به نام خدا

دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

Ethics in Cloud Computing

گزارش پروژه درس اخلاق حرفه ای در IT

فربد بهنامی نیا - ۹۳۲۳۹۲۳

استاد درس :

دکتر محمدحسین منشئی

اردیبهشت ۱۳۹۵

فهرست مطالب

عنوان **صفحه**

چکیده

در دنیای امروز و قرن ۲۱ با پیشرفت فناوری اطلاعات و اراتباطات همه چیز به سمت پردازش ابری منتقل شده یا در آینده خواهد شد . ساده ترین کارهای امروزه ی ما از جمله به اشتراک گذاری اتفاقات روزانه در شبکه های اجتماعی با دوستان ، پیام های اینترنتی و سایر ارتباطات در فضای مجازی مبنتی بر پردازش ابری هستند . در این گزارش ابتدا پردازش ابری معرفی می شود و بیان می شود که چرا در عصر کنونی پردازش ابری از مزایای خوبی برخوردار است . پیدایش مفاهیم اساسی رایانش ابری به دهه ۱۹۶۰ بازمی گردد . اهمیت و عملکرد رایانش ابری به گونه ای است که امروزه تمامی شرکت های بین المللی با تحقیقاتی گسترده و تلاشی خستگی ناپذیر در پی گسترش این فناوری بوده و هر روزه خدمات جدید و جالبی را در اختیار کاربران قرار می دهند . از دیگر جنبه هایی که باید راجع به پردازش ابری بررسی کرد رعایت موازین اخلاق حرفه ای ، حقوق و مقررات در قبال کاربران و همچنین ارائه کنندگان خدمات است . در این زمینه به چالش های کلی ابر ، امنیت ، و حریم شخصی در ابر پرداخته می شود . تمامی موارد گفته شده را دربارهٔ شرکت SAP ، سرویس هایش و ایمن سازی آنها بررسی می کنیم .

با توجه به اینکه این تکنولوژی روز به روز پیشرفت می کند دو مبحث مهم و بزرگ در دنیای امروز و انتقال آنها به فناوری پردازش ابری را که می توان خدمات بانکداری آنلاین و سیستم های مدیریت منابع انسانی نامید ، بررسی می کنیم . اهمیت و جنبه های چگونگی ورود و پایداری این خدمات را به عرصه محاسبات ابری را بررسی می کنیم که از چه جهاتی می تواند به صرفه باشد و از چه جهاتی نمی تواند و مشکلات و خطرات ممکن را بیان می کنیم .

فصل اول
مقدمه

با مرور سناریوهای محاسبات قبل از اعلام و در دسترس بودن محاسبات ابری می یابیم که کاربرانی که نیاز به محاسبات داشتند می بایست در منابع محاسباتی سرمایه گذاری می کردند مانند : سخت افزار ، نرم افزار ، شبکه و ذخیره سازی ؛ این سرمایه گذاری ها طبعا هزینه های زیادی داشت که باید برای خرید منابع محاسباتی ، نگهداری آنها ، حفظ و عملیاتی کردن آنها صرف می شد . بعد از گذشت مدتی همچنین برنامه ها و منابع در نسخه های جدید عملکردی بهتر داشتند و کاربران مجبور به خریدن دوباره این منابع می شدند . علی الخصوص برای شرکت هایی که به قدرت و منابع محاسباتی عظیمی نیاز دارند در مقایسه با اقتصاد های کلاسیک و فردی ، هزینه ای رو به افزایش را خواهد داشت . [1]

از طرفی می توان فقط هنگامی که نیاز باشد از شرکتی که اینگونه سرویس ها را ارائه می دهد استفاده کرد و هزینه را فقط برای آن مدت پرداخت کرد . با این کار در مقایسه با سرمایه گذاری های عظیم هنگام خریدن کل زیر ساخت های محاسباتی ، فقط برای یک سرمایه گذاری منطقی هزینه می شود . در نتیجه می توان محاسبات ابری را یک مکانیسم بهره برداری ، استخدام کردن و یا گرفتن خدمات از منابع و یا زیرساخت های محاسباتی به سطوح

سازمانی یا فردی به میزان مورد نیاز دانست که پرداخت ها تنها برای مدت محدودی از خدمات مصرف می گردد . برای درک بهتر این موضوع به مثالی در زمینه توزیع برق توجه کنید ؛ ما می توانیم توسط ژنراتور هایی ، برق مورد نیاز روشنایی و لوازم برقی خود را تامین کنیم درصورتیکه می توان با پرداخت مبلغی به صورت ماهیانه این کار را به شرکت های تولید و توزیع کنندهٔ برق سپرد . [1]

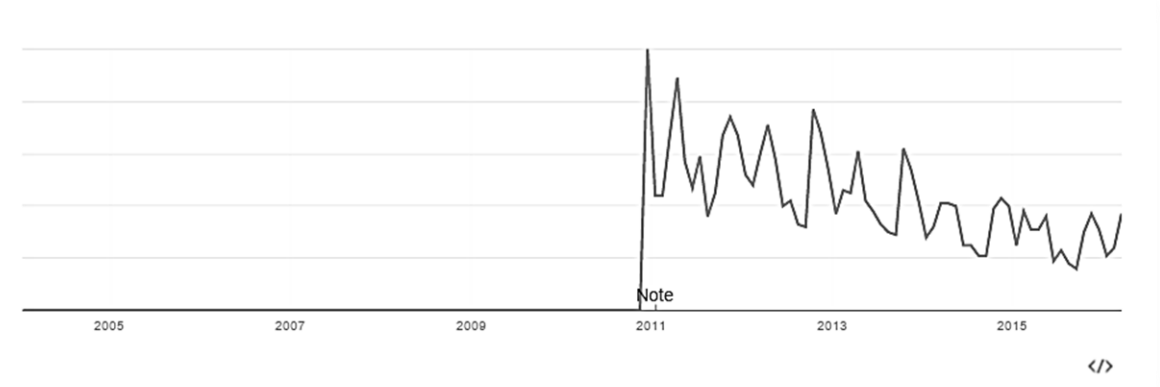
بنابراین پردازش ابری در گرفتن خدمات از منابع محاسباتی مورد نیاز است . در نتیجه دلیل نیاز به پردازش ابری را می توان اینگونه بیان کرد که باعث حذف سرمایه گذاری های عظیم در سطح هزینه های عملیاتی می شود . پردازش ابری بسیار اقتصادی است . کمترین نفع این نوع پردازش این است که حتی وقتی ما لپ تاپ خود را گم می کنیم یا کامپیوتر شخصی ما آسیبی می بیند یا دزدیده می شود اطلاعات و فایل های ما ایمن باقی می مانند . [1]

از دلیل های اصلی برای نیاز و استفاده از پردازش ابری می توان به راحتی و قابل اعتماد بودنش اشاره کرد . به این وسیله دیگر هرکجا که باشیم کافیست برای دسترسی به اطلاعاتمان یک کامپیوتر که به اینترنت متصل باشد را در اختیار داشته باشیم . با این حال افرادی هم هستند که سعی در دسترسی به اطلاعات شخصی ما دارند که در نتیجه این مهم است که یک دسترسی کنترل شده ای را با کلمه ی عبوری قوی و توجه به همه اصول حریم شخصی آن سرویس ابری که داریم استفاده می کنیم ، فراهم آوریم . [1]

پیدایش مفاهیم اساسی رایانش ابری به دهه ۱۹۶۰ بازمی گردد . رایانش ابری مفهوم ابر را به گونه ای گسترش می دهد که سرورها را نیز علاوه برزیر ساخت های شبکه در برگیرد . در یک اصطلاح ساده پردازش ابری عبارت است از ذخیره و دسترسی داده ها و برنامه ها بر روی بستر اینترنت از راه دور یا از کامپیوتری در مکانی دیگر به جای استفاده از هارد درایو[۱] کامپیوتر خودمان . در واقع پردازش ابری استعاره ای از اینترنت است . هنگامی که ما از طریق هارد درایور یک کامپیوتر برای ذخیره سازی اطلاعات یا انجام یک برنامه استفاده می کنیم در اصطلاح به آن ذخیره سازی و محاسبات محلی[۲] می گویند . برای اینکه این مورد پردازش ابری تلقی شود ما نیاز به دسترسی به اطلاعات یا برنامه های خود بر روی بستر اینترنت داریم . نتیجه ی نهایی یکسان است اما با داشتن ارتباط آنلاین[۳] پردازش ابری می تواند در هرکجا ، هرزمان ، و توسط هر وسیله ای انجام شود . [1] در زیر شکل های ۱-۱ و ۱-۲ دربارهٔ مجبوبیت واژه پردازش ابری را در کشور ما بر اساس منطقه و گذشت زمان مشاهده می کنید . [2]

---

۱ Hard Drive
۲ Local Storage and Computing
۳ Online Connection



شکل ۱-۱: محبوبیت با گذشت زمان

شکل ۱-۲ : محبوبیت بر اساس منطقه

فصل دوم
معرفی تخصصی پردازش ابری

تعریف

بنا به تعریف معمول پردازش ابری از طرف موسسه ملی استاندارد و فناوری[1] :

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., Networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. " [3]

این تعریف به این معناست که همه ی منابع محاسباتی و یا زیر ساخت های آن که از فروشندۀ ابر و یا سایت های ارائه دهندگان در دسترس هستند ، بر روی بستر اینترنت از هر مکان دور و توسط هر دستگاه کامپیوتر محلی قابل

[1] National Institute of Standards and Technology (NIST)

دستیابی هستند (نمود دسترسی آسان و فراگیر که در تعریف آمده است) . به علاوه استفاده یا دسترسی فقط برای هزینه کردن سطحی از استفاده بر اساس نیازها و خواسته های کاربران است که به مدل های " پرداخت براساس جلو رفتن " [۱] و " پرداخت به ازای استفاده " [۲] معروف می باشند . [1]

مبانی پردازش ابری

۵ ویژگی مهم :

ویژگی های زیر از ویژگی های اساسی یک پردازش ابری است که توسط موسسه ملی استاندارد و فناوری ارائه شده و باید توجه داشت که در صورت فقدان هر یک از ویژگی های زیر در یک پردازش ، آن رایانش دیگر پردازش ابری محسوب نمی شود .

