دومین همایش الکترونیکی پژوهش های نوین در علوم و فناوری EMA
شرکت علم موران آسمان
دانشگاه آزاد اسلامی واحد کرمان

امنیت در محاسبات ابری

علی جباری* ، ساناز دژم

دانشجوی کارشناسی موسسه آموزش عالی مهر اروند*

mohsenjabari909@yahoo.com

استاد موسسه آموزش عالی مهر اروند

sanaz.dejam@yahoo.com

Security in the Cloud

Ali jabari *

Sanaz dejam

چکیده:

در چند سال گذشته، رایانش (محاسبات) ابری رشد زیادی داشته است که از یک مفهوم کسب و کار امیدوارکننده به یکی از بخشهای به سرعت در حال رشد صنعت IT تبدیل شده است. در حال حاضر، شرکتهایی که با ضربه ی رکود اقتصادی مواجه شدند، تشخیص دادند

که با وارد شدن در محیط رایانش ابری می توانند دسترسی سریعتری به برنامه های کاربردی پیدا کنند و یا به طور چشمگیری می توانند منابع زیرساختاری خود را توسعه بدهند.در این مقاله، در مورد مسائل مدل‌های ارائه سرویس ابری و مسائل مختلف امنیتی مواجه در محاسبات ابری مطالعه می‌کنیم. بر اساس این مطالعه دقیق، پیشنهادات بیشتری ارائه می‌کنیم که می‌تواند برای غلبه بر نگرانی‌های امنیتی در ابر دنبال شود. اما همانطور که اطلاعات بیشتر و بیشتری از افراد و شرکتها روی ابرها قرار داده می شوند، نگرانی های در مورد امنیت این محیط ها افزایش می یابد. این مقاله در مورد مسائل امنیتی، الزامات و چالش هایی که ارائه دهندگان سرویس های ابری با آن در مهندسی ابری روبرو می شوند، بحث می کند. استانداردهای امنیتی توصیه شده و مدلهای مدیریتی برای پرداختن به مسائل تکنیکی است.

کلمات کلیدی:نگرانی های امنیتی ،تهدیدات امنیتی،امنیت دادها، محرمانگی، امنیت یکپارچه بین ابرها

۱)مقدمه

۲)نگران محاسبات ابری به عنوان یک رشته جدید در بخش فناوری اطلاعات پدید آمده است که هدف نیاز به افزایش ذخیره سازی را برآورده می‌سازد. هر گاه شرکتی کسب و کار خود گسترش می‌دهد، نیاز به زیرساخت، منابعی دارد که به طور مستقیم خواهان هزینه بالاتر است. برای غلبه بر این مسئله، ابر به عنوان یک امدادگر ارائه دهنده ویژگی‌های جذاب با حداقل هزینه ظهور کرده است. مشتری با ظهور ابر بسیار با انگیزه شده است که به آن اجازه می‌دهد هر کار مربوط به کسب و کار خود را با حداقل هزینه در اینترنت انجام دهد بسترهای ابری مختلفی وجود دارد مانند آمازون، Rackspace و غیره. این بسترها تقاضای کاربر را برآورده می‌سازند. هر شرکت می‌تواند فقط متصل شود و منابع مورد نیاز را تقاضا نماید و در نتیجه کار خود را بر روی اینترنت با حفظ داده‌های خود به صورت دست نخورده با شخص ثالث تکمیل نماید. اما سوالی که اینجا مطرح می‌شود این است که آیا داده‌های ذخیره شده با شخص ثالث امن هستند یا نه با توجه به این پرسش پاسخ داده نشده، ابر تاکنون به طور گسترده‌ای پذیرفته نشده است.

۲)نگرانیهای‌های امنیتی

مشکل اساسی که رخ می‌دهد این است که اگر به نگرانی‌های امنیتی رسیدگی شده باشد و مکانیزمی برای امنیت داده‌ها مستقر شده باشد، هزینه‌ها بسیار زیاد خواهند بود هدف کلی ابر داشتن هزینه‌های کمتر است اما اگر مکانیزم‌های امنیتی مستقر شده باشند، آنها خواستار سرمایه بزرگ برای سرمایه‌گذاری هستند. این یک مسئله باز برای مشتری و همچنین ارائه دهنده سرویس‌های ابری است. به این دلیل، یک علامت سوال در اعتبار محاسبات ابری وجود دارد.

شکل ۲. نگرانی‌های امنیتی محاسبات ابری

۳) تهدیدات امنیتی

با گسترده شدن فن‌آوری، به دلیل پیشرفت آن، مدل‌های ابری، بیشتر در معرض ابتلا به تهدیدات می‌باشند. در محاسبات ابری، نهاد اصلی، داده‌ها هستند و افزایش داده‌های جمع شده منجر به تهدیداتی مانند دزدیده شدن و یا سوء استفاده توسط کاربر غیر مجاز می‌شود و زمانی که تهدیدات افزایش می‌یابد، خطر ابتلا به نارسایی ذخیره‌سازی به وجود می‌آید که در شکل ۶ نشان داده شده است. بنابراین در اینجا باید برخی اصول امنیتی در ابر برای رسیدن به ثبات و پیشگیری از تهدیدات و خطرات استنباط شوند.

شکل ۶. تهدات امنیتی ابر

۳-۱) امنیت اطلاعات

در محاسبات ابری، امنیت اطلاعات، نقش مهمی ایفا می‌کند. همچون بسیاری از برنامه‌های کاربردی و فن‌آوری‌های دیگر، ابر با انواع مختلف تهدیدات امنیتی روبرو است. این تهدیدات ممکن است امنیت فیزیکی، از دست دادن داده‌ها، مسائل حقوقی و غیره باشند. مدل توسعه داده شده برای غلبه بر مسائل مربوط به امنیت اطلاعات، محرمانگی CIA، یکپارچگی، و دسترسی می‌باشدبنابراین ارائه امنیت داده‌ها به مشتری مسئولیت ارائه دهنده ابر است.

