امنیت در سیستم های توزیع شده:

امنیت ابر در مقابل فناوری های سنتی

محاسبات ابری یک موضوع بسیار مهم و محبوب در صنعتIT (فن‌آوری اطلاعات) است، اما خطرات مرتبط با این فن‌آوری هنوز هم به‌طور کامل حل نشده است. در این مقاله، یک رویکرد خوب برای تامین امنیت ناشی از خطرات محاسبات ابری ارائه شده است. تمرکز این رویکرد بر شناسایی خطرات موثر بر رایانش ابری و ایجاد یک چارچوب است که می‌توانند در انطباق پردازش و استراتژی کاهش خطرات به مدیران IT کمک کند. فشارهای اقتصادی ناشی از کسب‌وکار، نیاز به مدلی برای تحویل انعطاف‌پذیر، کاهش چشمگیر سرمایه‌گذاری و کاهش هزینه عملیاتی را افزایش می‌دهد. محاسبات ابری برای بهره بردن از این فشارهای اقتصادی با هزینه اقتصادی کم و مدل انعطاف‌پذیر و با رعایت امنیت و حریم خصوصی به کار برده می‌شود. چارچوب ارائه شده توسط این مقاله به متخصصان کمک می‌کند تا درک روشن‌تری از خطرات مبادلات مرتبط با محیط‌های محاسبات ابری به‌دست آورند.

معرفی

فن‌آوری‌های محاسبات ابری در حال تغییر هستند و بسیاری از افراد از این سرویس‌ها بدون آگاهی از کارکرد آنها استفاده می‌کنند. به‌عنوان مثال، هر کسی که در گوگل جستجو می‌کند، در شبکه‌های اجتماعی پیامی به اشتراک می‌گذارد و یا از تلفن‌همراه استفاده می‌کند، از یک ابر استفاده می‌کند. برای برآورد اهداف این مقاله، محاسبات ابری (یا به سادگی، cloud) را تعریف می‌کنیم که شامل مدل تحویلIT (فناوری اطلاعات) جهت محاسبه، ذخیره‌سازی و سرویس شبکه نسبت به تقاضا، مجازی‌سازی، با منابع به اشتراک گذاشته شده بر روی شبکه می‌باشد. حضور همیشگی محاسبات ابری برای فناوری اطلاعات نسبت به گوشی‌های هوشمند رشد بیشتری دارد، برای مثال، با رشد 75٪ در

سراسر جهان در سال 2010 [1] برخوردار است و به طور مداوم در سال 2011 رشد داشته است (منبع [2] را ببینید). عوامل دیگری مانند تجاری شدن تکنولوژی و ظهور سیستم عامل‌های جدید (OS) و میان‌افزار برای ابرها، سطوح امنیتی جدیدی برای حملات ایجاد کرده است. ابرهای گسترده ذخیره‌سازی، بنا به نیاز سیرناپذیر به جمع‌آوری و ذخیره مقدار روزافزون داده‌ها ساخته شده است، که چالش‌های نظارتی جدیدی در این حوزه را به وجود آورده‌اند. علاوه بر این، فشار مالی بر سازمان‌های IT برای تولید سرویس‌هایی با بودجه کم، تقاضاهای موثری برای انطباق مدلهای جایگزین هستند که می‌توانند هزینه‌های فناوری اطلاعات را کاهش دهند. با این حال، استانداردهای ابر مجبور به استفاده از تعداد محدودی پیکربندی IT هستند که گاهی اوقات با نیازهای شرکت منطبق نیست [3، 4].

در این مقاله، تجزیه و تحلیل کیفی برای ایجاد یک مدل بیان شده است که می‌تواند به امنیت، پذیرش و کسب‌وکار خطرات مرتبط

با محاسبات ابری کمک کند. پردازش کیفی ما دیدگاه 68 متخصص ابر و امنیت را جمع‌آوری کرده است. این مقاله به‌دنبال تبادل آزاد اطلاعات و تعامل سازنده است. در متن این مقاله، کلمه "risk" به خطرات ناشی از امنیت، پذیرش، و خطرات کسب و کار برمی‌گردد. عبارت "traditional IT" به سرویس‌های IT اشاره دارد که با فرض میزبانی و مجازی‌سازی و یا گره مجازی با استفاده از تنظیمات بالا است.

IT سنتی غالبا تک مستاجره و نه به‌طورکامل خودکار است، و تفاوت قابل توجهی در سراسر نصب و راه اندازیVM (ماشین مجازی) دارد. علاوه‌براین، این مقاله به compliance اشاره دارد که فرآیند موردنیاز برای انجام کسب‌وکار را انجام می‌دهد. نمونه‌ها شامل مقررات انطباق مشترک FISMA (فدرال مدیریت امنیت اطلاعات)، HIPAA (قانون بیمه بهداشت و درمان و پاسخگویی به آن)، SAS 70 (بیانیه در استانداردهای حسابرسی شماره 70)، و PCI-DSS (پرداخت صنعت استاندارد امنیت) هستند.

در این مقاله، شواهد گردآوری شده، بر اساس مصاحبه با کارشناسان، برای کمک به شناسایی و تفسیر خطرات محاسبات ابری در مقایسه با خطرات IT سنتی برای کمک به تصمیم‌گیری بهتر در مورد ابر به تصویب رسیده است. برای افرادی

که ممکن است مایل به بررسی تحقیقات منتشر شده در امنیت محاسبات ابری هستند، منابع [5-11] پیشنهاد می‌شود.

متدولوژی

ما در این مقاله روش دلفی را انتخاب می‌کنیم [12]، یک روش ساختاریافته، زیرا پژوهش در مورد مسائل ناقص و کمیابی که اطلاعاتی در مورد آنها موجود نیست موفق عمل می‌کند. همچنین، روش دلفی در مواردی که تجزیه و تحلیل دقیق کمتر قابل اجرا است موثر است و تجزیه و تحلیل یک گروه از افراد بهترین منبع قابل دسترس از اطلاعات است. یکی از مزایای روش دلفی، تمایل به همگرایی پس از بازخورد پی‌درپی است [13]. با این حال، برای این مقاله، از دلفی اصلاح‌شده استفاده می‌کنیم که شامل یک مصاحبه، تکرارهای دلفی برای ساخت اجماع و تجزیه و تحلیل کمی با استفاده از صفحه گسترده calibration هستیم. کارشناسانی که در این مقاله شرکت کرده‌اند از متخصصان فن‌اوری اطلاعات، با تجربه بسیاری در زمینه محاسبات ابری و امنیت هستند. ملاقات کارشناسان، بحث در مورد موضوعاتی مانند خطرات ابر، ارزیابی خطرات ابر در مقایسه با خطرات سنتی آن، و طبقه‌بندی چارچوب ابر است. به عنوان بخشی از روش دلفی، خطرات ابر با استفاده از یک فرایند مرتفع می‌گردد. این فرآیند در طی یک دوره شش هفته‌ای صورت می‌گیرد، نتایج بدست آمده از دلفی با بحث 68 کارشناس و تلاش‌های آنان به ثمر رسیده است. ابزار کالیبراسیون شامل یک سطر برای هر یک از خطرات ابر شناسایی شده توسط پردازش دلفی است. خلاصه‌ای از فرآیند اصلاح شده دلفی و مثالی از ابزار کالیبراسیون در شکل 1 نشان داده شده است. علاوه‌براین، پردازش از یک الگوی هرمی و توافقی در مورد رتبه‌بندی هشت خطر بالای ابر و خطرات مرتبط با آن در مقایسه با سنتی استفاده می‌کند. پس از تکمیل پردازش دلفی اصلاح‌شده، یک نظرسنجی از 204 متخصص فن‌آوری اطلاعات برای مقایسه خطرات و نظرات 68 کارشناس با جمعی از متخصصان IT صورت گرفت. مخاطبان اصلی این مطالعه متخصصان IT با چندین سال تجربه هستند، اما لزوما کارشناسان امنیت ابر نیستند.

توجیه خطرات کلیدی ابر

بعد از اجماع و کالیبراسیون پردازش، داده‌ها به دو دسته اصلی تقسیم می‌شوند: آن مواردی که موجب افزایش و کاهش خطرات ابر در مقایسه با روش سنتی می‌شوند. این تقسیم‌بندی برای اعتبارسنجی کیفی فرضیه ایجاد شده است که محاسبات ابری خطرات جدیدی در مقایسه با روش سنتی دارند. بااین‌حال، آنچنان که انتظار می‌رود، ابرها و روش سنتی خطرات جالبی دارند. به‌عنوان مثال، بردارهایی که در ابرها و IT سنتی وجود دارند عبارتند از: عوامل انسانی، احراز هویت، اعتبارسنجی، SLA ها (در سطح سرویس)، حملات داس، و مدیریت رمزنگاری کلید. خطراتی که تنها در مجموعه ابر وجود دارند به شرح زیر هستند: مدیریت تصویر ابر، چند مستاجره، اسکریپت اتوماسیون ابر، نرم‌افزار مدیریت ابر. ازسوی‌دیگر، خطراتی که در مجموعه خطرات سنتی قرار دارند مانند مدیریت فیزیکی سرور و لپ‌تاپ، مدیریت فایروال‌های فیزیکی، طبقه‌بندی سخت‌افزار، و سرمایه‌گذاری منحصر به فرد هستند. تقریبا تمام متخصصان امنیت و ابر که معرفی شدند سطح جدیدی از حملات با خطرات امنیتی را ارائه می‌کنند. هنچنین آنها چند مستاجری، استانداردسازی و اتوماسیون، احراز هویت و اعتبارسنجی، نقطه پایانی دستگاه و عوامل انسانی مهم و خطرات کسب‌وکار را مورد توجه قرار داده‌اند. این هشت عامل خطر موجب ایجاد هرمی ابری از خطرات می‌شود (شکل 2).

