رایانش ابری

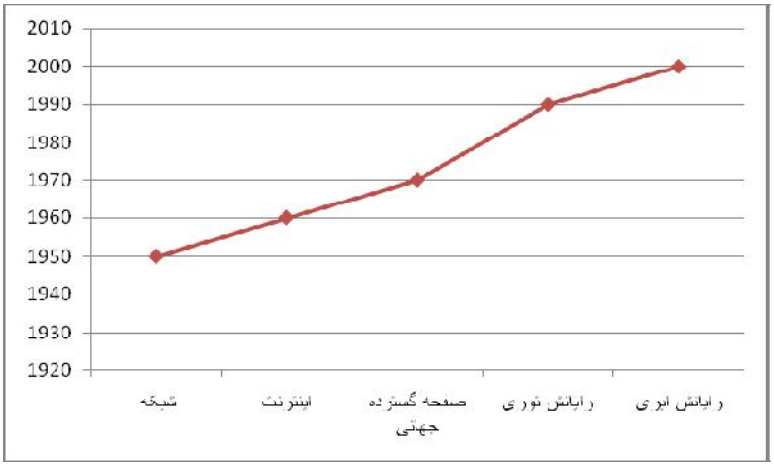
ساناز خلیلی، ریحانه جانیکه

چکیده

رایانش ابری از بستر اینترنت برای اتصال به میزبان شبکه، زیرساخت‌ها، برنامه‌های کاربردی و ارائه سرویس‌های قابل اعتماد استفاده می‌کند. در ابر هر سرویسی با توجه به نیاز مشتری ارائه می‌شود. در مجموع می‌توان ابر را ترکیبی از فناوری‌های موجود، سیستم‌های توزیع شده، چند پردازنده‌ای، فناوری‌های مجازی‌سازی و شبکه‌های مبتنی بر فضای ذخیره‌سازی داده‌های توزیع‌شده معرفی کرد.

مقدمه

امروزه پیشرفت و توسعه مرزهای دانش به گسترش تکنولوژی‌های محاسباتی وابسته شده است. به‌عنوان نقطه آغاز این تکنولوژی‌ها می‌توان به تشکیل شبکه کامپیوتری اشاره کرد که در آن تنها چندین کامپیوتر به هم متصل شده بودند. پس از آن این شبکه‌های کوچک به یکدیگر متصل شدند و اینترنت را به‌وجود آوردند که در اینترنت شبکه‌ها به اشتراک گذاشته شدند. در آن زمان به بستری برای تبادل اطلاعات از طریق اینترنت نیاز بود که مفهوم صفحه گسترده جهانی (WWW[1]) شکل گرفت که از طریق آن اطلاعات در میان کاربران به اشتراک گذاشته شد. در این راستا تکنولوژی جدیدی به نام رایانش توری[2] شکل گرفت که در آن منابع از راه دور به اشتراک گذاشته شدند و هدف آن افزایش کارایی و توان پردازشی بود. در عصر حاضر با روش جدیدی به نام رایانش ابری روبرو هستیم که در این روش سرویس‌ها از طریق اینترنت به اشتراک گذاشته می‌شوند. در شکل1 سیر تکاملی رایانش ابری نشان داده شده است.



با توجه به رشد روز افزون تکنولوژی و تنوع نیاز کاربران در حوزه فناوری اطلاعات، جایگاه رایانش ابری نمود بیشتری پیدا می‌کند، چرا که گسترش زیر ساخت محاسباتی در هر سازمان نیازمند صرف هزینه و زمان و نیروی انسانی بسیاری است که گاهی در توان عملیاتی یک سازمان نمی‌گنجد. از این رو سازمان‌ها برای پیشبرد اهداف خود تمایل به استفاده از چنین تکنولوژی‌هایی دارند. ولی اغلب نمی‌توانند هیچ تضمینی در خصوص امنیت اطلاعات و برنامه‌های کاربردی خود که نزد سرویس‌دهندگان ابر(CSP[3]) است،

