

رایانش ابری¹ ابزاری برای همکاری در محیط مجازی²: نگرانی کاربران، امنیت اطلاعات و حفظ حریم خصوصی

مهناز قنبرزاده³

عاطفه زارعی⁴

تاریخ دریافت: 95/07/26

تاریخ پذیرش: 95/10/14

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 مورد بررسی قرار گرفته شده است.

روش‌شناسی: روش این پژوهش، پیمایش - توصیفی است و با استفاده از پرسشنامه محقق‌ساخته، دیدگاه و نظرات 67 نفر از دانشجوی تحصیلات تکمیلی مقطع دکترای علوم پایه ورودی 93-94 پژوهشگاه ملی مهندسی ژنتیک و زیست‌فناوری گردآوری شده است. با استفاده از نرم‌افزار اس.پی.اس.اس⁵ نسخه 22 به سؤالات و آزمون‌های پژوهش پاسخ داده شده است و پاسخ‌ها نیز با آمار توصیفی و استنباطی تجزیه و تحلیل شده‌اند.

یافته‌ها: وفاداری خدمت‌گراها نسبت به داده‌ها و اطلاعات کاربران از اهمیت بالایی برخوردار است؛ گرچه آن‌ها تلاش‌هایی را در جهت کاهش نگرانی‌های کاربران و جذب اعتماد آن‌ها انجام می‌دهند؛ ولی اطلاعات و حفظ حریم خصوصی در محیط ابری از امنیت کمتری برخوردار است.

نتیجه‌گیری: با توجه به نگرانی و دغدغه‌های نسبت به حفظ حریم خصوصی و امنیت اطلاعات نتایج نشان می‌دهد، که کاربران استفاده بسیار اندکی از خدمات ارائه شده توسط خدمات‌گرهای ابری می‌کنند.

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 دانش‌شناسی، دانشگاه آزاد اسلامی واحد همدان Atefehzareei@gmail.com

⁵ SPSS

فناوری رایانش ابری اخیراً یکی از مهم‌ترین مباحث توسعه نظام‌های اطلاعات مطرح شده است (لین و دیگران¹، 2014)؛ به طوری که آورام² در سال 2014 میلادی، رایانش ابری را به صورت مدل جدیدی برای میزبانی و ارائه خدمات در اینترنت مطرح کرده است. این فناوری نوین نظام‌های اطلاعاتی، دسترسی به منابع محاسباتی تجمیعی و مشترک قابل پیکربندیرا آسان و فراگیر کرده است. در رایانش ابری، قابلیت‌های فناوری اطلاعات به منزله خدماتی عرضه می‌شود که بدون نیاز به دانش دقیق از فناوری‌های زیرساختی و کمترین تلاش مدیریتی در دسترس قرار می‌گیرد (صدرالساداتی و کارگر، 1391). به گونه‌ای که با توجه به قابلیت‌ها و خدمات فناوری رایانش ابری، آن را به منزله یک نوآوری مهم در تبادل اطلاعات و حوزه‌ای که در آن، سرمایه‌گذاری گسترده‌ای انجام گرفته، شناخته‌اند (آرمبراست³ و دیگران، 2010).

مؤسسه ملی فناوری و استانداردهای آمریکا⁴: رایانش ابری، مدلی برای دسترسی پذیری آسان کاربران از طریق شبکه به مجموعه‌ای از منابع رایانشی قابل تغییر و قابل پیکربندی (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 فراهم‌کننده خدمات به سرعت فراهم شده یا آزاد (رها) شود. رایانش ابری به معنی توسعه و به کارگیری فناوری رایانه بر مبنای اینترنت است؛ در واقع، قابلیت‌های رایانه‌ای به صورت 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.

رایانش ابری برای صرفه‌جویی در هزینه‌های سرمایه‌گذاری اولیه نیز مورد استفاده قرار گرفته است. در اپ‌باکس⁵ و گروپ‌آن⁶، نمونه‌هایی برای کاربردهای روزمره از رایانش ابری است. 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 جو⁷، 2011).

در این فناوری، کاربران می‌توانند از طریق خدمات عرضه‌شده رایانش ابری و ابزارهای مختلف به برنامه‌ها، فضاهای ذخیره‌سازی، پردازش، و حتی سکوها توسعه برنامه‌های کاربردی در اینترنت دسترسی داشته باشند. خدمات فراهم‌شده از طریق رایانش ابری از نوع ابزار محاسباتی⁸ است، و به این معنا که خدمات مورد استفاده کاربران در سرورها عرضه می‌شود و پرداخت‌ها، همانند سایر خدمات عمومی (مثل برق و آب) بر اساس میزان استفاده انجام می‌شود (فتوتی، 1393).

¹ Lian et al.

² Avram

³ Armbrust et al.

