5th International Conference on Modern Research's in MANAGEMENT, ECONOMICS & ACCOUNTING
Saint Petersburg RUSSIA 28 July 2016
پنجمین کنفرانس بین‌المللی پژوهش‌های نوین در مدیریت، اقتصاد و حسابداری
۷ مردادماه ۱۳۹۵
سن پترزبورگ - روسیه

مدیریت مخاطره‌های مالی در ابر

رسول بهره مند
۱- دانشجوی کارشناسی ارشد دانشگاه شاهد
r.bahrehmand@shahed.ac.ir
امین اله مه آبادی
۲- عضو هیئت علمی گروه کامپیوتر، دانشگاه شاهد
Mahabadi@shahed.ac.ir

چکیده

این روزها رایانش‌ابری در حال تبدیل شدن به یک شعار شناخته شده‌است. شرکت‌های زیادی مانند: آمازون، گوگل، مایکروسافت و غیره، در توسعه سیستم‌های رایانش‌ابری، و افزایش سرویس‌هایشان برای ارایه به تعداد بیشتری از کاربران شتاب گرفته‌اند. هرچند مسائل مربوط به امنیت و حریم خصوصی، یک مانع قوی برای کاربران برای انطباق با سیستم‌های رایانش‌ابری ایجاد می‌کنند. هدف از نگارش این گزارش ارائه یک مرور جامع از وضعیت جاری و مشکلات امنیتی و مالی در موسسات مالی از قبیل بانک‌ها در محیط‌های ابری است. ما در اینجا پس از ارایه توضیحاتی پیرامون رایانش‌ابری، ویژگی‌ها، معماری، انواع، و مسایل مرتبط دیگر مخاطرات امنیتی و مالی را مورد بررسی قرار می‌دهیم. ۸ بعد امنیتی داریم که اینها مهمترین مشخصه‌ی نشان دهنده امنیت و حریم‌خصوصی (شامل دسترسی‌پذیری، محرمانگی، جامعیت‌داده، شفافیت، پاسخگویی، کنترل، تضمین و ممیزی) هستند. علاوه بر این، مزایا و معایب ورود صنعت به ابر را نیز بررسی می‌کنیم. در ادامه به دنبال ارائه تصویری از حرکت یکی از محیط‌های مالی به سمت ابر را بررسی می‌کنیم. هدف ما در پایان این تحقیقات این است که آیا محیط‌های مالی به سمت ابر بروند؟ اگر جواب مثبت است چه قسمت‌هایی از محیط و داده‌های ما قابلیت انتقال به ابر را دارند.

واژگان کلیدی: رایانش ابر، مخاطره‌مالی در ابر، مخاطره مالی در بانک، دسته‌بندی مخاطره‌های مالی، مزایای ابر.

مقدمه

امروزه تقریباً در تمامی کاربردهای علمی و مهندسی استفاده از رایانه‌ها امری اجتناب‌ناپذیر می‌باشد. هرچند که در سال‌های اخیر پیشرفت‌های سریع در فنّاوری ساخت رایانه‌ها پاسخگوی بسیاری از نیازهای قدیمی بوده‌است، اما روند روبه‌رشد حجم محاسبات علمی به‌خصوص در کاربردهایی که نیازمند محاسبات پیچیده و یا درگیر با داده‌های فراوان می‌باشند، توان پردازش بیشتری را طلب می‌کند. مدل رایانش‌ابری بر پایه‌ی شبکه‌های رایانه‌ای مانند اینترنت است که الگویی تازه برای عرضه، مصرف و تحویل خدمات رایانشی (شامل زیرساخت، نرم‌افزار، بستر و سایر منابع رایانشی) با به کارگیری شبکه ارایه می‌کند. دلیل تشبیه اینترنت به ابر در این است که اینترنت همچون ابر جزئیات فنی‌اش را از دید کاربران پنهان می‌سازد و لایه‌ای از انتزاع را بین این جزئیات فنی و کاربران به وجود می‌آورد. یکی از ویژگی‌های رایانش ابری داشتن انواع مدل می‌باشد که این خود به مشتریان ابر این اجازه را می‌دهد که انتخاب گسترده‌ای داشته باشند: ابر عمومی، ابر خصوصی، ابر ترکیبی و ابر انجمنی (NIST, 2014). برای ابر سرویس‌های زیادی وجود دارد که در اینجا به سه عدد از مهمترین سرویس‌ها اشاره شده‌است: زیرساخت به عنوان خدمات، چارچوب(یا بستر) به عنوان خدمات و نرم افزار به عنوان خدمات (NIST, 2014)، (Amazon, 2014)، (Microsoft, 2014) و (صادق زاده و بهره پور ، ۱۳۹۱).مزایای اصلی رایانش ابری عبارتند از: چابکی، هزینه، نابستگی به دستگاه و مکان، چند مستاجری، قابلیت اطمینان، مقیاس پذیری، امنیت، نگهداری و سنجش پذیری.

بررسی مهم‌ترین مخاطرات بانک‌ها

در جدول ۱ اصلی‌ترین مخاطرات بانک‌ها درمحیط رایانش‌ابری قرار دارند و با توجه به بررسی و مصاحبه با کارشناسان این مخاطرات با توجه به اهمیت آنها امتیازدهی شده‌اند. این مخاطرات با مطالعه مقالات، مجلات و پایان‌نامه‌های بسیاری جمع‌آوری شده‌اند.

