بررسی نقش امنیت به‌عنوان مهم‌ترین چالش در بکارگیری رایانش ابری در سازمان‌ها

یوسف ترابی گلسفید

دکتری تخصصی، استادیار دانشکده علوم و فنون چالوس، دانشگاه امام حسین(ع)، ایران

Yousef.torabi@chmail.ir

(تاریخ دریافت ۹۴/۷/۱۴؛ تاریخ پذیرش ۹۵/۱/۲۷)

چکیده:

در اواخر اولین دهه قرن ۲۱ دنیای IT شاهد شکوفایی فنّاوری جدیدی به نام رایانش ابری بوده است و شرکت‌های پیشرو در صنعت فناوری اطلاعات سعی در بکارگیری آن در فرآیندهای خدمات خود به مشتریان داشته‌اند، به‌طوری‌که برترین این شرکت‌ها امروزه از رایانش ابری به‌عنوان یک مزیت رقابتی مهم نسبت به شرکت‌های هم‌پایه‌ی خود استفاده می‌کنند. این فنّاوری نسبتاً جدید علیرغم چالش‌های بسیار مهم ، به‌سرعت در حال رشد و توسعه است. در ابتدای ظهور آن، بسیاری از محققان تصور می‌کردند که رایانش ابری به‌زودی فراگیر خواهد شد ولی تحقیقات اخیر حاکی از آن است که امنیت بزرگ‌ترین سد پیش روی این فناوری است.

در این پژوهش سعی شده است تا حدی به بررسی چالش‌های امنیتی این فنّاوری پرداخته و اینکه چرا مسئله امنیت باعث عدم استقبال کاربران و مدیران IT از این فناوری گردیده است. در ابتدا به مقدمه و تعریف رایانش ابری پرداخته سپس مزایا و منافع استفاده از آن و همچنین معایب و مشکلات امنیتی در آن بیان‌شده و در نهایت یک تجزیه‌وتحلیل امنیتی برای آن ارائه شده است.

واژه‌های کلیدی:

رایانش ابری – امنیت - امنیت در رایانش ابری

Role of security as the biggest challenge in adopting cloud computing in organizations

Yousef Torabi Gelsefid

PhD, Assistant professor of Science and Technology of Chalus, University of Imam Hussein (AS), Iran

(Submitted: 2015/Oct/6; Accepted: 2016/Apr/15)

Abstract:

At the end of first decade of 21st century in IT world, we have seen the dehiscence of a new technology called cloud computing, leading companies in IT industry have tried to apply it as a customer service processes in which nowadays, the most superior of these companies use the cloud computing as an important competitive advantage to their equal companies. In spite of very important challenges, this relatively new technology, is growing and developing fast. At the advent of it, a lot of researchers thought that cloud computing will soon be comprehensive but recent research indicates that security is the biggest barrier facing this technology. In this study, it has been tried to investigate the security challenges of this technology and also why security caused lack of interest in IT managers and users of this technology. At first an introduction and definition of cloud computing will be discussed then the benefits and advantages of its use as well as its flaws and security problems have been expressed and finally a security analysis is submitted for it.

Key words:

cloud computing, security, security of cloud computing

۱- مقدمه

رایانش ابری نگاه متفاوتی است به اینترنت. تا این اواخر از اینترنت بیشتر در انتقال داده‌ها و بین ابزارهای متصل به اینترنت استفاده می‌شد و تقریباً تمام محاسبات و پردازش‌ها به‌صورت محلی روی کامپیوترهای کاربران یا سیستم‌های داخلی سازمان‌ها انجام می‌گرفت. در مدل رایانش ابری، اینترنت رسانه‌ی دسترسی به منابع و خدمات رایانشی بر روی سیستم‌هایی است که در نقاط جغرافیایی مختلف و تقریباً نامعینی مستقر هستند.

این مفهوم به اوایل سال ۱۹۶۱ برمی‌گردد، زمانی که پروفسور ژان مک کارتی پیشنهاد کرد که فناوری تسهیم زمانی رایانه[1] می‌تواند به آینده‌ای منجر شود که قدرت محاسبات و نرم‌افزارهای کاربردی خاص می‌توانند از طریق یک مدل کسب‌وکار صنایع همگانی[2] فروخته شوند[۱]. این ایده در اواخر همان دهه بسیار مشهود شد، اما در اواسط دهه‌ی ۱۹۷۰ معلوم شد فنّاوری‌های مبتنی بر فناوری اطلاعات روز قادر نیستند این‌چنین مدل محاسباتی مربوط به آینده را تقویت کنند.