⁴ National Institute of Standard Technology (NIST)

⁵ Dropbox

⁶ Groupon

⁷ Lee Hong Joo

⁸ Utility Computing

سه مدل اصلی ارائه خدمت در محاسبات ابری عبارتند از:

سس¹: عرضه‌کننده به منزله خدمت، همه برنامه‌های کاربردی که بر روی ابر کار می‌کنند و خدمتی مستقیم را به مشتریان عرضه می‌کنند، در این لایه قرار می‌گیرند. نرم‌افزار به‌منزله خدمت، این امکان را می‌دهد تا به نصب و راه‌اندازی برنامه روی سامانه کاربر نیازی نباشد. ویژگی اصلی این برنامه، دسترسی بر پایه شبکه به‌منظور مدیریت متمرکز و از راه دور است (جادیجا، مؤدی²، 2012). در این لایه، عرضه‌کننده خدمت، مسئول امنیت فیزیکی است. کاربر نیز قادر به مدیریت زیرساخت‌های ابر مانند شبکه، سرورها، فضاهای ذخیره‌سازی، سیستم‌عامل و حتی برنامه‌های کاربردی با اختیارات محدود است (وینکلر³، 2011)؛ در این لایه، عرضه‌کننده خدمت به‌منظور عرضه خدمات بهتر به کاربران باید اجزای امنیتی زیر را فراهم کند (تیانفیلد⁴، 2011): امنیت داده‌ها، امنیت شبکه، یکپارچگی داده‌ها، تجزیه‌کردن داده‌ها، دسترسی به داده‌ها، مکان‌یابی داده‌ها، احراز هویت و اصالت، محرمانه‌بودن داده‌ها، امنیت نرم‌افزار، نقض داده، مجازی‌سازی، دسترس‌پذیری، پشتیبان‌گیری، مدیریت هویت و روند ثبت‌نام (ملکشاهی، حقانی و حقانی، 1392).

پاس⁵: سکو به‌منزله خدمت، که اگر یک لایه بالاتر ببینیم، با این بخش روبه‌رو خواهیم شد. چیزی که با عنوان سکو در اینجا از آن یاد شده، به دو محیط متفاوت برمی‌گردد: محیط توسعه نظام و محیط اجرای آن. این لایه میزبان محیط‌های مختلف برای عرضه خدمات است. سکو به‌منزله خدمت، فراهم‌کننده بستری برای پیاده‌سازی نرم‌افزارهای موردنیاز و درواقع پشتیبانی از چرخه حیات نرم‌افزار برای کاربر است (زیسایس و لیکاس⁶، 2011). در این لایه، هم کاربر و هم عرضه‌کننده خدمت، هر دو در برقراری امنیت سهیم هستند. کاربر، برنامه کاربردی تحت زیرساخت ابر را تهیه می‌کند؛ اما قادر به مدیریت زیرساخت‌های ابر با کنترل نرم‌افزار بر روی شبکه‌ها و سرورها و فضاهای ذخیره‌سازی نیست (وینکلر، 2011)؛ کاربر قادر به کنترل مدیریت برنامه کاربردی است و هرگونه تدابیر امنیتی برای میزبان و جلوگیری از نفوذ و تضمین در دسترس‌نبودن داده‌های برنامه کاربردی بر عهده عرضه‌کننده خدمت است (ملکشاهی، حقانی و حقانی، 1392).

ایس⁷: ساختار به‌منزله خدمت، در فضای ابری، استفاده از منابع محاسباتی زیرساختی از قبیل تجهیزات ذخیره‌سازی، شبکه‌ها و سرورها برای عرضه خدمات به کاربران نهایی استفاده می‌شود. کاربران نهایی می‌توانند نرم‌افزارهای دلخواه از قبیل سیستم‌های عامل و نرم‌افزارهای کاربردی را پیاده‌سازی و اجرا کنند؛ آمازون بی.سی.28، نمونه‌ای از آن‌ها است. مشتری، زیرساخت پایه‌ای را کنترل نمی‌کند؛ اما معمولاً می‌تواند ماشین‌های

¹ SaaS

² Jadeja & Modi

³ Winkler

⁴ Tianfield

⁵ PaaS

⁶ Zissis & Lekkas

⁷ IaaS

⁸ Amazon EC2

مجازی را با سیستم‌عامل‌های انتخابی که وی مدیریت می‌کند راه‌اندازی نماید (صدرالساداتی و کارگر، 1391).

از سوی دیگر این فناوری، شانس بزرگی برای سازمان‌های بزرگ و شرکت‌های فناوری اطلاعات در کشورهای توسعه‌یافته است؛ اما این فرصت‌ها با چالش‌هایی مانند امنیت نیز روبه‌رو است (منسف و گیگادو¹، 2011). در واقع 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 را 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 خواهند آورد (ملکشاهی، حقانی و حقانی، 1392).