۱. خدمات مبنی بر تقاضا [۳] : کاربر می تواند به صورت اتوماتیک شخصاً و بدون نیاز به تعامل انسانی با هر یک از فراهم آورندگان سرویس ها ، تا جایی که بخواهد قابلیت های محاسبات را تنظیم و استفاده کند و نیاز به نیروی انسانی به صورت تمام وقت نیست .
۲. دسترسی گسترده به شبکه [۴] : قابلیت ها بر روی شبکه و از طریق مکانیزم های استانداری که استفاده از وسایل کم ضخامت (مانند تبلت ها و گوشی های هوشمند) را ترویج می کنند ، در دسترس هستند .
۳. ادغام الاستیک منابع [۵] : منابع محاسباتی فیزیکی و مجازی مختلف ارائه دهندگان برای خدمت به مصرف کنندگان متعدد با استفاده از یک مدل چند مستاجر [۶] (اجاره توسط چندین کاربر) ادغام شده اند ، که به صورت پویا اختصاص داده شده و با توجه به تقاضای مصرف کنندگان دوباره اختصاص داده می شود . یک احساس استقلال محل [۷] (از نظر جغرافیایی) وجود دارد که در آن کاربر کنترل یا دانشی بر مکان و ابعاد دقیق منابع تامین شده ندارد اما ممکن است قادر به مشخص کردن مکان در سطوح بالاتر مثل کشور ، ایالت یا مرکز داده باشد . نمونه ای از منابع گفته شده شامل ذخیره سازی ، پردازش ، حافظه و پهنای باند شبکه است .
۴. کشش سریع [۸] : پردازش ابری می تواند امکان افزایش خودکار و سریع حجم و درخواست را به صورت اتوماتیک فراهم آورد . در واقع بر حسب نیاز قابلیت انعطاف پذیری سریع دارد . از نظر کاربر اینچنین به نظر

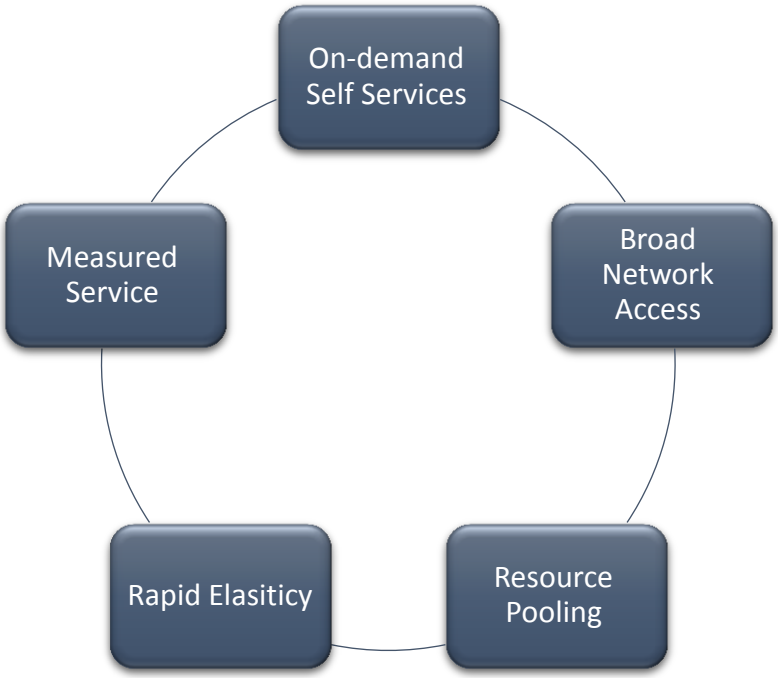
---

[۱] *pay-as-you-go*
[۲] *pay-as-per-use*
[۳] *On-demand self-service*
[۴] *Broad network access*
[۵] *Elastic resource pooling*
[۶] Multi-tenant model
[۷] location independence
[۸] *Rapid elasticity*

می رسد که گویا این قابلیت ها وسرویس ها نا محدود هستند می توانند با هر حجم ومقداری در هر زمانی قابل دسترس باشند .

۵. خدمات اندازه گیری [۱] : سیستم های ابری به طور اتوماتیک استفاده از منابع را به وسیله ی قابلیت اندازه گیری در بر خی از سطوح متناسب با خدمات ، کنترل و بهینه می کند . استفاده از منابع می تواند مدیریت ، کنترل و گزارش شود که شفافیت را برای هر دو ارائه دهنده و مصرف کننده در مورد روش و میزان استفاده از سرویس مربوط ، فراهم می کند .

در نمودار زیر این پنج ویژگی مهم پردازش ابری نمایش داده شده است . [1] همچنین پردازش ابری دارای ویژگی های دیگری نظیر از پیش تعریف شدن کیفیت انواع سرویس هایی که ارائه می شوند [۲] ، مبنی بر اینترنت بودن ، سادگی استفاده ، مقیاس پذیر بودن و به صرفه بودن است .[4]



شکل ۲-۱ : چرخه ویژگی های مهم در پردازش ابری

[۱] *Measured service*
[۲] Predefined quality of service (QoS)

اکو سیستم ابری

اکوسیستم ابری اصطلاحی است که برای توضیح محیط کامل یا سیستمی از اجزا یا اشخاصی که به خاطر باهم کار کردن برای فعال کردن و حمایت از خدمات ابری به یکدیگر وابسته هستند ، به کار می رود . به طور دقیق تر اکوسیستم ابری یک محیط پیچیده شامل شرح هر آیتم یا نهاد همراه با تعامل آنهاست . یک اکو سیستم ابری از تعامل اجزا و سازمان ها با افراد ، که با هم به عنوان بازیگرانی که می توانند مسئولِ ارائه و یا مصرف خدمات ابری باشند شناخته شده اند ، را می توان به صورت زیر طبقه بندی کرد : [1]

۱. استفاده کنندگان خدمات ابری [۱] (*CSUs*) : مصرف کنندگان شخصی ، شرکت ها ، و یا دولت و نهاد های عمومی .
۲. فراهم کنندگان خدمات ابری [۲] (*CSPs*) : شرکتی که خدمات ابری را تهیه یا فراهم می کند و آنها را مدیریت یا از آنها نگهداری می کند .
۳. شرکای سرویس های ابری [۳] (*CSNs*) : شخص یا شرکتی که از ساختار سرویس هایی که به وسیله ی فراهم کنندگان خدمات ابری ارائه می شود حمایت می کند . [1]

اپلیکیشن های ابری

یک اپلیکیشن ابری یک برنامه ی اپلیکیشنی (کاربردی) است که بر روی ابر عمل می کند یا اجرا می شود . این اپلیکیشن می تواند ویژگی هایی همانند یک دسکتاپ اپلیکیشن[۴] محض از خود بروز دهد و هم می تواند ویژگی هایی مانند اپلیکیشن های مبتنی بر وب محض از خود بروز دهد . یک دسکتاپ اپلیکیشن به طور کامل در یک دستگاه واحد در محل کاربر ساکن است و از طرف دیگر ، یک برنامه تحت وب به طور کامل در یک سرورِ از راه دور ذخیره می شود و بر روی اینترنت از طریق یک رابط مرورگر قابل دسترسی است . اپلیکیشن های ابری مانند دسکتاپ اپلیکیشن ها پاسخ سریع و امکان کار به صورت آفلاین را فراهم می کنند و همانند وب اپلیکیشن ها نه تنها به طور ثابت بر روی یک سرور محلی هستند بلکه می توانند به آسانی به طور آنلاین به روز شوند . پس با فرض اینکه کاربر دارای یک اتصال منطقی پر سرعت به اینترنت است ، نرم افزار ابری که خوب نوشته شده باشد تمام تعاملات یک نرم افزار دسکتاپ را همراه با قابلیت حمل از یک برنامه تحت وب فراهم می کند . اپلیکیشن ابری می تواند از طریق مرورگری که به اینترنت وصل است استفاده شود . همچنین یک اپلیکیشن ابری می تواند بر خلاف اپلیکیشن

---

۱ *Cloud service users*
۲ *Cloud service provider*
۳ *Cloud service partners*
۴ desktop applications

های وب در هر شرایط حساسی که حتی دستگاه های با ارتباط بی سیم ممنوع است ، استفاده شود . نمونه ای از اپلیکیشن های ابری ، ایمیلِ مبتنی بر وب است . [1]

منافع و مضررات

یکی از جذبه های پردازش ابری دسترسی آن است . اگر اپلیکیشن ها و اسناد و مدارک ما به جای اینکه بر روی کامپیوتر دفتر کارمان ذخیره شده باشد بر روی ابر باشد ، ما می توانیم در هر زمان و هر کجا به آنها دسترسی داشته باشیم و از آنها برای کارهای مان حتی وقتی که ما در محل کار ، خانه یا حتی خانه دوستمان هستیم استفاده کنیم . مجموعه ای تلفیقی از نکاتی که مزایای محاسبات ابری را توجیه می کنند را می توانیم به شرح زیر بیان کنیم : [1]