با وجود این، زمانی که هزاره چرخید، این مفهوم جان تازه‌ای گرفت و فنّاوری رایانش ابری در چرخه‌های فناوری شروع به پدیدار شدن کرد.

۲- معرفی رایانش ابری

رایانش ابری مدلی است برای فراهم آوردن امکان دسترسی سلف‌سرویس و بنا به تقاضا به مجموعه‌ای از خدمات و منابع رایانشی مثل شبکه‌ها، سرویس‌دهنده‌ها، رسانه‌های ذخیره‌سازی و برنامه‌های کاربردی از طریق شبکه (اینترنت)، طوری که به‌سرعت و با حداقل دخالت تأمین‌کنندگان و فروشندگان، و متناسب با نیاز مصرف‌کنندگان بتواند تدارک دیده شده و در معرض استفاده قرار گیرد[۱]. این بدین معنی است که دسترسی به منابع فناوری اطلاعات در زمان تقاضا و بر اساس میزان تقاضای کاربر به‌گونه‌ای انعطاف‌پذیر و مقیاس‌پذیر از راه اینترنت به کاربر تحویل داده می‌شود. واژه‌ی «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. 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 و کاربران به وجود می‌آورد. به‌عنوان‌مثال آنچه یک ارائه‌دهنده‌ی 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 و اطلاعات روی سرورها ذخیره می‌گردند و بر اساس تقاضا در اختیار کاربران قرار می‌گیرد. جزئیات از دید کاربر مخفی می‌مانند و کاربران نیازی به تخصص یا کنترل در مورد فناوری زیرساخت ابری که از آن استفاده می‌کنند ندارند[۲].

۳- مزایا و منافع استفاده از رایانش ابری

چون مشتریان عموماً زیرساختی که در محیط‌های رایانش ابری استفاده می‌شود، را خود فراهم نمی‌کنند می‌توانند از مخارج زیاد رها شوند و منابع را به‌عنوان یک سرویس مصرف کنند، فقط با پرداختن بهای آن‌ها استفاده می‌کنند. ارائه‌های بسیاری از رایانش‌های ابری، به‌صورت محاسباتی همگانی و مدل صدور صورت‌حساب اتخاذ شده است که افراد بر پایه‌ی یک حق اشتراک صورت‌حساب دریافت می‌کنند.

به‌وسیله‌ی اشتراک گذاشتن قدرت محاسبات میان کاربران متعدد، نرخ بازدهی عموماً بهبود می‌یابد. زیرا سرورهای رایانش ابری برای عدم استفاده نمی‌خوابند. این عامل به‌تنهایی می‌تواند به‌طور قابل‌توجهی هزینه‌های زیرساخت را کاهش و سرعت توسعه نرم‌افزارهای کاربردی را افزایش دهد. اثر سودمند دیگر استفاده از این مدل آن است که ظرفیت (حجم) کامپیوتر به‌طور چشمگیری افزایش می‌یابد، چون مشتریان نیازی به اداره کردن نرم‌افزارهای کاربردی‌شان را در زمان اوج مصرف، هنگامی‌که بارگیری پردازش بسیار زیاد است، را ندارند. پذیرش مدل رایانش ابری به دلیل دسترسی بیشتر به پهنای باند پُرسرعت‌تر، توانمند خواهد بود[۳].

[1] Computer time- sharing technology
[2] Utility – type business model

اجاره‌ی چندگانه[3]، اشتراک منابع و هزینه را در میان تعداد زیادی کاربر قادر می‌سازد. مزایای عمده یک رویکرد اجازه چندگانه شامل:

۱- زیرساخت مرکزی و هزینه‌های کمتر.

۲- افزایش توانایی در زمان اوج مصرف.

۳- بهبود کارآیی برای سیستم‌هایی که اغلب همگانی هستند.

۴- تخصیص پویای CPU، ذخیره‌سازی و پهنای باند شبکه.

۵- عملکرد سازگار که به‌وسیله ارائه‌دهنده سرویس بررسی شده است[۴].

۴- چالش‌ها و ریسک‌های رایانش ابری

بزرگ‌ترین چالش‌های ارائه‌دهندگان ابر، امنیت ذخیره‌سازی داده‌ها، دسترسی پُرسرعت به اینترنت و استانداردسازی است. ذخیره‌سازی حجم زیادی داده مربوط به حریم خصوصی کاربران، هویت و اولویت‌های ویژه‌ی نرم‌افزاری در وضعیت‌های متمرکز، بسیاری از مسائل مربوط به حفاظت داده‌ها را افزایش می‌دهد. این مسائل به‌نوبه خود، تردیدهایی راجع به چارچوب‌های قانونی را ناشی می‌شود که بایستی در یک محیط مبتنی برابر پیاده‌سازی شوند.