نتایج حاصل از نظرسنجی شرکت آی.دی.سی.² از 244 مدیر فناوری اطلاعات نشان داده‌است که در بین 9 چالش اساسی مطرح در حوزه رایانش ابری، امنیت بزرگ‌ترین چالش است که با کسب 74/5 درصد، مقام نخست دغدغه‌های مدیران سازمان‌ها را به خود اختصاص داده است.

در صنعت فناوری اطلاعات مهم‌ترین عامل موفقیت یک نظام، حفظ امنیت اطلاعات است (ساجدوا³، 2010). یک نظام محاسبات ابری باید در تمامی جنبه‌ها امنیت داشته باشد که بسیاری از این جنبه‌ها به تنظیمات ابر مربوط می‌شود (رایان⁴، 2013)؛ بنابراین برای ساخت یک نظام امن باید موضوعاتی از جمله طراحی معماری امن، به حداقل رساندن سطوح حمله، جلوگیری از نفوذ هکرها و کنترل دسترسی به داده‌ها در نظر گرفته شود (ملکشاهی، حقانی و حقانی، 1392)؛ بنابراین مدل‌های امنیتی در خدمات محاسبات ابری باید با قوانین و مقررات ملی مطابقت داشته باشند؛ این مقررات و قواعد در ابتدا به منظور محافظت از اطلاعات است که می‌تواند برای شناسایی افراد از آن استفاده شود (پیرسون، 2009). 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 داخل سازمان و در مقابل متولی داده (تأمین‌کننده) خارج از سازمان قرار دارد و این یک چالش برای کنترل دسترسی به داده ایجاد می‌کند.

علاوه بر چالش‌های فوق مزایای محاسبات ابری عبارتند از: کیفیت خدمت، قابلیت اطمینان، مدیریت از راه دور، کاهش هزینه، کارایی، قابلیت اعتماد و شهرت؛ البته محاسبات ابری دارای معایبی نیز هست؛ از جمله وابسته بودن توان پردازشی به پهنای باند، امنیت حریم خصوصی، و حفظ و نگهداری داده‌ها (ماتیس⁵، 2011).

¹ Monsef & Gigado

² International Data Corporation (IDC)

³ Sachdeva

⁴ Ryan

⁵ Mathise

پژوهش‌های پیشین نیز نشان داده‌است، محاسبات ابری همواره با چالش‌هایی روبه‌رو بوده‌است که امنیت اطلاعات و حفظ حریم خصوصی از مهم‌ترین آن‌ها است و ارائه‌دهندگان این فناوری باید سعی در کاهش نگرانی‌های کاربران خود و جذب آن‌ها داشته باشند و راهکارهایی برای استفاده از این محیط ارائه کنند. این موضوع در مقاله‌های باغشاهی و دیگران (1391)، (صدرالساداتی، کارگر، 1393)، هاشمی¹ (2013)، ویتا² (2012)، زهیر تایر³ (2014) ادوارد جی. آمروسو⁴ (2014) بیان شده‌است. در بررسی‌های (صدرالساداتی، کارگر، 1393)، باغشاهی و دیگران (1391) رایانش ابری را به‌منزله یک ابزار دسترسی آسان و کم‌هزینه در فضای مجازی⁵ تلقی شده‌است که سازمان‌ها می‌توانند با استفاده از آن، توانایی بهره‌وری و صرفه‌جویی در منابع فناوری اطلاعات و افزایش توان محاسباتی را فراهم نمایند. زهیر تایر (2014) و ادوارد جی. آمروسو (2014) فضای ابری را سرورهای مجازی‌سازی، پایگاه داده و برنامه‌های کاربردی معرفی می‌کنند و آن را یک پایگاه⁶ مستعد برای اشتراک‌گذاری داده‌های بزرگ دانسته‌اند.

دانشگاه‌ها و مؤسسات آموزش عالی از جمله مراکزی هستند که برای همکاری و تبادل اطلاعات علمی از فضای مجازی، به‌ویژه رایانش ابری، استفاده می‌کنند. در این مراکز، تعداد قابل توجهی از کاربران فضاهای مجازی را دانشجویان تحصیلات تکمیلی تشکیل می‌دهند. مطالعات و مقالات در موضوع رایانش ابری به‌صورت مروری و تحلیلی ارائه شده است. بر همین اساس بر آن شدیم تا پژوهشی در زمینه شناسایی امنیت اطلاعات و حفظ حریم خصوصی افراد برای همکاری در محیط ابری را از دیدگاه دانشجویان مقطع دکتری علوم پایه ورودی 93-94، پژوهشگاه ملی مهندسی ژنتیک و زیست‌فناوری انجام دهیم؛ بنابراین، پژوهش حاضر در صدد برآمد تا دیدگاه آنان را در استفاده از رایانش ابری برای همکاری در فضای مجازی بررسی کند. در این راستا پاسخ به پرسش‌های زیر مدنظر گرفت:

- 1- استفاده از کدام یک از ابزارهای رایانش ابری بیشتر است؟
- 2- کدام یک از مؤلفه‌های پذیرش و بهره‌گیری از فناوری رایانش ابری از اهمیت بیشتری برخوردار است؟
- 3- کدام یک از مؤلفه‌های ویژگی‌های محیط ابری از اهمیت بیشتری برخوردار است؟

فرضیه‌های پژوهش

- 1- پذیرش و بهره‌گیری فناوری رایانش ابری بیشتر از حد متوسط است.
- 2- اهمیت ویژگی‌های ابری و هر یک از مؤلفه‌های آن بیشتر از حد متوسط است.

¹ Hashemi

² Wentao

³ Zahir Tari

⁴ Edward G. Amoroso

⁵ Cyberspace

⁶ Platform

روش‌شناسی

در پیمایش حاضر، کل جامعه آماری 100 نفر دانشجوی مقطع دکتری علوم پایه ورودی 93-94 پژوهشگاه ملی و مهندسی ژنتیک و زیست‌فناوری بودند که با استفاده از فرمول کوکران 79 نفر به عنوان نمونه انتخاب شدند. ابزار جمع‌آوری داده‌ها، پرسشنامه پژوهشگرساخته است. در مجموعه 100 پرسشنامه توزیع شده، 67 پرسشنامه جمع‌آوری شد. داده‌های گردآوری شده با استفاده از نرم‌افزار اس.پی.اس.اس. نسخه 22 و پرسش‌های پژوهش با استفاده از آمار توصیفی و فرضیه‌ها با آمار استنباطی تحلیل شدند. برای پاسخ به پرسش‌های پژوهش از شاخص‌های میانه و میانگین بهره گرفته شده است. میانه برای سنجش وضعیت کیفیت گویه‌ها و میانگین برای رتبه‌بندی کردن آنهاست. با توجه به طیف لیکرت و رتبه‌ای بودن داده‌ها، حد وسط این طیف یعنی عدد 3 ملاک سنجش وضعیت است، اگر میانه بیش از 3 باشد وضعیت مطلوب، برابر 3 متوسط و کمتر از 3 نامطلوب است؛ از آنجاکه داده‌ها نیز رتبه‌ای هستند از میانگین رتبه‌ای موجود در آزمون فریدمن استفاده می‌شود. با آزمون تی تک‌نمونه‌ای فرضیه‌ها تحلیل می‌شوند. پیش از تعیین روش آماری مناسب برای تحلیل، فرضیه نرمال بودن مشاهدات به صورت استنباطی با استفاده از آماره کلموگروف-اسمیرنوف، بررسی شد. پایایی پرسشنامه نیز از طریق محاسبه ضریب آلفای کرونباخ محاسبه شد که بیش از 0/7 به دست آمد؛ بنابراین پرسشنامه در این پژوهش دارای قابلیت اعتماد است.

پژوهشگاه ملی مهندسی ژنتیک و زیست‌فناوری

یافته‌ها

پرسش 1. استفاده از کدام یک از ابزارهای رایانش ابری بیشتر است؟

جدول 1. توزیع فراوانی و درصد استفاده از ابزارهای فناوری رایانش ابری

درصد	فراوانی	ابزارهای رایانش ابری
25/4	17	Drop Box
19/4	13	Google Drive
67/2	45	Gmail
0/0	0	SkyDrive
3/0	2	Box
100/0	67	کل

داده‌های جدول 1 نشان می‌دهد Gmail با 67/2 درصد (45 نفر) بیشترین ابزار مورد استفاده در میان ابزارهای فناوری رایانش ابری است.

پرسش 2. کدام یک از مؤلفه‌های پذیرش و بهره‌گیری از فناوری رایانش ابری از اهمیت بیشتری برخوردار است؟

جدول 2. توزیع فراوانی و درصد پذیرش و بهره‌گیری دانشجویان مقطع دکتری علوم پایه از فناوری رایانش ابری

