کنفرانس ملی چشم انداز ۱۴۲۰ و پیشرفت های
تکنولوژیک مهندسی برق، کامپیوتر و فناوری اطلاعات

مروری بر ذخیره سازی و انتقال امن پیام در شبکه های مبتنی بر رایانش ابری

سجاد قاسمی[۱]، فرشاد کیومرثی[۲*]، بهزاد زمانی دهکردی[۳]

[۱] دانشجوی کارشناسی ارشد، گروه کامپیوتر، واحد شهرکرد، دانشگاه آزاد اسلامی، شهرکرد، ایران
[۲] استادیار، گروه کامپیوتر، واحد شهرکرد، دانشگاه آزاد اسلامی، شهرکرد، ایران
[*] نویسنده مسئول
[۳] استادیار، گروه کامپیوتر، واحد شهرکرد، دانشگاه آزاد اسلامی، شهرکرد، ایران
Sajad.ghasemi1986@chmail.ir

خلاصه: رایانش ابری مدلی است که دسترسی به منابع محاسباتی، سرورها، منابع کاربردی و انواع سرویس ها را با سرعت مناسب و به آسانی فراهم می کند. هزینه پایین و مقرون به صرفه بودن آن، رایانش ابری را به یک بستر ایده آل برای به کارگیری معماری سرویس محور تبدیل کرده است. اما مهمترین چالش این فن آوری تامین امنیت آن است که موجب عدم اطمینان مدیران برخی سازمانها به آن می گردد. در این مقاله رویکرد های ایجاد امنیت در ذخیره و انتقال داده به فضای ابر، بررسی می شود.

کلمات کلیدی: رایانش ابری، امنیت داده، انتقال داده، رمز نگاری، احراز هویت سرور

۱. مقدمه

با ورورد رایانه به زندگی انسان ها و فراگیر شدن آن و تسهیل و تسریع در انتقال اطلاعات تحت شبکه های کامپیوتری، همواره بحث حفظ امنیت تبادل اطلاعات و جلوگیری از به سرقت رفتن آن مطرح بوده است. از طرفی با ظهور فن آوری رایانش ابری در امر انتقال و پردازش داده ها و بواسطه ویژگی هایی از قبیل محبوبیت، سرعت و تسهیل در پردازش داده ها موجب شد تا اکثر سازمان ها و شرکت ها به استفاده از این فن آوری روی آورند. مدل رایانش ابری یکی از تکنولوژی های به روزی است که به تازگی به مرحله ظهور رسیده است؛ وقتی از رایانش ابری صحبت می کنیم بهتر است به دو بخش آشکار و پنهان آن را تقسیم بندی کنیم، بخش آشکار آن سمت کاربر و خدمات قابل دسترس آن است و بخش پنهان شامل سیستم های کامپیوتری، سرورها و نرم افزار های نصب شده بر روی آن که از دید کاربر پنهان است. برنامه های رایانش ابری عملاً نامحدود بوده و کاربران می توانند داده ها و برنامه هایشان را از هرجا و هر زمانی مورد استفاده قرار دهند. از جمله ویژگی های مفید این مدل می توان به افزایش سرعت پردازش، عدم وابستگی به نرم افزار و سیستم عامل خاص، به اشتراک گذاری منابع اشاره نمود؛ رایانش ابری نیاز های سخت افزاری پیشرفته روی سرویس گیرنده را کاهش می دهد اما چالش امنیت را به وجود می آورد که با سیاست هایی از قبیل کنترل دسترسی، رمزنگاری داده ها و استفاده از احراز هویت سرور می توان امنیت مورد نظر را تامین کرد. در این مقاله در قسمت ۲ به خصوصیات رایانش ابری، قسمت ۳ چالش های پیش رو در رایانش ابری، قسمت ۴ امنیت ذخیره و انتقال داده در فضای ابر بررسی می

شود و در قسمت ۵ روش های ایجاد امنیت ذخیره و انتقال داده در فضای ابر از جمله، استفاده از ابر خصوصی و تعیین سطح دسترسی رمزنگاری داده ها استفاده از پیام soap[۱] و استفاده از احراز هویت سرور AAA[۲] بررسی و آینده ای از این فناوری نو ظهور بررسی می شود.