نتایج نشان می‌دهد که مخاطره‌های ۱، ۲، ۵، ۶، ۹ و ۱۵ نمره‌ی ۴,۴۵ را دارند که این نشان می‌دهد بانک در اتخاذ ابر تا حد زیادی با مخاطرات مواجه می‌شود و مخاطره ۳ نمره‌ی ۴,۳۵ را دارد که این هم تقریبا مخاطره تا حد زیاد را نشان می‌دهد. به هر حال مخاطره‌های ۴، ۷، ۸، ۱۰ و ۱۴ نمره‌ی بین ۲,۶۵ تا ۳,۲۳ را کسب کرده‌اند که این نمره نشان‌دهنده‌ی حد وسط مخاطره می‌باشد.

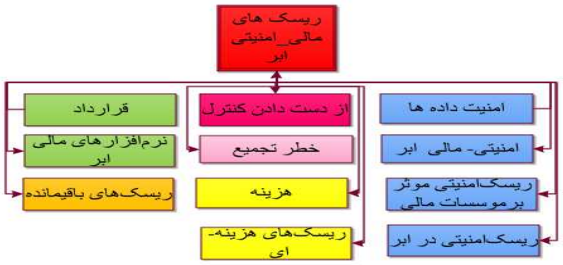
جدول ۱: امتیازدهی به مخاطره‌های بانکی

مخاطره‌های بانک‌ها درابر	نمره	خطا
۱- تا چه اندازه بانک شما با مخاطره Vendor Lock-in در اتخاذ رایانش ابری مواجه است؟	۴,۴۵۰۰	۰,۷۴۹۳۶
۲- تا چه اندازه بانک شما با مخاطره Loss of Governance در اتخاذ رایانش ابری مواجه است؟	۴,۴۵۰۰	۰,۷۴۹۳۶
۳- تا چه اندازه بانک شما با مخاطره Compliance Challenges در اتخاذ رایانش ابری مواجه است؟	۴,۳۵۰۰	۰,۷۳۵۵۴
۴- تا چه اندازه بانک شما با مخاطره Loss of Business Reputation در اتخاذ رایانش ابری مواجه است؟	۳,۲۲۵۰	۱,۱۴۳۲۶
۵- تا چه اندازه بانک شما با مخاطره Loss of Cloud Service termination or failure در اتخاذ رایانش ابری مواجه است؟	۴,۴۵۰۰	۰,۷۴۹۳۶
۶- تا چه اندازه بانک شما با مخاطره Availability of Services در اتخاذ رایانش ابری مواجه است؟	۴,۴۵۰۰	۰,۷۴۹۳۶
۷-تا چه اندازه بانک شما با مخاطره Resource Exhaustion در اتخاذ رایانش ابری مواجه است؟	۲,۹۵۰۰	۰,۷۱۴۳۲

۸- تا چه اندازه بانک شما با مخاطره Data transfer bottle necks در اتخاذ رایانش ابری مواجه است؟	۲,۹۵۰۰	۰,۷۱۴۳۲
۹- تا چه اندازه بانک شما با مخاطره Intercepting data in transit در اتخاذ رایانش ابری مواجه است؟	۴,۴۵۰۰	۰,۷۴۹۳۶
۱۰- تا چه اندازه بانک شما با مخاطره Distributed denial of service در اتخاذ رایانش ابری مواجه است؟	۲,۹۵۰۰	۰,۷۱۴۳۲
۱۱- تا چه اندازه بانک شما با مخاطره Subpoena and e-discovery در اتخاذ رایانش ابری مواجه است؟	۴,۴۵۰۰	۰,۷۴۹۳۶
۱۲- تا چه اندازه بانک شما با مخاطره Changesof jurisdiction در اتخاذ رایانش ابری مواجه است؟	۴,۴۵۰۰	۰,۷۴۹۳۶
۱۳- تا چه اندازه بانک شما با مخاطره Privacy Data در اتخاذ رایانش ابری مواجه است؟	۴,۳۵۰۰	۰,۷۳۵۵۴
۱۴- تا چه اندازه بانک شما با مخاطره Licensing در اتخاذ رایانش ابری مواجه است؟	۲,۶۵۰۰	۰,۴۸۳۰۵
۱۵- تا چه اندازه بانک شما با مخاطره enforcing contracts که خود آستانه‌ی حوزه‌های قضایی مختلف است (و از این‌رو در مخاطره‌های اجرایی این موضوع مشکل‌زا می‌باشد) در اتخاذ رایانش ابری مواجه است؟	۴,۴۵۰۰	۰,۷۴۹۳۶

دسته‌بندی مخاطرات

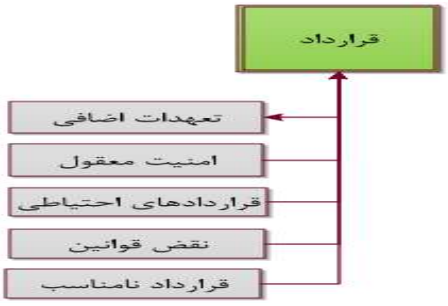
در شکل ۱ کلیه مخاطراتی بررسی شده مشاهده می‌شود. این دسته‌بندی مخاطرات را از ابعاد مختلف مورد ارزیابی قرار می‌دهد. در این مقاله فقط دسته مخاطرات قراردادی، نرم‌افزارهای مالی ابر، از دست دادن کنترل، خطر تجمیعی و هزینه مورد بررسی قرار کرفته‌اند.



