برای شناسایی افراد مورداستفاده قرار بگیرد (پیرسون، ۲۰۰۹). یکی از نگرانی‌های امنیتی در پردازش ابری، افشای داده به اشخاص و یا نظام‌های غیرمجاز است. زمانی که یک سازمان، داده‌های خود را در ابر قرار می‌دهد، مالک داده (مستأجر) در

---

[1] IaaS
[2] Amazon EC2
[3] Monsef & Gigado
[4] International Data Corporation (IDC)
[5] Sachdeva
[6] Ryan

داخل سازمان و در مقابل متولی داده (تأمین‌کننده) خارج از سازمان قرار دارد و این یک چالش برای کنترل دسترسی به داده ایجاد می‌کند.

با توجه به چالش‌های ذکرشده می‌توان مزایایی برای محاسبات ابری برشمرد که عبارتند از: کیفیت خدمت، قابلیت اطمینان، مدیریت از راه دور، کاهش هزینه، کارایی، قابلیت اعتماد و شهرت؛ محاسبات ابری علاوه بر داشتن مزایا باید دارای معایبی چون وابسته‌بودن توان پردازشی به پهنای باند، امنیت حریم خصوصی و حفظ و نگهداری داده‌ها باشند (ماتیس[1]، ۲۰۱۱).

نتایج در پیشینه‌های پژوهش نشان می‌دهد که محاسبات ابری همواره با چالش‌هایی روبه‌رو است که امنیت اطلاعات و حفظ حریم خصوصی از مهم‌ترین آن‌ها می‌باشد و ارائه‌دهندگان این فناوری باید سعی در کاهش نگرانی‌های کاربران خود و جذب آن‌ها داشته باشند و همچنین به ارایه راهکارهایی برای استفادهٔ ازاین محیط بپردازنند، که درمقاله‌های باغشاهی و دیگران (۱۳۹۱)، (صدرالساداتی، کارگر،۱۳۹۳)، هاشمی[2] (۲۰۱۳)، وینتاو[3] (۲۰۱۲)، زهیر تایر[4] (۲۰۱٤) ادوارد جی. آمروسو[5] (۲۰۱٤) بیان شده است. دربررسی‌های(صدرالساداتی، کارگر،۱۳۹۳)، باغشاهی و دیگران(۱۳۹۱) به این مورد اشاره شده است که رایانش ابری را به‌منزلهٔ یک ابزار دسترسی آسان و کم‌هزینه در فضای مجازی است که سازمان‌ها می‌توانند با استفاده از رایانش ابری، توانایی بهره‌وری و صرفه‌جویی در منابع فناوری اطلاعات و افزایش توان محاسباتی را فراهم نمایند. زهیر تایر(۲۰۱٤) و ادوارد جی. آمروسو(۲۰۱٤) فضای ابری را سرورهای مجازی‌سازی، پایگاه داده و برنامه‌های کاربردی معرفی می‌کنند وآن را یک پایگاه[6] مستعد برای اشتراک‌گذاری داده‌های بزرگ دانسته‌اند.

دانشگاه‌ها و مؤسسات آموزش عالی ازجمله مراکزی هستند که برای همکاری و تبادل اطلاعات علمی از فضای مجازی به‌ویژه رایانش ابری استفاده می‌کنند و در این مراکز، قشر عظیمی از کاربران فضاهای مجازی را دانشجویان تحصیلات تکمیلی تشکیل می‌دهد. مطالعات و مقالات در زمینهٔ رایانش ابری به‌صورت مروری و تحلیلی ارائه شده است. بر همین اساس بر آن شدیم تا پژوهشی در زمینهٔ شناسایی امنیت اطلاعات و حفظ حریم خصوصی افراد برای همکاری در محیط ابری را از دیدگاه دانشجویان مقطع دکتری علوم پایه، پژوهشگاه ملی مهندسی ژنتیک و زیست‌فناوری انجام دهیم؛ بنابراین، سؤال‌ها و فرضیه‌های زیر را می‌توان برای پژوهش حاضر متصور شد:

---

[1] Mathise
[2] Hashemi
[3] Wentao
[4] Zahir Tari
[5] Edward G. Amoroso
[6] Platform

۱. میزان استفاده از رایانش ابری برای همکاری در فضای مجازی از دیدگاه جامعهٔ موردپژوهش چگونه است؟
۲. نقش رایانش ابری در امنیت و حفظ حریم خصوصی از دیدگاه جامعهٔ موردپژوهش چگونه است؟
۳. نقش رایانش ابری در حفظ امنیت اطلاعات از دیدگاه جامعهٔ موردپژوهش چگونه است؟
٤. بین مؤلفه‌های همکاری، حریم خصوصی و امنیت خصوصی در فضای مجازی تفاوت معناداری وجود دارد.
۵. بین مؤلفه‌های اهمیت امنیت در حریم خصوصی، ارتباطی و محیطی تفاوت معنی‌داری وجود دارد.

روش‌شناسی

پژوهش حاضر از نظر هدف، کاربردی است. روش پژوهش، پیمایشی- تحلیلی است. کل جامعهٔ آماری این پژوهش را ۱۰۰ دانشجوی مقطع دکتری علوم پایهٔ ورودی ۹۳-۹٤ پژوهشگاه ملی و مهندسی ژنتیک و زیست‌فناوری تشکیل داده شده است. به‌منظور انجام آمار استنباطی برای پژوهش، تعداد نمونهٔ آماری با استفاده از فرمول کوکران، معادل ۷۹ نفر محاسبه شد. ابزار جمع‌آوری داده‌ها، پرسشنامهٔ محقق‌ساخته است. در مجموعهٔ ۱۰۰ پرسشنامهٔ توزیع‌شده، ٦۷ پرسشنامه جمع‌آوری شد. داده‌های گردآوری شده با استفاده از نرم‌افزار اس.پی.اس.اس. نسخه ۲۲ و با آزمون‌های تی‌تست تک‌نمونه‌ای، رتبه‌بندی فریدمن، تی‌تست زوجی نمونهٔ مستقل و آنالیز واریانس تحلیل شدند. پیش از تعیین روش آماری مناسب برای تحلیل، فرضیهٔ نرمال‌بودن مشاهدات به‌صورت استنباطی با استفاده از آمارهٔ کلموگروف- اسمیرنف، بررسی شد. پایایی پرسشنامه نیز از طریق محاسبهٔ ضریب آلفای کرونباخ محاسبه شد که بیش از ۰/۷ به دست آمد؛ بنابراین پرسشنامه در این پژوهش دارای قابلیت اعتماد است.

یافته‌ها

تحلیل توصیفی

از مجموعهٔ ٦۷ نفر در گروه نمونه، زنان با ٦۲/۷ درصد، تحصیلات در مقطع کارشناسی ارشد با ٦۲/۲ درصد و گروه سنی ۱۸ تا ۲۵ با ٤٤/۸ درصد بیشترین حجم گروه نمونه را تشکیل داده‌اند و همچنین:

جدول ۱. فراوانی ویژگی‌های فناوری رایانش ابری

ویژگی‌های محیط ابری		بسیار زیاد	زیاد	متوسط	کم	بسیار کم	بدون پاسخ	کل
استفاده	فراوانی	٤	٨	١٦	١٦	**٢٢**	١	٦٧
	درصد	٦/٠	١١/٩	٢٣/٩	٢٣/٩	**٣٢/٨**	١/٥	١٠٠/٠
اطلاعات	فراوانی	٠	٨	٢٠	**٢١**	١٨	٠	٦٧
	درصد	٠٠/٠	١١/٩	٢٩/٩	**٣١/٣**	٢٦/٩	٠٠/٠	١٠٠/٠
مزایا	فراوانی	٠	١١	**٢٢**	١٩	١٤	١	٦٧
	درصد	٠٠/٠	١٦/٤	**٣٢/٨**	٢٨/٤	٢٠/٩	١/٥	١٠٠/٠
آموزش	فراوانی	١٣	١٧	**٢١**	١١	٥	٠	٦٧
	درصد	١٩/٤	٢٥/٤	**٣١/٣**	١٦/٤	٧/٥	٠٠/٠	١٠٠/٠
وفاداری	فراوانی	**٣٣**	١٧	١١	٥	١	٠	٦٧
	درصد	**٤٩/٣**	٢٥/٤	١٦/٤	٧/٥	١/٥	٠٠/٠	١٠٠/٠
قوانین و	فراوانی	٢	٥	٢١	**٢٤**	١٥	٠	٦٧
مقررات	درصد	٣/٠	٧/٥	٣١/٣	**٣٥/٨**	٢٢/٤	٠٠/٠	١٠٠/٠

با توجه به یافته‌های پژوهش که در جدول شماره ۱ مشاهده می‌شود:

- استفاده رایانش ابری با فراوانی بسیار کم (۲۲) ۳۲/۸ درصد، دریافت اطلاعات با فراوانی کم (۲۱) ۳۱/۳ درصد، مزایای رایانش ابری با فراوانی متوسط (۲۲) ۳۲/۸، آموزش کاربری رایانش ابری با فراوانی متوسط (۲۱) ۳۱/۳ درصد، وفاداری سیستم رایانش ابری با فراوانی بسیار زیاد (۳۳) ٤۹/۳ درصد و قوانین و مقررات در فضای ابری با فراوانی متوسط (٢٤) ۳۵/۸ درصد بیشترین حجم گروه نمونه را تشکیل می‌دهند؛ بنابراین از نظر گروه نمونه، اطلاعات کم، استفادهٔ بسیار کم از فناوری رایانش ابری و مزایای متوسط، بیشترین حجم نمونه را تشکیل داده است. همچنین از نظر خدمات، سرویس‌گرهای فضای ابری وفاداری، درجهٔ اهمیت بالاتری دارند.

جدول ۲. انواع سرویس‌گرهای فناوری رایانش ابری

	فراوانی	درصد
Drop Box	۱۷	۲۵/٤
Google Drive	۱۳	۱۹/٤
Gmail	٤٥	٦۷/۲
SkyDrive	۰	۰/۰
Box	۲	۳/۰
کل	٦۷	۱۰۰/۰

همان‌طور که در جدول شماره ۲ مشاهده می‌شود:

- استفاده از Gmail با فراوانی ٤٥ و کسب ٦۲/۲ درصد، بیشترین حجم در گروه نمونه را که از امنیت بالایی برخوردار می‌باشد، تشکیل داده است.

جدول ۳. آماره‌های توصیفی فناوری رایانش ابری

	تعداد	میانگین	میانه	انحراف معیار	کمترین مقدار	بیشترین مقدار
همکاری در محیط مجازی	٦۷	۳/۰۰۰۰	۳/۰۰۰۰	۰/۸٦۸٤٥	۱/۳۳	٥/۰۰
امنیت و حفظ حریم خصوصی	٦۷	۳/۰٤۱۰	۳/۰۰۰۰	۱/۰۳۲۲٤	۱/۰۰	٤/۷٥
حفظ امنیت اطلاعات	٦۷	۲/٥۲۸٤	۲/٦۰۰۰	۰/۷۹۹۰۲	۱/۰۰	٤/٤۰

همان‌طور که در جدول شماره ۳ مشاهده می‌شود، امنیت و حفظ حریم خصوصی با میانگین ۳/۰٤ درصد دارای بیشترین اهمیت در بین متغیرها است.