خطرات Hypervisor

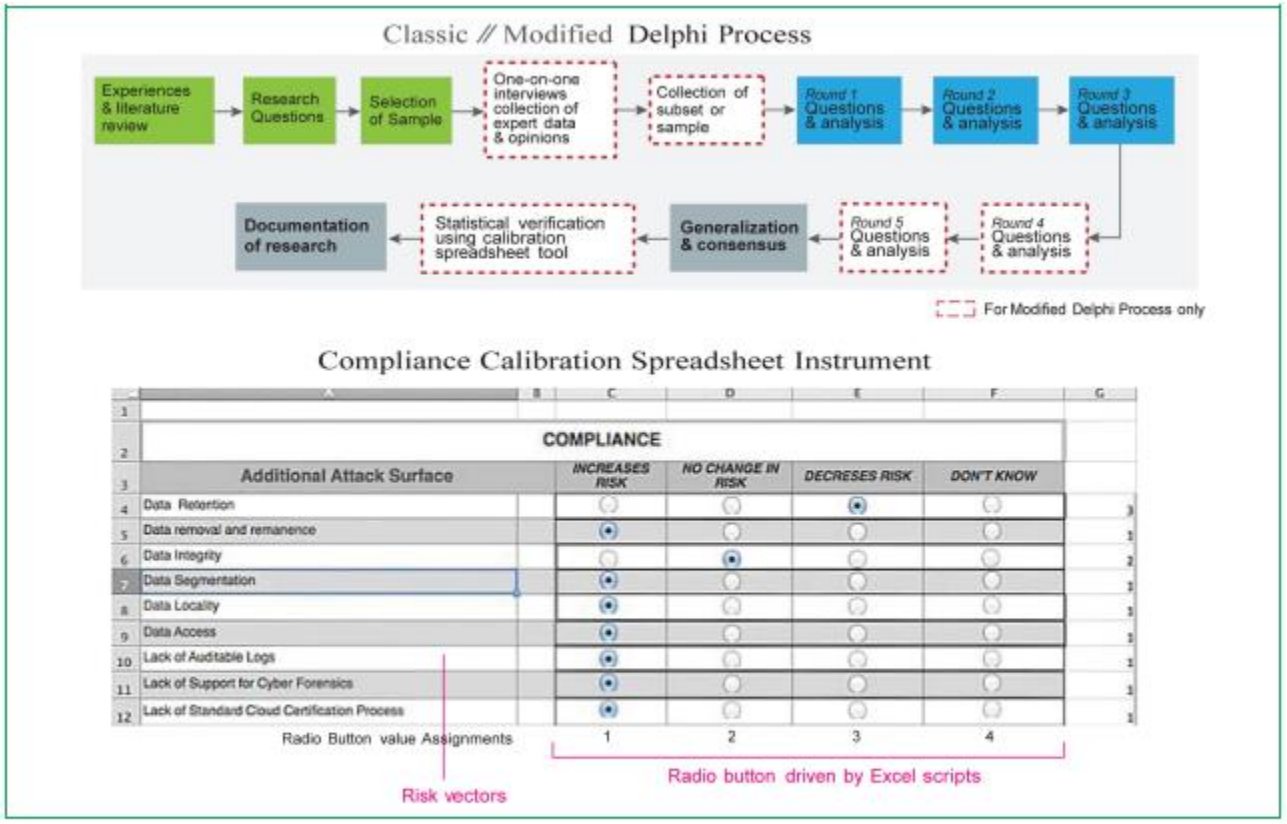

Figure 1

Methodology. The Modified versus Classic Delphi Research process is shown schematically at the top of the figure, and the Compliance Calibration Spreadsheet Instrument is shown at the bottom of the figure.

بیشتر عوامل خطر مرتبط با hypervisor یکی از موضوعات مهم است که نوسط متخصصان بیان شده است. تنها متخصصانی که با این عوامل موافق نیستند تجربه‌ی زیادی در پردازش مرکزی دارند. آنها پردازش مرکزی LPAR (بخش منطقی)- تقسیم‌بندی ماشین فیزیکی به چندین ماشین منطقی با استفاده از معماری چیپ‌های IBM POWER- را راهی برای مجازی‌سازی می‌دانند.

امروزه هیچ یک از محاسبات ابری از فن‌آوری پردازنده مرکزی بنا به محدودیت هزینه استفاده نمی‌کنند؛ بااین‌حال، می‌تواند جداسازی بهتری باشد. به‌عنوان‌مثال، پردازنده مرکزی IBM Z10 * براساس طراحی تراشه IBM POWER است که، از میکروپروسسر x86 اینتل ** متفاوت است. یکی از مزایای استفاده از مجازی‌سازی پردازنده مرکزی LPAR، دسترسی به آدرس حافظه بدون همپوشانی است. که امکان خطرات ماشین‌های مجازی نوعی از معماری

سخت‌افزار x86 را از بین می‌برد. علاوه‌براین، LPARs رجیسترهای جداگانه برای hypervisor و سیستم‌عامل دارند که، خطر فرار hypervisor در طول سرریز بافر را از بین می‌برد [14]. خطر مرتبط با hypervisorها را می‌توان به راحتی از طریق گزینه‌های ارزان با استفاده از ماشین‌های مجازی فوق‌العاده بزرگ که کل میزبان فیزیکی را هدر می‌دهند کاهش داد. بنابراین انتظار می‌رود که، استراتژی کاهش hypervisor شامل مبادلات امنیت و هزینه باشد. کاربران می‌توانند یک سیستم ابر با استفاده از LPARs پیاده‌سازی کنند، اما این پیکربندی می‌تواند به‌طور قابل توجهی با استفاده از ماشین‌های مجازی بر روی سخت‌افزار مشخصی هزینه‌های فوق العاده بزرگی ایجاد کند.

سیستم ابر هنوز مدل سیستم IT نسبتا جدیدی است که راه زیادی پیش رو دارد و بسیاری از کارشناسان معتقدند که یکی از بزرگترین خطرات عوامل ناشناخته است، زیرا اجزای نرم‌افزار و مدل خارج از اندازه‌گیری خطرات آماری عمل نمی‌کند. در حدود سه سال گذشته، ابرها از یک الگوی نسبتا ناشناخته به IT با محبوبیت شدید انتقال یافتند، 60٪ از مشتریان شرکت در تلاش برای حرکت به فناوری ابر برای رسیدن به بازده بیشتر بودند [15، 16]. فن‌اوری ابر معمولا ترکیبی از سخت‌افزار مشخص با برداشت جدید نرم‌افزار از مفاهیم قدیمی مانند hypervisor است. بااین‌حال، مدل کسب‌وکار (1) پرداخت فقط برای مقدار استفاده شده است؛ (2) سرویس‌های وب مرتبط با SOA است (معماری سرویس‌گرا)، و (3) اتوماسیون جدید فن‌آوری ها، ترکیبی بسیار مفیدی برای محاسبات ابری ایجاد می‌کند. این پدیده موجب ایجاد بسیاری از برنامه‌های جدید مانند سرویس مس‌شود، و در حال حاضر میلیون‌ها نفر از کاربران در حال مصرف ابرهای با نرم‌افزار هنوز کامل نشده هستند. قابل درک است که به‌طور مداوم در مورد امنیت مسائل و خطرات مرتبط با ابر بحث کنیم.

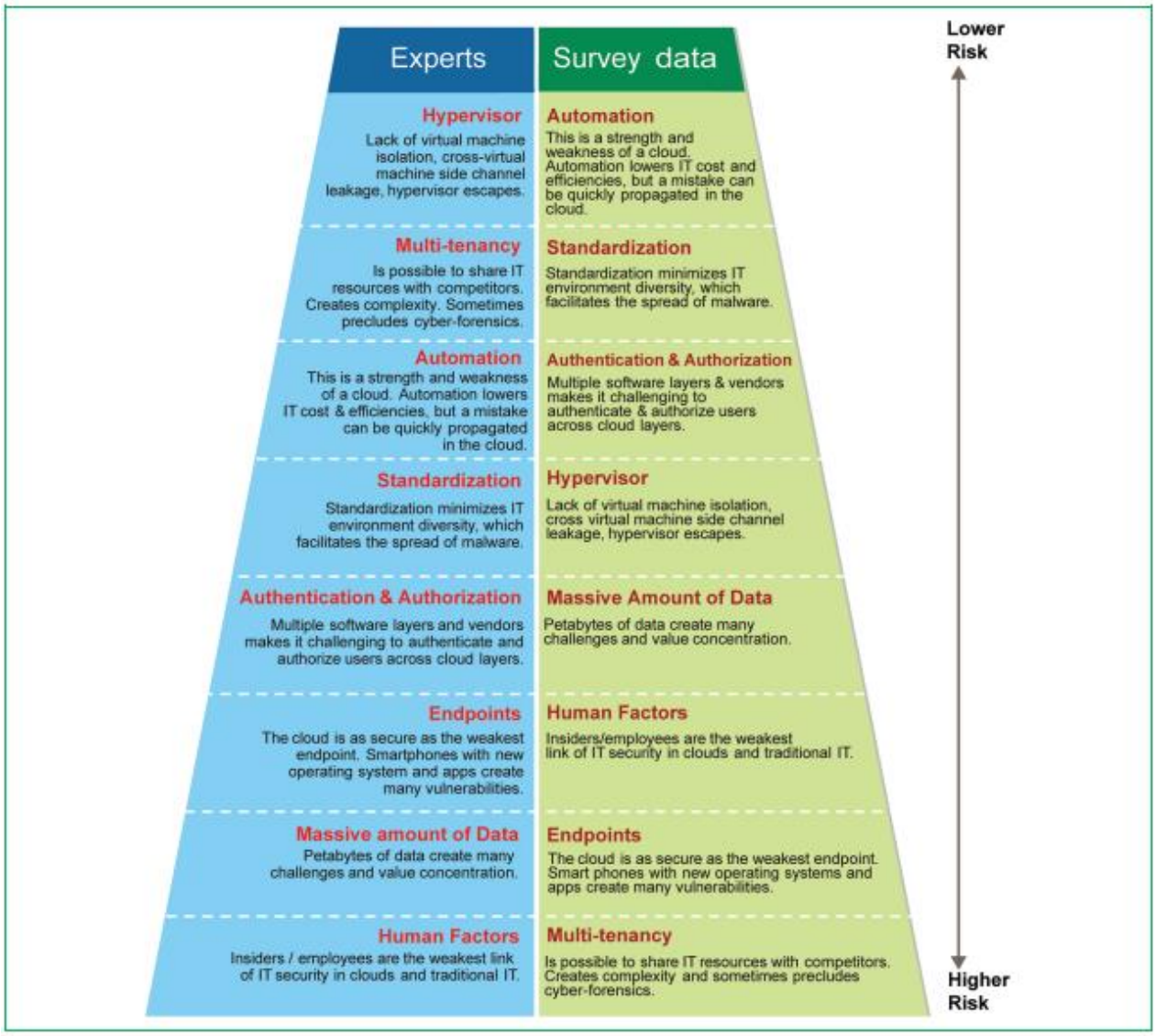

Figure 2

Pyramid of cloud risks comparison between experts and survey participates. Differences on the pyramids highlight several of the possible misconceptions relating to cloud security risks.

چند مستاجره

عامل خطر در چند مستاجره مربوط به مسائل و چالش‌هایی مرتبط با به اشتراک‌گذاری فیزیکی منابع IT مانند CPU، حافظه، سوئیچ شبکه، فایروال‌ها، سخت‌افزار و نرم‌افزار و سایر اجزاء است. چند مستاجره به‌طور بالقوه می‌تواند منجر به اشتراک‌گذاری منابع با رقبای شرکت در بهره‌برداری متقابل برای اخذ اطلاعات شود. علاوه‌براین، اگر مشتری توسط دادگاه برای رسیدگی به پرونده داده‌ها ولاگ‌ها در چند مستاجره احضار شود ممکن است داده‌هایی از اتصال به

ماشین‌های مجازی در یک سرور فیزیکی به دست آید. علاوه‌براین، چند مستاجری همراه با مجازی‌سازی باعث می‌شود تا پیاده‌سازی ابزار ردیابی برای اعمال سایبری پزشکی قانونی در محیط ابر دشوار شود که ممکن است منجر به عدم تطابق با مقررات گردد.