۲. رایانش ابری[۳]

منابع و سرویس های مورد درخواست بر روی بستر اینترنت که قابلیت توسعه و اطمینان بالایی دارند را ابر می گویند و رایانش ابری یک روش محاسباتی است که در آن منابع با قابلیت گسترش پویا و عموماً به شکل مجازی توسط ارائه دهندگان خدمات بر روی اینترنت فراهم و تحویل میشوند. این روش محاسباتی مزایای بسیاری برای کاربران خود دارد و از جمله آن میتوان به عدم نیاز به داشتن دانش فنی یا اعمال کنترل بر روی زیرساخت اشاره کرد. در این مدل محاسبات، از توان پردازش می توان به عنوان یک سرویس یا خدمت توسعه و به کارگیری فناوری کامپیوتر بر مبنای اینترنت، صحبت کرد. در واقع رایانش ابری، توسعه و بکارگیری فناوری کامپیوتر بر مبنای اینترنت است. سرویس های ارائه شده در ابر، برنامه های کاربردی را به صورت برخط فراهم می کنند به طوری که با مرورگرهای وب قابل دسترسی هستند. در این زمان نرم افزارها و داده ها بر روی سرورها ذخیره شده اند؛ در طول استفاده از رایانش ابری کاربر بدون اینکه بفهمد سرویس کجاست و یا چگونه آن را تحویل می گیرد صورت می پذیرد[۱]. رایانش ابری دارای ساختاری شبیه تودهای ابری متشکل از سرویسها و کاربردهای بسیاری است که کاربران از هر جای دنیا و با استفاده از اینترنت پرسرعت و پرداخت هزینه از آنها استفاده می کنند و کامپیوتر منفرد جای خود را به ابر با میلیون ها کاربر داد.

خصوصیات کلیدی رایانش ابری: رایانش ابری دارای خصوصیات ویژه و منحصر به فردی می باشد که خاص سبک خودش است یکی از این خصوصیات ارائه سرویس مبنی بر تقاضا است به این معنی که کاربر با پرداخت هزینه از منابع سخت افزاری- نرم افزاری استفاده می کند، ویژگی دیگر و خاص آن استفاده از اینترنت به عنوان بستر جهت تحویل و ارائه سرویس می باشد. ویژگی دیگر غنی بودن ابراز منابع است و مانند یک استخر پرآب است و این منابع به وسیله تکنیک مجازی سازی از محل فیزیکی خود مستقل شده اند[۲]؛ بنابراین به راحتی میتوانند در بستر شبکه جا به جا شوند؛ از جمله ویژگیهای دیگر می توان به مقیاس فوق وسیع، مجازی سازی، چند کاربردی، قابلیت اطمینان و سرویس مبتنی بر تقاضا اشاره کرد.

انواع سرویس های رایانش ابری: سرویس های ارائه شده در رایانش ابری را می توان به انواع مختلفی تقسیم بندی کرد. از مدل XAAS[۴] یا هر چیزی بعنوان سرویس می توان استفاده کرد[۱]. می توان مفاهیم مختلفی از جمله نرم افزار، زیربنا، زیرساخت نیروی انسانی، امنیت وغیره باشد. saas[۵]، paas[۶]، iaas[۷] سه مدل اصلی تحویل سرویس در محاسبات ابری هستند. این سه نوع سرویس بنیان سرویسهای رایانش ابری را تشکیل می دهند و به همین علت از آنها در معماری لایه ای رایانش ابری استفاده می شود. در واقع برای تفکیک سرویس از مدل XAAS استفاده می شود که IAAS ، PAAS و SAAS از نمونه های مهم این مدل هستند، سرویسهای ارائه شده در IAAS در پایین ترین سطح و بسیار نزدیک به سخت افزار مانند منابع اصلی (فضای ذخیره سازی، زیر ساخت شبکه یا توان پردازشی) قرار گرفته اند. PAAS در این جا به عنوان سرویس و در دو محیط متفاوت توسعه سیستم و محیط اجرا،

---

[۱] Simple Object Access Protocol

[۲] Authentication ،Authorization ،Accounting

[۳] Cloud Computing

[۴] X as a service

[۵] Software as a service

[۶] Platform as a service

[۷] Infrastruature as a service

قابلیت اجرا دارد، تمامی برنامه های کاربردی که به روی ابر کار میکنند و آنان که سرویس مستقیم را به مشتریان عرضه میدارند در لایه SAAS قرار میگیرند. سرویسهای این لایه به دو بخش سرویسهای پایه و سرویسهای مرکب تقسیم می شوند.