تحلیل استنباطی

پاسخ به سؤال‌های پژوهش

۱. **میزان استفاده از رایانش ابری برای همکاری در فضای مجازی از دیدگاه جامعهٔ موردپژوهش چگونه است؟**

جدول ٤. همکاری در فضای مجازی با استفاده از فناوری رایانش ابری

نام متغیر	میانگین	انحراف معیار	اختلاف میانگین	آماره آزمون t	سطح معناداری	فاصله اطمینان ٪۹۵	
						کران پایین	کران بالا
همکاری در فضای مجازی	۳/۰۰	۰/۸٦۸	۰/۰۰۱	۰/۰۰۱	۰/۹۹۹	-۰/۲۱۱۸	۰/۲۱۱۸

همان‌طور که در جدول شمارهٔ ٤ مشاهده می‌شود، این آزمون به‌منظور مقایسهٔ میانگین یک متغیر با مقداری ثابت طراحی شده است. فرضیه‌های موردبررسی در آن به‌صورت زیر هستند:

$$\begin{cases} H_0: \mu \leq ۳ \\ H_1: \mu > ۳ \end{cases}$$

متغیر همکاری در فضای مجازی دارای میانگین ۳/۰۰ با انحراف معیار ۰/۸٦۸ است. ازآنجایی‌که سطح معناداری این آزمون ۰/۹۹۹ شده و از ۰/۰۵ بیشتر است؛ لذا فرض صفر در سطح خطای ۰/۰۵ رد نمی‌شود؛ یعنی میانگین این متغیر در جامعه برابر با عدد ۳ بوده است. از طرفی چون اختلاف میانگین نمونه ۰/۰۳۳ شده است، بازهٔ تغییرات اختلاف این متغیر ۰/۲۱۱- تا ۰/۲۱۲ است و بین کران‌های پایین و بالای فاصلهٔ اطمینان ۹۵ درصد برای اختلاف میانگین با عدد ۳ یکی منفی و یکی مثبت است؛ لذا میانگین این متغیر در جامعه، برابر ۳ بوده است. درنتیجه، نقش استفاده از رایانش ابری برای همکاری در فضای مجازی در حد متوسط بوده است.

۲. نقش رایانش ابری در امنیت و حفظ حریم خصوصی از دیدگاه جامعهٔ موردپژوهش چگونه است؟

جدول ۵. میزان امنیت و حفظ حریم خصوصی در فناوری رایانش ابری

نام متغیر	میانگین	انحراف معیار	اختلاف میانگین	آماره آزمون t	سطح معناداری	فاصله اطمینان ٪۹۵	
						کران پایین	کران بالا
امنیت و حفظ حریم خصوصی	۳/۰٤	۱/۰۳	۰/۰٤۱	۰/۳۲۵	۰/۷٤٦	-۰/۲۱۱	۰/۲۹۲

با توجه به نتایج جدول شماره ۵، این آزمون به‌منظور مقایسهٔ میانگین یک متغیر با مقداری ثابت، طراحی شده است. فرضیه‌های موردبررسی در آن به‌صورت زیر هستند:

$$\begin{cases} H_0: \mu \leq ۳ \\ H_1: \mu > ۳ \end{cases}$$

متغیر امنیت و حفظ حریم خصوصی دارای میانگین ۳/۰٤ با انحراف معیار ۱/۰۳٤ می‌باشد. چون سطح معناداری این آزمون ۰/۷٤٦ به دست آمده و از ۰/۰۵ بیشتر است؛ لذا فرض صفر در سطح خطای ۰/۰۵ رد نمی‌شود؛ یعنی میانگین این متغیر در جامعه برابر با عدد ۳ بوده است. از طرفی چون اختلاف میانگین نمونه ۰/۰٤۱ شده است، بازهٔ تغییرات اختلاف این متغیر از ۰/۲۱۱- تا ۰/۲۹۲ می‌باشد و بین کران‌های پایین و بالای فاصلهٔ اطمینان ۹۵ درصد برای اختلاف میانگین با عدد ۳، یکی منفی و یکی مثبت است. لذا میانگین این متغیر در جامعه، مساوی ۳ بوده است. درنتیجه نقش رایانش ابری در امنیت و حفظ حریم خصوصی در حد متوسط بوده است.