۱. دستیابی به مقیاس اقتصادی [۱] : می توانیم حجم خروجی و بهره وری را با سیستم های کمتر افزایش و در نتیجه هزینه ها برای هر واحد پروژه یا محصولات را کاهش دهیم .
۲. کاهش هزینه زیرساخت های فناوری : می توان به داده ها و اطلاعات با کمترین هزینه های پیش رو به روش " پرداخت بر اساس جلو رفتن " دسترسی داشته باشیم . به این معنا که استفاده و پرداختی که مبتنی بر تقاضا می باشد ، شبیه به خواندن میزان مصرف برق در خانه است .
۳. جهانی کردن نیروی کار : مردم در سطح جهان می توانند به وسیلهٔ اینترنت به ابر دسترسی داشته باشند .
۴. ساده کردن فرآیندهای کسب و کار : امکان انجام دادن کار بیشتر در زمان کمتر با صرف منابع کمتر .
۵. کاهش هزینه های سرمایه : نیازی به خرج کردن پول های هنگفت در سخت افزار ، نرم افزار و یا هزینه های صدور پروانه نیست .
۶. دسترسی فراگیر [۲] : داده ها و اپلیکیشن ها می توانند در هر زمان و هر کجا به وسیلهٔ هر دستگاه محاسباتی در دسترس باشند و زندگی را آسانتر می کنند .
۷. کنترل پروژه ها به طور مؤثرتر : استفاده از بودجه ی تخصیص یافته ، بهینه تر می شود و از نظر زمانی پروژه ها سروقت و بدون مشکل مالی به سرانجام می رسند .
۸. آموزش شخصی ، کمتر مورد نیاز است : افراد کمتری با یک منحنی یادگیری حداقل در مورد مسائل سخت افزار و نرم افزار کارهای بیشتری روی ابر انجام می دهند.
۹. به حداقل رساندن تعمیر و نگهداری و صدور مجوز نرم افزار [۳] : چون در این مرحله نرم افزار ها به عنوان خدمات (SaaS) ارائه می شوند ، که به آنها Off-premises software گفته می شود ، یعنی بر روی یک سرور از راه دور قرار دارند و از ابر به جای بکار گیری تک تک روی سیستم ها ، استفاده می کند در نتیجه تعمیر و نگهداری و آپدیت آنها راحت تر است .

---

۱ *Achieve economies of scale*
۲ *Pervasive accessibility*
۳ *Minimize maintenance and licensing software*

۱۰. بهبود انعطاف پذیری : امکان ایجاد تغییرات سریع در محیط کار بدون به خطر انداختن مسائل جدی . [1]

ریسک ها و مضرات پردازش ابری مشخص است . مشخص ترین نکته در این باره این است که اگر ما اتصال به اینترنت خود را از دست بدهیم دسترسی خود به ابر و در نتیجه به داده ها و اطلاعات از دست می دهیم . [1] همچنین ایدهٔ پردازش ابری نگرانی های بسیاری را درباره امنیت و حریم خصوصی از طرف حقوقدان ها برانگیخته است . در صورتی که اطلاعات شخصی و حساس استفاده کنندگان در اختیار هکرها قرار گیرد سوءاستفاده می کنند و حتی هکرها می توانند از دسته افراد کارمند شرکت های ارئه دهنده باشند و نهایت سوءاستفاده را انجام دهند . همانطور که گفتیم به دلیل اینکه کاربر از محل دقیق پردازش خبر ندارد کنترلی بر روند پردازش ندارد . همچنین همانطور که در تاریخچه گفتیم به دلیل جدید بودن موضوع قوانین و مقررات مشخصی برای پیگیری افراد خاطی وجود ندارد . امکان انتقال به یک سرویس دهندهٔ دیگر وجود ندارد . در ادامه مسائل حریم خصوصی و امنیت جداگانه بررسی خواهند شد . [4] [5]

سرویس های ابری

به دلیل اینکه بعدا به موضوعات مرتبط به آن اشاره خواهد شد باید نکته دیگری را در اینجا به آن بپردازیم و آن سه مدل عمده برای ارئهٔ سرویس می باشد . سه سرویسی که منابع مبتی بر پردازش ابری در اختیار کاربران قرار می دهند عبارتند از : [1]

۱. نرم افزار به عنوان سرویس [۱] (**SaaS**)
۲. پلتفرم به عنوان سرویس [۲] (**PaaS**)
۳. زیرساخت به عنوان سرویس [۳] (**IaaS**)

۱) **SaaS** : قابلیت هایی که برای کاربر فراهم شده است به جهت استفاده از اپلیکیشن های ارائه دهندگان است که روی زیرساخت های ابری نظیر شبکه ، سرورها ، سیستم عامل ها و فضای ذخیره سازی اجرا می شوند . اپلیکیشن های می توانند به وسیله ی ابزار های کاربری مختلفی در دسترس باشند . کاربر هیچ کنترل یا مدیریتی بر لایه های زیرساختی ابری ندارد . از اپلیکیشن های معروفی که به عنوان سرویس ارائه می شوند می توان به اپلیکیشن مدیریت روابط با مشتری (CRM) [۴] ، تجزیه و تحلیل هوش کسب و کار [۵] و نرم افزار های حسابداری آنلاین [۶] اشاره کرد .

---

[۱] Software as a Service
[۲] Platform as a Service
[۳] Infrastructure as a Service
[۴] customer relationship management
[۵] business intelligence analytics
[۶] online accounting software

۲) **PaaS** : قابلیت هایی که برای کاربر فراهم شده است برای استقرار بر روی زیر ساخت های ابری که توسط کاربر ایجاد شده و یا اپلیکیشن هایی است که با استفاده از زبان های برنامه نویسی ، کتابخانه ها ، خدمات ، و ابزار هایی که توسط ارائه دهنده خدمات حمایت می شوند بدست آمده ، می باشد . کاربر هیچ کنترل یا مدیریتی بر لایه های زیرساختی ابری ندارد ولی بر اپلیکیشن های مستقر شده و احتمالا تنظیمات محیط های میزبانی نرم افزار کنترل دارد . ارائه دهندگان PaaS شبکه ، سرورها و فضاهای ذخیره سازی را فراهم می کنند و سطح مقیاس پذیری و نگهداری را کنترل می کنند . کاربر عموما فقط برای سرویس های استفاده شده هزینه ای پرداخت می کند . به عنوان نمونه Google App Engine و Microsoft Azure Services مثال هایی از ارائه دهنده گان PaaS هستند .

۳) **IaaS** : قابلیت هایی که برای کاربر فراهم شده است به جهت پردازش ارائه ، ذخیره سازی ، شبکه و دیگر منابع اساسی محاسباتی طبق اصل پرداخت به اضای استفاده است که آن شخص می تواند نرم افزار های دلخواهی را مستقر و اجرا کند که می تواند شامل سیستم عامل ها و اپلیکیشن ها باشد . کاربر هیچ کنترل یا مدیریتی بر لایه های زیرساختی ابری ندارد ولی بر سیستم های عامل ، ذخیره سازی و اپلیکیشن های بکار گرفته شده و احتمالا کنترل محدود شده ای بر انتخاب اجزای شبکه (مانند دیوارهای آتش میزبان [۱]) دارد . سرویس وب آمازون [۲] مثال رایجی از یک تامین کننده IaaS است .

تفاوت اساسی بین PaaS و IaaS در مقدار کنترلی است که کاربر دارد . به طور کلی سازمان هایی که از قبل از پکیج های نرم افزاری یا اپلیکیشن هایی برای مقاصدی معین برخوردار بوده اند و می خواهند آنها را بر روی ابر نصب و اجرا کنند باید برای استفاده IaaS را به جای PaaS انتخاب کنند . [1] شکلی که در صفحه بعد آمده رابطه این سه را نشان می دهد .

روشهای پیاده سازی در پردازش ابری

روشهای بکار گیری و پیاده سازی راه هایی را توضیح می دهند که با آنها خدمات ابری پیاده سازی می شوند و یا بر حسب ساختار سازمانی در اختیار کاربر قرار می گیرند . در واقع اشکال متفاوت منابع پردازش ابری است . [1]

۱. ابر خصوصی [۳] : از زیرساخت های ابری که برای استفاده ی خاص یک شرکتی که شامل چند کاربر (مثل واحد های تجاری) است می باشد . ممکن است توسط یک شخص ثالث نیز مدیریت شود و عمل کند