شکل ۱: ریسک‌های مالی- امنیتی

مخاطرات قرارداد

یکی از مهمترین مخاطره‌هایی که اغلب در ابر نادیده گرفته می‌شود، مخاطره‌ای است که در هنگام قرارداد با ارائه‌کنندگان خدمات ابر نهفته است. در هنگام قرارداد مخاطره‌هایی وجود دارد که ما چند مورد از آنها را بررسی می‌کنیم (شکل۲). با توجه به بررسی‌های زیادی که صورت گرفته‌است احتمال رخ دادن این مخاطره بسیار زیاد است ولی اثر آن متوسط است. علت این مخاطره را می‌توان در فقدان منابع و تکنولوژی‌های استاندارد، انتخاب ارائه کننده‌ی ضعیف و همچنین شفافیت در نحوه‌ی تعامل و استفاده از منابع دانست. به طور کلی این یک مخاطره‌ی خطرناک می‌باشد که در هر سه سرویس مهم ابر (نرم‌افزار، چارچوب و زیرساخت) وجود دارد.



شکل۲: مخاطره‌ی قرارداد

تعهدات اضافی: همیشه مدیران مخاطره، با بخش‌های حقوقی در مورد شرایط قرارداد ارائه کنندگان‌ابر، همکاری می‌کرده‌اند تا دراصطلاح کمتر "فروشنده پسند[1]" باشد و همچنین تلاش می‌کردند تا هرگونه ضررهای ناشی از در اختیار گرفتن مسئولیت مالی بوسیله‌ی ارائه‌کنندگان ابر را کاهش دهند. اما ارائه‌کنندگان ابر هم معمولاً مایل به پرداخت غرامت نبوده‌اند، و همچنین

[1]vendor-friendly"

محدودیت‌های مسئولیتی و یا شرایط دیگر (به خصوص در بخش‌های حفظ حریم خصوصی و امنیت) را قبول نمی‌کردند. ارائه کنندگان ابر برای این کارشان دلایل زیادی دارند که بخواهند به آن استناد کنند، ولی شایع‌ترین آن این است که این تعهدات و وظایف اضافی، ارائه مدل با قیمت پایین را به چالش می‌کشد (یعنی اگر ارائه‌کنندگان ابر این وظایف را داشته باشند حتما هزینه‌هایی بابت همین وظایف و تعهدات اضافی بر سازمان تحمیل خواهند کرد) و همچنین به دلیل اینکه ارائه‌کنندگان ابر نمی‌دانند که داده‌های چه مشترکانی[۲] در ابر ذخیره شده است، آنها نمی‌توانند مسئول جداسازی را برگزینند و همچنین امنیت را تامین کنند.

امنیت معقول: صرف نظر از این دلایل، بسیاری از ارائه‌کنندگان ابر تمایلی به مخاطره‌های مالی قرارداد ندارند، آنها مخاطره‌ها را به مشترکان انتقال می‌دهند. شرایط نامطلوب در توافقنامه ابر ممکن است مخاطره مشتریان را افزایش دهد. تعاریف کلیدی که به عنوان مثال تعریفی از "حادثه امنیتی" را شامل می‌شوند، ممکن است تعهداتی که برای پاسخ مناسب و به موقع به حوادث و همچنین رسیدگی به الزامات قانونی مشتریان را داشته باشد، به اندازه کافی گسترده نباشند. بسیاری از ارائه کنندان ابر هنگامی که مشتریان بر روی الزامات ویژه‌ی اندازه گیری امنیت یا به طور عمومی و کلی تر "امنیت معقول[۳]" استاندارد پافشاری می‌کنند در امضای قرارداد عقب گرد می‌کنند.

قراردادهای احتیاطی: مشتریان ممکن است قراردادهای محدودی را با ارائه‌کنندگان فرعی برای ذخیره یا پردازش داده‌هایشان ببندند. اگر الزاماتی وجود نداشته باشد مشتریان پس از دو یا سه مرحله خودشان را در حالتی خواهد دید که به کلی از ارائه-کننده‌ی اولیه یا اصلی جداشده‌اند. شکست در پای این مذاکره (یعنی پاسخ مناسب به مسائل امنیتی و حقوق ارزیابی قانونی) می‌تواند خطر ابتلا به مخاطره را داشته باشد. در این خصوص، ارائه‌کنندگان ابر باید بیشتر مشتریان توجه کنند و مشتریان باید در به بدست آوردن هرچه بیشتر کنترل در مفاد قرارداد توجه کنند.