چالش‌های دیگر در مدل رایانش ابری واقعیتی است که نفوذ کاوش پهنای باند در آمریکا، بسیار بیشتر از بسیاری از کشورهای اروپا و آسیا است. رایانش ابری، بدون ارتباطات پُرسرعت (باسیم و بی‌سیم) غیرقابل‌دفاع است. بدون پهنای باندهای پُرسرعت، سرویس‌های رایانش ابری نمی‌توانند در سطح وسیع در دسترس باشند.

نهایتاً، استانداردهای فنی استفاده‌شده برای پیاده‌سازی سیستم‌های کامپیوتری متنوع و نرم‌افزارهای کاربردی که برای کار رایانش ابری لازم است، ایجاد شوند هنوز کاملاً تعریف‌نشده، مورد بازنگری همگانی قرار نگرفته و بخش‌های پنهان آن به تصویب نرسیده است[۳].

زیرساخت به‌عنوان یک سرویس (IaaS)، خط‌مشی به‌عنوان یک سرویس (PaaS)، نرم‌افزار به‌عنوان یک سرویس (SaaS)، سه مدل کلی رایانش ابری هستند. هر یک از این مدل‌ها، اثر متفاوتی بر امنیت نرم‌افزار دارا هستند[۶]. با وجود این، در یک سناریوی نوعی جایی که یک نرم‌افزار در ابر میزبان است، دو سؤال متداول امنیتی را افزایش می‌دهد:

۱- امنیت داده چگونه است؟

۲- امنیت کد چگونه است؟

امنیت، قابلیت دسترسی و قابلیت اطمینان، موضوعات کیفیتی مهمی برای کاربران خدمات ابر هستند. جنز و دیگران[4] اشاره می‌کنند که امنیت یک چالش برجسته میان سایر چالش‌های کیفیتی است[۶].

بر طبق مقاله معماری‌های امنیتی برای رایانش ابری، کاربران احساس امینت و اطمینان دارند، زمانی‌که آنها واقعاً می‌فهمند که عملیات چطور در حال انجام و اجراشدن است. گرچه، رایانش ابری آسایش زیادی برای کاربران به‌وسیله‌ی رهاسازی آنها از نیاز به دانستن جزئیات فرآیندها فراهم می‌کند، کاربران را مجبور می‌کند به ارائه‌دهنده‌ی سرویس‌های ابری، کسی‌که نگران کاربران بسیاری است، اعتماد کنند. در بازار امروزه، آگاهی درباره‌ی مسائل رایانش ابری بیشتر به سمت مسائل قابلیت اطمینان و امینت سوق دارد. به‌عنوان‌مثال؛ در تحقیقی که توسط فوجیتسو اداره شد، با بررسی مسئله در رایانش ابری از نظر مشتری، معلوم گردید امنیت، عملیات پایدار، سیستم پشتیبانی و قابلیت اطمینان و ایمنی بالاترین رتبه‌ها را در نگرانی‌های کاربران دارند. در آن تحقیق نشان داده شده است که سیستم‌های فناوری اطلاعات رایانش ابری برای کاربران غیرمشهود است و قابل‌درک است که مشتریان قویاً می‌خواهند از اطلاعات‌شان به‌طور کامل محافظت شود و خدمات ارائه‌شده پایدار باشند. این نگرانی‌های ذیل به‌ویژه در بین مشتریان راجع به امنیت افزایش یافته است:

۱- داخل مرکز داده یکسان، موردهای متعددی وجود دارد که در آن اطلاعات به بیش از یک مشتری تعلق دارند و این اطلاعات بر روی کامپیوتر یکسانی مستقر شده‌اند. در این‌چنین مواردی، آیا چنین مجموعه‌های متفاوتی از اطلاعات به‌طور شایسته نگهداری می‌شوند؟

۲- آیا بایستی نگران باشیم که در یک مرکز داده، اطلاعات نشت پیدا کنند یا تحریف شوند؟

۳- چون خط‌مشی سیستم یک ارائه‌دهنده سرویس‌های ابری به‌وسیله انواع زیادی از محیط‌های مشتریان به

[3] Multi-tenancy

[4] Gens et.al.