پذیرش این فن‌آوری در 10 سال اخیر بسیار مهم بوده و افزایش قابل توجهی داشته است و منجر به چالش‌های مهمی در زیرساختهای IT شده است. بااین‌حال، ابرها به طور قابل توجهی بنا به پتانسیل موجود در آنها به چالش کشیده می‌شوند. علاوه‌براین، ماهیت چالش مصرف ابر با احترام به حریم خصوصی و قابلیت بازبینی قابل تصحیح است. قوانین نظارتی جدیدی که نیاز به حفظ اسناد برای مدت طولانی دارند، فشار زیادی برای ذخیره‌سازی بیشتر و مقرون به صرفه مطابق با مقررات ابر ایجاد می‌کند؛ اما اگر کنترلی بر منابع ذخیره‌سازی صورت نگیرد خطرات دیگری افزایش می‌یابند.

اتوماسیون و استانداردسازی

محاسبات ابری ویژگی‌های خود را با خودکارسازی بسیاری از فرآیندهایIT مانند تأمین و استقرار ماشین‌های مجازی جدید، مدیریت، پشتیبان‌گیری، تعادل بار، نظارت بر امنیت و فرآیندهای دیگر انجام می‌دهند. مدیران محیط ابر، هزاران سرور از طریق داشبورد ابر و استقرار فرآیندها با "push of a button"(به‌عنوان مثال، به راحتی) انجام می‌دهند. اما اگر یک اشتباه در اسکریپت اتوماسیون ساخته شده رخ دهد، مانند یک خطا، می‌تواند بسیار به سرعت تکرار شود. استانداردسازی دربردارنده‌ی خطر مرتبط با به حداقل رساندن تعداد انواع ماشین‌های مجازی موجود در ابر است. استانداردسازی کمک می‌کند تا محیط همگن ایجاد شود، اما در زمان یکسانی، می‌تواند موجب کاهش گسترش ویروس‌ها و یا نرم‌افزارهای مخرب در ابرها گردد.

یک سرمایه‌گذاری عظیم در اتوماسیون منجر به یکی از مزایای ابر می‌شود و ارائه‌دهندگان ابر از اتوماسیون برای به‌دست آوردن مقیاس اقتصادی، مدیریت تعداد زیادی از ماشین‌ها استفاده می‌کنند. اتوماسیون هزینه پایینی را به ارمغان می‌آورد زیرا توانایی به کارگیری تعداد زیادی از سرورها را به‌صورت همزمان دارد – بیشتر کارشناسان ادعا می‌کنند که 10000 سرور برای هر مدیر در محیط‌های IT از جمله گوگل و آمازون وجود دارد. در ابرهای خصوصی با ظرفیت

کمتر، تعداد در محدوده‌ای بین 60 تا 100 سرور برای هر مدیر است. همانطور که گفته شد، اتوماسیون موجب افزایش انعطاف‌پذیری با حداقل تلاش ممکن می‌شود. علاوه‌براین، تقسیم کار موثر در روند ایجاد و حفظ فرآیندهای اتوماسیون نقش بسزایی دارد، چرا که دانش نیاز به اشتراک‌گذاری بین مدیران ندارد.

این مزایا بسیار قانع‌کننده هستند، اما این قدرت نیز یک ضعف به حساب می‌آید. همانطور که گفته شد، اتوماسیون می‌تواند بازده زیادی ارائه کند، اما یک اشتباه در یک اسکریپت می‌تواند به سرعت گسترش یابد و با عواقب فاجعه‌باری همراه گردد. حوادث ناخواسته، مانند طوفان معکوس آمازون، توسط اتوماسیون تشدید می‌یابد، بنابراین منطقی است که انتظار طوفان‌های ابر بیشتری را در آینده داشته باشیم. از آنجا که بخش بزرگی از اتوماسیون ابر، کنترل کاربر ابر است، استراتژی خاصی برای این مورد وجود ندارد. به‌طورکلی، اتوماسیون یک بردار خطرناک‌تر از hypervisor و چندمستاجری است.

استانداردسازی جنبه دیگری نیز دارد که می‌تواند نقاط ضعف و مزایایی داشته باشد. مثلا، اگر یک سرور بدون استانداردسازی مجازی شود، نتیجه آن پیچیدگی بیشتر خواهد بود که در حال حاضر وجود دارد. فرایند استانداردسازی وجود دارد که موجب کاهش تنظیمات و ایجاد یک تعداد محدودی از تنظیمات IT قابل استفاده‌ی مجدد می‌شود و می‌تواند تنها با چند کلیک ماوس خودکار شود [18-20]. این همکاری بین استانداردسازی و اتوماسیون توسط Bittman به هنگام بحث در مورد طراحی برای مجازی‌سازی بهتر اعلام شد [20]، و افراد دیگری مانند Oberle و Fisher [18] به عدم وجود استانداردسازی به‌عنوان یکی از موانع اصلی برای تصویب ابر اذعان کردند. بااین‌حال، این مورد درکار Ring و همکارانش بود [19]. در چارچوب مورد آزمایش انها برای محیط‌های ابر قدرت استانداردسازی برای ایجاد تنظیمات ساده‌تر که بسیار آسان خودکار می‌شوند به وضوح نشان داده شده است. ازسوی دیگر، استاندارد تنوع محیط IT را به حداقل می‌رساند، در نتیجه موجب گسترش ویروس‌ها و نرم‌افزارهای مخرب در سراسر محیط ابر می‌شود. مشابه جهان زیستی، تنوع می‌تواند در برابر ویروس محافظت شود زیرا چالش‌های بیشماری وجود دارد که نیاز به پیچیدگی و کدهای بیشتری برای حمله کردن به از آن تنظیمات به جای فقط چند استاندارد VMS دارند. این یکی

از دلایلی است که چرا هوشیاری و دقت در تعمیر و نگهداری نرم‌افزار با استفاده از آخرین نرم‌افزارها به ویژه در محیط‌های ابری مهم است.

احراز هویت و اعتبارسنجی

عامل خطر احراز هویت و اعتبارسنجی در ارتباط با چالش رو در رو با تعداد زیادی از کاربران و اشیاء داده است. احراز هویت سنتی و مدیریت دسترسی (IAM) فن‌آوری است که شناسه‌ها و ACL ها (لیست کنترل دسترسی) را برای 10،000 کاربر و همچنین به خوبی حفاظت از چند میلیون اشیاء مدیریت می‌کند که به سادگی در ابری با مقیاس 200 میلیون کاربر و 100 میلیارد فایل کار نمی‌کند. IAM بر روی یک مدل متمرکز که در محیط توزیع‌شده نیست مانند ابر پیش‌بینی می‌کند. سرعت دسترسی بنا به درخواستهای ابر بسیار سریع‌تر تغییر می‌کند و باعث ایجاد چالش‌های جدید و خطرات می‌شود. چندین سیستم مدیریت هویت و کنترل خدمات احراز هویت از راه دور ایجاد شده است، اما هنوز هیچ شرکتی درجه استانداردی تعریف نکرده است. احراز هویت هنوز مسئله‌ای بسیار مهم است چرا که احراز هویت کاربران نیاز به عبور امن از لایه‌های ابر دارد. از سوی دیگر، فن‌آوری‌های جدید مانند OAuth تأیید (استاندارد باز برای احراز هویت) قادر به کاهش برخی از این خطرات هستند. استانداردهای باز جدید مانند OAuth اجازه می‌دهند تا کاربران توکن‌ها را به جای اعتبار به لایه‌هایی از سرویس‌های ابری برسانند و خطر سرقت هویت و یا جعل هویت به حداقل برسد. با این حال، این فن‌آوری‌ها هنوز هم در مراحل اولیه هستند و همه ارائه‌دهندگان و خدمات ابر به صورت همزمان ار آنها پشتیبانی نمی‌کنند. مثلا، برنامه گوگل موتور ** از OAuth پشتیبانی می‌کند [21]، اما احراز هویت تنها با توجه به حساب‌های خدمات گوگل انجام می‌گیرد، ایجاد خطر تکثیر هویت بین محیط LDAP (دسترسی به دایرکتوری سبک پروتکل) و خدمات گوگل انجام می‌گیرد. علاوه براین، برای پیکربندی یک نرم‌افزار وب گوگل یکی از نیازها ایجاد چند XML (زبان نشانه‌گذاری) فایل‌های web.xml یا YAML (زبان نشانه‌گذاری app.yaml) برای تعریف نرم‌افزار و دسترسی به امتیازات آن می‌باشد. این نوع متدولوژی بسیار درشت دانه است و از سایر موارد مورد نیاز کسب وکار مانند مجوز پشتیبانی نمی‌کند. مثال دیگر ارائه شده توسط کارشناسان مایکروسافت

Azure ❋❋ است که از SAML (زبان نشانه‌گذاری امن) و STS (سرویس توکن امنیت) برای حمایت از راه‌حل مدیریت توزیع هویت پشتیبانی می‌کند. پروتکل SAML از روش‌های احراز هویت SSO و به‌حداقل رساندن تقلید هویت بین مشتری و ارائه دهنده ابر پشتیبانی می‌کند [22]. عدم وجود استانداردسازی ابر با توجه به روش‌های تأیید هویت و مجوز موجب گسترش غیرسازگار راه‌حل‌های اختصاصی شده است که خطرات امنیتی قابل توجهی تولید می‌کنند.

نقطه‌ی پایانی

ظهور دستگاه‌های تلفن‌همراه فشار قابل توجهی بر کسب‌وکار و پشتیبانی از رابط گرافیکی با دستگاه جدید ایجاد کرده‌اند. دستگاه‌های جدید موبایل مانند تلفن‌های همراه و تبلت‌ها بخشی از ابر تلفن‌همراه هستند و چابکی عظیمی برای کارکنان ارائه کرده‌اند. در زمان یکسانی، این فن‌آوری آسیب‌پذیری زیادی به راه‌حل‌های ابر وارد کرد. به‌عنوان مثال، ارائه‌دهندگان خدمات بهداشتی تحت فشار زیادی برای حمایت از برنامه‌های کاربردی اپل برای بررسی سوابق پزشکی در هر زمان و هر مکانی هستند. این مسئله یک چالش بزرگ است چرا که بسیاری از دستگاه‌های تلفن‌همراه مطابق با حداقل استانداردهای امنیتی نیستند و نرم‌افزارهایی که آنها استفاده می‌کنند در چرخه حیات قرار دارند [23].

