۱۴۰۱/۱۰/۳۰
چهارمین همایش ملی مهندسی کامپیوتر و نرم افزار
4TH NATIONAL CONFERENCE ON COMPUTER AND SOFTWARE ENGINEERING

گذری بر امنیت در سیستم‌های مبتنی بر رایانش ابری و روش‌های افزایش امنیت در رایانش ابری

محمدجواد حسین‌پور[۱]، هادی رنجبر[۲]

دانشگاه آزاد اسلامی واحد استهبان، استهبان، ایران

Hosseinpoor.mohammadjavad@gmail.com

چکیده:

با گسترش روز افزون استفاده از ابر و رایانش ابری، اهمیت و توجه به مساله امنیت بیش از پیش مورد توجه قرار می‌گیرد. رایانش ابری یک شیوه برای استفاده از منابع محاسباتی و یک مدل برای ارائه سرویس با استفاده از اینترنت است به طوریکه توانایی، توان محاسباتی و بهره‌وری را افزایش داده و منجر به صرفه‌جویی در منابع سازمان‌ها می‌شود. همچنین رایانش‌ابری راهی کارآمد برای دسترسی به داده‌ها در هر مکان و هر زمان فراهم می‌کند. در کنار مزایای رایانش ابری و استفاده فرآوان از این تکنولوژی تهدیدات نو ظهور فرآوانی به وجود خواهد آمد. در این مقاله به بررسی معماری و تهدیدات موجود در این حوزه پرداخته می‌شود.

واژگان کلیدی: رایانش ابری، امنیت در ابر، چالش، تهدیدات

۱- مقدمه:

اکثر شرکت ها در حال تغییر روش‌های قدیمی خود و انتقال به سیستم‌های مبتنی بر ابر هستند که راهی کارآمد برای دسترسی به داده ها در هر کجا و در هر زمان فراهم می‌کند. رایانش ابری مدلی برای فراهم کردن دسترسی آسان کاربران از طریق شبکه به مجموعه‌ای از منابع رایانشی قابل «تغییر» و «پیکربندی» همانند شبکه ها، سرورها، فضای ذخیره‌سازی، برنامه کاربردی و سرویس ها است[۱]. اما، امنیت داده ها یکی از موانع اصلی در اتخاذ محاسبات ابری برای سازمان ها است. شرکت‌های فناوری بزرگی در این زمینه فعال هستند که خدمات بسیار زیادی را ارائه می‌کنند. آمازون و گوگل از پایه گذاران در زمینه ی رایانش ابری در دنیا هستند. واضح است که هر ایده یا روش جدید دارای مزایا و معایبی است، از جمله مزایای

---

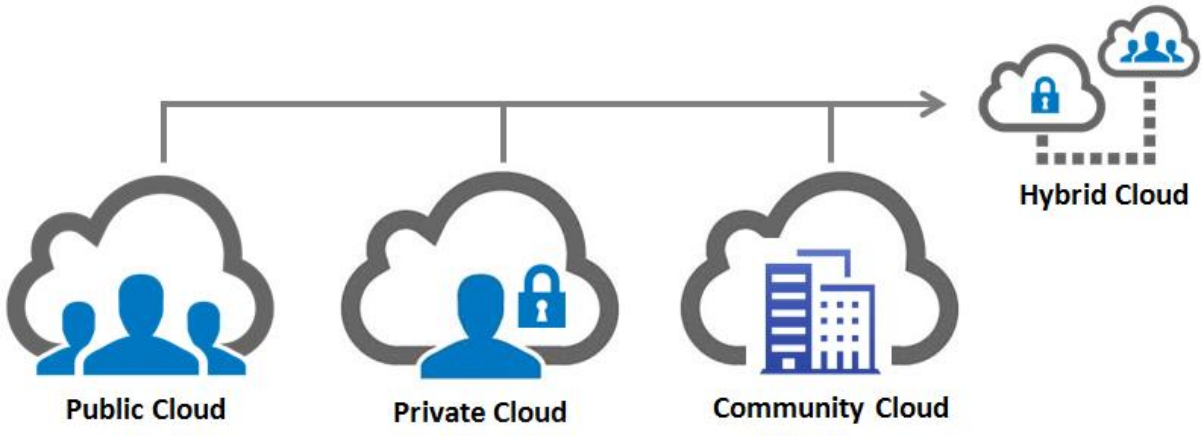
[۱]- عضو هیات علمی و استادیار بخش مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد استهبان، ایران