اشتراک گذاشته‌شده، آیا قابلیت اطمینان نمی‌تواند یک مسئله باشد؟ برای مثال، اگر یک برنامه مخرب از جمله یک ویروس به خدمات نفوذ کند، آیا امکان ندارد که همه محیط‌هایی که از خدمات استفاده می‌کنند را تحت تأثیر قرار دهد؟

۴- زمانی که چندین سرویس ابری هم‌زمان استفاده می‌شوند تا کار را انجام دهند، ارتباط بین این وظایف سخت می‌شود. آیا قابلیت اطمینان سرویس تضمین شده است؟[۷]

۵- مزیت‌های امنیتی در محیط‌های ابری

ارائه‌دهندگان فعلی خدمات ابر، سیستم بسیار زیادی را به کار می‌گیرند. آنها پردازش‌های پیچیده و کارکنان خبره‌ای برای نگهداری سیستم‌هایشان دارند که شرکت‌های کوچک ممکن نیست به آنها دسترسی داشته باشند. به‌عنوان یک نتیجه، مزیت‌های امنیتی مستقیم و غیرمستقیمی برای کاربران ابر وجود دارد. در اینجا ما تعدادی مزیت‌های امنیتی کلیدی یک محیط رایانش ابری را معرفی می‌کنیم:

۱- تمرکز داده: در یک محیط ابر، ارائه‌دهنده‌ی سرویس مراقب مسائل ذخیره‌سازی است و شرکت‌های کوچک نیاز ندارند تا پول زیادی برای وسایل ذخیره‌سازی فیزیکی بپردازند. همچنین، ذخیره‌سازی مبتنی برابر، راهی برای متمرکز کردن سریع‌تر و به‌صورت بالقوه ارزان‌تر ارائه می‌کند. این به‌طور ویژه برای شرکت‌های کوچک مفید است که نمی‌توانند پول اضافی به متخصصان امنیتی برای نظارت بر داده‌ها بپردازند.

۲- واکنش رویداد: ارائه‌دهندگان زیرساخت به‌عنوان یک سرویس می‌توانند یک سرور قانونی اختصاصی بسازند که بر پایه زمان موردنیاز مورداستفاده واقع شود. تعدادی موارد سرمایه‌گذاری، یک پشتیبان از محیط می‌تواند به‌راحتی ایجاد شود و بر روی ابر بدون تأثیر گذاشتن بر مسیر معمولی شرکت قرار گیرد.

۳- زمان رسیدگی تصویر قانونی[5]: پیاده‌سازی‌های متعدد ذخیره‌سازی ابری، یک جمع مقابله‌ای یا خرد کردن پنهانی را نشان می‌دهد. برای مثال، آمازون S3، MD5[6] را ایجاد کرد که به‌صورت خودکار، هنگامی‌که شما یک شیء را ذخیره می‌کنید، خرد می‌کند[۷].

۴- واقعه‌نگاری: در یک پارادیم سنتی محاسبات، به‌صورت فراوان، واقعه‌نگاری اغلب یک چاره‌اندیشی پس از اتمام کار است. در یک ابر، نیاز ذخیره‌سازی برای ثبت استاندارد وقایع، به‌صورت خودکار حل شده است[۵].

طبق گزارش ENISA، محیط‌های رایانش ابری مزایای ذیل را دارند:

۱- امنیت و مزایای مقیاس: انواع اندازه‌گیری‌های امنیتی، هنگامی‌که در یک مقیاس وسیع پیاده‌سازی می‌شوند، ارزان‌تر هستند. این شامل انواع اندازه‌گیری‌های دفاعی از جمله فیلترینگ، مدیریت پچ و ...، می‌باشند. دیگر مزایای مقیاس شامل: موقعیت‌های چندگانه، واکنش بی‌وقفه به وقایع، مدیریت تهدید.

۲- امنیت به‌عنوان یک متمایزکننده بازار: نگرانی عمده برای بسیاری از مشتریان ابر، بحث امنیت است. بسیاری از مشتریان بر اساس شهرت، گزینه‌هایی را به خاطر قابلیت اطمینان، یکپارچگی و انعطاف‌پذیری خریداری می‌کنند. این یک انگیزه قوی برای ارائه‌دهندگان است که اقدامات امنیتی خود را بهبود بخشند.

۳- واسط کاربر استانداردشده برای مدیریت کردن سرویس‌های امنیتی: فراهم‌کنندگان بزرگ ابر، می‌توانند یک میانجی کاربر منبع باز استاندارد شده را ارائه دهند تا فراهم‌کنندگان سرویس‌های امنیتی را مدیریت کند.

۴- پیمایش سریع و هوشمند منابع: توانایی ارائه‌دهندگان ابر برای تخصیص دوباره منابع به‌صورت پویا برای فیلترینگ، شکل‌دهی ترافیک، تعیین هویت، رمزگذاری و ... در اندازه‌گیری‌های دفاعی، مزایای واضحی برای انعطاف‌پذیری دارد.