میانگین	میانه	بسیار کم	کم	متوسط	زیاد	بسیار زیاد	مؤلفه‌های پذیرش و بهره‌گیری از فناوری رایانش ابری	
							فراوانی	درصد
2/84	2	22	16	16	8	4	فراوانی	میزان استفاده
		32/8	23/9	23/9	11/9	6/0	درصد	
2/84	2	18	21	20	8	0	فراوانی	دریافت اطلاعات
		26/9	31/3	29/9	11/9	00/0	درصد	
3/07	2	14	19	22	11	0	فراوانی	مزایا و امکانات
		20/9	28/4	32/8	16/4	00/0	درصد	
4/27	3	5	11	21	17	13	فراوانی	آموزش و یادگیری از طریق رایانش ابری
		7/5	16/4	31/3	25/4	19/4	درصد	
5/14	4	1	5	11	17	33	فراوانی	وفاداری فضای رایانش ابری
		1/5	7/5	16/4	25/4	49/3	درصد	
2/84	2	15	24	21	5	2	فراوانی	آشنایی با قوانین و مقررات رایانش ابری
		22/4	35/8	31/3	7/5	3/0	درصد	

داده‌های جدول 2 نشان‌دهنده آن است که با میانه 4 (بیشتر از حد متوسط) و بیشترین میانگین، 5/64، کاربران وفاداری فضای رایانش ابری زیاد ارزیابی کرده‌اند. آموزش و یادگیری آنها از فضای ابری متوسط است و در سایر موارد کم است. کمترین مؤلفه با میانه 2 و میانگین 2/84 مربوط به میزان استفاده کاربران از فناوری رایانش ابری، دریافت اطلاعات از فضای رایانش ابری و میزان آشنایی با قوانین و مقررات رایانش ابری است.

پرسش 3. کدام یک از مؤلفه‌های ویژگی‌های محیط ابری از اهمیت بیشتری برخوردار است؟

برای پاسخ به این پرسش، وضعیت هر یک از گویه‌های مؤلفه‌های ویژگی‌های محیط ابری در جدول‌های 3 تا 5 بررسی شدند و در نهایت خود مؤلفه‌ها در جدول 6 رتبه‌بندی شدند.

جدول 3. توزیع فراوانی و درصد همکاری در محیط مجازی

میانگین	میانه	بسیار کم	کم	متوسط	زیاد	بسیار زیاد	همکاری در محیط مجازی	
							فراوانی	درصد
2/31	3	3	11	23	20	10	افزایش همکاری در	افزایش اشتراک اطلاعات
		4/5	16/4	34/3	29/9	14/9	فراوانی	درصد
2/07	3	8	13	20	17	9	افزایش انگیزه همکاری	در اشتراک دانش
		11/9	19/4	29/9	25/4	13/4	فراوانی	درصد
1/62	3	18	13	21	10	5	ترغیب به استفاده از	رایانش ابری
		26/9	19/4	31/3	14/9	7/5	فراوانی	درصد

داده‌های جدول 3 بیانگر آن است که با میانه 3، هر سه گویه همکاری در محیط مجازی از وضعیت یکسانی برخوردار است و با میانگین 2/31 گویه افزایش همکاری در اشتراک اطلاعات از اهمیت بیشتری برخوردار است.

جدول 4. توزیع فراوانی و درصد امنیت و حفظ حریم خصوصی

میانگین	میانه	بسیار کم	کم	متوسط	زیاد	بسیار زیاد	امنیت و حفظ حریم خصوصی	
							فراوانی	درصد
2/66	3	15	10	12	15	15	تبادل اطلاعات	امنیت در انتقال اطلاعات
		22/4	14/9	17/9	22/4	22/4	فراوانی	درصد
2/31	3	11	12	23	17	4	امنیت در ذخیره اطلاعات	امنیت در انتقال اطلاعات
		16/4	17/9	34/3	25/4	6	فراوانی	درصد
2/48	3	9	10	22	16	10	امنیت در ذخیره اطلاعات	امنیت در عرضه‌کنندگان
		13/4	14/9	32/8	23/9	14/9	فراوانی	درصد
2/56	3	8	10	25	15	9	امنیت در عرضه‌کنندگان	خدمات ابری و مراکز داده
		11/9	14/9	37/3	22/4	13/4	فراوانی	درصد

داده‌های جدول 4 نشانگر آن است که گویه‌های امنیت و حفظ حریم خصوصی نیز از وضعیت متوسطی برخوردار هستند و گویه تبادل اطلاعات با میانگین 2/66 اهمیت بیشتری دارد.

جدول 5. توزیع فراوانی و درصد حفظ امنیت اطلاعات

میانگین	میانہ	بسیار کم	کم	متوسط	زیاد	بسیار زیاد	حفظ امنیت اطلاعات	
							فراوانی	درصد
2/37	3	10	22	27	7	1	فراوانی	امنیت برای اطلاعات شخصی
		14/9	32/8	40/3	10/4	1/5	درصد فراوانی	
2/43	3	14	14	26	13	0	فراوانی	امنیت برای حریم خصوصی فیزیکی
		20/9	20/9	38/8	19/4	0	درصد	
2/53	3	12	26	17	12	0	فراوانی	امنیت برای حریم خصوصی ارتباطی
		17/9	38/8	25/4	17/9	0	درصد	
2/66	3	11	13	32	9	2	فراوانی	امنیت برای حریم خصوصی محیطی
		16/4	19/4	47/8	13/4	3	درصد	

داده‌های جدول 5 گویای آن است که با میانہ 3 نیز هر چهار گویه حفظ امنیت اطلاعات در حد متوسط هستند. گویه امنیت برای حریم خصوصی محیطی با میانگین 2/66 از اهمیت بالاتری برخوردار است.