---

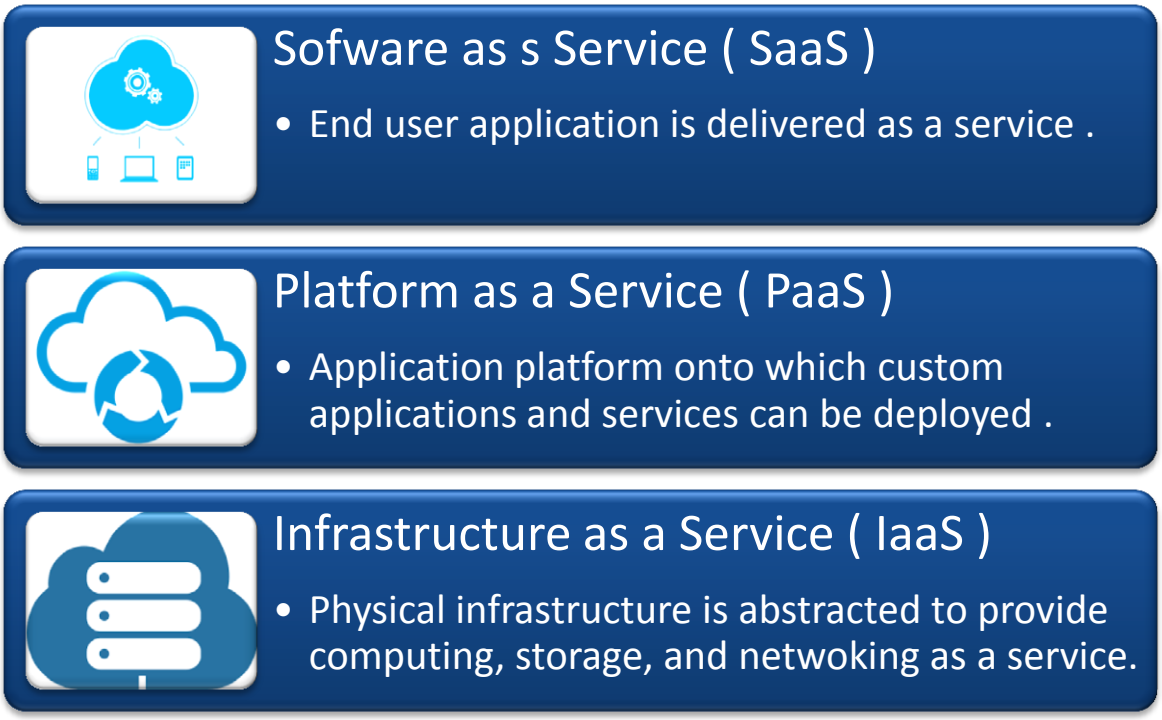
[۱] host firewalls
[۲] Amazon Web Services (AWS)
[۳] *Private cloud*

یعنی می تواند سرور در خود محل وجود داشته باشد و یا در مکانی دیگر باشد و از آنجا مدیریت شود ولی آن فضای ابر اختصاصی برای خود همان شرکت است .

۲. ابرهای عمومی : از زیرساخت های ابری که برای استفاده عموم باز است . ممکن است توسط یک سازمان تجاری ، آکادمیک و یا دولتی مدیریت شود و عمل کند ولی در مکان ارئه دهندهٔ سرویس ابری قرار دارد .

۳. ابرهای انجمنی : از زیرساخت های ابری که به وسیله شرکت های متعدد به اشتراک گذاشته شده و یک گروه مشخصی را حمایت می کند که دغدغه های خود را به اشتراک گذاشته اند . ممکن است که توسط خود شرکت ها یا شخص ثالث مدیریت شود و عمل کند . و همچنین می تواند در خود محل یا در مکانی دیگر وجود داشته باشد .

۴. ابرهای هیبریدی : از زیرساخت های ابری است که ترکیبی از دو یا بیشتر از دو زیرساخت ابری متمایز (از سه نوعی که در بالا گفته شد) می باشد که موجودیت های منحصر به فردی را در خود دارند اما به وسیلهٔ تکنولوژی های استاندارد شده ای که داده ها و اطلاعات را به قابل حمل بودن قادر می سازد ، بهم پیوند خورده اند . [1]



شکل۲-۲ : سه مدل سرویس پیشنهادی - SPI

فصل سوم
رایانش ابری : امنیت و چالش های پیش رو

امنیت فاکتور مهمی است که باید در محیط های رایانش ابری در نظر گرفته شود . این فصل به جنبه های مختلف امنیت خواهد پراخت . امنیت در پردازش ابری را بیان می کنیم .در مورد امنیت داده ها و اطلاعات ، امنیت مجازی سازی ، صحبت می کنیم . چالش های امنیتی ، تشخیص هویت و مدیریت دسترسی را نیز بررسی خواهیم کرد [6] .

به عنوان مقدمه برای اینکه بدانیم امنیت از چه موقع موضوع مهمی شد مطالبی را بیان می کنیم . تعیین سرنوشت اطلاعات [1] به حق یا توانایی فرد در بکارگیری کنترل شخصی روی مجموعه ای ، استفاده و افشای اطلاعات شخصی آنها توسط دیگران ، اشاره دارد . تعیین سرنوشت اطلاعات به یک مفهوم چالش برانگیز برای ترویج و ایمنی در جهانی از عبور اطلاعات نامحدود از افراد به سازمان ها ، بین اشخاص و بین سازمان ها ، در سطح جهانی بدل گشته است . اطلاعات شخصی ، چیزهایی هستند که هویت امروزه ی ما را تشکیل می دهند پس باید مسئولانه مدیریت

[1] Informational self-determination

شوند ، که اگر چنین نشود باعث تضعیف پاسخگویی می شود و اطمینان در جامعهٔ اطلاعاتی در حال تحول ما ، دچار فرسایش می شود . [7]

از همان ابتدای ارتباطات و فناوری اطلاعات ، درباره امنیت اطلاعات و رازهای نظامی و داده های محرمانه نگرانی های قابل توجهی وجود داشته است . در اواخر قرن ۲۰ ام و سالهای اول قرن ۲۱ ام پیشرفت های چشمگیری در زمینه های ارتباط های مخابراتی ، سخت افزار و نرم افزار های کامپیوتری و رمزگذاری داده ها مشاهده شده است . امکان کوچکتر بودن ، قدرتمندتر بودن و ارزان و به صرفه تر بودن تجهیزات محاسباتی ، پردازش الکترونیکی داده ها را در دسترس کسب و کارهای کوچک و کاربران خانگی قرار داد . این کامپیوتر ها به سرعت توسط اینترنت به یکدیگر پیوستند . رشد سریع و رواج استفاده از پردازش الکترونیکی داده ها و تجارت الکترونیک که در بستر اینترنت انجام می شد ، همراه با ظهور بیشتر تروریسم بین المللی ، نیاز به متدهایی بهتر برای حفاظت از کامپیوترها و اطلاعاتی که آنها ذخیره ، پردازش و منتقل می کنند بیشتر احساس می شد . رشته های آکادمیکی از امنیت کامپیوتر و اطمینان از اطلاعات ، همراه با سازمان های حرفه ای متعدد در به اشتراک گذاری اهداف مشترک ، از حصول اطمینان از امنیت و قابلیت اطمینان سیستم های اطلاعاتی ، پدید آمده است .

اکوسیستم های دیجیتالی جدید چالش های امنیت و حریم خصوصی پیچیده ای را نمایان می کنند . اساساً ، نیاز به فراهم کردن راه های انعطاف پذیرتر و کاربر پسندتر برای اعتبار بخشی و تصدیق کاربران لازم است . بدون مدیریت بهتر هویت های دیجیتال ، نه تنها به بحث و جدل بر سر مشکلات کنونی مانند سرقت هویت ، اسپم [۱] ، بدافزار ، و تقلب سایبری ادامه می دهیم ، بلکه قادر به اطمینان بخشی به کاربران جهت انتقال اطلاعات مهم و اپلیکیشن هایشان بر روی بستر وب ، نیستیم . [7] پردازش ابری صنعت IT را در یک دهه گذشته متحول کرده است . حال چه چیز از پردازش ابری بین عوام و خواص مردم جذاب است ؟ این صنعت برای اینکه استفاده از پردازش ابری را در محاسبات کاربر پسند[۲] تر بکند بر روی مواردی از جمله : زمان و امور مالی ، مردم و ارتباط ، جایگزینی سخت افزار ، انرژی کارآمد ، مطالعاتی از شرکت های Accenture, Microsoft, and WSP Environment and Energy ، سبز شدن [۳] (به معنای کمک به محیط زیست) و آینده ابر و محیط زیست ، سرمایه گذاری کرده است . [6]

---

۱ Spam
۲ user friendly
۳ *Going green*

الزامات امنیتی

به طور کلی امنیت اطلاعات بر اساس سه اصل محرمانه بودن ، صداقت و تمام و کمال بودن ، و در دسترس بودن می باشد . ریسک های امنیتی مانند ویروس ها ، کرم ها ، تروجان ها ، کلاهبرداری و غیره نباید نادیده گرفته شوند . وقتی که به فضای ابر برسند نه تنها یک کاربر در خطر قرار می گیرد بلکه همه ی ابر و استفاده کنندگان از آن نیز در خطر قرار می گیرند . در روابط بین زیرساخت های فیزیکی و صاحب اطلاعات ، روش قدیمی ، بر اساس مالکیت سخت افزاری کامپیوتری است که اطلاعات در آن ذخیره شده است اما با پردازش ابری ، استفاده کنندگان دارنده ی زیرساخت های پردازشی نیستند و دیگر مشخص نیست که چه کسی دارنده و کنترل کننده ی اطلاعات است . همواره ریسک افشای اطلاعات شخصی وجود دارد . معمولا از کاربران خواسته می شود تا اطلاعات شخصی خود را به درستی وارد کنند تا هویتشان ثبت شود . با توجه به این موضوع اطلاعات شخصی اگر به طور مناسبی حفاظت نشوند ، می توانند مورد سوءاستفاده قرار بگیرند . [8]

برای اینکه بفهمیم چرا امنیت IT به سختی قابل دستیابی است باید موارد زیر را در نظر داشته باشیم :

۱. تعداد افراد متخصص ، باتجربه و حرفه ای در زمینه امنیت کم هستند .
۲. امنیت عالی هزینه ای زیاد دارد .
۳. کارکنان امنیتی و IT بر فهمیدن محتوای داده ها علاقه و انگیزه هایی دارند .
۴. هر منبعی که به پایگاه داده متصل باشد به تمامی داده ها دسترسی دارد . [8]

چالش های کلی ابر

استفاده از ابر فرصت های متعددی را مانند فعال کردن خدماتی برای استفاده ، بدون اینکه هیچ درک درستی از زیرساخت های آن وجود داشته باشد ، فراهم می کند . پردازش ابری با استفاده از مقیاسی اقتصادی کار می کند . امروزه با وجود اینکه ابر ، یک تکنولوژی رایج و همه گیر است ، مسائل زیادی پیرامون آن وجود دارند . چهار مورد بعدی مسائل اصلی را پیرامون پردازش ابری بیان می کنند . [6]

۱. سیاست حریم [۱] : برای تست اینکه برنامه ای کار می کند و توسعه می یابد ، یک سیاست حریم عبارت است از یک مطالعه مقدماتی قبل از انتقال برنامه به محیط تولید .
۲. مسائل قابلیت همکاری [۲] : مشکلات و مسائلی است که در راه بدست آوردن اپلیکیشنی با قابلیت همکاری بین دو فراهم کننده محاسبات ابری وجود دارد . در نتیجه نیاز به اصلاح داده ها و یا تغییر منطق اپلیکیشن ها را در پی دارد .