۳. چالش های ابری

امنیت و حریم خصوصی، دسترسی پذیری، همکاری و تعامل، قابلیت اطمینان و انعطاف پذیری پایین در سفارشی کردن از جمله این چالش های رایانش ابری هستند. بزرگترین مانع در پذیرش رایانش ابری امنیت و حریم خصوصی است. اینکه کاربران و سازمانها داده های خود را بیرون از سازمان خود نگهداری کنند، پذیرفتنی نیست زیرا افراد غیر مجازی می توانند به این داده ها دسترسی داشته باشند و قابل ذکر است که راه حل قابل قبول و تأیید شده ای از امنیت ارائه نشده است؛ در صورت بروز مشکل در زیرساخت حجم وسیعی از سیستم های وابسته به آن از کار خواهند افتاد و این فاجعه است که مشتریان ابر باید از دسترس پذیری بسیار بالایی برخوردار باشند[۸].

۴. انواع امنیت

چالش های امنیتی در سطوح مختلف از جمله سطح شبکه و سطح میزبان و سطح کاربرد بررسی می شود. مسائل امنیت زیرساخت رایانش ابری را با توجه به اینکه بخشی از امنیت توسط ارائه دهنده تولید می شود با تعیین مرزهای اعتماد می توان تشخیص داد[۳]. در این بخش امنیت داده در ذخیره سازی و رایانش ابری بررسی می شود.

امنیت داده و ذخیره سازی: امنیت داده پیچیدگی زیادی دارد و روش های حفاظت از داده شامل ویرایش، کوتاه سازی، مجهول سازی و... می باشدکه با نگرانی های زیادی روبرو است[۳]، اما نه تنها در این حیطه هیچ استانداردی وجود ندارد، بلکه هیچ برنامه ای که منجر به توسعه و اعتبار در پیاده سازی باشد وجود ندارد.

امنیت داده در رایانش ابری: برای انتقال داده از محیط سنتی پردازش به محیط ابر، برای یک مشتری ابر دو موضوع قابل توجه خواهد بود؛ اول اینکه محل ذخیره داده مکانی غیر از مکان ماشین کاربر خواهد بود و دوم محل ذخیره داده از یک محیط تک کاربره به یک محیط چند کاربره تغییر پیدا می کند. این تغییرات باعث بوجود آمدن نگرانی مهم از بابت افشای داده می شود[۱]. از دید سازمانها، مشکل افشای داده یک ریسک بزرگ می باشد، با این حال تمایل کاربران به دریافت خدمات بهتر، سریعتر و مطمئن تر، بالا رفته است؛ کنترل دسترسی به داده و تعیین صلاحیت یکی از مواردی است که بیشترین تحقیقات را در بحث امنیت داده ابر به خود اختصاص داده است، در صورت نبود امنیت کافی داده، این امکان وجود دارد که یک نفوذگر، به داده های ذخیره شده در ابر دسترسی پیدا کند. بنابراین یکی از موارد مهم و قابل توجه در عرصه رقابت ارائه دهندگان ابر ارائه سیاست های مطمئن و کار آمد برای برقراری امنیت داده می باشد.

۵. روش های ایجاد امنیت در انتقال داده وذخیره در فضای ابر

استفاده از ابر خصوصی (تحت شبکه داخلی) و تعیین سطح دسترسی: پیشنهاد می شود به منظور تامین امنیت ابر از ابر خصوصی استفاده شود. در این طرح سیستم ها از طریق تکنولوژی LAN[۸] بوسیله مسیر یاب ها و مودم های بی سیم و باسیم به یکدیگر متصل می شوند؛ و پس از نصب نرم افزار های مربوطه بر روی سرویس گیرنده، سرویس دهنده به صورت تصادفی بر اساس الگوریتم انتخاب شده و نام کاربری، رمز عبور و سطح دسترسی کابران توسط مدیر سیستم تعیین می گردد[۴]. به منظور شناسایی و کنترل فعالیت های کاربران در ابر، از آدرس های IP[۹] از قبل تعیین شده و نام کاربری استفاده می گردد.