1 _World Wide Web
2 _Grid Computing
3 _cloud service provider

حاصل کنند. البته راه‌کارهای امنیتی توسط ارائه‌دهندگان برای تضمین امنیت اطلاعات مشتریان اعمال می‌شود، ولی به دلیل اینکه همه چیز در ابر کاملاً شفاف[1] است و کاربران هیچ اطلاعی از این مکانیزم‌ها ندارند، گاهی مسئله را سخت و دشوار جلوه می‌دهد.
با وجود اینکه تعاریف زیادی از رایانش ابری وجود دارد، ولی می‌توان گفت یک اتفاق نظر کلی هم در صنعت محاسبات و هم در دانشگاه وجود دارد که منابع موردنیاز و سرویس‌ها در سراسر اینترنت را فراهم می‌کند. این نوع محاسبات به سازندگان و توسعه‌دهندگان اجازه می‌دهد تا برنامه‌های کاربردی مورد نظر خود را نوشته و در محیط ابر اجرا کنند.
انواع سرویس‌ها در ابر به سه دسته زیرساخت به‌عنوان سرویس (Iaas[2])، Platform به‌عنوان سرویس (Paas[3]) و نرم افزار به‌عنوان سرویس (Saas[4]) تقسیم می‌شوند.
از جمله مزایایی که می‌توان برای رایانش ابری برشمرد، کیفیت سرویس، قابلیت اطمینان، مدیریت از راه دور، کاهش هزینه، کارایی، قابلیت اعتماد و شهرت است.

1- آشنایی با پردازش ابری

ایده پردازش ابری بسیار ساده است و عبارت است از حفظ اطلاعات بر روی سروری در اینترنت و محل استقرار این کامپیوتر اهمیتی ندارد. این امکان وجود دارد که یک سری از اطلاعات بر روی تعداد بسیاری از رایانه‌ها و نه فقط یک رایانه حفظ و نگهداری شود. بدین ترتیب از این تعبیر استفاده می‌شود که اطلاعات در جایی در هوا و ابرها است.
تا زمان برقراری اتصال به اینترنت و دارا بودن پهنای باند کافی، می‌توان با استفاده از هر دستگاهی که توانایی برقراری ارتباط با اینترنت را دارد، به سرور مورد نظر دسترسی یافت و از اطلاعات خود استفاده کرد.
انتقال اطلاعات به ابر بدین معنی است که دیگر لزومی در به خاطر سپردن محل ذخیره‌سازی فایل‌ها، پشتیبان‌گیری از تمام اطلاعات، انتقال اطلاعات از دستگاهی به دستگاه دیگر یا اعمال مشابه دیگر نیست. ابرها اجازه ایجاد بانک اطلاعاتی، حفظ و توسعه آن تا هر زمانی را می‌دهند.

یکی از دشوارترین اعمال برای مدیران شرکت‌ها یا بخشی از اداره‌ها، خریداری کامپیوتر و نرم‌افزارها و لیسانس مربوطه برای هر نرم‌افزار است که مستلزم هزینه است. اما در پردازش ابری تنها وظیفه‌ای که بر عهده کاربران است، ارتباط برقرار کردن با ابر است که به‌سادگی اتصال به یک سرور اینترنت بوده و از آن به بعد تمام کارها توسط ابر رایانه‌ای پردازش می‌شوند.
استفاده از خدمات ایمیل تحت وب، نمونه‌ای از کاربردهای ابر رایانه‌ای است که اطلاعات و پردازش‌های ایمیل بر روی رایانه اجرا نمی‌شود و توسط یک ابر رایانه‌ای کنترل و مدیریت می‌شود.