---

۱ *Threshold policy*
۲ *Interoperability issues*

۳. هزینه های پنهان [۱] : پردازش ابری درباره هزینه های پنهان چیزی به ما نمی گوید . در یک نمونه از تحمیل هزینه های شبکه ، شرکت هایی که دور از محل ارائه دهندگان ابر هستند می توانند تاخیر را به خصوص هنگامی که ترافیک سنگین وجود دارد تجربه کنند .

۴. رفتار غیر منتظره [۲] : به عنوان نمونه آزمون هایی که برای اعتبار سنجی و یا آزادی منابع استفاده نشده ، انجام می شود نتایج غیر منتظره نشان می دهند . بنابراین نیاز به برطرف کردن مشکلات قبل از اجرای اپلیکیشن ها بر روی ابر دیده می شود . [6]

جنبه های امنیتی

نگرانی های امنیتی در ابر آنچنان تفاوتی با سرویس های پیشنهادی غیر ابری ندارد . موارد و زمینه های مورد تحقیق درباره مسائل مربوط به امنیت کنونی در پردازش ابری عبارتند از : [6]

۱. قابل اعتماد بودن اپلیکیشن های توزیع شده ی مبنی بر اینترنت ، مانند سیستم های تجارت الکترونیکی ، که بستگی شدید به مسیر اعتماد در بین طرف های درگیر دارد .

۲. نیاز روزافزون نسل جدیدی از کاربران اپلیکیشن های تجاری و مبتنی بر ابر ، نیاز به نسل بعدی پایگاه داده ها که باید به شدت مقیاس پذیر ، کارآمد ، سریع ، قابل اعتماد و امن باشند را به دنبال دارد . به منظور مقیاس کردن خدمات ابری به طور قابل اعتماد به میلیونها توسعه دهنده خدمات و میلیاردها کاربر نهایی ، نسل بعدی رایانش ابری و زیرساخت های پایگاه داده ها باید به دنبال تکاملی شبیه به آنچه که منجر به ایجاد شبکه های مخابراتی مقیاس پذیر شده است ، باشند .

۳. در آینده ارائه دهندگان خدمات ابری مبتنی بر شبکه ، به وسیله فناوری مجازی سازی قادر به اختصاص تنها سطوح مُجاز محاسبه ، شبکه و منابع ذخیره سازیِ مجازی به برنامه های مخصوص براساس زمان واقعی تقاضای کسب و کار می باشند . همچنین در عین حال در دسترس بودن ، عملکرد ، و امنیت با هزینه معقول را برای تضمین کامل سطح خدمات ارائه می دهند . [6]

امنیت داده

با توجه به زیرساخت ها و هزینه های عظیم ، سازمان ها به آرامی به فناوری پردازش ابری روی می آورند . داده ها در زیرساخت های ارائه دهندگان خدمات ابری ذخیره می شوند . از آنجایی که داده ها فقط در محدوده سازمان ها باقی نمی مانند ، چالش های پیچیده ی زیادی را به وجود آورده است . مانند : [6]

---

[۱] *Hidden costs*
[۲] *Unexpected behavior*

۱. نیاز به حفاظت از اطلاعات محرمانه ی کسب و کارها ، دولت و اماکن نظارتی .
۲. فقدان استانداردها در مورد چگونگی بازیافت فضای دیسک و پاک کردن داده های موجود به صورت ایمن توسط ارائه دهندگان خدمات ابری .
۳. نگرانی های نظارت ، گزارش دادن و انطباق .

چنین مسائلی سطح نگرانی در مورد خطرات امنیتی در ابر را بالا می برد . [6]

امنیت مجازی سازی شده [1]

مجازی سازی ، فناوری است که عملیات سرور و مرکز داده را به یک جزء کلیدی در ایجاد یک زیر ساخت انعطاف پذیر و مبنی بر تقاضا ، سوق می دهد . وقتی مجازی سازی را برای پردازش ابری به کار می بریم روشن می شود که ابزار های مدیریتی که در بکارگیری های فیزیکی مبتنی بر سرور [2] (سرورهای فیزیکی) استفاده می شوند پاسخگوی یک محیط مجازی شده ی پویا [3] نمی باشند . [6] مجازی سازی عمدتا بر روی سه چیز تمرکز می کند : مجازی سازی شبکه ، مجازی سازی ذخیره سازی ، مجازی سازی سرور .

نقاط مهم نگرانی در مجازی سازی به شرح زیر است :

۱. یک تهدید جدید : مجازی سازی باعث تغییر در ارتباط بین سیستم عامل و سخت افزار می شودکه دیدگاه امنیتی سنتی را به چالش می کشد یعنی می توان اینگونه گفت که برای یک کاربر متوسط ، وضعیت امنیتی واقعی یک کامپیوتر شخصی متصل به اینترنت به سختی قابل درک است .
۲. نگرانی های ذخیره سازی : یکی دیگر از نگرانی های امنیتی در مجازی سازی ماهیت تخصیص دادن و آزاد کردن منابع است مانند ذخیره سازی محلی در ارتباط با ماشین های مجازی . در طول استقرار و بهره برداری از یک ماشین مجازی ، داده ها بر روی حافظه ی فیزیکی نوشته شده اند . اگر آنها قبل از منبع هایی که می خواهند به ماشین مجازی بعدی دوباره تخصیص داده شوند ، پاک نشوند در معرض افشاء قرار می گیرند .
۳. مدیریت ترافیک : یکی دیگر از روش های نظری که ممکن است پتانسیل محدود کردن جریان ترافیک بین ماشین های مجازی را داشته باشد ، استفاده از جداسازی برای جمع آوری و جداسازی طبقات مختلف ماشین های مجازی از یکدیگر خواهد بود . یک راه برای مدیریت جریان ترافیک بین ماشین های مجازی استفاده از VLAN ها برای منزوی کردن ترافیک بین ماشین های مجازی یک مشتری و ماشین های مجازی مشتری دیگر است . [6]

---

[1] Virtualization Security
[2] physical server-based deployment
[3] highly dynamic virtualized

نگرانی های حریم شخصی

باید تاکید شود که همه انواع پردازش ابری ریسک های حریم شخصی و محرمانگی یکسانی را به وجود نمی آورند . بستگی دارد که چه اطلاعاتی منتشر شده ، طریقه ارتباط آن با یک شخص خاص چیست و آیا آنها با رضایت فرد منتشر شده اند یا نه . در واقع این حقوق از زمانی که به جای اینکه رضایتمندی یک ابزار برای محافظت از حقوق افراد باشد، یک مکانیزم برای گارانتی کردن ادامه دار بودن جریانِ داده و اطلاعت است ، نادیده گرفته می شود . رایج ترین شکل از رضایتِ صریح و روشنِ امروزه قراردادهای مکتوب است . با این حال ، در جهان معاملات الکترونیکی ، رضایتمندیِ صریح و روشن به آسانی قابل دستیابی نیست . هیچ چارچوب جامع برای حفاظت از منافع در برابر حفظ حریم خصوصی از اپلیکیشن های جدید تکنولوژیکِ در حال ظهور وجود ندارد . [8]

تقریبا هر دولتی در سراسر جهان یک سری اصولی دارد که اجازه ی دسترسی به اطلاعاتی که بر روی ابر قرار دارند را می دهد . ارائه دهندگان خدمات ابری باید بر روی همهٔ این پیامدهای حریم خصوصی و امنیتی بحث کنند و در صورت لزوم داده ها را رمزگذاری کنند . این کار باید مطابق قوانین فعلی دولتی انجام پذیرد تا اینکه در آینده از آن به عنوان یک تهدید ملی یاد نشود . [8] بسیار جالب است توجه کنیم که اطلاعات می توانند در دو یا چند مکان مختلف ذخیره شده باشند و اگر ارائه دهنده، این اطلاعات را بدون اطلاع صاحب آن تغییر دهد شامل نقض قانون و پیگرد قانونی می شود . [8]

یکی از بزرگترین نگرانی های حریم خصوصی خطر تسویهٔ اطلاعات محرمانه است که می تواند عارضه ای عمده را با توجه به این موضوع که داده ها می توانند در نقاط مختلف جهان استفاده و ذخیره شوند ، بر جای بگذارد . تطابق با قوانین و مقررات در نقاط مختلف جغرافیایی می تواند بسیار چالش برانگیز باشد . اگر چه قانون به خودی خود می تواند یک راه حل برای مشکل حریم خصوصی باشد ، در طول سالیان ثابت شده است که در بعضی از موارد شکست خورده است . [8]

یکی دیگر از خطرات امنیتی توسط محاسبات ابری مخلوطی از دارایی های اطلاعاتی است که معمولا در نتیجهٔ سیستم های با دسترسی بالا و فاقد بکارگیری شبکه های خصوصی ، ایجاد می شوند . [8]