رمز نگاری پیام و داده : با توجه به ناامن بودن فضای ابر، به واسطه استفاده از رمزنگاری داده و پیام می توان تا حدودی از سرقت اطلاعات خود جلوگیری کرد. بگونه ای که اگر ارائه کننده های فضای ابر هم به داده های ما دسترسی پیدا کنند، آنها را بصورت رمز نگاری و اطلاعات غیر قابل استفاده یافت می کنند و برای فهم اطلاعات و بهره وری از آن باید آن را رمز گشایی کنند[۴]. در نرم افزار پیام رسان کاربر پیام خود را ارسال می کند و بعد از کلیک کردن بر روی گزینه ارسال پیام آن توسط الگوریتم از پیش تعیین شده، رمزینه می شود و در کانال ارتباطی قرار می گیرد، بعد از دریافت پیام توسط کاربر مورد نظر بوسیله کلید خصوصی، پیام رمز گشایی می گردد.

رمز گذاری با استفاده از استاندارد AES[۱۰] و الگوریتم ریجندل[۱۱] در این مدل رمز گذاری، رشته ای از متن با طول ثابت دریافت می شود، بعد از آن عملیات اصلی نگاشت رمز بر روی متن اعمال شده و یا همان طول اصلی به خروجی ارسال می شود، این الگوریتم شامل حدود ۱۶ مرحله می باشد، متنی که قرار است رمز شود ابتدا در یک جایگشت خاص قرار می گیرد و سپس عملیات های وابسته به کلید بر روی آن اعمال شده و در نهایت در جایگشت نهایی قرار می گیرد. الگوریتم ریجندل یک سیستم رمز قطعه ای با طول قالب داده ۱۲۸، ۱۹۲ و ۲۵۶ بیت است، طول کلید نیز مستقل از طول قالب ۱۲۸، ۱۹۲ و ۲۵۶ بیت می باشد، این الگوریتم دارای ساختاری با بسط کلید است که از روی کلید اصلی بسته به تعداد دورها، تعدادی زیر کلید تولید می کند که در هر دور به قالب داده اضافه می شوند. الگوریتم شامل سه تبدیل مهم MixColumn، ShiftRow و SubByte است که اولی یک تابع جایگزینی غیر خطی و تامین کننده امنیت سیستم و دومی و سومی توابعی خطی برای افزایش گسترش و اختلاط الگوریتم اند[۴]، در این رمز قطعه ای، ساختار سیستم رمزگذار دقیقاً مشابه سیستم رمزگذار نیست چون با افزایش طول کلید تعداد دور های الگوریتم افزایش می یابد، زمان اجرا و سرعت الگوریتم به طول کلید وابسته است.

رمز گذاری با استفاده از الگوریتم همریختی کامل: رمزنگاری همریختی کامل شامل چهار روش، الگوریتم تولید کلید، الگوریتم رمزنگاری، الگوریتم رمزگشایی و الگوریتم ارزیابی اضافی است، رمزنگاری همریختی کامل شامل دو نوع همریختی اصلی، الگوریتم تکثیر رمزنگاری همریختی کامل و الگوریتم افزایشی رمزنگاری همریختی کامل است، ضرب و جمع با خواص همریختی در الگوریتم رمزنگاری همریختی تا قبل از سال ۲۰۰۲ فقط از جمع و یا ضرب همریختی پشتیبانی می شد[۵]. الگوریتم رمزنگاری همریختی کامل یک الگوریتم جستجوی رمزنگاری است که می تواند از تعدادی الگوریتم جمع و تعدادی الگوریتم ضرب در داده های رمزنگاری تشکیل شده باشد.

الف) الگوریتم رمز نگاری: p، q و r پارامتر های رمز نگاری می باشند که در آن p عددی فرد و مثبت است و q عدد صحیح بزرگ و مثبتی است. p و q در مرحله تولید کلید مشخص می شوند؛ p یک کلید رمز نگاری است و r عددی تصادفی که در هنگام رمزنگاری انتخاب می شود. برای محاسبه m و دریافت متن رمز نگاری شده از فرمول ۱ استفاده می شود.

$$c = m+2r+pq \qquad (۱)$$

ب) الگوریتم رمز گشایی: با توجه به فرمول ۲ و چون pq کمتر از 2r+m است پس از فرمول ۳ می توان نسبت به رمز گشایی اقدام نمود.