۳. نقش رایانش ابری در حفظ امنیت اطلاعات از دیدگاه جامعهٔ موردپژوهش چگونه است؟

جدول ٦. میزان حفظ امنیت اطلاعات در فناوری رایانش ابری

نام متغیر	میانگین	انحراف معیار	اختلاف میانگین	آماره آزمون t	سطح معناداری	فاصله اطمینان ۹۵٪	
						کران پایین	کران بالا
امنیت اطلاعات حفظ	**۲/۵۳**	**۰/۷۹۹**	**-۰/٤۷۱**	**-٤/۸۳۲**	**۰/۰۰۱**	**-۰/٦٦٦**	**-۰/۲۷٦**

همان‌طور که در جدول شماره ٦ مشاهده می‌شود، این آزمون به‌منظور مقایسهٔ میانگین یک متغیر با مقداری ثابت، طراحی شده است. فرضیه‌های موردبررسی در آن به‌صورت زیر هستند:

$$\begin{cases} H_0: \mu \leq ۳ \\ H_1: \mu > ۳ \end{cases}$$

متغیر حفظ امنیت اطلاعات دارای میانگین ۲/۵۳ با انحراف معیار ۰/۷۹۹ می‌باشد. چون سطح معناداری این آزمون ۰/۰۰۱ شده و از ۰/۰۵ کمتر است؛ لذا فرض صفر در سطح خطای ۰/۰۵ رد می‌شود؛ یعنی میانگین این متغیر در جامعه برابر با عدد ۳ نبوده و به‌طور معنی‌داری متفاوت با آن است. از طرفی چون اختلاف میانگین نمونه ۰/٤۷۱- شده است و بازه تغییرات اختلاف این متغیر از ۰/٦٦٦- تا ۰/۲۷٦- می‌باشد، بین کران‌های پایین و بالای فاصلهٔ اطمینان ۹۵ درصد برای اختلاف میانگین با عدد ۳، هر دو عدد منفی است. لذا میانگین این متغیر در جامعه، مساوی ۳ نبوده و به‌طور معنی‌داری از ۳ کمتر است. درنتیجه، رایانش ابری در حفظ امنیت اطلاعات مؤثر نبوده است.

آزمون فرضیه‌ها

۱. استفاده از فناوری رایانش ابری باعث می‌شود که بین میزان تأثیر همکاری، حفظ حریم خصوصی و امنیت اطلاعات در فضای مجازی تفاوت معناداری وجود داشته باشد.

جدول ۷. آزمون مقایسهٔ همکاری، حفظ حریم خصوصی و امنیت اطلاعات در فضای مجازی

تعداد	آماره کای دو	درجه آزادی	سطح معناداری
٦٧	٦/٦٥	٢	٠/٠٣٦

با توجه به اینکه سطح معناداری کمتر از ۰/۰۵ است، میزان تأثیر همکاری، حفظ حریم خصوصی و امنیت اطلاعات در فضای مجازی یکسان نیست و امکان رتبه‌بندی وجود دارد؛ بنابراین:

جدول ۸. رتبه‌بندی همکاری، حفظ حریم خصوصی و امنیت اطلاعات در فضای مجازی

متغیرها	میانگین رتبه‌ها	اولویت
همکاری در فضای مجازی	۲/۱۳	**۱**
امنیت و حفظ حریم خصوصی	۲/۱۲	**۲**
حفظ امنیت اطلاعات	۱/۷۵	**۳**

همان‌طور که در جدول شماره ۸ مشاهده می‌شود، رایانش ابری بیشترین تأثیر را بر همکاری در فضای مجازی داشته است. پس از آن، امنیت و حفظ حریم خصوصی در مرتبهٔ دوم قرار دارد. حفظ امنیت اطلاعات، کمترین تأثیر را دارد.

۲. در محیط ابری بین اهمیت امنیت در حریم خصوصی فیزیکی، ارتباطی، محیطی و اطلاعات شخصی تفاوت معناداری وجود دارد.