حریم خصوصی محدود به شرکت ها و سازمان ها نیست بلکه مسئله ی افشا کردن اطلاعات شخصی است . در یک مورد در فوریهٔ ۲۰۱۰ ، یک قاضی ایتالیایی تصمیم به دادن حکم ۶ ماه زندان تعلیقی برای شورای جهانی حریم خصوصی گوگل [۱] و دو نفر از مدیران شرکت های دیگر ، گرفت . این مورد نیاز عمومی به حفظ حریم خصوصی و مجبور کردن مدیران به پاسخگویی ، که برای اولین بار در تاریخ حفظ حریم خصوصی تصور می شود ، را اثبات می

---

[۱] Google’s global privacy council

کند . [8] معمولا یک ارائه دهنده ابر ، خدمات ابر و یا زیرساخت ها را بدون قرارداد فردی ارئه می دهد . در صورتی که کاربر با شرایط عمومی منتشر شده از خدمات محدود شود ، جلوگیری از ارائه دهنده برای به دست آوردن انواع حقوق اطلاعات ، بسیار سخت خواهد بود . [8]

هسته حریم خصوصی که قانون از آن محافظت می کند باید به وضوح از نظر استفاده های مضر و اصلاحات تعریف شده باشد . مضرات قابل تصور باید توسط ارتباطات و آموزش و پرورش منتقل بشود ، نه با قوانین و مقررات . وقتی مردم استفاده از اطلاعات در کسب و کار ، مزایای جریان آزاد (اطلاعات) ، و هزینه های حریم خصوصی را درک کنند ، به احتمال زیاد حریم خصوصی شان را به طریقه ی خوبی اولویت بندی می کنند که انتظار نمی رود . [8]

فصل چهارم
شرکت SAP و پردازش ابری

در این فصل ابتدا در مقدمه ای SAP را معرفی می کنیم و سرویس های SAP را بیان می کنیم و پیاده سازی آنها در ابر را بررسی می کنیم . انواع حملات ممکن و یک مکانیزم ایمن سازی برای مقابله با حملات بیان می کنیم .

معرفی SAP

یک شرکت نرم‌افزاری چند ملیتی آلمانی است که عمده شهرتش را مدیون تولید نرم‌افزارهای سازمانی در زمینه مدیریت عملیات تجاری و روابط با مشتریان است . دفتر مرکزی این شرکت در والدورف در ایالت بادن – وورتمبرگ آلمان واقع شده و دفاتر و شعب دیگری نیز در نقاط مختلف جهان در ۱۳۰کشور دارد . این شرکت در سال ۱۹۷۲ توسط پنج تن از مهندسان سابق IBM کار خود را تحت عنوان « تحلیل سیستم‌ها و توسعه برنامه‌ها » شروع کرد . پس از مدتی این عنوان را به « سیستم‌ها ، محصولات و برنامه‌های پردازش داده » که سه حرف اول اسم شرکت است (و به انگلیسی : Systems, Applications & Products in Data Processing) تغییر داد . از همان زمان محصولات این شرکت به « راهکارهای SAP » مشهور شد . SAP در صنعت نرم‌افزارهای برنامه‌ریزی منابع سازمان (EPR) ، مدیریت روابط با مشتری (CRM) ، و نرم‌افزارهای فروش و بازاریابی با چند رقیب سرسخت مبارزه

می‌کند. شرکت اوراکل بزرگ‌ترین رقیب SAP است . این دو تاکنون دعاوی زیادی با یکدیگر داشته‌اند . یکی دیگر از رقیبانش ، شرکت مایکروسافت می باشد . [9] در یک مورد دعوای Oracle و SAP در سال ۲۰۱۰ میلادی هیئت منصفه ای در کالیفرنیا ، SAP را به جرم سرقت فناوری از اوراکل یک میلیارد و ۳۰۰ میلیون دلار جریمه کرد . این بیشترین مجازات برای نقض حق مولف تا سال ۲۰۱۰ است . جریمه ۲۰ برابر بیشتر از ارزیابی SAP بود . ارزش سهام اوراکل در پی اعلام این خبر ۱/۵ درصد افزایش پیدا کرد . [14]

سرویس های SAP و ابر

حال قبل از بحث در امنیت و ایمن سازی ابری SAP باید در مورد سرویس های SAP به طور مختصر مطالبی را بدانیم .

۱. برنامه ریزی منابع سازمانی (ERP) [۱] : این سرویس به دلایلی مشخص هنوز یکی از بیشترین به راهکار های به کار گرفته شده است . ERP با پروسه های اساسی کسب و کار در هر شرکتی سروکار دارد مانند: حسابداری مالی ، تولید ، و منابع انسانی. در واقع SAP ERP تضمین می کند که سفارشات می توانند پذیرفته، انجام ، ردیابی ، و پرداخت شوند . از اجزای اصلی آن می توان سیستم های فروش و توزیع ، طرح تولید ، مدیریت کیفیت ، مدیریت انبار ، مدیریت پروژه ، را نام برد . منابع انسانی و مدیریت سرمایه انسانی ، وظایفی را برای حقوق و دستمزد ، مدیریت زمان ، انعام ، مشوق ها ، گزارش های قانونی ، و برنامه ریزی هزینه ارائه می دهد . [10]

۲. مدیریت ارتباط با مشتری (CRM) [۲] : CRM فرایندهایی را برای تعامل با مشتریان مانند بازاریابی ، فروش ، خدمات ، و پشتیبانی از معاملات فراهم می کند . پیاده سازی CRM بر روی ابر به دلیل بالا بودن تعداد اجزا جاوا و ABAP به یک تلاش کاملا پیچیده بدل شده است . بنابراین فروش اینترنتی SAP از لحاظ فنی یکی از پر خواستار ترین سناریوهای کسب و کار برای پیاده سازی ابر است . [10]

۳. مدیریت زنجیره تامین (SCM) [۳] : پوشش پیش بینی نیازهای آینده بر اساس داده های تاریخی توسط برنامه ریزی تقاضا ، بهینه سازی توزیع متقابل سفارشات بر روی حمل و نقل های در دسترس و قابلیت های تولید توسط برنامه ریزی شبکه های تامین ، برنامه ریزی دقیق تولید . [10]

۴. مدیریت ارتباط با تامین کننده (SRM) [۴] : برای خرید و تدارکات ادارات است که پوششی کامل فرآیند از قرار دادن سفارش تا پرداخت صورتحساب را ارائه می دهد . [10]

---

[۱] Enterprise Resource Planning

[۲] Customer Relationship Management

[۳] Supply Chain Management

[۴] Supplier Relationship Management

۵. مدیریت چرخه محصولات (PLM) [۱] : راهکار SAP برای توسعه محصول ، تضمین کیفیت همانند مدیریت مواد خطرناک ، بهداشت صنعتی و ایمنی، و حفاظت از محیط زیست . اگر انتقال این فایل های بزرگ یک چالش به زیرساخت های ابر تحمیل کند ، سرور cash محلی در محل مشتری می تواند مستقر شود . [10]

۶. مدیریت عملکرد شرکت (CPM) [۲] : بخشی از مدیریت عملکرد مالی SAP است و جایگزین مدیریت استراتژیک شرکت ((Strategic Enterprise Management (SEM) شده است . با توجه به این واقعیت که این راه حل ها بر اساس استاندارد های نرم افزار های مبتنی بر وب سرور های SAP نیستند ، لازم است اقداماتی ضروری برای پیاده سازی آنها بر زیرساخت های ابر عمومی یا خصوصی انجام شود . [10]

۷. سامانه ی مدیریت مخاطرات (GRC) [۳] : راهکاری مناسب برای انطباق قانون Sarbanes Oxley Act و مدیریت هویت های ناهمگن می باشد . سیستم تجارت جهانی تضمین می کند که کمپانی ها هیچ گونه کالایی را که در لیست سیاه قرار دارد به کشورها صادر نخواهند کرد (بجز مواردی که مربوط به بیانیه های گمرکی یا بررسی وضعیت مالی مشتری ها باشد) همچنین محیط اطراف ، سلامت و امنیت (EH&S) ، مدارکی که برای بهداشت ، امنیت صنعتی و حفاظت از محیط زیست لازم است را مدیریت می کنند مانند سلامت برگه های اطلاعاتی مواد اولیه [۴] ، Trem Cards ها و اعلامیه های غیرمفید .

پیام خوب در رابطه با گسترش پردازش ابری این است که تمامی مولفه ها بر پایهٔ اپلیکیشن سرورهای مبتنی بر وبِ استانداردِ SAP هستند . حتی کنترل دسترسی ، برای تفکیک وظایف بازرسی نرم افزار ها به صورت ABAP کد گذاری شده است ، لذا می توان به عنوان IaaS در زمینه ی پردازش ابری پیاده سازی شوند .

ایمن سازی SAP بر روی ابر

مانند بسیاری از کسب و کار های خدماتی IT ، برنامه های کاربردی SAP هدف اصلی حمله کنندگان هستند . برنامه های کاربردی SAP از آنجایی که اطلاعات حساس و اختصاصی و یا اطلاعات حیاتی ماموریت ها را ذخیره می کنند، برای کسب و کار ها ضروری هستند . سرقت اطلاعات و یا اختلال در سیستم می تواند به از کار افتادگی کسب و کار و باعث خسارت های مالی قابل توجه منجر شود . برنامه های کاربردی SAP مانند دیگر سیستم ها نسبت به حمله ها آسیب پذیر هستند . این حمله ها عبارتند از : [11]

---

[۱] Product Lifecycle Management
[۲] Corporate Performance Management
[۳] Government-Risk-Compliance
[۴] material safety data sheets

۱. Denial-of-service (DoS) Attack : حمله کننده اقدام به ساختن ترافیک ساختگی و ایجاد یک موج عظیم اطلاعاتی در یک شبکه می کند . بنابراین با این حجم زیاد درخواست ها برای سرور ها باعث افزایش حجم عملیات آنها می شود و دسترسی کاربر برای گرفتن خدمات از سرویس دهنده قطع می شود .