تمرکز بر مقادیر

با ظهور مراکز داده mega IT ایجاد شده توسط IBM، گوگل، مایکروسافت، آمازون، یاهو، و بسیاری دیگر، این انبار عظیم شامل ده‌ها هزار سرور است که خطرات و چالش‌های جدید بسیاری ایجاد می‌کند. مقدار زیاد و تراکم سخت‌افزار می‌تواند به‌صورت آماری ذخیره‌سازی و یا خرابی روزمره سرور در ابر را تضمین کند [24، 25]. همچنین، مراکز داده بزرگ تهدیدی جدی برای این مسئله به شمار می‌آیند. تمرکز بر مقادیر موجب تغییر در هر زمان نمی‌شود، زیرا تغییر در مراکز بزرگ داده‌ها با کاهش بودجه و بازده انرژی همراه است. بیشترین مقادیر در ابر متمرکز است و اهداف خدماتی ابر بزرگتر خواهد شد. علاوه‌براین، انتظار و تقاضا برای دردسترس بودن داده‌ها در همه جا یک چالش بزرگ ایجاد

کرده است که گاهی برخلاف انسجام داده‌ها است. پایگاه‌های داده‌های توزیع‌شده جدید، نه ب اساسSQL (زبان پرس‌وجو ساختارمند)، در هزینه پایین دسترسی در ابر محبوب هستند. پایگاه داده‌های سنتی رابطه‌ای SQL با دقت و مطابق با ACID قوانین (اتمیک بودن، ثبات، انزوا، دوام) تنظیم شده‌اند، اما آنها دسترس پایین‌تری در داده به‌دلیل مکانیسم commit دو مرحله‌ای دارند. با حجم انبوه از داده‌ها، به‌طورخاص بالاتر از 10 پتابایت، هزینه مرتبط با حمل و پشتیبان‌گیری از داده‌ها به‌صورت نمایی رشد می‌کند. فن‌آوری‌های جدید مانند هادوپ **، NoSQL، Cassandra **، و IBM سیستم فایل موازی عمومی (GPFS *) برای کمک به رسیدگی این نوع داده در ابرها ایجاد شده‌اند. بااین‌حال، این نوع از ابزار گاهی اوقات دسترسی را به جای دقت بهینه‌سازی می‌کند بنابراین این مورد می‌تواند یکپارچگی و امنیت در مسائل را ایجاد کند. علاوه‌براین، تراکم عظیم داده‌ها در ابرها موجب ایجاد تراک مقادیر می‌شود. حجم انبوهی از داده با چالش تقاضای سیری‌ناپذیر برای دردسترس بودن بدون دقت و صحت داده روبهه‌رو هستند. دردسترس بودن و دقت داده‌ها از الزامات است. به‌عنوان یک پارتیشن از داده‌ها برای افزایش دردسترس بودن، ثبات کاهش می‌یابد و زمانی که پارتیشن‌های داده برای افزایش ثبات کاهش می‌یابد وارونگی اتفاق می‌افتد، اما دردسترس بودن کاهش می‌یابد [26].

عوامل انسانی

متاسفانه، همه کارشناسان معتقدند که مهم‌ترین خطر امنیتی موثر بر ابرها عوامل انسانی است، زیرا بیشتر رفتارهای متقابلانه به دلیل تهدید دورنی است. در برخی موارد خطر دورنی در ابرها از IT سنتی بالاتر است زیرا ویژگی تراکم مقادیر ابرها زیاد است. کارشناسان ما توضیح داده‌اند که چگونه ارائه‌دهندگان ابر تلاش گسترده‌ای برای نصب ابزار نظارت پیچیده در پایانه‌های کنسول و داشبورد مدیر انجام داده‌اند. این ابزار نظارتی ساخته شده توسط مدیران سیستم، برای نظارت بر کارکنان مخرب و یا ناراضی ساخته شده‌اند که ممکن است با سرقت اطلاعات و یا خرابکاری در سیستم در ارتباط باشند. با این حال، این عامل خطر، انتظار ادامه یک مشکل برای آینده قابل پیش‌بینی را به همراه دارد،

همانطور که هکر معروف جهان کوین میتنیک می‌گوید [27] ، شکستن فایروال انسانی آسان است. علاوه براین، بیش از 70 درصد مصاحبه‌ی کارشناسان برای این مقاله در مورد خطر حملات مهندسی اجتماعی هشدار می‌دهد.

امنیت ابر و انطباق با چارچوب خطرات

در این بخش، بر خطرهای موثر در امنیت ابرها تمرکز خواهیم داشت. تقاضای پذیرش می‌تواند شامل قوانین و مقررات دولتی، فرآیندهای صنعتی و الزامات کسب و کار خاص باشد. انطباق نظارتی دولت شامل قانون Sarbanes-Oxley در سال 2002 (SOX) است، که به ایجاد استانداردهای جدید حسابرسی برای افزایش شفافیت کسب‌وکار و رفتار اخلاقی کمک می‌کند.

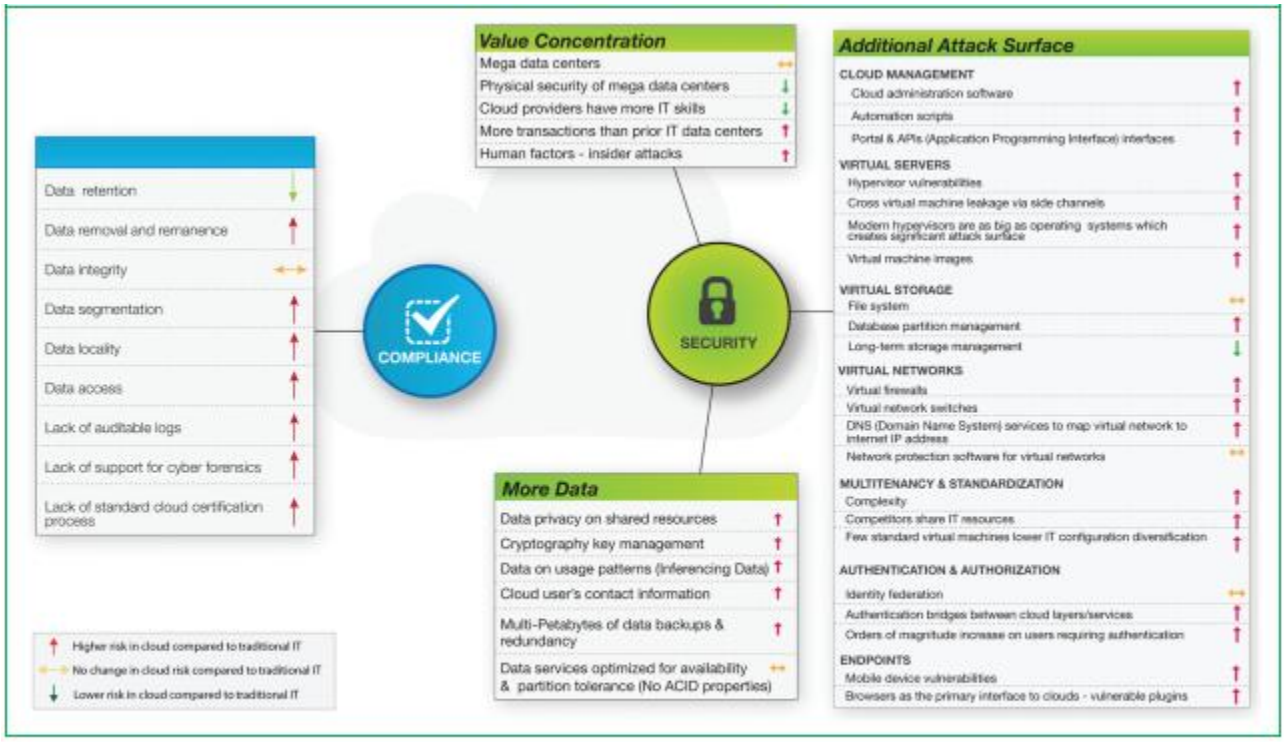

Figure 3

Cloud Security and Compliance Risks Framework. (IP: Internet Protocol.)

مثال دیگری از مقررات نسبتا جدید، قانون اصلاحات و مصرف کننده داد-فرانک وال استریت (Dodd-Frank) مصوب سال 2010 است. این قانون به موسسات مالی محدود نمی‌شود و بر حکومت و جبران اجرایی شرکت‌های مستقر در آمریکا تاثیر می‌گذارد. علاوه‌براین، مقررات انطباق صنعت بسیاری وجود دارد، مانند قوانین مرتبط با FFIEC (موسسات

مالی فدرال)، ISO (سازمان بین‌المللی استانداردسازی) X2700، NIST (موسسه ملی استاندارد و فناوری)، HIPAA، PCI-DSS، و غیره. چالش اصلی ایجاد یک سرویس IT است که بتواند از روند پیوستن به روش‌های کسب‌وکار نظارتی، تجاری و برای رسیدن به سطح انطباق مطلوب اطمینان حاصل کند.

امنیت ابر و چارچوب خطرات (شکل 3) یک بردار کلیدی موثر بر محیط ابر و به منظور تسهیل درک ابر و انطباق خطرات را نشان می‌دهد. هر بردار خطر به یک فلش اختصاص داده شده است که خطر در ارتباط با ابر را در مقایسه با روش سنتی به تصویر می‌کشد. چارچوب ارائه شده در این مقاله از یک فلش قرمز رنگ برای بیان خطر، یک فلش زرد افقی برای بردار خطر بین ابرها و تغییر تنظیمات IT سنتی، و یک فلش رو به پایین سبز برای ابراز خطر کمتر استفاده شده است.

بردارهای امنیتی به سه دسته سازماندهی شده‌اند: خطراتی که توسط سطح حمله، تراکم مقادیر و اطلاعات بیشتر نشان داده می‌شوند. سطح حمله جدید، نتیجه‌ی کدهای اضافی مورد نیاز برای مدیریت ابر و خدمات است. مدیریت ابر شامل فرایند اتوماسیون ابر است، که متشکل از هزاران اسکریپت است که نمونه‌برداری، به تصویر کشیدن، و چرخه عمر پایان به پایان برای راه‌حل‌های مجازی در ابر را خودکارسازی می‌کند. متاسفانه، سطح بلوغ نرم‌افزار مدیریت ابر، نسبتا کم است، و به ناچار به سمت آسیب پذیری متمایل است.