جدول ۹. خلاصهٔ آزمون، امنیت در حریم خصوصی فیزیکی، ارتباطی، محیطی و اطلاعات شخصی

تعداد	آماره کای دو	درجه آزادی	سطح معناداری
٦٧	**۳/۷۱**	**۳**	**۰/۲۹۵**

با توجه به اینکه سطح معناداری بیشتر از ۰/۰۵ است، امنیت در حریم خصوصی فیزیکی، ارتباطی، محیطی و اطلاعات شخصی یکسان است؛ بنابراین امکان رتبه‌بندی وجود ندارد.

جدول ۱۰. رتبه‌بندی حریم خصوصی فیزیکی، ارتباطی، محیطی و اطلاعات شخصی

متغیرها	میانگین	اولویت
امنیت اطلاعات شخصی	۲/٦۳	-
حریم خصوصی فیزیکی	۲/۵۷	-
حریم خصوصی ارتباطی	۲/٤۷	-
حریم خصوصی محیطی	۲/۳٤	-

همان‌طور که در جدول شماره ۱۰ ملاحظه می‌شود، بین میانگین متغیرهای حریم خصوصی فیزیکی، ارتباطی، محیطی و اطلاعات شخصی تفاوت معناداری وجود ندارد و از نظر کاربران، حفظ حریم و امنیت اطلاعات به یک اندازه مهم هستند.

نتیجه‌گیری

از بدو پیدایش فناوری رایانش ابری، حفظ امنیت اطلاعات و حریم خصوصی از دغدغه‌ها و نگرانی‌های کاربران فضای مجازی بوده است. طرفداران حفظ حریم خصوصی، مدل ابری را موردانتقاد قرار داده‌اند؛ زیرا ارائه‌دهندگان خدمات ابری می‌توانند کنترل و نظارت کامل قانونی و یا غیرقانونی بر روی داده‌ها و ارتباطات بین کاربران خدمت و میزبان ابر داشته باشند.

با توجه به اهداف این پژوهش که بررسی میزان همکاری در فضای مجازی با استفاده از فناوری ابری با توجه به نگرانی و دغدغه‌های کاربران در مورد حفظ حریم خصوصی و امنیت اطلاعات است، نتایج نشان می‌دهد که علیرغم اطلاعات کم کاربران از مزایای این فناوری، واستفادهٔ بسیار کمی از خدمات عرضه‌شدهٔ سرویس‌گرهای ابری، آنها معتقد هستند که، وفاداری سرویس‌گرهای ابری نسبت به داشتن قوانین و مقررات و آموزش لازم برای استفاده محیط ابری، از اهمیت بالایی باید برخوردار باشد.

همانطور که باغشاهی و دیگران، صدرالساداتی، کارگر، هاشمی، وینتاو، زهیر تایر، ادوارد جی. آمروسو، در مطالعات خود امنیت و حفظ حریم خصوصی را از چالش‌های مهم رایانش ابری عنوان کردند. یافته‌های این پژوهش هم نشان می‌دهد که **کاربران** نقش فناوری رایانش ابری در همکاری و امنیت و حفظ حریم خصوصی فضای مجازی در حد متوسط و در حفظ امنیت اطلاعات بسیار ضعیف دانسته‌اند بنابراین چالش امنیت و حفظ حریم خصوصی، بزرگ‌ترین مانع بر سر راه پذیرفته‌شدن فناوری رایانش ابری در بین کاربران است. بدیهی است که این فناوری باید به نگرانی‌ها و دغدغه‌های کاربران خود اهمیت داده و در جلب اعتماد آن‌ها تلاش بیشتری