۵- ممیزی و ارزیابی گردآوری‌ها: رایانش ابری می‌تواند تصاویر اختصاصی و قانونی برای هر میزان استفاده از ماشین‌های مجازی ارائه کند که بدون ایجاد زیرساخت‌ها در محیط آفلاین قابل دستیابی هستند، آنها به کاهش زمان برای تحلیل‌های قانونی منجر می‌شوند.

۶- معایب امنیتی در محیط‌های ابری

با وجود مزیت‌های امنیتی، پارادیم رایانش ابری همچنین تعدادی چالش‌های امنیتی کلیدی را معرفی می‌کند. در اینجا، ما تعدادی از این چالش‌های کلیدی را بیان می‌کنیم:

[5] Forensic Image Verification Time
[6] Message – Digest algorithm 5

۱- موقعیت داده: به‌طورکلی، کاربران ابر از موقعیت دقیق مرکز داده آگاه نمی‌شوند و همچنین آنها هیچ کنترلی بر مکانیزم‌های فیزیکی پردازش داده ندارند. بیشتر ارائه‌دهندگان معروف سرویس ابر، مراکز داده‌ای در نقاط مختلف دنیا دارند. ارائه‌دهندگان سرویس متعددی همچنین مزیتی برای مراکز داده‌ای جهانی‌شان دارند. با وجود این، در بسیاری از موارد، نرم‌افزارهای کاربردی و داده‌ها ممکن در کشوری ذخیره شوند، که می‌توانند مسائل قضایی داشته باشد. برای مثال، اگر داده کاربر در کشور x ذخیره شود، سپس ارائه‌دهندگان سرویس، در معرض نیازمندی‌های امنیتی و الزامات قانونی کشور x قرار گیرند. این موارد ممکن است اتفاق بیافتد درحالی‌که کاربر، اطلاعاتی از این مسائل ندارد.

۲- بازجویی: بازجویی یک فعالیت غیرقانونی در محیط‌های ابر، می‌تواند غیرممکن باشد. سرویس‌های ابر، خصوصاً مشکل است بازجویی شوند، زیرا داده‌ها برای کاربران متعدد در یک مکان قرار می‌گیرند و می‌تواند همچنین در بین مراکز داده منتشر شده باشند. کاربران، دانش اندکی در مورد توپولوژی شبکه محیط تحت استفاده دارند. ارائه‌دهنده‌ی سرویس نیز می‌تواند مواقعی بر امنیت شبکه کاربران سرویس اعمال کند.

۳- تفکیک داده‌ها: داده در ابر، نوعاً در یک محیط به اشتراک گذاشته‌شده، با داده سایر مشتریان است. رمزگذاری نمی‌تواند به‌عنوان یک راه‌حل خاص برای مسائل تفکیک داده فرض شود. در موقعیت‌های متعددی، مشتریان نمی‌خواهند داده‌ها را رمزگذاری کنند زیرا موردی باشد که هنگامی‌که رمزگذاری می‌شود، داده‌ها تخریب شوند.

۴- قابلیت دوام بلندمدت: ارائه‌دهندگان سرویس باید ایمنی داده‌ها را در موقعیت‌های در حال تغییر کسب‌وکار از جمله ادغام‌ها و مالکیت‌ها تضمین کنند. مشتریان باید به قابلیت دسترسی به داده‌ها در این موقعیت‌ها مطمئن شوند. ارائه‌دهنده سرویس ابر بایستی ایمنی داده‌ها در شرایط بد کسب‌وکار مانند طولانی شدن قطع برق را تضمین کنند.

۵- سرورهای به خطر افتاده: در موقعیتی که یک سرور به خطر می‌افتد، کاربران نیاز دارند سرورهای خود را ببندند تا زمانی که آنها یک پشتیبان از داده‌ها دریافت کنند. این دلایل نگرانی‌های قابلیت دسترسی با بیشتر خواهد کرد.

۶- مطلوبیت منظم: ارائه‌دهندگان قدیمی سرویس ابر در معرض نفوذ ممیزی‌های خارجی و گواهی‌های امنیتی هستند. اگر یک ارائه‌دهنده‌ی سرویس ابری به این ممیزی امنیتی وفادار نباشند، آن به کاهش آشکار در اعتماد مشتریان منجر می‌شود.

۷- بازیافت: ارائه‌دهندگان سرویس ابر باید امنیت داده در حوادث طبیعی و ساخته دست بشر را تضمین کنند[۸].

۷- رایانش ابری و سازمان‌ها

یکی از تحلیل‌گران مؤسسه IDC که در ماه فوریه ۲۰۰۹ در انجمن پردازش ابری IDC سخنرانی کرد، می‌گوید: «مهم‌ترین نگرانی سازمان‌هایی که تمایل دارند از سرویس‌های ابری استفاده‌کنند، امنیت اطلاعات است. بر اساس اظهارات IDC، حدود ۷۵ درصد از مدیران IT نگران امنیت سرویس‌های پردازش ابری هستند.»