$$m = (c \bmod p) \bmod 2 \qquad (۲)$$

---

[۸] local area network

[۹] Internet Protocol

[۱۰] Advanced Encryption Standard

[۱۱] Rijndeal

$$(c \bmod p) \bmod 2 = (2r + m) \bmod 2 = m \quad (۳)$$

تأیید مالکیت همریختی افزایشی: فرض کنید دو سری متن m1 و m2 وجود دارد، نحوه رمز نگاری و تبدیل آنها به متن رمز شده طبق فرمول های ۴ و ۵ است، همچنین با توجه به فرمول ۶ ، فرمول ۷ حاصل می شود و تا زمانی که $(m_1+m_2) + 2(r_1+r_2)$ کمتر از مقدار p باشد، این الگوریتم طبق فرمول ۸ شرایط همریختی افزایشی را فراهم می کند[۶].

$$c_1 = m1+2r_1+pq_1 \quad (۴)$$

$$c_2 = m2+2r_2+pq_2 \quad (۵)$$

$$m_3 = m_1 +m_2 \quad (۶)$$

$$c_3 = (c_1+ c_2) =(m_1+m_2)+2(r_1+r_2)+p(q_1+q_2) \quad (۷)$$

$$c_3 = (c_1+c_2) \bmod p+(m_1+m_2)+2(r_1+r_2) \quad (۸)$$

استفاده از پیام soap؛[۱۲] Soap پیام های متنی مبتنی بر xml[۱۳]هستند که برای تبادل داده های رمز نگاری شده بین وب سرور و کاربر با استفاده از پروتکل های مختلف از جمله HTTP؛[۱۴] SMTP[۱۵]و MIME[۱۶]به کار می روند [7]. پیام soap به دو قسمت سرپیام و بدنه تقسیم می شود، که در آن سرپیام soap از دو قسمت رمز امنیتی منطقی (دودویی) و برچسب زمانی تشکیل شده است که قسمت رمز امنیتی حاوی تاریخ ساخت و انقضای پیام soap می باشد[۶]. در شروع ارتباط با وب سرور، کاربر باید جهت ارسال درخواست خود از وب سرور مجوزی را دریافت نماید. پس از دریافت مجوز، کاربر قادر به ادامهء ارتباط با وب سرور و پیام soap می باشد.

حمله به پیام soap : هنگامی که کاربر درخواست خود را از طریق مرورگر خود به سمت وب سرور می فرستد، در سمت سرور پیام soap که شامل اطلاعات ساختاری تبادل اطلاعات بین سرور و مرورگر می باشد، ساخته می شود. به عنوان مثال مهاجم در پی حمله خود به پیام soap، با نگهداری سرپیام یک بسته قسمت بدنه آن را تغییر داده و بدنه ی ساختگی خود را در بسته جای گذاری می کند، مهاجم از طریق دستکاری بدنه soap و یا با استفاده از IP معتبر به ابر حمله می کند. حال چنانچه سرپیام بستهء فوق نشانه گذاری شده باشد مهاجم دیگر نمی تواند با ارائه IP معتبر به سرور حمله کند. این کار با استفاده از تعریف کلید RSA[۱۷]برای کاربر صورت می گیرد[۹]. از یک سیستم نامتقارن می توان برای نشان دادن صحت اینکه فرستنده پیام همان شخصی است که ادعا می کند، استفاده کرد. این عمل اصطلاحاً امضای دیجیتال نام دارد.

استفاده از احراز هویت سرور: در این رویکرد با افزودن برخی ویژگی ها، از جمله استفاده از احراز هویت سرور AAA در کنار رمزنگاری داده می توان لایه امنیتی به سیستم افزوده شود و بر خلاف روش های دیگر با داشتن بهترین عملکرد امنیت را بهبود داد. از ویژگی های این روش، مکانیسم احراز هویت سرور AAA است که کاربر برای ورود به ابر باید طی کنند، این سرور بر مبنای پروتکل EAP-TTLS[۱۸]عمل می کند و سه وظیفه احراز هویت، مجوز دهی و حسابرسی از اصلی ترین وظایف این سرور می باشد. در این رویکرد کاربر قبل از اتصال به سرور ابر جهت ذخیره سازی داده و دسترسی به خدمات ذخیره سازی ابتدا باید توسط سرور AAA احراز هویت شود و چون کلیه عملیات احراز هویت توسط سرور AAA انجام می شود سربار کمتری بر ابر وارد می شود و با عث می شود افت سرعت و کارایی در ابر نداشته باشیم[۱].