۲. Man-in-the-Middle (MITM) Attack : حمله کننده ها می توانند ارتباط های بین سیستمهای مربوط را به جهت سرقت اطلاعات رهگیری کنند .

۳. استفاده غیر مجاز : خودیها با دسترسی به منابع حیاتی می توانند از داده ها به منظور اختلاس ، جاسوسی ، و یا به سادگی برای آشفته کردن اوضاع سازمان استفاده کنند .

۴. Privilege Escalation : حمله کنندگان می توانند کاربران یا دستگاه های مشتریان را با دسترسی های بالاتر به منظور افزایش دسترسی به منابع حساس به خطر بیاندازند .

۵. Application Attack : آسیب رساندن به اپلیکیشن ها با باگ های نرم افزاری توسط حمله کنندگان .

۶. Social Engineering Attack : حمله کنندگان می توانند کاربران و مدیران را برای اجازه ی دسترسی داشتن به سیستم ها فریب دهند . تکنیک های آن اینگونه است که تظاهر می کنند یک مدیر شبکه هستند و از کاربر رمز عبورش درخواست می کنند ، از یک کارمند یا پیمان کار برای دسترسی فیزیکی به سیستم ها جعل هویت می کنند ، و یا ارسال ایمیل هایی که کاربر را به بازکردن لینک ها یا پیوست های ایمیل وادار می کند .

۷. Phishing Attack : حمله کنندگان می تواند با بکارگیری social engineering ، از ایمیل های جعلی برای ترغیب کاربر به باز کردن فایلهای پیوست شده مخرب یا کلیک کردن لینک هایی به وبسایت هایی که می توانند سیستم ها و دستگاه ها را به خطر بیاندازند ، استفاده کنند .

۸. Malware/Virus/Trojan/Worm : حمله کنندگان می توانند کدهایی را بر روی سیستم ها اجرا کنند که به آنها اجازه می دهد دستگاه را کنترل کنند و در آنها خرابکاری کنند .

۹. BotNet : حمله کنندگان می توانند از دستوراتی استفاده کنند و شبکه را کنترل کنند تا فعالیت های تعداد زیادی از سیستم های به خطر افتاده را مدیریت و هدایت کنند . این امر به ویژه در راه اندازی مقیاس های بزرگ حمله های DDoS مفید است .

حال از آنجایی که هیچ استراتژی امنیتی یا سیستمی ۱۰۰٪ در دفاع مقابل حملات موثر نیست ، مهم است که یک مدل تهدید محور پیاده کنیم که تمامی زنجیره های تهدید را در سراسر محیط IT برای ما بیان کند . یک مدل تهدید محور بر سخت شدن و ایمن سازی زیرساخت ها قبل از حمله ، امکان دید گسترده و کنترل برای شناسایی و بلاک کردن تهدیدات در طول یک حمله ، و به سرعت هدف گذاری ، محدود نگه داشتن ، و تعمیر نقص ها بعد از یک حمله متمرکز است . [11]

فصل پنجم
بانکداری آنلاین و ابر

بانک ها برای مردم و کشور به منظور توسعه اقتصادی انگیزه فراهم می کنند . آنها خرید های مالی و فروش را آسان ، امن و راحت می کنند . بسیاری از بانک ها از طریق های دستگاه خودپرداز ، بانکداری تلفن همراه ، بانکداری الکترونیکی و تلفن بانک معاملات مالی را فراهم می کنند . نکته ای بسیار مهم در ارائه خدمات بانکداری الکترونیکی کارآمد بودن ، قابل اعتماد و امن بودن برای مصرف کنندگان است . محیط ابر یک نمونه مناسب برای سازمان های بانکی جدید در مقیاس های کوچک و متوسط است به این خاطر که نیاز آنها به شروع با منابع کوچک و رشد تدریجی همگام با افزایش تقاضای خدمات را حذف می کند . انتقال بانک ها به پردازش ابری مزایای زیر را دارد ؛ [12]

- ✓ ارائه محیط های عملیاتی بهینه سازی شده ، مجازی و مقیاس پذیر .
- ✓ بانک ها می توانند بر چالش های کنونی و پیش رو غلبه کنند .
- ✓ فراهم شدن پهنای باندی پر سرعت برای دسترسی به خدمات بانکی آنلاین در زمانی در حد میلی ثانیه .
- ✓ خدمات بانکی می توانند با ادغام مؤثر چند کانال از لحاظ جغرافیایی پوشش داده شوند .

- ✓ بانک ها می توانند برای ارائه پیشنهادات جدید جذاب تر به نظر برسند .
- ✓ افزایش درآمد برای بانک های جدید کوچک و متوسط .
- ✓ امکان حذف شدن هزینه های اضافی ناشی از مراکز داده های در حال اجرای در خانه ها .
- ✓ امکان فراهم آوردن پلتفرم های انعطاف پذیر برای ساخت و ارائه خدمات بانکی پیشرفته به جامعه . [12]

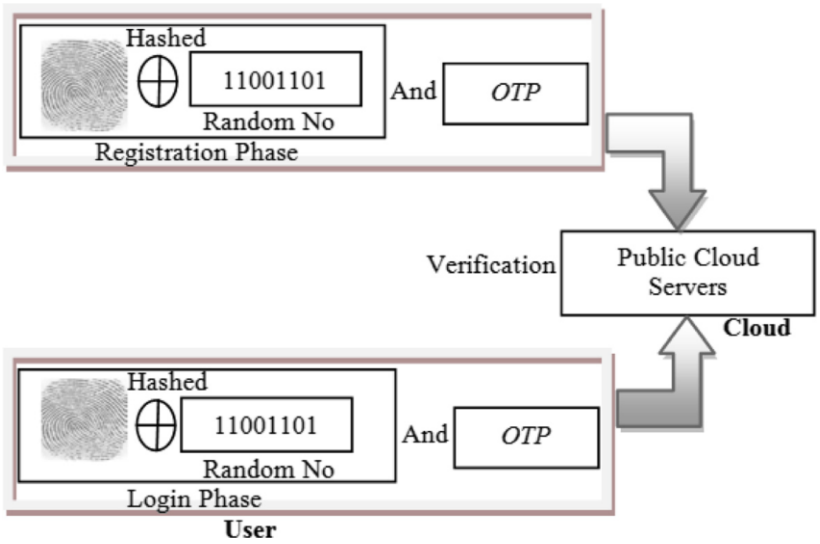
مشکلات و ریسک ها

نگرانی های امنیتی اطلاعات و حریم خصوصی از پیوستن سهامداران بانکی به سیستم عامل های مبتنی بر ابر جلوگیری می کند . از دیدگاه سازمان های بانکی خطرات زیادی همراه با راه حل های ابر عمومی در ارتباط است . به طور خلاصه در ادامه چندین مورد را بیان می کنیم ؛ [12]

۱. پیچیدگی در نظارت های بانکی ، انطباق و مدیریت حسابرسی .
۲. مشکلات در حفظ استانداردهای امنیتی ، قوانین حفظ حریم خصوصی منطقه ای و اقدامات اطلاعاتی .
۳. به طور بالقوه رابط های برنامه های کاربردی ابر ، از حمل و نقل آسان بهره نمی برند بنابراین سهامداران نمی توانند از یک ارائه دهنده ی خدمات ابری به دیگری حرکت کند و جا به جا شود . [12]

به دلیل ورود فناوری های جدید اینترنت تلفن همراه و دیگر فناوری های گسترده ی اینترنت ، کاربران اینترنت به تدریج در حال افزایش هستند . با این رشد ، می توان گفت که اینترنت در حال تبدیل شدن به ابزار روزانه برای تمام اقشار جامعه است که بسیاری از آنها افرادی هستند که از خدمات بانکداری آنلاین برای انتقال وجه ، پرداخت الکترونیکی صورتحساب، خرید الکترونیکی و امکانات دیگر استفاده می کنند . نقطه نظرات مشتری ها درباره ی سطح بالای امنیت ، ویژگی های پیشرفته ، و فناوری های کاربرپسندانه از دغدغه های اصلی هستند . ارائه این شرایط بسیار گران است . بسیاری از پروژه های IT در بخشهای بانکی به دلیل عدم درک نیازهای کاربر و بی سوادی تکنولوژیک شکست خورده اند . حالا با وجود راحتی در بانکداری آنلاین چرا همه افراد از آن استفاده نمی کنند ؟ پاسخ این است که ممکن است این سامانه و خدمات در معرض جرایم اینترنتی قرار بگیرند . اکثر حملات رایج در بانکداری الکترونیکی فیشینگ و فارمینگ هستند که اطلاعات محرمانه ی کاربر را می دزدند . بسیاری از بانک ها شناسه کاربری و رمز و نیز یکبار رمز (OTP) را برای تامین امنیت دسترسی آنلاین به حساب های مالی ارائه می دهند. این نوع فرآیند احراز هویت به طور کامل ایمن نیست ، زیرا کلمه عبور را می توان با dictionary attack به دست آورد . مدل پیشنهادی برای بیشتر امن کردن بانکداری آنلاین می تواند با استفاده از اثر انگشت باشد . در مرحله ثبت نام در سایت بانک نام کاربری و رمز و اثر انگشت گرفته می شوند و به صورت امن با عمل XOR کد گذاری و در سرور های بانک ذخیره می شوند . همانطور که در شکل ۱-۵ می بینیم پس از ثبت نام موقع اتصال و ورود به حساب کاربری از کاربر خواسته می شود تا هر بار اثر انگشت خود را با استفاده از یک secret key از طریق گوشی