به‌منظور درک علت باید مشکلات امنیتی را به بخش‌های کوچک‌تر تجزیه کنیم. در سازمان‌هایی که از سرویس‌های پردازش ابری استفاده می‌کنند، تمام مشکلات امنیتی در سه گروه اصلی جای می‌گیرند:

- امنیت پلتفرمی که در اقامتگاه سرویس‌دهنده‌ی ابری قرار دارد.
- امنیت ایستگاه‌های کاری (نقاط انتهایی) که در اقامتگاه کلاینت‌ها قرار دارد.
- امنیت داده‌هایی که از نقاط انتهایی به پلتفرم ارسال می‌شود.

آخرین نگرانی امنیتی یادشده که همان امنیت داده‌ای انتقالی است، عملاً با استفاده از تکنیک‌های کدگذاری، اتصالات ایمن و VPN حل شده است. تقریباً تمام سرویس‌های جدید ابری از این سازوکارها پشتیبانی می‌کنند و امروزه انتقال اطلاعات از نقاط نهایی به پلتفرم‌ها در یک فرآیند کاملاً ایمن انجام می‌گیرد.

۸- مشکلات امنیتی مربوط به اعتبارسنجی و کارکرد سیستم

امروزه، بزرگ‌ترین کابوس مدیران IT وجود مشکلات امنیتی مربوط به عملکرد پلتفرم‌های سرویس‌دهنده است. برای اغلب این افراد، یافتن شیوه مناسبی برای تأمین

امنیت سیستمی که امکان کنترل مستقیم آن وجود ندارد، فرآیند ساده‌ای نیست. پلتفرم سرویس‌های ابری به شکل یک سیستم متمرکز در مرکز داده سازمان نیست، بلکه، اغلب در یک دیتاسنتر ناشناخته در کشوری نامعلوم قرار گرفته است. به‌عبارت‌دیگر، اصلی‌ترین مشکل امنیتی پردازش ابری از وجود اشکال در اعتبار و اعتبارسنجی سرویس‌دهندگان ناشی می‌شود و در واقع دنباله همان مشکلاتی است که در جریان محول کردن بخشی از امور سازمان‌ها به تأمین‌کنندگان خارجی بروز می‌کند؛ متخصصان و مدیران سازمان‌ها با محول کردن امور حیاتی مانند تأمین امنیت اطلاعات کاری خود به تأمین‌کنندگان خارجی نامأنوس هستند. به هر حال می‌توان مطمئن بود که این مشکل نیز مانند مشکلات قبلی مربوط به تفویض اختیار انجام امور داخلی سازمان‌ها به تأمین‌کنندگان متفرقه رفع شده و تمام نگرانی‌های موجود درباره امنیت منابع از بین می‌رود.

حال این اظهارات بر چه اساسی است؟ پیش از هر چیز، تأمین امنیت مرکز داده‌ای که دربرگیرنده‌ی منابع پردازشی هستند، برای سرویس‌دهندگان بسیار ساده‌تر است. علت این امر ویژگی توزیع‌شدگی (مقیاس) پردازش ابری است. از آنجا که سرویس‌دهندگان، خدمات خود را به تعداد زیادی از کاربران عرضه می‌کنند، امکان تأمین امنیت تمام کاربران را به‌طور هم‌زمان دارند و در نتیجه می‌توانند از رویکردهای امنیتی مؤثرتر و پیچیده‌تر بهره بگیرند. البته، شرکت‌های گوگل و مایکروسافت نسبت به شرکت‌های کوچک و حتی مؤسسات بزرگی که از مراکز داده اختصاصی استفاده می‌کنند، منابع و امکانات بیشتری را برای تأمین امنیت اطلاعات در اختیار دارند.

دوّم این‌که استفاده از سرویس‌های ابری بین سازمان‌های مشتری و سرویس‌دهنده‌ی همواره بر اساس کیفیت موردتوافق طرفین در قراردادهایی انجام می‌شود که تمام مسئولیت‌های سرویس‌دهنده را در رابطه با مشکلات امنیتی پیش‌بینی کرده‌اند. سوّم این‌که ادامه کار سرویس‌دهندگان به‌طور مستقیم به سوابق کاری آنان مربوط است و به همین دلیل، همواره سعی می‌کنند امنیت اطلاعات را در بالاترین سطح ممکن تأمین کنند.