عامل خطر مجازی‌سازی به سه نوع تقسیم می‌شود: سرورهای مجازی، شبکه‌های مجازی و ذخیره‌سازی مجازی. همه این توانایی‌ها برای مجازی‌سازی منابع و به اشتراک‌گذاری در وظایف چندگانه است. قابلیت مجازی‌سازی یک سطح حمله اضافی، اما با انتخاب یک Hypervisor کوچک (به عنوان مثال، از نظر خطوط کد کوچک)، مانند Hypervisor نوع 1 می‌افزاید، که به‌طور قابل توجهی می‌تواند باعث کاهش خطر شود. دیگر مجازی‌سازی بسیار رایج محیط VM وسیع است. از آنجا که Hypervisor روند ایجاد VM جدید را ساده می‌کند، بسیاری از افراد تمایل به ایجاد ماشین‌های مجازی جدید به‌جای تنظیم مجدد قدیمی دارند. اگر ابر عملکرد خوبی به‌منظور بررسی و به‌روزرسانی اجرا در ماشین‌های مجازی غیرفعال نداشته باشد، می‌تواند به‌سرعت از تاریخ گذشته شود و نه تنها تبدیل به ویروس آسیب‌پذیری می‌شود بلکه عملکرد ضعیفی نیر خواهد داشت. تکنولوژی مجازی‌سازی موجب تسهیل در روند گرفتن تصاویر VM می‌شود،

که به‌طور قابل توجهی امنیت خطرات در دو جبهه را افزایش می‌دهد. ابتدا، راحتی در ایجاد تصویر VM موجب تسهیل به اشتراک‌گذاری VMها می‌شود. همزمان، اطلاعات نرم‌افزارهای مخرب و شاید محرمانه نیز می‌تواند ناخواسته در صورت فیلتر و یا حفاظت مناسب، به اشتراک گذاشته شود. خطر دوم که گرفتن تصویر ایجاد شده توسط نمایش سیستم مجازی در یک فایل است. در سیستم‌های سنتی، سیستم‌عامل از BIOS (خدمات ورودی و خروجی پایه) برای ارسال پشته داده‌ها به ROM (حافظه فقط خواندنی)، حفظ وضعیت اطلاعات و پردازش اجرایی استفاده می‌کند. در یک محیط مجازی شده، Hypervisor رابط BIOS را شبیه‌سازی می‌کند. به جای استفاده از ROM، در یک فایل بر روی دیسک که تصویر VM است می‌نویسد. اگر فایل تصویری رمزگذاری نشده باشد و یک فرد مخرب به دیسکی که در آن تصویر VM قرار دارد دسترسی یابد، تمام اطلاعات در VM در دسترس خواهند بود، حتی اگر VM در حال استراحت باشد (غیر فعال).

مجازی‌سازی ذخیره‌سازی قابلیت ارائه‌ی یک جایگزین کم هزینه برای ذخیره‌سازی سنتی را داراست. که اغلب برای حجم انبوهی از داده‌ها استفاده شده است- نوعی داده‌های بزرگ که در نهایت تقسیم شده‌اند. با نصب و راه‌اندازی داده‌های بزرگ (>10 TB) و چگالی بالا که مجازی‌سازی بر روی دیسک ایجاد می‌کند، تقریبا مسلم است که پارتیشن‌ها به وقوع می‌پیوندد. که دلیل برای پایگاه داده و سیستم فایل‌های توزیع‌شده جدید مانند GFS ** (سیستم فایل گوگل) است که برای کمک به پارتیشن‌بندی در ذخیره‌سازی داده‌های بزرگ ایجاد شده است [28]. بااین‌حال، تمام این فن‌آوری‌های جدید سطوح حمله اضافه می‌کنند. علاوه‌براین، فن‌آوری هنوز برای ایجاد پتانسیل آسیب‌پذیری نابالغ است. بااین‌حال، منافع آن برای افزایش کارایی و دردسترس بودن غیرقابل انکار است.

ابرها شبکه‌های تزیینی با ساختارهای منطقی ایجاد می‌کنند که قادر به اختصاص آدرس‌های خصوصی در میزبان مجازی هستند. شبکه مجازی‌شده مزایای بسیاری مانند انعطاف‌پذیری کامل در طبقه‌بندی شبکه دارد. شبکه مجازی‌شده نیز هر گونه محدودیت بر اساس آدرس IP فیزیکی (پروتکل اینترنت) ارائه شده توسط ارائه‌دهنده شبکه را حذف می‌کند و کل تنظیمات شبکه می‌تواند به راحتی در یک فایل که به‌راحتی قابل دسترسی و ترکیب با تصویر VM برای تکرار یک VM خاص نیست بلکه برای تمام راه‌حل‌های فناوری اطلاعات مرتب می‌شود. بااین حال، نقاط قوت

شبکه‌های مجازی نیز نقاط ضعف خود را دارند. به‌عنوان یک شبکه مجازی که در یک فایل حاوی مشخصات شبکه مرتب شده است، خطر دسترسی غیرمجاز به تنظیمات شبکه بسیار بالاتر از تنظیمات سنتی است که از شبکه فیزیکی دستگاه‌ها استفاده می‌کنند. مانند دیگر اطلاعات حساس، مشخصات فایل‌های شبکه نیز نیاز به محافظت و رمزگذاری دارند چرا که این فایل‌های اطلاعاتی می‌توانند برای هکرها و افراد مخرب بسیار مفید باشند. علاوه‌براین، مولفه‌های شبکه فیزیکی مانند فایروال و سوئیچ شبکه با اجزای نرم‌افزار جایگزین می‌شوند، بنابراین نیاز به حصول اطمینان داریم که این مولفه‌ها به‌طور منظم در معرض آسیب‌پذیری قرار نداند.

خطرات امنیتی ابر را می‌توان با اجتناب از rogue VM کاهش داد و تنها از تصاویر ایجاد شده توسط VM استفاده کرد. (در اینجا، ما از عبارت rogue VM برای اشاره به ماشین‌های مجازی ایجاد شده با استفاده از تصاویر VM مدیریت نشده از منابع غیرمعتبر استفاده می‌کنیم.) در صورت امکان، شرکت‌ها باید تصاویرVM شرکت خود را ایجاد کنند، و آن را بین کارکنان خود پخش کنند و تصاویر را در فایلی امن ذخیره کنند. بااین‌حال، اگر لازم به استفاده از ماشین‌های مجازی ارائه شده توسط فروشندگان بود، باید اطمینان حاصل کنیم که تصاویر VM یک امضای دارند که می‌تواند توسط فروشنده اصلی ردیابی شوند. اگر یک تصویر VM یک امضای نداشته باشد، توصیه به استفاده از آن نمی‌شود. علاوه‌براین، غیرفعال و یا محدود کردن استفاده از ابزار خطرناک مجازی که اغلب توسط هکرها برای شکستن یک محیط مجازی مورد استفاده قرار می‌گیرد توصیه نمی‌شود. بعضی از این ابزار از کانال‌های ارتباطی خصوصی بین hypervisor و سیستم عامل میزبان استفاده می‌کنند که اجازه می‌دهد ارتباطات cross-VM رخ دهد. به‌عنوان مثال، ابزار VMchat، VMCat، و VMftp از ComChannel در نرم‌افزار VMware ** برای دسترسی در سراسر VM ها استفاده می‌کنند. بنابراین باید دنبال توصیه‌های پیکربندی ارائه شده توسط فروشنده hypervisor از یک حیط مجازی باشیم تا شکستن محیط بسیار مشکل گردد. در سال 2010، VMware نشان داد که چگونه برای پیکربندی hypervisor خود عمل کنیم. این راهنما باید برای هر کسی از نرم‌افزار VMware استفاده می‌کند دردسترس باشد [29]. دیگر توصیه‌های اضافی بر اهمیت امنیت تمرکز دارند تا اطمینان حاصل شود که توسعه‌دهندگان ممیزی‌های امنیتی منظمی در برنامه‌های کاربردی وب برای جلوگیری از حملات رایج، از جمله حمله SQL انجام

می‌دهند. علاوه‌براین، ممیزی منظم شخص ثالث و تست نفوذ باید برای به دست آوردن ایده‌های تجربی در سطح امنیتی ارائه‌دهندگان ابر صورت گیرد.

توسعه‌ی چارچوب، برخی از خطرات را کشف می‌کند. برای مثال، چندین قانون نیاز مشترک به ذخیره‌سازی امن داده‌ها دارند. یک فرآیند باید در محلی قرار گیرد تا از باقی‌مانده داده‌ها برای بازسازی اطلاعات حذف شده اطمینان حاصل کند. برای مثال، در مورد تنظیم HIPAA، حذف PHI (اطلاعات بهداشتی شخصی) بدین شکل صورت می‌گیرد که ذخیره‌سازی فیزیکی به‌طور کامل پاک می‌شود. هر گونه اثری از اطلاعات واقعا باید از هر دو نمونه حذف شوند. این نوع از نیازمندی نشان‌دهنده‌ی یک چالش معنی‌دار در خدمات ابر است، زیرا محل ذخیره‌سازی و مدیریت‌ها برای تعیین مشکل است. مشتریان ابر با نیازمندی‌های HIPAA می‌توانند حذف روش خاصی را در SLA برای مدیریت ذخیره‌سازی درخواست کنند. با این حال، از آنجا که ارائه‌دهندگان ابر در حال حاضر رابط‌های برنامه‌نویسی نرم‌افزار حسابرسی (API ها) را برای فعال کردن تایید یا حذف مناسب اطلاعات ارائه کرده‌اند، یک مسئله قابل اعتماد بین مشتریان ابر و ارائه‌دهندگان ابر پا برجاست. بدون ممیزی رابط‌های برنامه کاربردی به‌منظور بررسی روش‌های ارائه‌دهنده ذخیره‌سازی ابر و ارائه‌دهنده خدمات مدیریت (MSP)، مشتری ابر می‌تواند خطرات حسابرسی زیادی را متحمل شود. مسئولیت پذیرش با فروشندگان نیست بلکه با نهادها است. برای مثال، یک فروشنده ابر ممکن است روش SLA ها را دنبال کند و مشتری ابر ممکن است با توجه به عدم اجرای صحیح فروشنده در درخواست‌ها شکست بخورند. از آنجا که ارائه‌دهندگان ابر معمولا مشتریان خود را برای مجازات مشخص نمی‌کنند، هر گونه مسئولیت مالی متوجه کاربر می‌گردد.

اطلاعات بهداشت و درمان، اطلاعات دولت، اطلاعات کارمندان و معاملات مالی از اطلاعات به شدت تنظیم شده هستند که انطباق از الزامات آنها است. محل مورد نیاز در داده‌ها شامل نیاز به دانستن سایت فیزیکی واقعی سرور و خدمات ذخیره‌سازی و یا استفاده از داده‌ها است. بسیاری الزامات مشخص شده، منطقه، شهرستان، و یا کشوری است که در آن داده‌ها باید قرار گیرند. اگر الزامات مکانی ارضا نشود، بسیاری از مقررات تصریح مجازات پرهزینه خواهد بود. در برخی موارد، کسب‌وکار می‌تواند مجوز خود را از دست بدهد. با توجه به این ابهام که اکثر ارائه‌دهندگان ابر صرفا در

سرویس‌های ذخیره‌سازی خلاصه می‌شوند، مشتریان ابر لازم نیست توانایی نظارت یا ممیزی خودکار بر محل ذخیره‌سازی ابر که مصرف می‌کنند داشته باشند. خطر عدم انطباق در مورد مکان داده در ابر بالاتر از خدمات IT سنتی است، که در آن CIO کنترل کامل مکان فیزیکی سرورها و ذخیره‌سازی را دارد.