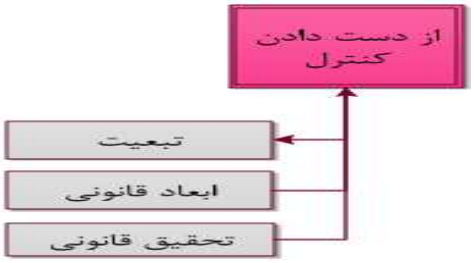
نقض قوانین: اگر یک ارائه کننده‌ی ابر از نقوضی که بر روی اطلاعات مشتریان اثر می‌گذارد، نگران باشد، و با این حال وظیفه‌ی خود که در قرارداد آمده‌است (یعنی توجه به نقوض، تعمیر و نگهداری) عمل نکند، در این صورت مشتری نمی‌تواند مخاطره-های قانونی و انطباق خود با تعهدات قانونی را کاهش دهد. در نهایت بدون قدرت چانه‌زنی و یا اهرم رقابتی برای ارائه‌کنندگان ابر، در پرداخت غرامت و همچنین در مساله نامحدود بودن مسئولیت‌ها در حفظ حریم شخصی و نقض داده‌ها بسیار سخت است که به توافق برسند.

قرارداد نامناسب: قراردادهای ارائه‌کنندگان ابر به طور معمول با محدودیت در دسترسی (هم در محدودیت‌های پولی و هم در خسارات سلب مسئولیت) آغاز می‌شود که این اغلب در پوشش ضرر و زیان بالقوه یک مشتری که در پی نقض داده‌ها بوسیله‌ی ارائه کننده‌ی ابرصورت می‌گیرد، ناکافی است. بدون رجوع به قرارداد مناسب، مشتریان خودشان را مسئول کامل نقوض داده‌ها می‌یابند که از نظر فنی تقصیر آنها نیست.

از دست دادن کنترل

یکی دیگر از مخاطره‌های قابل توجه که رایانش ابری ارائه می‌کند از دست دادن کنترل در انتقال داده‌ها به ابر و همچنین دسترسی به شبکه برون‌سپار می‌باشد. مثلا در یک محیط سنتی IT، سازمان توانایی این را دارد که سیستم‌های خود را ارزیابی و تنظیم کند به طوری که آنها با استانداردها و مقررات سازگاری داشته باشند (شکل۳). با توجه به بررسی‌های زیادی که صورت گرفته‌است احتمال رخ دادن این مخاطره زیاد و اثر آن هم بسیار زیاد است. علت این مخاطره را می‌توان در عدم وضوح نقش‌ها و مسئولیت‌ها، عدم وضوح صاحبان دارایی، فقدان منابع و تکنولوژی‌های استاندارد، انتخاب ارائه کننده‌ی ضعیف و همچنین ذخیره‌ی داده‌ها در چندین حوزه و فقدان شفافیت درباره‌ی آن دانست.

[2]data subscribers
[3]reasonable security



شکل ۳: مخاطره‌ی ازدست‌دادن کنترل

تبعیت: برای نمونه یک سازمان، داده‌ها را برای یک ارائه کننده‌ی ابر که عضو اتحادیه اروپا می‌باشد ارسال می‌کند، در نتیجه باید از الزامات حفاظت داده‌ها و راهنمایی‌های این اتحادیه تبعیت کند. اما یک سازمان را می‌توان ناسازگار تلقی کرد اگر اطلاعاتی را که به یک حوزه‌ی قضایی ارسال می‌کند قانون یا نقشی را نقض کند. از آنجایی که بسیاری از ارائه‌کنندگان ابر از انبارهای داده واقع در چندین حوزه‌ی قضایی استفاده می‌کنند، سازگاری باعث افزایش مخاطره می‌شود. چشم انداز نظارتی همیشه درحال تغییر، خود باعث افزایش مخاطره نقض می‌شود. وقایع اخیر در آژانس امنیت ملی و نگرانی در خارج از کشور ایالات متحده مانند شرکت های فناوری خارج از ایالات متحده، فقط باعث تقویت مخاطره های بالقوه شده اند.

ابعاد قانونی: یکی دیگر از مخاطره‌های کنترل بر داده که در ابر گسترش یافته است، بُعد قانونی داده می‌باشد. ممکن است یک نقض امنیتی در یک سیستم رخ بدهد، مهم است که از نظر قانونی تشخیص داده شود که چه داده‌هایی ممکن است به خطر بیافتند، اما ابر در این مورد با چالش‌هایی مواجه می‌باشد. اولین چالش، ارائه‌کننده‌ی ابر ممکن است دسترسی محدود داشته باشد یا حتی از نظر قانونی اجازه ورود به محیط ابر را نداشته باشد. مورد دوم، در یک ابر عمومی، داده‌های شما ممکن است با داده‌های دیگر شرکت‌ها آمیخته شود. مورد سوم، می‌تواند باعث افزایش چالش‌های قانونی مربوط به دسترسی به داده‌ها شود. داده‌های شما ممکن است با داده‌های سازمان (یا سازمان‌های دیگر) به اشتراک گذاشته شود که اگر این داده‌ها مربوط به مرکز سوم معتبر باشد باعث ایجاد محدودیت در دسترسی می‌شود.