[۲]- دانشجوی کارشناسی ارشد مهندسی نرم‌افزار، دانشگاه آزاد اسلامی واحد استهبان، ایران

رایانش ابری میتوان به عدم محدودیت مکانی و زمانی، اشتراک گذاری ساده منابع و همچنین کاهش هزینه‌های سرمایه‌ای و عملیاتی اشاره کرد، از معایب رایانش ابری نیز میتوان به دسترسی محدود به سرویس دهنده، هزینه‌های بالا پهنای باند، مشکلات مربوط به تغییر سرویس‌دهنده و احتمال آسیب‌پذیری در شرایط بحران اقتصادی اشاره کرد. همچنین احتمال نشت دیتای کاربران و سازمان‌ها وجود دارد زیرا که داده‌های کاربران و سازمان‌های تجاری با هم در یک پلتفرم قرار می‌گیرند که هرکسی می‌تواند به آن دسترسی داشته باشد[۲]. در رایانش ابری و برون سپاری منابع، اطلاعات یا داده ها در طیف وسیعی از منابع توزیع می‌شود که مشتریان نمی‌توانند آنها را کنترل کنند.

۲- مدل‌های پیاده‌سازی ابر:

به طور کلی ۴ مدل برای پیاده‌سازی ابر در نظر گرفت[۳][۴]. این ۴ مدل به طور خلاصه در شکل زیر نمایش داده شده‌اند:



شکل ۱ – مدل‌های پیاده سازی ابر

در ادامه به تشریح هر کدام از این ابرها می‌پردازیم:

1) ابرهای عمومی (public cloud): همانطور که از نام آن مشخص است، در ابر عمومی همه می‌توانند به سرویس‌ها دسترسی داشته باشند. به عبارت دیگر، مشتریان متعدد از منابع محاسباتی که یک ارائه د هنده خدمات واحد فراهم می‌کند استفاده می‌کنند. از منظر امنیت، به دلیل عمومی بودن این نوع سرویس، امنیت پایینتری نسبت به انواع دیگر خود دارد.
2) ابر خصوصی (private cloud): فقط برای یک سازمان خاص قابل دسترسی است. در اینجا ، منابع محاسباتی فقط در اختیار یک سازمان است و آنها آن را کنترل می‌کنند. همچنین به دلیل خصوصی بودن آن، امنیت بهتر ی نسبت به ابر عمومی ارائه میدهد.

3) ابر اجتماع (community cloud): در اینجا، فروشنده شخص چندین سازمان که هدف‌های مشترکی در جامعه سازمانی خود دارند می تواند میزبان یک زیرساخت جامعه باشد. می توان آن رابه عنوان یک ابر خصوصی نام برد با این تفاوت که توسط مجموعه ای ازسازمان ها قابل دسترسی است.

4) ابر ترکیبی (Hybrid cloud): یک ابر ترکیبی است از ابر عمومی و خصوصی تا بتوان از مزایا ی هر دو مدل استفاده کند. در اینجا، فعالیت‌هایی که حیاتی هستند در ابر خصوصی انجام می‌شوند در حالی که سایر فعالیت‌های غیر حیاتی در ابر عمومی انجام می‌شوند.

۳- تهدیدات امنیتی در ابرها و راهکارهای مقابله با آن[3]:

اعتماد را می‌توان به بدین صورت توصیف کرد که : طرف الف به طرف ب اعتماد می‌کند اگر طرف الف معتقد باشد که طرف ب است مطالق انتظار او رفتار خواهد کرد. بنابراین یک سمت در صورتی قابل اعتماد است که طرفین یا افراد در یک معامله به آن جزء اعتماد داشته. این مهم رابطه بین استفاده کننده‌گان و ارائه کننده‌گان خدمات ابری را بیش از پیش تشریح می‌کند. در ادامه به بررسی تهدیدات امنیتی موجود در ابرها می‌پردازیم، زیرا که اگر کاربری بخواهد از خدمات مختلف رایانش ابری استفاده کند بهتر است از تهدیدات موجود در این زمینه آگاهی داشته باشد. پس از بررسی تهدیدات امنیتی در این بخش، راهکارهایی برای این تهدیدات نیز ارائه می‌شود