شکل 1- نمونه‌ای از تعاملات یک کاربر با شبکه توسط رایانش ابری

2- معماری پردازش ابری

معماری پردازش ابری عبارت است از دو بخش ابتدایی و انتهایی که توسط یک شبکه به هم متصل می‌شوند. بخش ابتدایی، اطلاعات و شکل ظاهری نرم‌افزارها و در واقع بخش قابل مشاهده برای کاربران است. بخش انتهایی، ابر رایانه‌ای است که پردازش‌ها را در بر می‌گیرد. نرم‌افزاری که برای ارتباط با بخش انتهایی مورد استفاده قرار می‌گیرد نیز جزء بخش ابتدایی است و شبکه‌ای که این دو بخش را به هم متصل می‌کند، معمولاً اینترنت است. بخش انتهایی، از چندین کامپیوتر و سرور و واحدهای ذخیره تشکیل

1 _Transparency
2 _ Infrastructure as a service
3 _Platform as a service
4 _Software as a service

شده است. از نظر نرم‌افزاری، ابر می‌تواند دارای هرگونه نرم‌افزاری باشد. در این میان، رایانه نیز وظیفه مدیریت ابر و نظارت بر ترافیک و تبادل اطلاعات را بر عهده دارد.
در داخل خود رایانه‌ها نرم‌افزارهای چند منظوره‌ای رابط[1] نیز وظیفه تنظیم پردازش‌ها و ارسال اطلاعات به ابر را دارند. با افزایش تعداد کاربران یک ابر، اطلاعات نیز به همین ترتیب افزایش می‌یابد. برای ذخیره اطلاعات انبوه در ابعاد فعالیت‌های یک شرکت، نیاز به واحدهای ذخیره بسیار پیشرفته و پرحجم است. در بعضی از ابرها از تمام اطلاعات داخل شبکه یک کپی تهیه و از آن به‌عنوان پشتیبان نگهداری می‌شود تا بتواند در صورت ایجاد اخلال در ابر، مورد استفاده قرار گیرد.

3- تهدیدهای امنیتی موجود در رایانش ابری و راه‌حل کاهش آنها

رایانش ابری با وجود داشتن مزایای زیاد، همواره دارای تهدیدهای امنیتی بی‌شماری برای اطلاعات درحال تبادل است که باعث می‌شود مشتریان از بهره بردن از مزایای ابر باز بمانند. برخی از این تهدیدها در ادامه آورده شده اند.

3-1- تهدیدهای داخلی

این نوع تهدیدها از درون سازمان‌های ارائه‌دهنده سرویس به‌وجود می‌آیند. به این معنی که مشتریان داده‌های مهم و حیاتی خود را در فضای ابر میزبان ذخیره می‌کنند. اگر کارکنان سازمان به‌علت داشتن دسترسی به این داده‌ها، از اطلاعات مشتریان سوء استفاده کنند، شرکت ارائه‌دهنده‌ی ابر، شهرت خود را در بین مشتریان از دست خواهد داد.
از روش‌های مقابله با این چالش می‌توان به اجرای دقیق مدیریت زنجیره تامین، شفافیت شیوه‌های مدیریتی، امنیت اطلاعات و وجود یک سیستم گزارش‌گیری از نقص‌های امنیتی برای جلوگیری از انواع حمله‌ها اشاره کرد.

3-2- تهدیدهای خارجی

با وجود اینکه تهدیدهای داخلی برای ارائه‌دهندگان ابر یک تهدید بزرگ است ولی تهدیدهای خارجی هم می‌توانند تاثیر بسیار زیادی داشته و باعث بروز خسارت‌هایی به سیستم و فرآیندهای آن شوند. نقاط ضعف یک سازمان ارائه‌دهنده می‌تواند راهی برای مهاجمان خارج از سازمان باز کرده و باعث حملات مخرب خارجی شود، به‌طور مثال مهاجمان می‌توانند از ضعف APIها[2] و کانال‌های ارتباطی استفاده کرده و سازمان را مورد حمله قرار دهند.
برای حفاظت سازمان در برابر چنین تهدیدهایی استفاده از فایروال‌ها و سیستم‌های تشخیص و پیشگیری از نفوذ، بسیار ضروری است. همچنین پیاده‌سازی یک Honey Pot و استفاده از قانون AAA[3] ضروری است.