یکی دیگر از نگرانی‌های انطباق توانایی انجام پزشکی قانونی کامپیوتری است. به‌عنوان مثال، HIPAA، PHI، و FFIEC، نیاز به تشخیص تقلب دارند، و این خواسته به خدمات فناوری نیاز دارد که می‌تواند قابلیت‌های سایبری پزشکی قانونی را پشتیبانی کند. در هنگام کار با داده‌های حساس و معاملات باید پشتیبانی منظم، کسب‌وکار نیاز به پزشکی قانونی کامپیوتری دارد. هنگامی که یک دعوای حقوقی مطرح می‌شود، کسب‌وکار نیاز به تولید شواهد کافی برای برآوردن درخواست دادگاه برای کسب اطلاعات بیشتر دارد. پزشکی قانونی سایبری به لاگ‌ها، جزئیات تاریخ دسترسی به داده‌ها، پیکربندی سخت‌افزار، تصاویر VM، شبکه توپولوژی، و بسیاری از نقاط دیگر داده نیاز دارد که می‌تواند به تکثیر کل محیط کمک کند. بسیاری از داده‌های آرشیوی ماهانه معمولا برای ایجاد یک الگو، شواهدی کافی از سهل‌انگاری و یا تقلب را نیاز دارند. بااین حال، بسیاری از ابرها اطلاعات لازم را جهت تولید مجدد محیط حفظ نمی‌کنند. جنبه‌ی پویا ابر که در آن ماشین‌های مجازی به‌طور مداوم ایجاد و نابود می‌شوند، بدون لاگ و نقاط داده ناقص هستند، که تولید مجدد محیط را بسیار دشوار می‌کند. حفظ داده‌ها برای یک دوره زمانی طولانی هزینه‌های قابل توجهی در پیش دارد و مدیران IT نیاز به مبادلات پرهزینه و انطباق خطرات نمی‌بینند. بااین حال، از آنجا که در حال حاضر ابزار پزشکی قانونی پاسخگو نیستند بازتولید محیط ابر به عنوان یک چالش باقی‌مانده است و حفظ اطلاعات اضافی با عدم بلوغ فنی کمکی نمی‌کند. بااین حال، انتظار می‌رود که ابزار پزشکی قانونی ابر بهتر عمل کنند و حفظ داده‌ها بسیار مفید عمل خواهد کرد.

چارچوب خطرات کسب‌وکار ابر

چارچوب خطرات کسب‌وکار، که در شکل 4 نشان داده شده است، هزینه تقسیم، بهره‌وری، کنترل، دردسترس بودن و پیچیدگی حقوقی است. هزینه (به‌عنوان مثال، کاهش سرمایه‌گذاری و کاهش هزینه‌های عملیاتی) یکی از معدود

عواملی است که کارشناسان به اتفاق آرا بر آن نظر مثبت دارند. به نظر می‌رسد کارشناسان به باور قاطع در مورد مزایای قابل توجهی که مدل ابر برای کسب‌وکار به ارمغان می‌آورد رسیده‌اند.

مدل کسب‌وکار ابر حذف به سرمایه‌گذاری را نیاز می‌کند و هزینه های عملیاتی را به طور قابل توجهی کاهش می‌دهد و انعطاف‌پذیری در پرداخت را میسر می‌کند چراکه یک پرداخت فقط برای مقداری مصرف است. علاوه براین، مهارت‌ها و آموزش‌های مورد نیاز برای حفظ ماشین‌های مجازی ابر به‌طور قابل توجهی پایین‌تر از تخصص و بینش لازم برای حمایت سنتی است. این نقطه خاص در مهارت نه تنها توسط کارشناسان بلکه در بسیاری از منابع دیگر پشتیبانی شده است [22، 30]. انعطاف‌پذیری در پرداخت با توجه به چه استفاده شده است، مدل به کارگفته شده در ابر توسط ارائه‌دهندگان آمازون، GoGrid و Rackspace است. بنابراین ما قادر به پیدا کردن هر گونه نظر متفاوتی با توجه به مزایای داشتن یک ساختار پرداخت انعطاف‌پذیر برای ابرها نیستیم.

درک چگونگی محاسبه هزینه‌های ماشین‌های مجازی براساس یک سناریوی داده شده از اهمیت کلیدی برخوردار است زیرا قیمت ماشین‌های مجازی به طور قابل توجهی براساس پیکربندی و ارائه‌دهنده متفاوت است. پس از محاسبه هزینه‌های ماشین‌های مجازی، گام بعدی ارزیابی هزینه‌های کلی مرتبط با ابر در مقایسه با مرکز دادهIT مستقر در خانه است. مقایسه هزینه‌ی ابر در مقابلIT سنتی باید با در نظر گرفتن حجم کار موثر انجام یافته در محیط‌های ابری نسبت به سنتی باشد و، نیز، چه ویژگی‌هایی باعث می‌شود حجم کار برای ابرها نامناسب باشد. یافته‌های این مقاله به جای سازگاری با انتظارات تعجب آور نیست، چرا که حجم کار با متغیر یا الگوی تقاضا bursty کاندید خوبی برای خدمات ابر است. همچنین الگویbursty می‌تواند با پیک‌های قابل پیش‌بینی ناشی از تفاوت در خواسته‌ها با توجه به زمان در روز، روز درهفته و یا الگوهای دوره‌ای مانند مالیات ایجاد شود. برای مثال، در ایالات متحده، بسیاری از وب سایت‌های بانکی خانه، زمان اوج از ساعت 16:00-19:00 است. اولین موج از تقاضاها در سواحل شرق و غرب حرکت در این زمان رخ می‌دهد.

با حجم کار قابل پیش‌بینی، IT سنتی به‌سمت overprovision زیرساخت‌های فناوری تمایل می‌یابد، که به‌طور معمول شامل بالاترین تقاضای ممکن است، به علاوه یک بافر برای ایمنی.

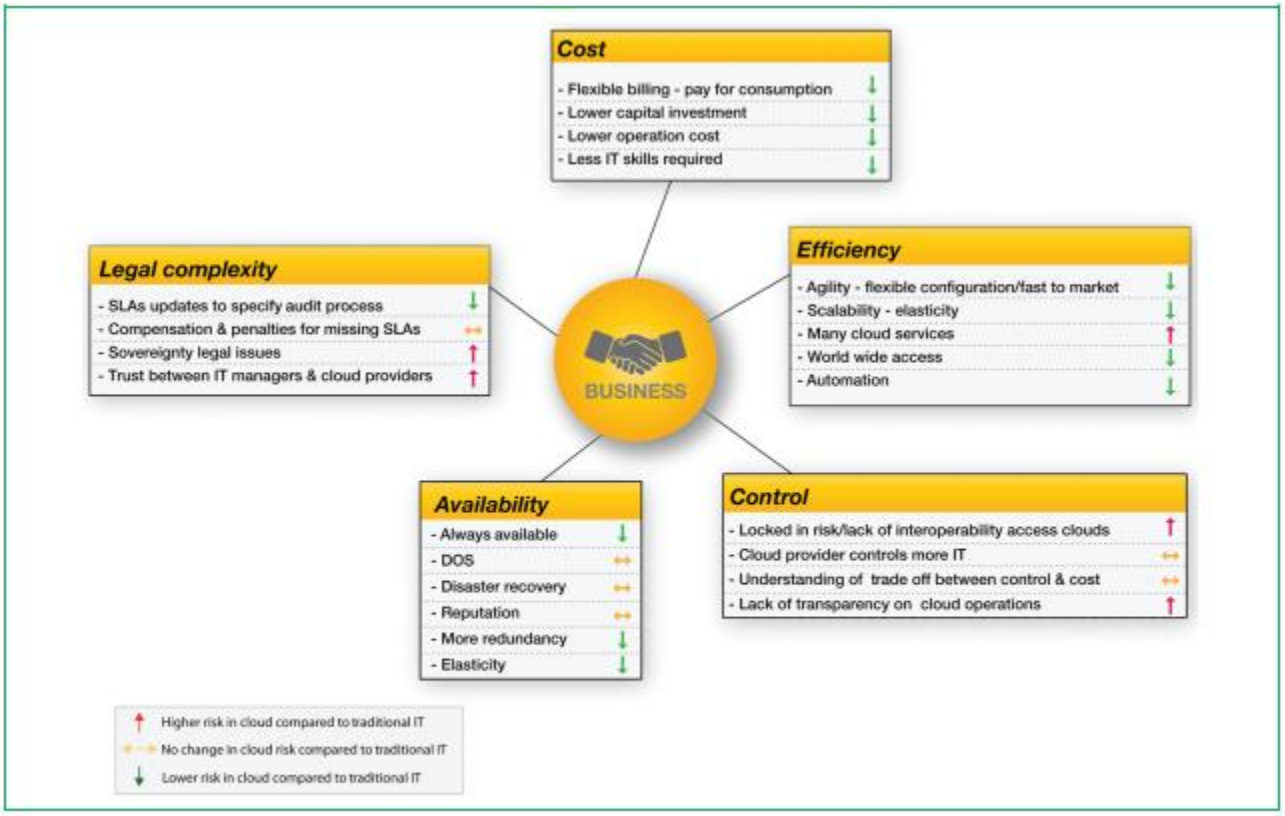

Figure 4

Cloud Business Risks Framework.

مشکل این نوع رویکرد هزینه سرمایه (CAPEX) قابل توجه آن است، اما بسیاری از تجهیزات برای مدت طولانی در دوره بیکار می‌مانند. تفاوت بین نیازهای متوسط و اوج می‌تواند با نرخ متوسط (PAR) در حدود دو یا سه قابل توجه قرار گیرد، که به معنی افزایش 100٪ تا 200٪ در اوج حجم متوسط باشد. الگوهای قابل پیش‌بینی مرتبط با چرخه کسب‌وکار، تبلیغات و فروش و یا رویدادهای خاص سالانه مانند کریسمس و مالیات می‌تواند مقادیر PAR از 4 تا 10تولید کند. راه‌حل‌ها با الگوهای bursty غیرقابل پیش‌بینی نامزد خوبی برای ابرها هستند زیرا کشش ابر خطر اجرای خارج از ظرفیت را کاهش می‌دهد.