تحقیق قانونی: یک کلید در محدودیت‌های قانونی و مخاطره‌های عملیاتی که مرتبط با نقض داده‌های ارائه‌کنندگان ابر است، توانایی مشتریان در انجام یک تحقیق قانونی به صورت مستقل می‌باشد، که به صورت سنتی شامل گرفتن یک تصویر از کامپیوترهایی است که به صورت بالقوه در معرض خطراند. به علاوه، از دست دادن کنترل نگرانی‌هایی از قبیل موارد زیر را نیز شامل می‌شود:

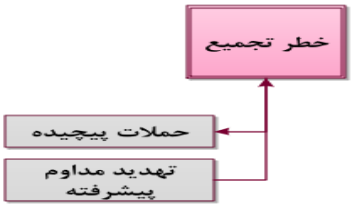
در محیط ابر، شما نمی‌توانید همسایگان خود را انتخاب کنید. عاملی که می‌تواند هم بر داده شما و هم بر محصول شما اثر بگذارد. برای مثال اگر شما داده های خود را در زیرساخت‌های به اشتراک‌گذاشته که به عنوان (به صورت) جزئی‌اند (یا خرده فروش)، ذخیره کنید، شما می‌توانید همان مشکلاتی را که آنها در طول فصل تعطیلات تجربه می‌کنند، تجربه کنید! حتی اگر آن را برای هسته‌ی تجارت خود به کار نگیرید.

Outage بویسله ارائه‌کنندگان ابر بسیار شایع شده‌است. یک سازمان به ارائه کنندگان ابر برای دستیابی به داده‌های حیاتی که در شبکه عمل می‌کند متکی است. ممکن است کنترل قابل توجه‌ای از دست برود پس باید ارائه دهنده‌ی ابر یک outage را امتحان کند.

بسیاری از ارائه کنندگان نرم‌افزار به عنوان سرویس فاقد تکنولوژی برای به کارگیری در محیط ابرشان می‌باشند. در عوض آنها زیرساخت هایشان را برون‌سپاری می‌کنند و با مرکز معتبر سوم که ارائه‌کننده‌ی زیرساخت می‌باشند قرارداد می‌بندند. این ترتیب ارائه در ارائه می‌تواند باعث سخت شدن پیگیری الزامات برای مقررات سازگاری، گزارش حادثه داده‌ها، مسئولیت قرارداد و مسایل دیگر شود(Achara, 2016)، (Bracy And Jedidiah, 2015) و (Wallace And Matthew, 2014).

خطر تجمیع

مزایای پی‌درپی رایانش‌ابری باعث افزایش سطح امنیت ارائه شده می‌شود و برای بیشتر شرکت‌ها این منفعت است. در این قسمت با توجه به شکل ۴ چند مخاطره مورد بررسی قرار گرفته‌اند.



شکل۴: مخاطره‌ی تجمیع

حملات پیچیده: شما باید فقط شرکت‌هایی را انتخاب کنید که پولشان را در بانک‌های بزرگ سپرده‌گذاری می‌کنند، چراکه آنها ارائه‌کننده‌ی امنیت‌اند. این خود باعث می‌شود که به مخاطره حملات پیچیده گرفتار شوند، چراکه ثروت تجمیع یک بانک بیشتر از ثروت تجمیع یک شرکت به تنهایی (Single) است. مجرمانی که به مهارت‌های بالایی دستیابی دارند، هم بودجه و هم صبر برای سازماندهی کردن حملات به نحوه‌ی احسن به خرج می‌دهند.

تهدید مداوم پیشرفته: جهان سایبری از نظر جرم و جنایت با محیط واقعی فرقی ندارد، حتی حملات آن پیشرفته‌تر است. اغلب به حملات تهدید مداوم پیشرفته[۴] در مقابل تکنولوژی شرکت‌های بسیار پیچیده و سایر موسسات در حال بزرگ شدن اشاره دارند. رایانش‌ابری یک تجمیع که در معرض خطر است ایجاد می‌کند که سازمان ها قبلاً با آن مواجه نبوده‌اند. در همین زمان مخاطره تجمیع یکی دیگر از دلایلی است که، چرا ارائه‌کنندگان ابر برای ارائه‌ی یک قرارداد مطلوب‌تر به مشتریان خود بی‌میلی نشان می‌دهند.

هزینه

یک از رایج‌ترین مزیت‌هایی که باعث شده است که سازمان‌ها با رایانش ابری توافق کنند کاهش هزینه‌های تکنولوژی می‌باشد و هیچ کس اختلاف نظر در این موضوع ندارد. به صورت بالقوه، تعداد زیادی هزینه‌ی پنهان به همراه رایانش‌ابری وجود دارد که ممکن است هرگز بررسی و رسیدگی نشود (شکل ۵). در ادامه هریک از موارد تشریح شده‌اند.

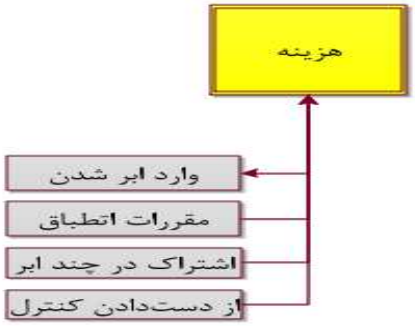
وارد ابر شدن: برای مثال هزینه‌های تخصیص‌داده‌شده به انتقال داه‌ها و شبکه خود، به ارائه کننده‌ی ابر دیگر چقدر می‌باشد؟ هنگامی که داده های یک شرکت در یک ابر ساکن است، این شرکت بسیار به آن ارائه کننده متکی می باشد. ارائه کننده‌ی ابر این را می‌داند که حرکت به سوی یک ابر بسیار راحت است اما رفتن از آن به یک ارائه کننده‌ی دیگر بسیار مشکل.