3-3- کنترل دسترسی

در رایانش ابری داده‌های مشتریان در مکان ناشناخته‌ای که از دید کاربران پنهان است ذخیره می‌شود و مشتریان هیچ‌گونه کنترل و مدیریتی روی داده‌های حیاتی خود ندارند و هیچ‌گونه آگاهی از مکانیزم امنیتی که توسط ارائه‌دهنده پیاده‌سازی شده، ندارند. از دست دادن کنترل روی داده‌های حیاتی و سرویس‌های بحرانی و حساس می‌تواند در هر سازمانی اختلال ایجاد کند.
عدم کنترل روی داده‌های حساس از سوی مشتریان ممکن است باعث از دست رفتن داده‌ها شود. این امر موجب از بین رفتن نام تجاری و شهرت سازمان‌های ارائه‌دهنده ابر شود.
برای کاهش مشکلات کنترل دسترسی و افزایش دسترس‌پذیری و کارایی، ایجاد توافق‌نامه در سطح سرویس SLA[4] بین سرویس‌دهنده و مشتری الزامی است. همچنین استفاده از یک احراز هویت بسیار قوی و فرآیند مجوزدهی، منجر به کاهش این چالش می‌شود. منظور از احراز هویت قوی این است که سازمان‌ها برای کاربران خود از روش Single Sign On استفاده کنند تا کاربران برای دسترسی به همه سرویس‌ها و برنامه‌های کاربردی مورد نظر در هر قسمت از محیط ابر، از یک احراز هویت واحد استفاده کنند.

---

1 _Middleware
2 _Application Programing Interface
3 _Authorization-Authentication-Accounting
4 _Service-level agreement

3-4- وقفه در سرویس دهی

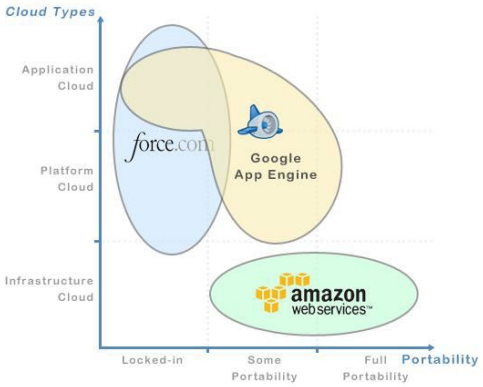
ماهیت اصلی رایانش ابری ارائه سرویس است، هر گونه اختلال در ارائه سرویس می‌تواند منجر به قطع سرویس و از بین رفتن شهرت سازمان ارائه دهنده‌ی ابر شود. اگر مهاجمان بتوانند به اعتبارنامه ورود سازمان سرویس‌دهنده و اعتبارنامه ورود مشتریان دسترسی پیدا کنند، می‌توانند داده را تغییر داده، سرویس‌ها را مورد حمله قرار داده و آنها را متوقف کنند. ازجمله حمله‌هایی که می‌توان در این چالش‌ها برشمرد، حمله‌های DOS ، DDOS ، Phishing و Froud است. این تهدید در اثر وجود ثبت‌نام نسبتاً ضعیفی است که در محیط رایانش ابری به‌وجود می‌آید و می‌تواند باعث حمله هکرها به سیستم شود. در واقع ثبت نام بدین معنی است که به هر مشتری برای دریافت سرویس‌ها یک حساب کاربری معتبر از سوی سرویس‌دهنده داده می‌شود. یکی از راه‌حل‌های موجود برای کاهش این چالش، عدم به اشتراک‌گذاری حساب کاربری بین مشتریان یک ارائه‌دهنده است که با استفاده از یک احراز هویت چندعامله انجام می‌شود. ارائه‌دهنده ابر باید بتواند دائماً ترافیک شبکه مشتری را بازرسی کند و با یک سیستم پیشگیری از نفوذ، از هر اقدام خرابکارانه‌ای جلوگیری کند.