یکی دیگر از مزایای کسب‌و کار ابرها این است که قادر به انتخاب بسیاری از وظایف سنگین برای حفظ ظرفیت بالای سیستم هستند. که در تضاد با IT سنتی، عدم مجازی‌سازی، چند مستاجره است، و تعداد کمی کار برای بهینه‌سازی حجم کار جهت حفظ بهره‌برداری بالا انجام می‌گیرد. در IT سنتی، بسیاری تنظیمات حجم کار به دلیل مشکلات مرتبط با خدمات به عهده‌ی شخص است. وضعیت در ابرها بسیار متفاوت است. فن‌آوری اتوماسیون و مجازی‌سازی

موجب تسهیل حرکت ماشین‌های مجازی به حجم کار زیاد می‌شود، درنتیجه استفاده از منابع IT به حداکثر می‌رسد. به‌عنوان مثال، راه‌حل‌های موجود برای محدوده‌های زمانی مختلف که تقاضای زیادی دارند می‌تواند برای حفظ استفاده از سخت افزار بالاتر ترکیب شوند. ابرها تمایل به کار در 95٪ در مقایسه با استفاده از IT سنتی در 15 درصد را ارند [31]. با استفاده از این شکاف در بهره برداری از سخت افزار، تعجب آور نیست که ارائه‌دهندگان ابر قادر به ارائه منابع در چنین هزینه‌ی پایینی باشند.

در IT سنتی، خرابی به علت شکست سخت افزار بسیار متفاوت از خرابی در ابرها است. مسئله این نیست که چه زمانی سرور یا VM در ابر شکست خواهد خورد، اما سرعت ابر در بهبود یک شکست می‌باشد. در IT سنتی، شکست یک سرور فیزیکی می‌تواند یک رویداد دراماتیک باشد، و گاهی اوقات مقدار قابل توجهی زمان برای بهبود نیاز داشته باشد. حتی در مورد دسترسی بالا سیستم‌های با پایگاه داده آینه، فرایند بازیابی برای جایگزینی سیستم شکست خورده و بازیابی پیکربندی با دسترسی بالا طول می‌کشد. بهبود ممکن است نیاز به تنها چند ساعت تلاش داشته باشد، یا ممکن است روزها یا حتی هفته‌ها طول بکشد. از سوی دیگر، بازیابی شکست در ابر در عرض چند دقیقه با توجه به اسکریپت خودکار و استفاده از تصاویر استاندارد VM رخ می‌دهد. اتفاقاتی که در یک مرکز داده سنتی فاجعه بار است. این یک تناقض است، چرا که شکست در ابرها شایع‌تر از روش سنتی است؛ بااین حال، با توجه به افزونگی قابل توجه، خطر ابتلا به نارسایی تا حد زیادی کاهش می‌یابد. ممکن است بپرسید که چرا ابرها بیشتر از IT سنتی شکست می‌خورند؟ این شکست در نتیجه حجم انبوهی از سیستم‌های ذخیره‌سازی در حال اجرا و در 95٪ استفاده در مراکز داده مگا است. با بررسی معادله احتمال شکست در مدت زمان P(t)، می‌توانیم مشاهده کنیم که متوسط زمان برای شکست (MTTF) کاهش می‌یابد، احتمال وقوع شکست افزایش می‌یابد:

$$P(t)_{\text{failure}} = 1 - e^{-kt}, \text{ where } k = 1/MTTF$$

معادله نمایی توزیع شکست به ما کمک می‌کند نرخ شکست در طول زمان بر اساس MTTF را مدل‌سازی کنیم[32]. چرا که ابرها تمایل به MTTF پایین‌تر از سایر مراکز داده دارند و میزان شکست در ابرهای بالاتر از IT سنتی است [33، 34]. همچنین ممکن است بپرسید چرا MTTF در ابرها نسبت به IT سنتی تمایل به کمتر دارد؟ این مسئله‌ای

است که بسیاری از سیستم‌های کامپیوتری و ذخیره‌سازی در حال مطالعه آن هستند. چندین مرجع داده در دسترس از اینتل [32] و دیگران [24، 33] پیشنهاد داده‌اندکه یک محصول جانبی با استفاده بالا از منابع در محیط‌های ابری کوتاهتر از MTTF است. براساس تجارب مرتبط با مراکز داده بزرگ، کارشناسان شرکت کننده در این مطالعه بر این عقیده هستند که MTTF پایین توسط دو عامل ایجاد می‌گردد: ابرها از منابع با شدت بیشتری استفاده می‌کنند و سخت‌افزار در بسیاری از ابرها، سخت‌افزار با MTTF پایین است. هر دو این عوامل می‌تواند به پایین بودن MTTF در ابر کمک کند [32]. در کنفرانس انجمن توسعه اینتل در سال 2011، Siewert Sam و Greg Scott آمار مشابهی نشان دادند [32]. که در تضاد با IT سنتی قرار دارد، که در آن سخت‌افزار 85 درصد از زمان را بیکار اجرا می‌شود و ذخیره‌سازی و سرویس‌دهنده معمولا از کیفیت برتری برخوردار هستند. عامل اصلی MTTF پایین در ابرها مشخص نیست، اما یک معیار رایج توسط ارائه‌دهندگان ابر است.

همانگونه که پیشنهاد شد، ابرها با وجود شکست ثابت سیستم به دلیل افزونگی بزرگ و اتوماسیون، توهم "همیشه در دسترس بودن" را ارائه می‌کنند. اتوماسیون امکان بازیابی بسیار سریع دارد، که به حداقل رساندن خرابی سیستم کمک می‌کند. زمان کوتاه‌تر بهبودی، در دسترس بودن بهتری ارائه می‌کند. به‌طور مشابه، افزونگی بیشتر یک سیستم، در دسترس بودن بهتری به همراه دارد [30].

از دیدگاه حقوقی بسیاری از مسائل در ارتباط با قرارداد ابر، به دلیل قوانین مبهم و محدود (به‌عنوان مثال، مرز بین کشور) و عدم سابقه برای هدایت دادخواهی وجود دارد. اکثر قراردادهای استاندارد براساس " شبیه" هستند، که به معنی سرویس بدون هیچ وعده‌ای است. هیچ تضمینی وجود ندارد که سرویس ابری مناسب خواهد بود و یا انتظارات مشتری را برآورده خواهد کرد. نه تنها ارائه‌دهندگان ابر SLA ها را ارائه می‌کنند بلکه کسانی وجود دارند که اطمینان براساس دسترسی را مشخص می‌کنند. همچنین، فقدان استانداردها یک مشکل برای قرارداد ابر است چرا که هیچ راه‌حل متحدی برای ارائه خدمات ابر وجود ندارد و هیچ معیار استانداردی برای کمک به تعیین کیفیت خدمات وجود ندارد.

جریان داده مرزی معمول است چرا که داده‌ها در کشورهای مختلف قرار دارند و سرویس ابری و مشتری در کشورهای مختلف دیگر واقع شده‌اند. جریان داده‌ای که از مرزهای یک کشور بنا به صلاحیت دادگاه‌های کشورهای مختلف عبور می‌کند به‌دلیل قوانین مبهم و متناقض می‌تواند هزینه های دعوی قضایی پرهزینه ایجاد کند. جریان داده مرزی بسیاری از مسائل بالقوه قانونی دارد که می‌تواند به‌دلیل کارکرد نامناسب از داده‌ها، نابرابری بین مقررات IT بسته به کشور و ابهام در مورد تعهدات در صورت بروز اختلاف بوجود آید. برای جلوگیری از برخی از این مشکلات، مدیران فناوری اطلاعات باید به‌طور کامل از برآوردن نیازهای کسب‌وکار و جلوگیری از ابهام در مورد نقش‌ها، مسئولیت‌ها و فرآیندهای مذاکره کنند ابر موافقت حاصل کنند.

نتیجه‌گیری

انتظار می‌رود که چارچوب توصیف شده در این مقاله توسط مدیران IT به‌عنوان راهی برای توجیه بسیاری از خطرات مرتبط با رایانش ابری و برای کمک به افزایش درک خطر ابر استفاده شود. علاوه‌براین، این مقاله از این فرضیه که مجموعه‌ای از خطرات ابر شامل برخی از خطرات جدید و همچنین خطرات در حال حاضر موجود درIT سنتی هستند پشتیبانی می‌کند. برخی خطرات امنیتی جدید ابر، از جمله چند مستاجری، سطح بالایی از اتوماسیون، و حجم مقادیر بالا در مرکز داده IT مگا برخی از خطرات جدید امنیتی هستند که در درجه بالاتری از روش سنتی قرار دارند. علاوه‌براین، خطرات ابر مربوط به ناتوانی در انجام پزشکی قانونی کامپیوتری مناسب، حاکمیت داده‌ها و پسماند داده‌ها (به‌عنوان مثال، داده‌های باقی‌مانده پس از تلاش برای حذف اطلاعات) است که بسیاری از خطرات جدید در ارتباط با ابرها در مقایسه با فناوری‌های سنتی افزایش می‌یابد. بااین حال، برخی از خطرات ابر در روش سنتی پابرجاست. براساس داده‌های جمع‌آوری شده، می‌توان نتیجه گرفت که بسیاری از خطرات محاسبات ابری متفاوت و مجزا از خطرات سنتی آن هستند، که روش سنتی هنوز هم نسبت به ریسک‌های ناشی از محاسبات ابری متفاوت است و خطراتی وجود دارد که در سراسر هر دو محیط به اشتراک گذاشته است، یک تقاطع خطر بین مجموعه خطرات ناشی از ابر و IT سنتی ایجاد می‌کند. در شکل 5 خواننده می‌تواند تقاطع بین دو مجموعه از خطرات را، دایره آبی برای ابر و دایره سبز برای

IT سنتی، مشاهده کند اما هنوز هم خطرات منحصر به فرد قابل توجهی در ارتباط با هر مجموعه وجود دارد. در گوشه پایین از شکل 5، ما می‌توانیم دیدگاه کسب‌وکار را ببینیم که مجموعه خطرات فناوری‌های سنتی (دایره سبز) بزرگتر از مجموعه خطرات ابر (دایره آبی رنگ) است.