مقررات انطباق: یکی دیگر از مخاطره‌های مخفی ابر که در واقع شامل هزینه‌های پنهان می‌شود مقررات انطباق می‌باشد. در حالی که بسیاری از ارائه کنندگان ابر به شایستگی تمام، انطباق با استانداردها به عنوان مزایای کلیدی و پتانسیل صرفه‌جویی را ایجاد می‌کنند با این حال بسیاری از مسئولیت‌هایی وجود دارد که نادیده گرفته می‌شوند و هزینه‌های مربوط به کارهای اجرایی فروشنده که بسیار زحمت می‌کشد. از آنجایی که بسیاری از مقررات و استانداردها، سازمان‌ها را پاسخگو، در برابر تخلفات فروشندگانشان یا عدم سازش آنها، مسئول می‌دانند. در حالی که ممکن است شما شبکه یا داده‌های خود را به یک مرکز سوم برون سپاری کنید، اما شما هرگز ممکن نیست بتوانید مسئولیت یا مخاطره خود را برون سپاری کنید. با توجه به بررسی‌های زیادی که صورت گرفته‌است احتمال رخ دادن این مخاطره بسیار زیاد است ولی اثر آن نیز همین طور می‌باشد. علت این مخاطره را می‌توان در فقدان منابع و تکنولوژی‌های استاندارد، انتخاب ارائه کننده‌ی ضعیف و همچنین شفافیت در نحوه‌ی تعامل و استفاده از منابع دانست. به طور کلی این یک مخاطره‌ی خطرناک می‌باشد.

[4]Advanced Persistent Threat(APT)

اشتراک در چند ابر: بسیاری از سازمان‌ها خودشان را درجایی می‌بینند یا به این موضوع می‌رسند که اشتراک در یک ابر کافی نیست و در اینجا به همین دلیل سرویس‌های ارائه‌شده از طریق یک ارائه‌کننده‌ی ابر که شامل اتصالاتی بر سطح اینترنت می‌شود، ممکن است قطع شود و یا دچار تجمع دوره‌ای شود.

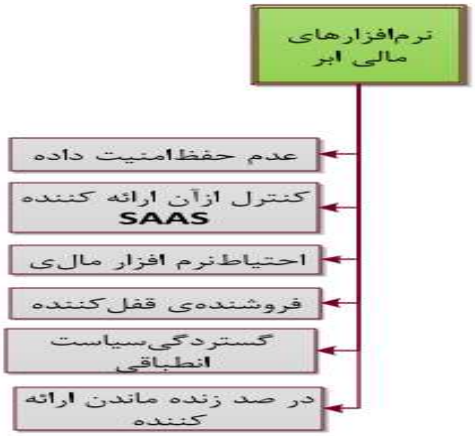
مخاطره از دست‌دادن کنترل: همچنین خدمات ابر می‌توانند بسیاری از حملات مخرب بر روی آن یا روی یک منبع بالادست، را کم کند. یک از راهها برای این سازمان‌ها به منظور کاهش این مخاطره‌ها، از طریق افزونگی سرویس‌های ارائه شده بوسیله‌ی قراردادهایی با چندین ارائه کننده‌ی سرویس می باشد. در نهایت هر مخاطره شناسایی شده تحت عنوان "از دست دادن کنترل" (که مهمترین آنها داده‌های قانونی است) می‌تواند همچنین به افزایش هزینه‌های ابرمنجر شود. هزینه‌های دیگری که لازم است مورد توجه قرار بگیرد شامل هزینه‌های قانونی بیشتر و پیامدهای مالیاتی مانند ممیزی و نظارت می‌شود.



شکل۵: مخاطره‌ی هزینه

مخاطرات مهم نرم‌افزارهای مالی ابر

تعداد زیادی از کارهای تجاری معتبر امروز از نرم‌افزارهای مالی ابر به عنوان بخشی از فعالیت‌های روزانه‌ی خود استفاده می‌کنند. آنها فرض می‌کنند که نرم‌افزار به عنوان سرویس ایمن و راحت برای استفاده است و در بهبود فاجعه به صورت درجا موثر است و هیچ مسائل کنترلی و رعایتی نیاز ندارد. اما این لزوماً درست نیست. جیمس استاتن می‌گوید: برای حرکت به سوی ابر، کارشناسان در زمینه‌ی اقتصادی و مالی ضرب المثل زیر را توصیه می‌کنند: خریددار مراقب باش[5]. در دسته‌بندی دیگر مخاطره‌هایی را بررسی می‌کینم که خریدار باید قبل از خرید برنامه‌های مالی ابر دقت کند. این دسته بندی بوسیله‌ی گروه تخصصی جستجوی رایانش ابری انجام شده‌است. (شکل ۶).



شکل۶: مخاطره‌ی نرم‌افزارهای مالی ابر

عدم حفظ امنیت داده: هیسر در این مورد می‌گوید: بزرگترین نگرانی من از دست دادن داده‌ها است. اگر بدترین اتفاق بیافتد، آیا شما می‌توانید سرویس دهنده‌ی خود را تصدیق کنید به طوری که داده‌های شما را بازیابی کند؟ و چه این

[5] Buyer beware!