جدول 5. میانگین مؤلفه‌های ویژگی‌های محیط ابری

میانگین	مؤلفه‌های ویژگی‌های محیط ابری
2/16	همکاری در محیط مجازی
2/05	امنیت و حفظ حریم خصوصی
1/78	حفظ امنیت اطلاعات
0/025	سطح معنی‌داری

جدول 5 که اصلی برای پاسخ به پرسش سوم پژوهش است با سطح معنی‌داری کمتر از 0/05 آزمون فریدمن گویای آن است که میان این سه مؤلفه ویژگی‌های محیط ابری اختلاف وجود دارد و با میانگین بیشتر 2/16 همکاری در محیط مجازی از اهمیت بیشتری برخوردار است؛ پس از آن به ترتیب، امنیت و حفظ حریم خصوصی و حفظ امنیت اطلاعات با میانگین‌های 2/05 و 1/78 قرار دارند.

فرضیه 1. پذیرش و بهره‌گیری فناوری رایانش ابری بیشتر از حد متوسط است.

جدول 6. آمار تک‌نمونه‌ای پذیرش و بهره‌گیری از فناوری رایانش ابری

تعداد	میانگین واقعی	میانگین مفروض
67	14/35	18
پذیرش و بهره‌گیری از فناوری رایانش ابری		

جدول 7. آزمون تک‌نمونه‌ای پذیرش و بهره‌گیری از فناوری رایانش ابری

مقدار آزمون تی	درجه آزادی	سطح معنی‌داری	اختلاف میانگین		برآورد فاصله‌ای	
			حد پایین	حد بالا	حد پایین	حد بالا
-9/05	66	0/00	-3/64	-4/44	-2/83	
پذیرش و بهره‌گیری از فناوری رایانش ابری						

از آنجایی که پذیرش و بهره‌گیری از رایانش ابری دارای توزیع نرمال است، برای تفسیر آن از آزمون تی تک‌نمونه‌ای/تک گروهی استفاده می‌کنیم. این آزمون، زمانی استفاده می‌شود که می‌خواهیم آن را با یک حالت معمول و رایج، استاندارد و یا حتی یک عدد فرضی و مورد انتظار مقایسه کنیم (حبیب‌پورگتابی و صفری‌شالی، 1388، 538). عدد مفروض در اینجا، ضرب تعداد سؤالات پذیرش و بهره‌گیری از فناوری رایانش ابری (6 پرسش) در 3 (حد وسط طیف لیکرت) است که برابر عدد 18 می‌شود، که این مقدار با میانگین واقعی مقایسه می‌شود. در تفسیر نتایج این آزمون همواره باید به اختلاف این دو میانگین یا اختلاف میانگین¹ و مقدار آزمون تی توجه کرد. هر چه تفاوت بین دو میانگین بیشتر باشد مقدار تی نیز بیشتر خواهد بود و هر چه اختلاف میانگین بیش‌تر باشد، سطح معنی‌داری کوچک‌تر (کوچک‌تر از 0/05) خواهد بود. توجه به مقادیر فاصله اطمینان (برآورد فاصله‌ای) در آزمون‌های تی، به تفسیر بهتر نتایج آزمون کمک می‌کند. در این برآورد، با توجه به مقادیر حد بالا² و حد پایین³، باید گفت که:

هرگاه حد پایین و بالا مثبت باشد، میانگین مورد انتظار از مقدار آزمون بزرگ‌تر است و تفاوت میانگین معنی‌دار است.

هرگاه حد پایین و بالا منفی باشد، میانگین از مقدار آزمون کوچک‌تر است و تفاوت میانگین معنی‌دار است.

هرگاه حد پایین منفی و حد بالا مثبت باشد، میانگین با مقدار مورد آزمون تفاوت معنی‌دار ندارد (حبیب‌پورگتابی و صفری‌شالی، 1388، 538).