---

[۱۱] Simple Object Access Protocol

[۱۲] Extensible Markup Language

[۱۳] Hypertext Transfer Protocol

[۱۴] Simple Mail Transfer Protocol

[۱۵] Multi-Purpose Internet Mail Extensions

[۱۷] رایج ترین و معروف ترین الگوریتم نامتقارن که مخفف حروف اول نام پدید آورندگان آن Rivest، Shamir و Adlemen است.

[۱۸] Extensible Authentication Protocol Tunneled Transport Layer Security

۶. نگاهی به آینده

با توجه به فراگیر شدن استفاده از فناوری رایانش ابری و تسریع و تسهیل انجام برخی امور بر بستر اینترنت، پیش بینی می شود سازمان ها جهت استفاده از این فناوری تمایل نشان دهند؛ اما دغدغه اصلی برخی سازمانها امنیت داده های سازمان است، بگونه ای که در برخی موارد حیات سازمان به امنیت داده های آن وابسته است و این دغدغه موجب عدم اطمینان به رایانش ابری و عدم استفاده از آن می گردد که این مسئله رویکردهایی را فرا روی محققان قرار می دهد.

۷. نتیجه گیری

با ظهور رایانش ابری مشکلات برخی روش های حل شد ولی مشکل امنیت یکی از مهم ترین چالش های پیش روی رایانش ابری است، کاربران و شرکت‌ها باید با برنامه و متفکرانه از رایانش ابری استفاده کنند و نباید تصور کنند که منابع نامحدود هستند و استفاده مجاز، زیرا موقعی به این موضوع پی می برند که منابع خود را از دست داده اند و هزینه پرداخت شده هم صرف شده است و مسئله بعد این است که استفاده کنندگان از ابر نباید در هزینه پایین سرمایه گذاری اولیه دچار اشتباه شوند و نباید پروژه ها را با سرعت و عجله توسعه دهند. با اجرای ترکیبی از روش های مطرح شده در این مقاله می توان امنیت فضای ابر، ذخیره و انتقال داده بر روی آن را در بستر اینترنت فراهم نمود و برای پویایی و بهره وری بیشتر سازمان و حفظ محرمانگی اطلاعات و پیشگیری از درز و سرقت اطلاعات بارگذاری شده در فضای ابر گامی رو به جلو برداشت.

مراجع

۱. ا. زمانی و م. جوانمرد.(۱۳۹۴)، "ارائه روشی برای ذخیره سازی امن داده ها در رایانش ابری،*"نخستین کنفرانس بین المللی مهندسی برق و علوم کامپیوتر*،

2. Alowolodu, O, D & Ogundele, O,S. (2013). Elliptic Curve Cryptography for securing Cloud Computing Applications. International Journal of Computer Applications, Vol. 6,pp: 1-7.
3. B. Rimal, E. Choi and I. Lump, (2009), "A Taxonomy and Survey of Cloud Computing Systems," INC, IMS and IDC.
4. Y. Chen.zh, (2010), "IT Auditing to Assure a Secure Cloud Computing," World Congress on Services,.
5. Bedra.A, (2010), "Getting started with Google App engine and clojure," IEEE Internet Computing, vol. 14(4), pp. 58-55.
6. Eludiora, S, Olatunde, A, Ayodeji, O, Adeniran, O, Onime, C & Kehinde, L (2012). A User Identity Management Protocol for Cloud Computing Paradigm. International Journal of Communications, Network and System Sciences, Vol 5, pp: 1-7.

7. Vanya Diwan et al., (2014), “Cloud Security Solutions: Comparison among Various Cryptographic Algorithms” International journal of advanced research in computer science and software engineering (IJARCSSE).
8. Hashizume et al.,(2013),”An analysis of security issues for cloud computing”, Journal of Internet Services and Applications (jisa).
9. Rashmi, (2013), “A Survey of Cryptographic Algorithms for Cloud Computing”, International Journal of Emerging Technologies in Computational and Applied Science (IJETCAS).