مشتری‌های پلتفرم‌های ابری علاوه بر مشکلات اعتباری و ارزیابی اعتبار، در مورد مشکلات امنیتی مربوط به نحوه‌ی عملکرد سیستم‌های ابری نیز نگرانی‌هایی دارند. با وجود این‌که بسیاری از سیستم‌های خانگی (در نتیجه تکامل درازمدت) از این ویژگی برخوردارند، هنگام استفاده از سرویس‌های ابری، اوضاع بسیار پیچیده‌تر می‌شود.

مؤسسه‌ی تحقیقاتی گارتنر در یک مقاله کوتاه با عنوان «ارزیابی خطرات امنیتی پردازش ابری» به بررسی هفت مورد از مهم‌ترین مشکلات امنیتی سرویس‌های ابری می‌پردازد. اغلب این مشکلات به نحوه‌ی عملکرد سیستم‌های ابری مربوط می‌شوند. مؤسسه گارتنر به‌ویژه بررسی سیستم‌های ابری را از جنبه‌های توزیع حق دسترسی به اطلاعات، قابلیت‌های بازیابی اطلاعات، پشتیبانی‌های تحقیقی و بازبینی‌های دوره‌ای توصیه می‌کند.

آیا محدودیتی وجود دارد که پیاده‌سازی عملی این ویژگی‌ها را غیرممکن کند؟ پاسخ قطعاً منفی است. هر اقدامی که امکان انجام آن در یک سازمان وجود دارد، انجام آن توسط یک سیستم ابری نیز امکان‌پذیر است. اصولاً مشکلات امنیتی به نحوه طراحی محصولات و سرویس‌های ابری بستگی دارند. پیش از ورود به بحث امنیت پلتفرم‌های پردازش ابری باید مشکلات قانونی و ممیزی مهمی را برطرف کنید. مشکل زمانی بروز می‌کند که تفکیک اطلاعات بین کلاینت یک سرویس‌دهنده در یک محیط ابری انجام می‌شود و این تفکیک معمولاً فرآیند اطمینان از رعایت قوانین مدون و استانداردها را پیچیده‌تر می‌کند. با وجود این‌که مشکل مذکور بسیار بااهمیت است، شکی وجود ندارد که این مشکل نیز دیر یا زود حل می‌شود. از یک‌طرف با توسعه پردازش ابری، فناوری‌های مورداستفاده برای نظارت بر اجرای قوانین نیز بهبود می‌یابد. از طرف دیگر قانون‌گذاران پیچیدگی‌های فنی محیط پردازش ابری را در قوانین جدی در نظر می‌گیرند.

۹- کاربران رایانش ابری در سازمان‌ها

در یک «دنیای ابری» ایده‌آل از آنجا که اطلاعات درون تجهیزات ذخیره نمی‌شود، امنیت پردازش ابری در سطح پلتفرم و از طریق ارتباط با تجهیزات جانبی تأمین می‌شود. این مدل هنوز برای استفاده عملی مناسب نیست و اطلاعاتی که به پلتفرم می‌رسد، در حقیقت، در نقاط انتهایی سیستم ساخته، پردازش و ذخیره می‌شود.

به این ترتیب، به نظر می‌رسد، تجهیزات جانبی محیط‌های ابری همواره درگیر مشکلات امنیتی خواهند بود. در حقیقت، بر اساس یک تئوری قوی‌تر این مشکلات به مرور زمان وخیم‌تر هم می‌شوند. اغلب تهدیدات امنیتی از جانب شبکه جهانی و ورود به زیرساخت سازمانی کلاینت ایجاد می‌شوند. در سیستم خانگی مشکل اصلی هنگام تعامل با پلتفرم بروز می‌کند، اما در محیط ابری نقاط انتهایی محافظت نشده دچار مشکلات امنیتی می‌شوند. چنان‌که پیش از این گفته شد، سطح امنیتی پلتفرم‌های ابری جهانی مانند گوگل و مایکروسافت به دلیل بهره‌مندی از امکانات و قابلیت‌های بسیار زیاد، متخصصان حرفه‌ای و منابع نامحدود بسیار بالاتر از سطح امنیتی است که توسط سیستم‌های مستقل سازمانی تأمین می‌شود. به همین دلیل، مهاجمان خارجی از بی‌نتیجه ماندن حمله‌های خود نسبت به سرویس‌دهندگان حفاظت‌شده اطمینان دارند. در نتیجه، مجرمان دنیای مجازی حمله‌های خود را متوجه تجهیزات جانبی دنیای ابری می‌کنند. مفهوم اصلی پردازش ابری که شامل دسترسی همیشگی و بدون محدودیت مکانی به یک پلتفرم است، احتمال وقوع چنین وقایعی را افزایش می‌دهد.