۳-۱- امنیت اطلاعات:

رایانش ابری از ترکیب چندین تکنولوژی مختلف تشکیل شده است به همین دلیل امنیت اطلاعات در آن با تهدیدات بسیاری روبه‌رو است. تهدیداتی مانند حمله توسط مشتری، امنیت فیزیکی، وضعیت حقوقی، از دست دادن داده ها و آسیب پذیری تکنولوژی‌های به اشتراک گذاشته شده، ارائه دهنده ابر را تهدید می‌کند. امنیت داده ها و برنامه‌های کاربردی باید توسط ارائه دهنده‌ی ابر تضمین شود.[۵]

راهکار: ارائه دهندگان ابر باید محرمانگی، یکپارچگی و دسترسی پذیری یک مدل امنیتی را برای مشتریان فراهم کنند .

۳-۲- امنیت فیزیکی :

امنیت فیزیکی بدین معنی است که استفاده‌کنندگان از ابر باید در برابر خطرات فیزیکی ایمن باشند .این امنیت نه تنها شامل امنیت در برابر مهاجمان بلکه حفاظت در برابر خطرات و بلایای طبیعی مانند سیل و خطاهای انسانی مثل

[3] threat vector in cloud computing and solutions to deal with them

خاموش کردن تهویه هوا است، به همین دلیل محل قرارگیری مراکز داده اهمیت دارد .مشتریان زمان انتخاب ارائه دهنده‌ی خدمات ابر باید مراقب محل قرارگیری مراکز داده باشند .داده ها در ابتدا باید از لحاظ فیزیکی امن باشند.[۶]

راهکار: ارائه زیرساخت های امن. محل خاصی برای قرارگیری مراکز داده در نظر گرفته شده و تمامی ورود و خروج پرسنل به مرکزداده مورد بررسی قرار گیرد.

۳-۳- محل داده ها

ارائه دهندگان خدمات ابری مراکز داده زیادی در جهان دارند و برنامه‌های کاربردی و داده‌های حساس ممکن است در کشورهای خارجی ذخیره شوند. این امر می‌تواند موجب نگرانی شرکت‌ها و دولت‌ها شود. برای داده‌های غیرقانونی ، قوانین کشوری که داده ها در آن ذخیره می‌شوند اجرا می‌شود .این رویداد می‌تواند یک مشکل باشد، زیرا قوانین کشوری که داده‌ها در آن ذخیره می‌شود برای مجرمین اجرا خواهد شد.

راهکار: مشتریان استفاده کننده از خدمات ابری به دلیل حساس بودن بعضی از اطلاعات مشتریان باید ارائه دهنده‌ی رایانش ابری در کشور خود را ترجیح دهند زیرا که داده‌های حساس باید به دلیل امنیت میهن محافظت شوند. بنابریان داده‌های هر مشتری باید در کشور خود ذخیره شوند.

۳-۴- نشت داده‌ها:

ممکن است داده‌هایی که در ابر ذخیره می‌شوند حاوی اطلاعات مهم یا حساسی باشند که کاربران غیرمجاز این داده‌ها را به سرقت ببرند و علیه کاربران هدف استفاده کنند. این یکی از تهدیدات اصلی در امنیت ابر است زیرا ممکن است افرادی به داده‌هایی که در فضای ابری نگهداری می‌شوند دسترسی پیدا کنند. هر چه داده‌ها بیشتر در معرض خطر قرار گیرند،حجم تهدیدات افزایش می‌یابد.

راهکار: ارائه دهنده‌ی خدمات ابری باید از به روز بودن تمامی سیستم‌های خود در تمامی حال اطمینان حاصل کند. همچنین یک تیم فنی و امنیتی باید نظارت بر این اطلاعات را انجام دهد. علاوه بر آن در سمت مشتری، تمامی پروتکل‌های امنیتی به درستی پیاده سازی شوند.