¹ Mean Difference

² Upper

³ Lower

مقدار آزمون تی تک‌نمونه‌ای (9/05-) در جدول 7، نشان می‌دهد که با اطمینان 95 درصد و سطح خطای کوچک‌تر از 0/05 تفاوت معنی‌داری بین دو میانگین واقعی و مفروض وجود ندارد؛ هم‌چنین حد پایین و بالا هر دو منفی است؛ بنابراین میانگین از مقدار آزمون کوچک‌تر و تفاوت میانگین معنی‌دار نیست. ضمن آنکه براساس جدول 6، مقدار میانگین واقعی (14/35) از مقدار میانگین مفروض (18) بزرگتر است؛ بنابراین فرضیه موجود تأیید نشد و پذیرش و بهره‌گیری از فناوری رایانش ابری کمتر از حد متوسط است؛ چنانچه، میانه اغلب گویه‌های آن نیز برابر 2 بود.

فرضیه 2. اهمیت ویژگی‌های ابری و هر یک از مؤلفه‌های آن بیشتر از حد متوسط است.

جدول 8. آمار تک‌نمونه‌ای ویژگی‌های محیط ابری و مؤلفه‌های آن

میانگین مفروض	میانگین واقعی	تعداد	مؤلفه‌های ویژگی‌های محیط ابری
9	9	67	همکاری در محیط مجازی
12	12/16	67	امنیت و حفظ حریم خصوصی
12	10/31	67	حفظ امنیت اطلاعات
33	31/47	67	ویژگی‌های محیط ابری

جدول 9. آزمون تک‌نمونه‌ای ویژگی‌های محیط ابری و مؤلفه‌های آن

برآورد فاصله‌ای		اختلاف	سطح	درجه	مقدار	مؤلفه‌های ویژگی‌های محیط ابری
حد بالا	حد پایین	میانگین	معنی‌داری	آزادی	آزمون تی	
0/63	-0/63	0/00	1/00	66	0/00	همکاری در محیط مجازی
1/17	-0/84	0/16	0/74	66	0/32	امنیت و حفظ حریم خصوصی
-0/87	-2/49	-1/66	0/00	66	-4/16	حفظ امنیت اطلاعات
0/309	-3/35	-1/52	0/1	66	-1/66	ویژگی‌های محیط ابری

الف. ویژگی‌های محیط ابری

• همکاری در محیط مجازی

مقدار آزمون تی تک‌نمونه‌ای (0/00) در جدول 9، نشان می‌دهد که با اطمینان 95 درصد و سطح خطای بالاتر از 0/05 (سطح معنی‌داری 0/1) تفاوت معنی‌داری بین دو میانگین واقعی و مفروض وجود ندارد؛ ازسویی، حد پایین و بالا یکی مثبت و دیگری منفی است؛ ازاین‌رو، میانگین با مقدار مورد آزمون تفاوت معنی‌دار ندارد؛ لذا، فرضیه موجود تأیید نمی‌شود. در جدول 7، میانگین واقعی برابر میانگین مفروض است؛ بنابراین اهمیت همکاری در محیط مجازی متوسط است.

• اطمینت و حفظ حریم خصوصی

مقدار آزمون تی تک‌نمونه‌ای (0/32) در جدول 9، مبین آن است که با اطمینان 95 درصد و سطح خطای بالاتر از 0/05 (سطح معنی‌داری 0/74) تفاوت معنی‌داری بین دو میانگین واقعی و مفروض وجود ندارد؛ از طرفی، حد پایین و بالا یکی مثبت و دیگری منفی است؛ بنابراین، میانگین با مقدار مورد آزمون تفاوت معنی‌دار ندارد؛ از این رو، فرضیه موجود تأیید نمی‌شود. در جدول 7، میانگین واقعی تقریباً برابر میانگین مفروض است؛ لذا، اهمیت اطمینت و حفظ حریم خصوصی متوسط است.

• حفظ اطمینت اطلاعات

مقدار آزمون تی تک‌نمونه‌ای (4/16-) در جدول 9، نشانگر آن است که با اطمینان 95 درصد و سطح خطای کوچک‌تر از 0/05 تفاوت معنی‌داری بین دو میانگین واقعی و مفروض وجود ندارد؛ از سویی، حد پایین و بالا هر دو منفی است؛ از این رو، میانگین از مقدار آزمون کوچکتر و تفاوت میانگین معنی‌دار نیست. ضمن آنکه براساس جدول 8، مقدار میانگین واقعی (10/31) از مقدار میانگین مفروض (12) کوچکتر است؛ بنابراین فرضیه موجود تأیید نشد و اهمیت حفظ اطمینت اطلاعات کم است.

ب. بررسی ویژگی‌های محیط ابری

مقدار آزمون تی تک‌نمونه‌ای (1/66) در جدول 9، مبین آن است که با اطمینان 95 درصد و سطح خطای بالاتر از 0/05 (سطح معنی‌داری 0/74) تفاوت معنی‌داری بین دو میانگین واقعی و مفروض وجود ندارد؛ از طرفی، حد پایین و بالا یکی مثبت و دیگری منفی است؛ بنابراین، میانگین با مقدار مورد آزمون تفاوت معنی‌دار ندارد؛ از این رو، فرضیه موجود تأیید نمی‌شود. در جدول 7، میانگین واقعی (31/47) کمتر از میانگین مفروض (33) است؛ لذا، اهمیت ویژگی‌های ابری متوسط است؛ چنانچه مؤلفه‌های آن نیز، از اهمیت متوسطی برخوردار بودند.