کار چه مدت طول خواهد کشید؟ ابر مانند هوایی است که تنفس می‌کنیم، واقعا جالب است که با ابرکار می‌کنیم ولی صاحب آن هم نیستیم. مطمئن باشید که در ابر دزدی وسیع داده وجود ندارد، اما رد کردن اینکه آیا این کار اتفاق می‌افتد یا نه، کار سختی است. شفافیت امنیت ارائه‌کنندگان ابر وحشتناک است. هیسر می‌گوید: من مطمئن هستم که آنها کارهای زیاد و خوبی را برای امنیت انجام می‌دهند اما آنها نمی‌توانند این موضوع را خوب به ما تفهیم کنند. پس مسئولیت این کار هم بر دوش شرکت‌هاست تا کاری کنند که ما از امنیت داده‌ها در رایانش ابر مطمئن شویم. تجارت پس‌اندازی (مبتنی بر صرفه‌جویی) فکر می‌کند که به همین راحتی و فقط با استفاده از SAAS امنیت دادها حاصل می‌شود. .هیسر باز هم در این خصوص می‌گوید: ما از مدیریت نرم افزار خود به سوی مدیریت ارائه‌کنندگان می‌رویم و هیچ را ه منظم و سیستماتیکی هنوز برای این کار وجود ندارد و باز هم نظرش این است که خریدار احتیاط کن.

کنترل ازآن ارائه کنندگان نرم افزا به عنوان سرویس: بخشی از جذابیت ابر توانایی در برون‌سپاری قسمتی از کار را به ارائه کنندگان SAAS که معمولا به بخش تیم IT اختصاص داده شده‌است می‌باشد. این کار به IT در نوآوری در بخش‌های تجاری و ایجاد راه‌حل‌هایی که باعث تمایز شرکت و طرفداران ابر می‌شوند، کمک می‌کند. استدلال کنندگان اما با برون‌سپاری بخشی از کنترل از دست می‌رود. پل هامرمن: صحبت من به شرکت‌هایی که نمی‌خواهند بوسیله‌ی ارائه‌دهندگان SAAS در زمانی که بروزرسانی انجام می‌شود، اوامری به آنها دیکته شود، است. به هر حال یک تغییر یا سازگاری ویژه در مدیریت فهرست اموال، تولید یا یک حساب ، می‌تواند یک تجارت منحصر به فرد ایجاد کند. هامرمن می‌گوید: سیستم صدور حساب برای مثال نیازمند یک طیف گسترده‌ای از سازگاری برای کار کردن به صورت مطلوب می‌باشد.

احتیاط نرم افزارهای مالی: بیشتر شرکت‌ها در حال تبدیل شدن به برنامه‌های کاربردی مالی ابر هستند، کارشناسان می‌گویند که با احتیاط ادامه دهند. اما چه طور باید تصمیم گیرندگان احتمالات افتادن اتفاق بد را ارزیابی کنند؟ آنها باید در هنگام خرید از ارائه دهندگان ابر انتظارات واقع بینانه‌ای را داشته باشند و درصد زنده ماندن ارائه‌دهنده (که یک نوع جدیدی از ارتباط برای بسیاری از افراد محسوب می‌شود) را به طور مستمر ارزیابی کنند. نتیجه آن است که تغییر در ابر برابر این جمله نیست که: «این دیگه مشکل من نیست[۶]».

فروشنده ی قفل کننده: متخصصان امور مالی که قصد آمدن یا انتقال به دورن ابر را دارند باید ابتدا به این مساله خوب توجه کنند. آنچه که به عنوان خروج به نظر می‌رسد را باید بدانند. استاتن می‌گوید: اگر شما ندانید وقتی که می‌خواهید داده‌های خود را از ارائه‌دهنده‌ی فعلی خود خارج یا خلاص کنید شما ممکن است خودتان را در اصطلاح درحالت قفل شده ببینید. خوب است به این فکر کنیم که اگر فروشنده‌ی ابر یک بار مورد استفاده قرار بگیرد، دیگر کار تمام است. البته همیشه این گونه نیست روزگاری خواهد آمد که انتقال داده‌های حساس یک ضرورت شود. هیسر می گوید: انتقال ساختار داده از انتقال خود داده به بیرون سخت‌تر است. با توجه به بررسی‌های زیادی که صورت گرفته‌است احتمال رخ دادن این مخاطره بسیار زیاد است ولی اثر آن متوسط است. علت این مخاطره را می‌توان در فقدان منابع و تکنولوژی‌های استاندارد، انتخاب ارائه کننده‌ی ضعیف و همچنین شفافیت در نحوه‌ی تعامل و استفاده از منابع دانست. به طور کلی این یک مخاطره‌ی خطرنام می‌باشد که در هر سه سرویس مهم ابر (نرم‌افزار، چارچوب و

[6] not my problem anymore

زیرساخت) وجود دارد.

گستردگی سیاست های انطباقی: استاتن می‌گوید: بزرگترین مشکل ، مشکل انطباق است. اگر یک شرکت فقط در ایالات متحده تجارت کند و به صورت عمومی نباشد، پیروی از مقررات انطباق کننده فاکتور نگران کنند محسوب نمی‌شود. اما یک شرکت که با اروپا درتعامل است به راحتی گرفتار قوانین اروپا می‌شود چرا که یک برنامه‌ی کاربردی ابر مانند کوئیک‌بوک[۷]که یک سیستم مدیریت مالی است به قوانین اروپا پایبند نیست. برخی از ارائه‌دهندگان ابر ابزار ذخیره‌سازی اروپایی را ارایه می‌کنند. کسانی که کارهای تجاری را عهده دارند باید دقیقا چیزی را که ذخیره می‌کنند و همچنین جای ذخیره‌سازی را بدانند. که این کار کوچکی نیست. هیسر می‌گوید: اگر شما همه‌ی کارهایی را که می-توانید برای اطمینان از تطابق انجام دهید، باز هم برای نمایندگان دولتی در خصوص بررسی اینکه داده‌ها چگونه به کار گرفته شده است جای سوال باقی خواهد ماند.