۳-۵- حمله محروم‌سازی از سرویس (Denial of service attacks):

هر سرور به تعداد مشخصی از درخواست می‌تواند رسیدگی کند. بعد از رسیدن به این آستانه، سرور بیش از حد بارگذاری شده و به جای نمایش جواب درخواست کاربر یک پیغام خطا بازگردانی می‌شود. مهاجمان از این روش برای محروم‌سازی کاربرای در استفاده از خدمات استفاده می‌کنند. این حملات در لایه‌های مختلف علیه ابر یا یکی از مشتریان ابر می‌تواند اتفاق بیافتد که بسته به نوع و پوشش آن می‌تواند بر روی مشتریان دیگر نیز تاثیرگذاری کند. بنابراین ارائه‌کنندگان خدمات ابری باید سیستم‌های حفاظتی در مقابل این نوع حملات را در ابر پیاده‌سازی کنند.[۷]

راهکار: استفاده از سیستم‌های تشخیص نفوذ (IDS) برای مقابله با این نوع حمله‌ها

۳-۶- یکپارچگی داده:

یکپارچگی داده یکی از نگرانی‌های کلیدی در رایانش ابری است. اصطالح یکپارچگی داده اشاره‌ای به این واقعیت است که داده‌ها باید توسط کاربران دیگر غیرقابل تغییر باشد و در صورت دستکاری داده، کاملا قابل تشخیص باشد

راهکار: استفاده از امضای دیجیتال می‌توان تایید صحت داده را انجام داد. بدین گونه تضمین می‌شود که داده‌ها تغییری نکرده‌اند.

۳-۷- کنترل دسترسی (access control):

ارتباط بین مشتریان و ارائه دهندگان ابر با استفاده از رابط برنامه‌نویسی برنامه (API) انجام می شود.

وظیفه این رابط تامین و مدیریت سرویس‌های ارائه شده در ابر است. رابط‌های ضعیف سازمان‌های ارائه دهنده را در معرض خطرات امنیتی مختلفی قرار می‌دهد. خطراتی همانند : دسترسی غیر مجاز، مجوزهای ناشناس و ...[۸]

راهکار: پیاده‌سازی یک سیستم احراز هویت بسیار قوی و کنترل دسترسی مناسب

۳-۸- قابلیت حمل (portablility):

قفل شدگی یک مسئله ی مهم برای مشتریان ابر است .ارائه دهند ی سرویس یک سری قوانین خاص خود را دارد که مشتری بر اساس چنین قوانینی داده‌ها و برنامه‌های کاربردی خود را نزد ارائه دهنده ذخیره می‌کند .از آنجا که همه ی سازمان‌های ارائه دهنده سرویس از یک استاندارد مشترک پیروی نمی‌کنند، بنابراین امکان انتقال مشتریان از یک ارائه دهنده به ارائه دهنده‌ای دیگر امکانپذیر نمی‌باشد. به این مشکل قفل‌شدگی (vendor l ock-i n) می‌گویند.[۹]

راهکار: ارائه‌ی یک استاندارد جامع و رعایت آن توسط ارائه دهندگان

۳-۹- محرمانه بودن داده‌ها:

محرمانه بودن به این واقعیت اشاره دارد که هیچ‌کس به جز کاربر نباید به داده های خود دسترسی داشته باشد.[۳]

راهکار: رمزنگاری یک از روش‌های موثر در حفاظت از محرمانگی داده‌های کاربر است.

۳-۱۰- انتقال امن داده:

ارتباطات بین مشتریان و شبکه‌ی ارائه دهنده‌ی رایانش ابری از طریق اینترنت عبور است. این موضوع محلی برای تهدیدات زیاد است .اگر حمله کننده از شبکه مشترکی استفاده کند می‌تواند با استفاده از روش‌هایی متفاوت همانند حمله مرد میانی به جریان داده گوش کند.

راهکار: ارائه‌دهندگان خدمات ابری باید از انتقال اطلاعات بر یک بستر امن و رمزنگاری شده اطمینان حاصل کنند.