با بررسی تعداد حمله‌ها به کامپیوترهایی که در نقاط انتهایی سیستم قرار دارند، سرویس‌های امنیتی اطلاعات سازمانی باید به‌گونه‌ای تغییر کنند که بتوانند از تجهیزات جانبی محیط ابری محافظت کنند. انجام این کار برای تأمین امنیت اطلاعات سازمانی حیاتی است. جوزف توبولسکی مدیر بخش پردازش ابری در مؤسسه Accenture می‌گوید: «تصور می‌کنم بسیاری از اعتراضاتی که نسبت به پردازش ابری مطرح شده است، ریشه‌های احساسی دارد و در واقع نوعی عکس‌العمل افراد نسبت به این فناوری است.»

داگ منافی مدیرعامل Shumacher Group نیز با جنبه‌های احساسی موضوع آشنایی دارد. او می‌گوید: «بخش IT شرکت با فهرستی حاوی صد مورد از اقلام موردنیاز امنیتی به سراغ من آمدند. با دیدن فهرست به خود گفتم، اغلب این موارد حتی در دیتاسنتر اختصاصی ما نیز وجود ندارد.» تصمیم‌گیری درباره‌ی استفاده از پردازش ابری مانند رانندگی با یک اتومبیل برای نخستین بار است. از یک‌طرف احتمالاً بسیاری از آشنایان شما این مرحله را پشت‌سر گذاشته‌اند، اما از طرف دیگر وارد شدن به یک بزرگراه شلوغ برای اولین بار، می‌تواند تجربه ترسناکی باشد. به‌ویژه اینکه هر روز در خبرها داستان‌های وحشتناکی درباره‌ی تصادفات اتومبیل به گوش می‌رسد. با تمام این اوصاف، رانندگی در بزرگراه خطرناک‌تر از نوشیدن قهوه در یک قطار در حال حرکت یا ایستادن در ایستگاه اتوبوس نیست.

وضعیت پردازش ابری شباهت زیادی به وضعیت استفاده از نرم‌افزارها به شیوه سنتی دارد. محیط ابری نیازمند توجه به امنیت اطلاعات است، اما کاملاً مطمئن هستیم که برای مشکلات فعلی، راه‌حل‌های مناسبی وجود دارد. در مورد امنیت محیط ابری، نکات مهمی وجود دارد که اصولاً اولویت‌های متفاوتی (از حفاظت محیطی گرفته تا محافظت از تجهیزات جانبی) دارند. با وجود این، اگر توسعه‌دهندگان ابزارهای تأمین امنیت اطلاعات، شرکت‌ها را در حل این مشکلات یاری کنند، محیط ابری آینده‌ای روشن خواهد داشت.

۱۰- نتیجه‌گیری

امنیت در رایانش ابری مزایا و معایبی دارد که در این مقاله برخی از آنها بیان شد حال باید دید کی و کجا از آن استفاده می‌شود، باید سنجید ریسک استفاده از آن تا چه حد است و در صورت استفاده از آن تا چه حد امنیت به مخاطره می‌افتد، نقض امنیت داده‌ها و از دست رفتن داده‌ها خطرات کاملاً روشنی در این باره هستند. فناوری رایانش ابری در حال رشد و تکامل است و هنوز در مورد بسیاری از مسائل از جمله بعضی پتانسیل‌های این فناوری توافقی حتی در جامعه IT وجود ندارد.

منابع:

[1] Anthes, G., "Security in the cloud," Communications of the ACM, vol. 53, no. 11, 2010, pp. 16-18.

[2] Armbrust, M., Fox, O., Griffith, R., Joseph, A. D., Katz, Y., Konwinski, A., and Zaharia, M., "Above the clouds: a Berkeley view of cloud computing, 2009.

[3] Rittinghouse, J. W., and Ransome, J. F., Cloud computing: implementation, management, and security," CRC press., 2009.

[4] Catteddu, D., "Cloud Computing: benefits, risks and recommendations for information

security, in Web Application Security," Springer Berlin Heidelberg, pp. 17-17.
[5] "Craig Balding;" ITG2008 World Cloud Computing Summit, 2008.
[6] Gens, F., "New IDC IT Cloud Services Survey: Top Benefits and Challenges," IDC eXchange, 1 August 2015.
Available: http://blogs.idc.com/ie/?p=730
[7] Okuhara, M., Shiozaki, T., and Suzuki, T., "Security architecture for cloud computing," Fujitsu Sci. Tech. J, vol. 46, no. 4, 2010, pp. 397-402.
[8] Sangroya, A., Kumar, S., Dhok, J., and Varma, V. "Towards analyzing data security risks in cloud computing environments," In Information Systems, Technology and Management, Springer Berlin Heidelberg, 2010, pp. 255-265.