کند. هم‌چنین در پژوهش حاضر نتایج نشان می‌دهد که رایانش ابری بیشترین تأثیر را بر همکاری در محیط مجازی، امنیت و حریم خصوصی و کمترین تأثیر را بر امنیت اطلاعات دارد. اگرچه سرویس‌گرهای خدمات رایانش ابری در حال گسترش فضای امن و سالم و انجام تعهدات و افزایش وفاداری‌شان به دریافت‌کنندگان خدمات هستند و سعی دارند اعتماد کاربران خود را جلب کنند؛ اما به طرز چشمگیری نیاز به تلاش بیشتر در زمینه‌های مختلف وجود دارد تا خدمات شفاف و قابل‌اطمینانی برای افراد جامعه مهیا شود. رتبه‌های امنیت تبادل، انتقال و ذخیرهٔ اطلاعات در محیط ابری یکسان می‌باشد. با توجه به اینکه حریم خصوصی برای هر فرد به چهار شکل، فیزیکی، ارتباطی، محیطی و اطلاعاتی در نظر گرفته شده است و هم‌چنین بین امنیت متغیرهای اطلاعات شخصی، حریم خصوصی فیزیکی، ارتباطی و محیطی در محیط ابری، اختلافی نیست و یکسان هستند، حفظ ارتباطات شخصی و حریم خصوصی در فضای مجازی از اهمیت بالایی برای کاربران برخوردار است.

منابع

باغشاهی، سمیه سلطان...و [دیگران](۱۳۹۱). تحلیل چالش‌های امنیتی و تأثیر آن بر رایانش ابری. اولین کارگاه ملی رایانش ابری ایران، ۱۰،۱۱ آبان. دانشگاه صنعتی امیرکبیر، دانشکده مهندسی کامپیوتر و فناوری اطلاعات.۸-۲.

بنی‌رستم، حمید، هدایتی، علیرضا، خادم‌زاده، احمد (۱۳۹۲). ارائه رویکردهای نوین برای مقابله با چالش‌های امنیتی رایانش ابری. دومین کنفرانس توسعه کاربردهای صنعتی اطلاعات، ارتباطات و محاسبات، تبریز ۸ و ۹ آبان.٦-۲.

شرکت اینفوامن (۱۳۹۱). نگرانی، تهدیدها و کنترل‌های امنیتی در پردازش ابری. خبرنامه، شماره ۹. ٦-۱.

شرکت مدل‌سازان «مسنا»(۱۳۹۳).مروری بر پردازش ابری - گونه های پردازش ابری. http://masna.blog.ir.

صدرالساداتی، محسن، کارگر، محمدجواد (۱۳۹۱). چالش‌های امنیتی در رایانش ابری و ارائه راهکاری جهت بهبود امنیت آن در راستای توسعه خدمات عمومی دولت الکترونیک. هشتمین سمپوزیوم پیشرفت‌های علوم و تکنولوژی.۱۰-۱.

فتوتی، عباس (۱۳۹۳). آشنایی با رایانش ابری (فناوری کلاد). http://laitec.sharif.ir.

ملکشاهی، عاطفه، خاکسار حقانی، شهرزاد، خاکسار حقانی، مهسا (۱۳۹۱). بررسی امنیت و مروری بر حفظ حریم خصوصی و ارائه پیشنهادات و راهکارهایی در راستای بهبود امنیت در محاسبات ابری. هشتمین سمپوزیوم پیشرفت‌های علوم و تکنولوژی.۷-۱.

نقیان فشارکی، مهدی، طباطبایی، غلامحسن، تمتاجی، مصطفی (۱۳۹۳). ارائهٔ معماری مرجع امنیتی محیط رایانش ابر خصوصی سازمان. فصلنامه علمی -پژوهشی امنیت پژوهی،٤٧ (۱۳).۱۱۳-۹۱.

یعقوبی، نور محمد، شکوهی، جواد، جعفری، حمیرضا (۱۳۹۳). شناسایی و رتبه‌بندی عوامل کلیدی مؤثر بر به‌کارگیری رایانش ابری در سلامت الکترونیک. فصلنامه علمی– پژوهشی پژوهشنامهٔ پردازش و مدیریت اطلاعات. ۳۰ (۲). ۵۷۰-۵٤۷.

Armbrust, M., A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. 2010. A view of cloud computing. *Communications of the ACM* (53): 50-8.