۱۱-۳- در دسترس بودن داده ها (avai l abi l i ty):

در دسترس بودن داده‌ها هدف و غایت نهایی در انتقال سیستم‌ها به ابر است. ایده این است که محصولات، سرویس‌ها و ابزارها را برای مشتریان و کارمندان سازمان در هر لحظه و هر مکان و بر روی هر نوع دستگاهی فراهم نمود. هنگامی‌که داده‌ها در مکان‌های راه دور توسط ابر نگهداری می‌شوند، خطر خرابی سیستم ارائه دهندگان خدمات وجود دارد. اگر ابر قادربه ارائه خدمات نباشد، داده در دسترس نخواهد بود و این یک نقطه‌ی یگانه‌ی شکست می‌باشد. بدین معنی که در صورت خرابی سیستم‌های ارائه دهنده هیچکس قادر به دسترسی به سرویس نخواهد بود.

راهکار: استفاده از ارائه دهندگان سرویس‌های ابری مطمئن، به طوری که علاوه بر سیستم‌هایی برای مواجهه با موارد غیر مترقبه از قبیل قطعی برق، موارد امنیتی همانند دیوار آتش و ... را پیاده سازی کند.

۴- نتیجه‌گیری:

همه‌روزه شاهد این هستیم که سازمان‌ها بیشتر از قبل به سمت سیستم‌های ابر محور حرکت می‌کنند. این ایده که به داده‌های خود در هرکجا که هستید جذابیت زیادی برای مشتریان ارائه‌دهندگان ابری دارد. امنیت داده ها مسئله اصلی در ابر است. این مقاله جنبه‌های مختلفی از مسائل امنیتی مرتبط با محیط‌های ابری را درسطوح مختلف نشان می دهد. رایانش ابری تحولی عظیم در ارائه منابع و سرویس‌ها ایجاد می‌کند. ولی ایجاد این مهم نیازمند تامین امنیت و شناخت و برطرف نمودن چالش‌های احتمالی می‌باشد. در جایگاه مشتری ارائه‌دهندگاه خدمات ابری باید با توجه به فاکتورهای مهم گفته شده در این مقاله سعی در انتخاب بهترین ارائه‌دهنده خدمات ابری نمود زیرا که امنیت سخت‌افزاری و نرم‌افزاری این سیستم از مقوله‌های حائز اهمیت می‌باشد. همچنین جذابیت‌های رایانش ابری نباید منجر به قربانی شدن مقوله امنیت در رایانش ابری گردد. هرچند که امنیت در دنیای دیجیتال هیچ‌گاه امری صد در صد نبوده اما با رعایت و توجه به نکات ذکر شده می‌توان به درجه‌ی بالایی از اطمینان رسید.

منابع:

[1] A. Behl ,“Emerging Security Challenges in Cloud Computing”, word congress on Information and Communication Technologies , PP. 217-222, 2011.

[2] Computing: Study of Security Issues and Research Challenges" in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 4, ISSN: 2278-1323 (2018)

[3] Deepanshi Nanda, Sonia Sharma, "Security [۴] in Cloud Computing using Cryptographic Techniques", International Journal of Computer Science and Technology Vol. 8, Issue 2, (2017)

[4] N.N Mosola, M.T Dlamini, J.M Blackledge, J.H.P Eloff, H.S Venter, "Chaos-based Encryption Keys and Neural Key-store for Cloudhosted Data Confidentiality", in Southern Africa Telecommunication Networks and Applications Conference (SATNAC) (2017)

[5] H. Eken ،"Security threats and solutions in cloud computing،" in Internet Security (WorldCIS) ،2013 World Congress on ،2013 ،pp. 139–143.

[6] Nasim Soltani ،Shahrzad dehghani ،and behzad Soleimani Neisani ، "Security threats in cloud computing and solutions to them".

[7] Dharitri Talukdar, "Study on symmetric [۸] key encryption: An Overview", International Journal of Applied Research. 543-546; (10)1; (2015)

[8] D. Wallom et al. ،"myTrustedCloud: Trusted cloud infrastructure for security-critical computation and data managment،" in Cloud Computing Technology and Science (CloudCom) ،2011 IEEE Third International Conference on ،2011 ،pp. 247–254.

[9] N. Leavitt ،"Is cloud computing really ready for prime time،" Growth ،vol. 27 ،no. 5 ،pp. 15–20 ،. 2009