موبایل تایید کند و بعد از آن اثر انگشت hash می شود و با آن چیزی که در سرور بوده مطابقت داده می شود تا عملیات تایید هویت انجام شود . [12]



شکل۵-۱ مدل پیشنهادی برای تایید احراز هویت چند عاملی

فصل ششم
پردازش ابری در سیستم های مدیریت منابع انسانی

سیستم های سازمانی شامل برنامه های کاربردی متعدد یکپارچه از جمله تولید ، تدارکات ، توزیع ، حسابداری ، بازاریابی ، امور مالی ، منابع انسانی ، و غیره است . سیستم های سازمانی برای فعال کردن اتوماسیون در نظر گرفته شده اند به عنوان آنکه آنها در دسترس بودن اطلاعات در زمان واقعی ، بهبود دید روند ، و افزایش سطح اتوماسیون را ارائه دهند . فعالیت های تصمیم گیری در یک سیستم تا حد زیادی به سیستم های اطلاعاتی تکیه می کنند . ظهور فناوری های پردازش ابری به عنوان هم فرصت و هم چالش برای شرکتهای کوچک و متوسط ارزیابی شده اند . به عنوان یک راه حل جدید و قدرتمند برای ذخیره ، دسترسی و استفاده از اطلاعات از طریق اینترنت ، پردازش ابری اجازۀ نگه داشتن مقدار زیادی از داده ها بر ابر را می دهد و ظرفیت محاسباتی بالایی را برای هدایت نوآوری ها در توسعه سیستم های اطلاعاتی فراهم می کند . با این حال ، پردازش ابری هنوز در مراحل اولیه خود به سر می برد و پتانسیل های به کارگیری آن در برنامه های مختلف به طور کامل و همه جانبه هنوز در حال بررسی است . [13]

معماری سیستم های مدیریت منابع انسانی

تحت سیستم عامل ابر یکپارچه ، پردازش ابری به شرکتهای کوچک و متوسط اجازۀ دسترسی به خدمات مختلف را با سرعت و با خیال راحت ، می دهد . یک سیستم اطلاعات مدیریت منابع انسانی شامل ارائه دهندگان خدمات ابر ، کاربران مدیریت منابع انسانی ، و سیستم عامل های سرویس ابری است . ارائه دهندگان خدمات ابر به شرکتهای کوچک و متوسط انواع منابع ، راه حل ، و خدمات ابر را ارائه می کنند . از طریق سیستم عامل ابر سیستم اطلاعات ، ارائه دهندگان خدمات به شرکتهای کوچک و متوسط طیف گسترده ای از خدمات ابری را برای برآورده کردن خواسته آنها ارائه می کنند . شرکتهای کوچک و متوسط می تواند خدمات خاص را بر اساس خواسته های خود درخواست دهند ؛ علاوه بر این ، شرکتهای کوچک و متوسط مختلف می تواند منابع انسانی راروی یک سیستم عامل به اشتراک بگذارند . برای پیاده سازی سیستم های اطلاعاتی مبتنی بر رایانش ابری ، سیستم عامل ابر موجود و فناوری، برای ارائه خدمات مدیریت منابع انسانی ادغام شده اند . معماری سیستم اطلاعات شامل شش لایه است که از بالا به پایین به شرح زیر است عبارتند از : لایه دسترسی کاربر ، لایه تعامل ، لایه انتقال ، لایه نرم افزار به عنوان سرویس (SaaS) ، لایه بستر های نرم افزاری به عنوان یک سرویس (PaaS) ، و لایه زیرساخت به عنوان یک سرویس (IaaS) . سیستم اطلاعات می تواند منابع را بر اساس تقاضا از لایه های بالا به پایین اختصاص دهد و مشتریان SME از لایه پایین درخواست خدمات می کنند . به طور کلی ، سیستم اطلاعات ، همه ی خدمات را برای شرکتهای کوچک و متوسط از جمله پشتیبانی فنی ، خدمات مشترک ، مدیریت منابع انسانی ، خدمات مشاوره ، و سایر خدمات جانبی فراهم می کند . با توجه به ویژگی های اتصال و قابلیت همکاری ، سیستم مدیریت منابع انسانی مبتنی بر ابر می تواند مشکلات شرکت را مانند درگیری بین کارگران معمولی و پیمانکاران ، محدودیت منابع در فضا و مدیریت ، حل کند . [13]

فصل هفتم
نتیجه گیری

در این گزارش، ابتدا ابر و فناوری پردازش ابری و تعریف NIST که یک تعریف و معیاری استاندارد برای پردازش ابری بود را معرفی و دلیل روی آوری به این تکنولوژی را بیان کردیم . سپس با پرداختن به جزئیات پردازش ابری ، سرویس ها ، مضررات و فایده ها ، و کاربردهای محاسبات ابری را معرفی کردیم و در فصل سوم به چالش های کلی ابر ، جنبه های امنیتی ، امنیت داده و مسائل حریم شخصی حول پردازش ابری اشاره شد . از فصل سوم نتیجه می گیریم که با توجه به پیشرفت صنعت فناوری اطلاعات حفاظت از اطلاعات مهم ، ضرروی است و با پیشرفت هر چه بیشتر این حوزه نگرانی ها و انتظارات بالاتر می رود . از الزامات امنیتی فضای پردازش ابری نتیجه می گیریم که باید در این زمینه قوانین و مقررات بیشتر و محکم تری به تصویب برسند . همچنین می توان گفت شکی نیست که پردازش ابری در حال تبدیل شدن ، بیشتر به یک ابزار است تا یک قابلیت ساده ی پیاده شده بر روی شبکه . در مسائل حریم شخصی هم باید اطلاعاتی که از کاربر ذخیره می شود و دلیل آن به کاربر اطلاع داده شود . در آخر می توان نتیجه گرفت که مردم و شرکت ها تا وقتی که از همه ی جنبه های رایانش ابری علی الخصوص امنیتی و سیاست های حریم شخصی مطمئن نشده اند نمی توانند به آن اعتماد کنند و اطلاعات شخصی خود را به ارائه کنندگان خدمات ابری بسپارند . با متد پیشنهاد شده برای امن کردن در مقابل حمله ها یافتیم که مدل امنیتی ما باید همه ی جوانب تهدید را قبل ، در حین ، و بعد از حمله در نظر داشته باشد . همانطور که در فایده های بانکداری

آنلاین در ابر فهمیدیم ، سرعت پردازش و کار بالاتر می رود و محدودیت های مرزی حذف می شوند . همانطور که ذکر شد نگرانی های امنیتی و حریم خصوصی از پیوستن سهامداران بانکی به سیستم عامل های مبتنی بر ابر جلوگیری می کند . از دیدگاه سازمان های بانکی خطرات زیادی همراه با راه حل های ابر عمومی در ارتباط است . مدل پیشنهادی برای امن کردن ابر اثر انگشت همراه با رمزکردن آن پیشنهاد شد . در آخر این گزارش هم به سیستم های مدیریت منابع انسانی اشاره شد که پردازش ابری استفاده از ظرفیت های محاسباتی بالایی را برای آنها فراهم می آورد. همچنین در ادامه برای چنین سیستم هایی یک معماری ۶ لایه ای مبتنی بر ابر را بیان کردیم .

منابع

[1] K. Chandrasekaran, "Cloud Computing Fundamentals," in *Essentials of CLOUD COMPUTING*, 2015, pp. 9-26.

[2] Google, "Google Trends," [Online]. Available: https://www.google.com/trends/explore#q=Cloud%20computing&geo=IR&cmpt=q&tz=Etc%2FGMT-3%3A30.

[3] T. G. Peter Mell, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, 2011.

[4] Q. F. Hassan, "Demystifying Cloud Computing," in *DATA MINING*, Faculty of Computers and Information, Mansoura University, Egypt, 2011, pp. 16-21.

[5] M. J. Weil, "Come Rain or Shine: Understanding the Risks and Benefits of Cloud Computing," Charleston School of Law, 2012.

[6] K. Chandrasekaran, "Security in Cloud Computing," in *Essentials of CLOUD COMPUTING*, 2015, pp. 325-346.

[7] A. Cavoukian, "Privacy in the clouds," *Springer Identity Journal Limited*, pp. 89-108, 2008.

[8] V. Tchifilionova, "Security and Privacy Implications of Cloud – Lost in the Cloud," in *iNetSec 2010*, National Laboratory of Computer Virology, Bulgarian Academy of Sciences, 2011, pp. 149-158.

[9] "Wikipedia, the free encyclopedia," [Online]. Available: https://en.wikipedia.org/wiki/SAP_SE.

[10] T. S. ,. C. G. ,. J. M. ,. R. M. ,. M. T. ,. G. A. Michael Missbach, "From R/3 to S/4HANA," in *SAP on the Cloud*, Springer, 2013-2016, pp. 42-49.

[11] T. S. ,. C. G. ,. J. M. ,. R. M. ,. M. T. ,. G. A. Michael Missbach, "Securing SAP on the Cloud," in *SAP on the Cloud*, Springer, 2013-2016, pp. 75-85.

[12] L. P. Sabout Nagaraju, "Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway," *Cloud Computing : Advances, Systems and*

Applications, 2015.

[13] L. W. ,. Z. B. ,. Y. Y. L. ,. Y. X. Xiu Li Wang, "Cloud computing in human resource management (HRM) system for small and medium enterprises (SMEs)," pp. 1-12, February 2016.

[14] "Euronews," 24 11 2010. [Online]. Available: http://persian.euronews.com/2010/11/24/sap-hit-with-record-copyright-infringement-fine/.