Avram,G. (2014).Advantages and challenges of adopting cloud computing from an enterprise perspective *Procedia Technology*. 12.529 – 534.

Cloud-computing-survey Cloud Computing Survey(2012). http://northbridge.com.
E. Mathise, (2011). "Security Challenges and Solutions in Cloud Computing". Proc 5th IEEE. Int. Conf. on Digital Ecosystems and Technologies. 208-212.
Hashemi, Sajjad, (2013). Data Storage Security Challenges In Cloud Compoting. International Journal of Security, Privacy and Trust Management (IJSPTM). l 2. 4.230-242.
IEEE Computer Society, (2010). Sixth International Conference on Semantics, Knowledge and Grids. Security and Privacy in Cloud Computing: A Survey. 56-65.
K, Sachdeva, (2011). Cloud Computing: Security Risk Analysis and Recommendations. Master Thesis, University of Texas, Austin.International Journal of Computer Network and Information Security(IJCNIS). Vol. 6, No. 8.
Jadeja, Y. and Modi, K. (2012). "Cloud computing - concepts, architecture and challenges," in *Computing, Electronics and Electrical Technologies*
(ICCEET), International Conference on, p. 877-880
Lee Hong Joo. (2011). Analysis of business attributes in information technology environments. J Inform Process Syst.7(2):385–96.
Lian, J., D. Yen, and Y. Wang. (2013). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. ternational Journal of Information Management, http://dx.dio.org/10.1016/j.ijinfomgt.
E. Mathise,(2011) "Security Challenges and Solutions in Cloud Computing", Proc. 5th IEEE . Int. Conf. on Digital Ecosystems and Technologies. 208-212.
M. D. Ryan, (2013). Cloud computing security: The scientific challenge, and a survey of solutions. The Journal of Systems and Software. 86. 2263–2268.
M. Monsef, N. Gidado, (2011).—Trust and privacy concern in the Cloud. European Cup, IT Security for the Next Generation.1-15.
National Institute of Standards and Technology. The NIST definition of cloud computing; http://www.nist.gov/itl/cloud/upload/cloud-defv15.pdf
Pearson, S. A. (2009). Charlesworth, Accountability as a way Forward for Privacy Protection in the Cloud, Computing, Vol.5931, Springer.131-144.
Rabkin, I. Stoica, and M. Zaharia(2010). A view of cloud computing. ommunications of theACM (53). 8-50.
Welten, R.J.W. (2009). Towards the cloud-The role of trust and perceived privacy risk on the adoption of cloud computing. Master Thesis, Tilburg University, Netherlands.18-30.
Singh, M. Hemalatha, (2012). Cloud Computing for Academic Environment. International Journal of Information and Communication Technology Research. 2. 2. 97-101.
Tianfield, H, (2011). "Cloud Computing Archtectures", 2011 IEEE International Conference on Systems, Man, and Cybernetics (SMC), PP.1394-1395.
Velte, Toby, Velte, Anthony, & Elsenpeter, Robert. (2010). Cloud Computing.a practical approach: McGraw-Hill, Inc.855-870.
Wentao Liu. (2012). Research on Cloud Computing Security Problem and Strategy, in: 2nd International Conference on Consumer Electronics. Communications and Networks (CECNet.1216-1219.
Winkler, J.R, (2011). Securing the Cloud: Cloud Computer Security Techniques and Tactics, Technical EditorBill Meine, Elsevier Publishing.
Zissis. D. and D. Lekkas, (2011). "Securing e-Government and e-Voting with an open cloud computing architecture," *Government Information Quarterl y*, vol. 28, pp. 239-251.

استناد به این مقاله:

قنبرزاده، مهناز؛ زارعی، عاطفه (زودآیند). رایانش ابری، ابزاری برای همکاری در محیط مجازی: نگرانی کاربران، امنیت اطلاعات و حفظ حریم خصوصی. *مطالعات ملی کتابداری و سازماندهی اطلاعات*.