3-5- چند مستأجری

سرویس‌ها در ابر به کاربران متعددی ارائه می‌شوند. از این رو چندمستاجری مفهوم اصلی ابر است. ارائه‌دهنده، برنامه کاربردی و سخت‌افزار فیزیکی خود را برای اجرای ماشین مجازی مشتریان به اشتراک می‌گذارد. کاربران برای ارائه‌دهنده در حکم مستاجر هستند. هر ماشین در اختیار یک کاربر قرار می‌گیرد و این باعث بروز حمله ماشین‌های مجازی به یکدیگر می‌شود. برای غلبه بر این مشکل می‌توان از راه‌حل‌هایی نظیر دفاع در عمق که همان دفاع از زیر ساخت مجازی ابر در لایه‌های مختلف است، استفاده کرد. در واقع در یک محیط ابری باید یک دفاع لایه‌بندی‌شده برای حفاظت از محیط وجود داشته باشد. رویکرد دفاع در عمق تضمین می‌کند که تهدیدها مجبور به عبور از بیش از یک لایه باشند. از این رو سرویس‌دهندگان می‌توانند تعدادی از تهدیدها را در مراحل اولیه و قبل از انتشار در محیط ابر، شناسایی و مسدود کنند.

3-6- قابلیت حمل

هر ارائه‌دهنده سرویس در ابر، برای تعامل با مشتریان خود یک سری قوانین خاص خود را دارد که مشتری بر اساس چنین قوانینی داده‌ها و برنامه‌های خود را نزد ارائه‌دهنده ذخیره می‌کند. از آنجا که همه سازمان‌های ارائه‌دهنده سرویس از یک استاندارد مشترک تبعیت نمی‌کنند، بنابراین امکان مهاجرت مشتریان از یک ارائه‌دهنده به ارائه‌دهنده دیگر در ابر امکان‌پذیر نیست که به این موضوع Lock in گفته می‌شود. به‌عنوان مثال می‌توان مقایسه قابلیت حمل در بین سه ارائه‌دهنده Google ، Amazon و Force را در شکل زیر نمایش داد.



شکل2- نمودار مقایسه قابلیت حمل در بین سه ارائه‌دهنده رایانش ابری

همان‌طور که در شکل بالا نشان داده شده است، قابلیت حمل درآمازون از نظر زیرساخت رایانش ابری از بقیه بیشتر است. برای افزایش قابلیت حمل در بین ارائه‌دهندگان لازم است که یک استاندارد جامع تعریف شده و تمامی ارائه‌دهندگان موظف به رعایت این استاندارد شوند.

3-7- انتقال اطلاعات

زمانی که مشتریان اطلاعات خود را در ابر منتقل می‌کنند، این اطلاعات برای سازمان ارائه‌دهنده سرویس قابل دسترسی است، از این رو ممکن است مورد سوء استفاده قرار گیرد. همچنین ممکن است این اطلاعات در حین انتقال در ابر توسط یک خرابکار که در حال کنترل ترافیک شبکه است به سرقت برود. بنابراین برای امنیت اطلاعات در حال تبادل دو روش وجود دارد: در روش اول از رمزنگاری اطلاعات استفاده می‌شود به این معنی که مشتری اطلاعات خود را با استفاده از الگوریتم‌های رمزنگاری رمز نموده و برای ارائه‌دهنده ارسال کند. در روش دوم می‌توان از مکانیزم‌های امنیتی VPN [1] یا SSH Tunneling [2] استفاده کرد.