در صد زنده ماندن ارائه کنندگان: گارتنر می‌گوید: سلامت فنی و اقتصادی ارائه‌کنندگان ابر برای هرکسی که به ابر وابسته است یک نگرانی محسوب می‌شود. هیسر می‌گوید: با فرض مدیریت نرم افزار ، تجارت‌ها می‌توانند از طریق سلامت تجارت فروشندگان نرم‌افزار در امان باشند. اما اگر داده‌های شما در ابر کسی قفل شود تصمیم گیرندگان به ارزیابی متناسب برای اهدافشان به صورت مداوم نیاز دارند. هیسر می‌گوید: SAAS برنامه‌های کاربردی را به یک زنجیره‌ی تامین تبدیل می‌کند. این یک رابطه‌ی متفاوت از چیزی است که تجارت‌ها از آن استفاده می‌کنند. جامعه-ی IT باید از این تجارب درس بگیرد. شما باید از اینکه فروشندگان زنده‌اند مطمئن شوید و بدانید که حتی فروشندگان که زنجیره‌ی تامین خود را به خوبی مدیریت کنند هم از این امر مستثنی نیستند و این موضوع دوباره بر این جمله تاکید دارد که فروشنده حذر کن[۸](Kuchler And Margaret, 2014).

نتیجه‌گیری

رایانش ابر بطور چشمگیری موانع ورود به تجارت نرم‌افزاری را کاهش می‌دهد و برای شرکت‌ها روشهای جدید کسب سود را می‌نمایاند. ارائه دهندگان خدمات ابر از طریق تسهیم، بهبود دادن و سرمایه گذاری بیشتر در نرم‌افزار و سخت-افزار به سود دست می‌یابند. پتانسیل رشد این تکنولوژی بسیار بالا برآورد شده است. وقتی که برنامه ریزی‌های رایانش‌ابری در آینده‌ی نزدیک صورت بگیرد، موسسات مالی باید خدمات و مدل‌های تحویلی را انتخاب کنند که بهترین تطبیق را با نیازمندی‌ها، برای انعطاف عملیاتی، صرفه جویی در هزینه و مدل‌های پرداخت فقط به اندازه‌ی مصرف داشته باشد. شرکت گاپژمینی معتقد است که بانک‌ها یک رویکرد تکاملی تدریجی نسبت به خدمات رایانش-ابری، ارزیابی هر پروژه مبتنی بر انواع برنامه‌های کاربردی و ماهیت داده ها اتخاذ نمایند. پروژه‌هایی که مخاطره کمتری دارند شامل مدیریت‌روابط‌مشتری[۹] و مدیریت‌محتوایی‌سازمانی[۱۰] می‌شوند. پروژه‌های دارای مخاطره‌های بیشتر شامل سیستم های کاربردی تجارت مرکزی (اصلی) مانند مدیریت ثروت یا هسته‌ی بانک‌ها می‌شوند. در دراز مدت، کاپژمینی انتظار دارد که بانک‌ها یک برنامه کاربردی که آمیخته شده از سرویس‌های تحویلی مبتنی بر ابر و **ON**

[7] QIUCKBOOK
[8] Buyer Beware
[9] CRM
[10] ECM

Premise در میان ترکیبی از مدل‌های استقرار مبتنی بر ابر خصوصی، عمومی و ترکیبی همراه با خدمات اشتراکی ابر که تدریجا در سرویس مخلوط شده داشته باشند (خلاصه اینکه بانک‌ها یک برنامه‌ای داشته باشند که در بین انواع ابرها و داده هایی که مابین آنها به صورت اشتراکی وجود دارد بتواند کار کند).

منابع فارسی

صادق زاده، پیام، بهره پور، داود، ۱۳۹۱، تحلیل و بررسی چالش های امنیتی موجود در محاسبات ابری.

منابع لاتین

The NIST Definition of Cloud Computing ,(2014), National Institute of Standards and Technology.
Amazon EC2 Pricing, (2014), www.amazon.com.
Microsoft Azure Virtual Machines Pricing Details, (2014), www.microsoft.com.
S., Achara, R. , (2016), Rathi, Security Related Risks and Their Monitoring in Cloud Computing, International Journal of Computer Applications.
Bracy,S., Jedidiah, D.,(2015), European Parliament Votes in Favor of Proposed Data Protection Reform. PrivacyAssociation.org.https://www.privacyassociation.org/privacy_tracker/post/european_parliament_votes_in _favor_of_ proposed_data_protection_reform.

Wallace, F., Matthew, W., (2014), The Problem With Noisy Neighbors in the Cloud. AllThingsD.com.
Kuchler, J., Margaret, B.,(2015), Mobile Retail Traffic Represents 35 percent of the Thanksgiving Holiday Traffic