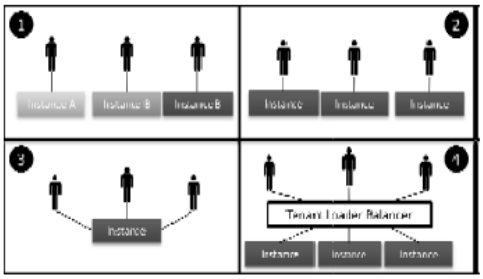
۳-۳) یکپارچگی داده‌ها

برای پیاده‌سازی ابر، زیرساخت مناسب مورد نیاز است، که شامل شماره دستگاه فیزیکی است. بنابراین برای هر مهاجم، بررسی مناسب هر داده‌ی باقی مانده مورد نیاز است تا بتواند آن را سرقت کند نیاز به اعمال محدودیت در شبکه به عنوان یک اصل برای امن نگه داشتن آن وجود دارد. هر سازمان باید بهترین ارائه دهندگان ابر را برای سالم و امن نگه داشتن داده‌های آن انتخاب کند.

۳-۴) چندمستاجری

ابر به عنوان بستر به صورت یک بسته کامل ارائه می‌شود که در آن چندین کاربر خواستار منابع مشابه و به اشتراک گذاری برنامه‌های مشابه برای اجرای ماشین‌های مجازی خود هستند که در شکل ۷ نشان داده شده است. با توجه به اشتراک گذاری منابع، سخت‌افزار یا

نرم‌افزار، احتمال این وجود دارد که اطلاعات به دلایلی به بیرون درز کنند [۱۱]. به اشتراک گذاشتن منابع، احتمال حمله بیشتر را افزایش می‌دهد.



شکل ۷. روش‌های چند مستاجری

۳-۵ وقفه در سرویس‌دهی

حملات مختلفی مانند فیشینگ یا تقلب هنوز هم تمایل به رخ دادن در ابر دارند. مهاجم تنها نیاز به اعتبار یک کاربر مجاز برای دستکاری داده‌های واقعی دارد [۱۶]. این نوع حمله بحرانی است زیرا می‌تواند منجر به حملات DOS یا DDOS شود. از این رو باید اطلاعات مهم حفظ شوند.

۵) محرمانگی

محرمانگی اساساً بدان معنی است که داده‌های فرستاده شده از شخص A به شخص B، باید تنها بین A و B باقی بمانند. هر شخص ثالثی نباید حق دسترسی به داده را داشته باشد. برای رسیدن به این محرمانگی، تکنیک‌های رمزنگاری باید دنبال شوند. تکنیک ممکن است رمزگذاری کلید متقارن یا رمزنگاری کلید نامتقارن باشد. در این روش، درست مثل دیگر تاییدات، کلید باید برای دسترسی واقعی کاربر مجاز به برنامه‌های مختلف ایمن بماند.

۶)امنیت یکپارچه بین ابرها

هر گاه مشتری خواستار منابع از بستر ابرهای مختلف باشد، نیاز به امنیت بیشتر بین ابر و مشتری وجود دارد. برای کار به عنوان یک موجودیت واحد برای یک مشتری خاص، نیاز به امنیت است که به شیوه‌ای یکپارچه کار کند به طوری که عملکرد برای هر کاربر در نگه داشتن امن برنامه‌های کاربردی ساده شود.

۷)نتیجه گیری

مسئله امنیت نقش مهمی در ممانعت از پذیرش محاسبات ابری ایفا کرده است. مسائل امنیتی مختلفی ، در محاسبات ابری امکان پذیر است ازجمله : در دسترس بودن، صداقت، محرمانه بودن، دسترسی به داده ها، تفکیک داده ها، حریم خصوصی، بازیابی، پاسخگویی، مشکلات چند مالکیتی و غیره. راه حل تغییر(از میان برداشتن) مسائل مختلف امنیتی ابری از طریق رمزنگاری، زیرساخت های ویژه کلید عمومی (PKI)، استفاده از ارائه دهندگان ابری متعدد، استانداردسازی API ها، بهبود حمایت ماشین های مجازی و حمایت قانونی می باشد.

منابع:

[۱]Farzad Sabahi, "Cloud Computing Security Threats and Responses", IEEE, 2011.

[۲]Kwang Mong Sim,"Agent Based Cloud Computing" IEEE Transactions on Service Computing, Vol 5, No.4 Oct-Dec, 2012.

[۳]Wentao Liu, " Research on Cloud Computing Security Problem and Strategy", IEEE, 2012.

[۴]Akhil Behl, Kanika Behl," An Analysis of Cloud Computing Security Issues", IEEE, 2012.

[5] M. Casassa-Mont, S. Pearson and P. Bramhall, "Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services", Proc. DEXA

2003, IEEE Computer Society, 2003, pp. 377-382

of Identity and Privacy: Sticky

Policies and Enforceable Tracing Services", Proc. DEXA

2003, IEEE Computer Society, 2003, pp. 377-382

[6] https://www.pcisecuritystandards.org/index.shtml

[7] http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_

Security_Standard, 24 January 2010

[8] J. Salmon, "Clouded in uncertainty – the legal pitfalls of

cloud computing", Computing, 24 Sept 2008,

http://www.computing.co.uk/computing/features/2226701/cl

ouded-uncertainty-4229153

[9] S. Pearson, "Taking Account of Privacy when Designing

Cloud Computing Services", CLOUD'09, May 23, 2009,

Vancouver, Canada

[10] Wikipedia, 20 January 2010,