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 استفاده کم کاربران از محیط ابری برای دریافت اطلاعات آنها بر این باور هستند که این خدمتگرها نسبت به کاربران خود وفادار می‌باشند و این موضوع از اهمیت ویژه‌ای برای ارائه‌دهندگان خدمات ابری برخوردار است. هم‌چنین به منظور آشنایی بیشتر با مزایا و امکانات این ابزارهای نوین فناوری نیاز به آموزش است. از طرفی دیگر کاربران با قوانین و مقررات موجود در محیط ابری آشنایی کمی دارند. همان‌طور که باغشاهی و دیگران، صدرالساداتی، کارگر، هاشمی، ویتتاو، زهیر تاپر، 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. نتایج پژوهش حاضر نشان می‌دهد که رایانش ابری بیشترین تأثیر را بر همکاری‌های محیط مجازی در هنگام اشتراک اطلاعات داشته است، و کمترین تأثیر را در امنیت و حریم خصوصی بر امنیت اطلاعات داشته است. خدمتگرهای رایانش ابری در حال گسترش فضای امن با مزایای و امکانات بسیار برای کاربران خود هستند تا بتوانند تعهدات و افزایش وفاداری‌شان را نسبت به کاربران خود نشان بدهند و در همه زمینه‌ها اعتماد آنها را خود جذب کنند. از طرفی دیگر برای کاربران در حریم خصوصی، حفظ ارتباطات شخصی و حریم خصوصی، در محیط ابری از اهمیت بسیار بالایی برخوردار است. نتایج پژوهش نشان می‌دهد که پذیرش و بهره‌گیری از فناوری رایانش ابری کمتر از حد متوسط است؛ همکاری در محیط مجازی و امنیت و حفظ حریم خصوصی متوسط ارزیابی شده است؛ ویژگی‌های رایانش ابری از اهمیت متوسطی برخوردار بوده است.

منابع

- باغشاهی، سمیه سلطان... و [دیگران] (1391). تحلیل چالش‌های امنیتی و تأثیر آن بر رایانش ابری. اولین کارگاه ملی رایانش ابری ایران، 10، 11 آبان. دانشگاه صنعتی امیرکبیر، دانشکده مهندسی کامپیوتر و فناوری اطلاعات. 8-2.
- بنی‌رستم، حمید، هدایتی، علیرضا، خادم‌زاده، احمد (1392). ارائه رویکردهای نوین برای مقابله با چالش‌های امنیتی رایانش ابری. دومین کنفرانس توسعه کاربردهای صنعتی اطلاعات، ارتباطات و محاسبات، تبریز 8 و 9 آبان. 6-2.
- شرکت اینفوامن (1391). نگرانی، تهدیدها و کنترل‌های امنیتی در پردازش ابری. خبرنامه، شماره 9. 6-1.
- شرکت مدل‌سازان «مسنا» (1393). مروری بر پردازش ابری - گونه‌های پردازش ابری. <http://masna.blog.ir>.
- صدرالساداتی، محسن، کارگر، محمدجواد (1391). 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. 10-1.
- فتوتی، عباس (1393). آشنایی با رایانش ابری (فناوری کلاد). <http://laitec.sharif.ir>.
- ملکشاهی، عاطفه، خاکسار حقانی، شهرزاد، خاکسار حقانی، مهسا (1391). 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. 7-1.
- نقیان فشارکی، مهدی، طباطبایی، غلامحسن، تمناجی، مصطفی (1393). ارائه معماری مرجع امنیتی محیط رایانش ابر خصوصی سازمان. فصلنامه علمی پژوهشی امنیت پژوهی، 47 (13). 113-91.
- یعقوبی، نور محمد، شکوهی، جواد، جعفری، حمیرضا (1393). شناسایی و رتبه‌بندی عوامل کلیدی مؤثر بر به‌کارگیری رایانش ابری در سلامت الکترونیک. فصلنامه علمی - پژوهشی پژوهشنامه پردازش و مدیریت اطلاعات. 30 (2). 570-547.
- 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 Computing. *International Journal of Security, Privacy and Trust Management (IJSPTM)*. 1 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. International 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 Architectures", 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 Editor Bill Meine, Elsevier Publishing,.
- Zissis. D. and D. Lekkas, (2011). "Securing e-Government and e-Voting with an open cloud computing architecture," Government Information Quarterly, 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.