3-8- APIهای ناامن

ارتباط بین مشتریان و ارائه‌دهندگان ابر از طریق APIها انجام می‌شود. وظیفه API، تأمین و مدیریت سرویس‌هایی است که قرار است در ابر ارائه شود. APIهای ضعیف می‌توانند سازمان‌های ارائه‌دهنده را در معرض تهدیدهای امنیتی مختلفی مانند دسترسی ناشناس، مجوز نامناسب و ... قرار دهند.
به‌منظور کاهش چنین مشکلاتی بهتر است از یک احراز هویت قوی و کنترل دسترسی مناسب استفاده شود.

3-9- رابط مدیریت دسترسی از راه دور

دسترسی مشتریان به سرویس‌ها در ابر از طریق رابط‌هایی در اینترنت انجام می‌شود و مجموعه بزرگی از منابع از این طریق در اختیار مشتریان قرار می‌گیرد. یک نقطه ضعف بسیار مهم در این زمینه، آسیب‌پذیری مرورگرهای وب است که می‌تواند تهدید جدی را در بر داشته باشد.
یک راه برای مقابله با این تهدید استفاده از پروتکل امن HTTPS برای ارائه دسترسی از راه دور است. راه دیگر بررسی نقاط آسیب‌پذیری مرورگرهاست و اینکه به‌طور مکرر باید مرورگرها به روزرسانی شوند. جدول زیر مقایسه‌ای بین راه حل‌های موجود برای چالش‌های امنیتی را نشان می‌دهد.

جدول 1- مقایسه نه راه‌حل موجود برای چالش‌های امنیتی

راه‌حل‌ها / چالش‌های امنیتی	مدیریت امنیت	سیستم گزارش گیری	فایروال	IDS & IPS	SLA	احرازهویت چندعاملی	دفاع در عمق	استانداردسازی	رمزنگاری	استفاده از پروتکل‌های امن	به روزرسانی مرورگرها
تهدیدات داخلی	✓	✓									
تهدیدات خارجی			✓	✓							
کنترل دسترسی					✓	✓					
وقفه در سرویس‌دهی			✓	✓		✓					
چندمستأجری							✓				
قابلیت حمل								✓			
انتقال داده						✓			✓	✓	✓
API ناامن						✓				✓	✓

1 _Virtual private network
2 _Secure shell tunneling

رابط مدیریت دسترسی از راه دور					✓					✓	✓

مزایا و چالش پردازش ابری در شرکت‌ها و شبکه‌های رایانه‌ای

- با استفاده از پردازش ابری، کاربران می‌توانند از هر کجا و در هر زمان به اطلاعات دسترسی یابند و وارد ابر شوند.
- هزینه خرید نرم‌افزارها تا حد بسیاری کاهش می‌یابد؛ زیرا دیگر نیازی به خرید یک نرم‌افزار برای هر کاربر نیست. تنها یک نرم‌افزار که برای پردازش ابری طراحی شده است، برای تمام یک مجموعه کافی است.
- پردازش ابری هزینه‌های سنگینی را که شرکت‌ها برای سخت‌افزار متحمل می‌شوند، کاهش می‌دهد. دیگر نیازی به خرید هارد دیسک‌های پرظرفیت و پردازشگرهای پیشرفته نیست. از طرفی نیاز به فضاهای ذخیره (Physical) نیست و با قرار دادن اطلاعات بر روی ابزار ذخیره دیگر، تنها هزینه اجاره و دسترسی به اطلاعات خود را می‌پردازید.
- تنها نگرانی پردازش ابری، امنیت اطلاعات و نفوذپذیری این سیستم است. در صنعت IT اولین عاملی که موفقیت یک سیستم را تضمین می‌کند، امنیت اطلاعات است.

4- مراجع

1- Bojanova, A. Semba, “Analysis of Cloud Computing Delivery Architecture Models” , workshops of International Conference on Advanced Information Networking and Application, PP.453-458, 2011

2- Sherin sreedharan, G.kalpana, “Security Issues and Solutions for Cloud Computing”, PP. 494-498, 2013