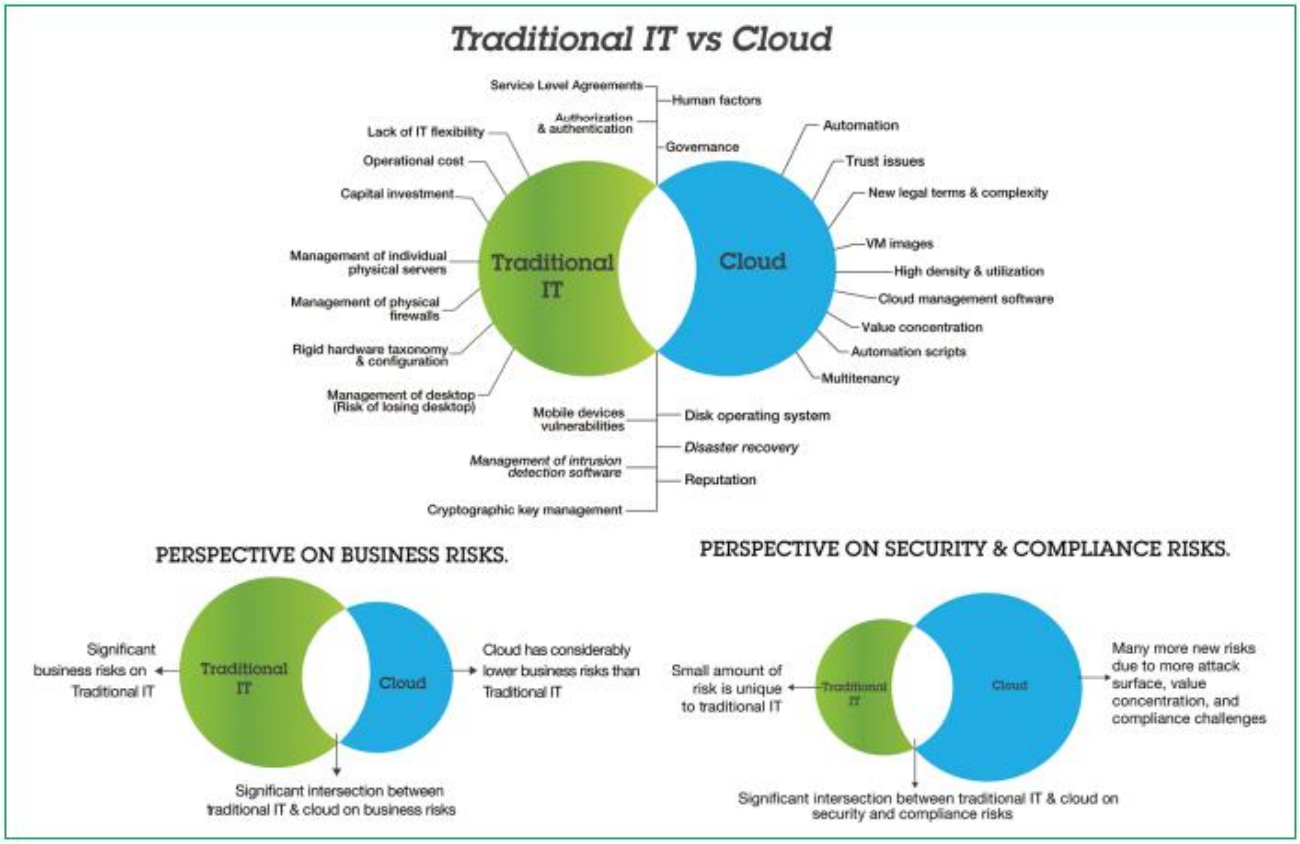

Figure 5

Traditional IT and cloud risks sets intersect, as shown on the top diagram. From the perspective of business risks, traditional IT has considerable more risks than clouds. However, from the perspective of security and compliance, clouds have more risks than traditional IT.

همانطور که در گوشه سمت راست پایین شکل5 نشان داده شده است، از دیدگاه امنیت، مجموعه خطرات ابر (دایره آبی) به‌طور قابل ملاحظه‌ای بزرگتر از خطرات IT سنتی (دایره سبز) تعیین می‌گردد، نتیجه‌گیری دوم از این مقاله، از دیدگاه امنیت و انطباق، ابرها خطرات بالاتری نسبت به IT سنتی دارند.

همچنین به این نتیجه می‌رسیم که در بسیاری از استراتژی‌های براساس کاهش برای ابر، سرعت پیشرفت تکنولوژی ابر بسیار بالاست و مزایای اقتصادی قابل توجهی را به همراه دارد، بنابراین پیش‌بینی می‌کنیم که بسیاری از خطرات

ابر که در این مقاله شرح داده شدند در طول زمان کاهش خواهند یافت و ابرها را تبدیل به یک مکان بسیار امن و احتمالا مدل تحویل IT ارجح برای هر سرویسی خواهند کرد.

References

1. S. K. Crook, C. J. Kolodgy, S. Hudson, and S. D. Drake, BWorldwide mobile security 2011–2015 forecast and analysis,[IDC, Framingham, MA, USA, Rep., Mar. 2011.

2. C. Arthur, BHalf of UK population owns a smartphone,[in Guardian, London, U.K., 2011. [Online]. Available: http://www.guardian.co.uk/technology/2011/oct/31/ half-uk-population-owns-smartphone

3. S. Ramgovind, M. M. Eloff, and E. Smith, BThe management of security in cloud computing,[in Proc. ISSA, Aug. 2010, pp. 1–7.

4. C. Liebert and M. Posey, BSecurity highlights from the 2010 U.S. WAN manager survey,[IDC, Framingham, MA, USA, Rep., Jan. 2011. [Online]. Available: http://www.idc.com/ research/viewdocsynopsis.jsp?containerId=226221&sectionId= null&elementId=null&pageType=SYNOPSIS.

5. T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and PrivacyVAn Enterprise Perspective on Risks and Compliance. Sebastopol, CA, USA: O'Reilly Media, 2009.

6. M. Christodorescu, R. Sailer, D. L. Schales, D. Sgandurra, and D. Zamboni, BCloud security is not (just) virtualization security: A short paper,[in Proc. ACM Workshop Cloud Comput. Sec., New York, NY, USA, 2009, pp. 97–102.

7. B. R. Kandukuri, R. Paturi V, and A. Rakshit, BCloud security issues,[in Proc. IEEE Int. Conf. Services Comput., Bangalore, India, 2009, pp. 517–520.

8. L. Edward, K. Amokrane, D. Lourdeaux, and J. Barthes, BAn ontology for managing a virtual environment for risk prevention,[in Proc. 1st Int. Conf. Integr. Intell. Comput., 2010, pp. 62–67.

9. C. Cachin and M. Schunter, BA cloud you can trust: How to ensure that cloud computing's problemsVData breaches, leaks, service outagesVDon't obscure its virtues,[in Proc. ICITST, Dec. 2001, pp. 214–219, IEEE.

10. P. Zech, BRisk-based security testing in cloud computing environments,[in Proc. 4th IEEE Int. Conf. Softw. Testing, Verification Validation, Berlin, Germany, Mar. 21–25, 2011, pp. 411–414.

11. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, BHey, you, get off of my cloud: Exploring information leakage in third-party compute clouds,[in Proc. ACM Conf. CCS, Chicago, IL, USA, Nov. 9–13, 2009, pp. 199–212.

12. G. J. Skulmoski, F. T. Hartman, and J. Krahn, BThe Delphi method for graduate research,[J. Inf. Technol. Educ., vol. 6, no. 1, pp. 1–21, 2007.

13. C. Okoli and S. D. Pawlowski, BThe Delphi method as a research tool: An example design considerations and applications,[Inf. Manage., vol. 42, no. 1, pp. 15–29, Dec. 2004.

14. D. Morton, BIBM mainframe operating systems: Timeline and brief explanation for the IBM system/360 and beyond,[IBM, Armonk, NY, USA, Rep., Sep. 2011. [Online]. Available: http://www.demorton.com/Tech/##OSTL.pdf.

15. T. J. Bittman and L. Leong, BVirtual machines will slow in the enterprise, grow in the cloud,[Gartner, Stamford, CT, USA, Rep. No. G00210732, Mar. 4, 2011.

16. E. C. G. T. Sacconaghi and M. R. Shah, BIT hardware: Does a move to large public clouds and data centers hurt or help server OEMs?[Bernstein Res., London, U.K., Rep., Apr. 6, 2011.

17. Richard, BAmazon says AWS outage was a FRe-mirroring Storm._,[in Cloud News Daily, Accessed Dec. 14, 2011. [Online]. Available: http://cloudnewsdaily.com/2011/04/amazon-saysaws-outage-was-a-re-mirroring-storm/

18. K. Oberle and M. Fisher, BETSI CLOUDVInitial standardization requirements for cloud services,[in Proc. GECON, 2010, pp. 105–115.

19. T. Rings, J. Grabowski, and S. Schulz, BOn the standardization of a testing framework for application deployment on grid and cloud infrastructures,[in Proc. Adv. Syst. Testing VALID Lifecycle Conf., 2010, pp. 99–107.
20. T. J. Bittman, BThe road map from virtualization to cloud computing,[Gartner, Stamford, CT, USA, Rep. No. G00210845, Mar. 3, 2011.
21. S. A. Almulla and C. Y. Yeun, BCloud computing security management,[in Proc. ICESMA, Sharjah, United Arab Emirates, 2010, pp. 1–7.
22. D. Chappell, Introducing the Azure Services Platform: An Early Look at Windows Azure, .Net Services, SQL Services, and Live Services, Oct. 2008, Report.
23. IBM X-Force 2011–Mid-Year Trend and Risk Report, IBM Corporation, Armonk, NY, USA, Sep. 2011.
24. E. Pinheiro, W. Weber, and L. A. Barroso, BFailure trends in a large disk drive population,[in Proc. 5th USENIX Conf. FAST, 2007, p. 2.
25. F. Brown and R. Ragan, BPulp google hackingVThe next generation search engine hacking arsenal,[in Proc. Black Hat, Las Vegas, NV, USA, 2011, pp. 1–70. [Online]. Available: https://media.blackhat.com/bh-us-11/Brown/BH_US_11_BrownRagan_Pulp_Google.pdf.
26. J. Browne, Brewer's CAP Theorem, Accessed Jan. 11, 2009. [Online]. Available: http://www.julianbrowne.com/article/viewer/ brewers-cap-theorem
27. K. D. Mitnick and W. L. Simon, The Art of Deception: Controlling the Human Element of Security. Hoboken, NJ, USA: Wiley, 2003.
28. S. Ghemawat, H. Gobioff, and S. Leung, BThe google file system,[in Proc. Symp. Oper. Syst. Principles, Lake George, NY, USA, Oct. 19–22, 2003, pp. 29–43.
29. VMware vSphere 4.0–Security Hardening Guide, VMware, Palo Alto, CA, USA, May 2010, pp. 1–70, Report.
30. B. S. G. Linden and J. York, BAmazon.com recommendations: Item-to-item collaborative filtering,[IEEE Internet Comput., vol. 7, no. 1, pp. 76–80, Jan./Feb. 2003.
31. M. Azua, The Social Factor : Innovate, Ignite, and Win through Mass Collaboration And Social Networking. Upper Saddle River, NJ, USA: IBM Press, 2009.
32. S. Siewert and G. Scott, BNext Generation Scalable and Efficient Data Protection,[in Proc. Intel Develop. Forum, 2011, pp. 1–30. [Online]. Available: http://ecee.colorado.edu/~siewerts/ SF11_STOS004_101F.pdf.
33. S. Subashini and V. Kavitha, BA survey on security issues in service delivery models of cloud computing,[J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 1, 2011.
34. B. Schroeder and G. A. Gibson, BDisk failures in the real world: What does an MTTF of 1,000,000 hours mean to you?[in Proc. 5th USENIX Conf. FAST, San Jose, CA, USA, 2007, pp. 1–16.