بررسی حملات امنیتی به ابر و راهکارهای مقابله با آنها

سمیرا طالبی[۱] ، حسن ختن لو [۲]
[۱]دانشجوی کارشناسی ارشد نرم افزار، کامپیوتر، دانشگاه آزاد اسلامی واحد علوم و تحقیقات همدان،
Smr.talebi@gmail.com
[۲]استادیار گروه کامپیوتر، دانشگاه بوعلی سینا، همدان
Khotanlou@basu.ac.ir

چکیده - رایانش ابری اصطلاحی است که برای ارائه خدمات میزبانی تحت اینترنت به کار رفته و به عنوان نسل بعدی معماری فناوری اطلاعات پیش بینی شده که پتانسیل بسیار خوبی را برای بهبود بهره وری و کاهش هزینه ها ارائه می دهد. در مقایسه با راه حل های سنتی که در آن سرویس های فناوری اطلاعات بر پایه کنترل های فیزیکی و منطقی بودند، رایانش ابری نرم افزارهای کاربردی و پایگاه داده ها را به سمت مراکز داده های بزرگ سوق داده است. با این حال ویژگی های منحصر به فرد رایانش ابری همواره با شمار بسیاری از چالش های امنیتی جدید و شناخته نشده همراه بوده است. در این مقاله به بررسی حملات به ابر از جمله: حملات بسته SOAP، تزریق نرم افزارهای مخرب، حملات سیل آسا، سرقت اطلاعات و راه حل های مورد نیاز با توجه به این حملات مورد بررسی قرار خواهد گرفت. هدف از این مقاله شناخت علت های اصلی حملات توسط مهاجمان و ارائه راه حل های نظری برای مشکلات آنها می باشد.

کلید واژه‌ها- حملات امنیتی ابر، جدول تخصیص فایل (FAT)، Hypervisor

۱. مقدمه

با توجه به تکامل در عرصه رایانش روش های بسیاری جهت توزیع منابع و پیشرفت استفاده از داده ها از قبیل خوشه بندی داده ها، رایانش توری و سیستم مدیریت پایگاه داده های توزیع شده معرفی شده اند. امروزه رایانش ابری مکانیزم در حال ظهور برای محاسبات سطح بالا به عنوان یک سیستم ذخیره سازی تلقی می شود که در آن ابرها به کاربران خود بر مبنای میزان استفاده از منابع هزینه دریافت کرده و سرویس های خود را در اختیار آنها قرار می دهند. از این رو می توان سرویس های ابری را در ایجاد انگیزه برای شروع یک کسب و کار با هزینه های مالی پایین تر سهیم دانست.رایانش ابری بسته به نوع توزیع منابع از سه لایه زیرساخت به عنوان سرویس، پلتفرم به عنوان سرویس و نرم افزار کاربردی به عنوان سرویس تشکیل شده است.

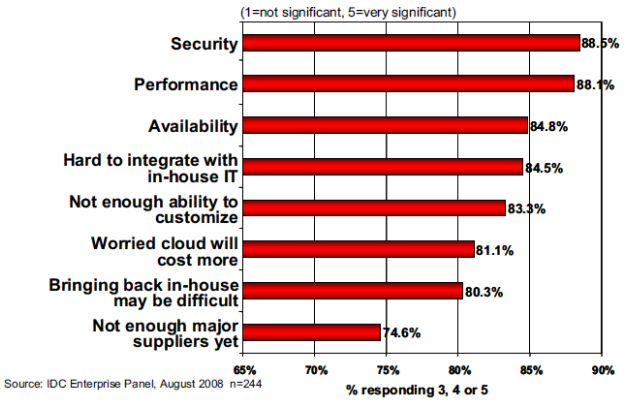
در پایین ترین سطح که لایه زیرساخت به عنوان سرویس (Iaas) نامیده می شود، پردازنده، حافظه و اجزای سخت افزاری توسط فراهم کننده سرویس ابری ارائه می گردد. لایه میانی یا پلتفرم به عنوان سرویس (Paas) میزبان محیط های مختلف برای ارائه خدمات می باشد. در آخر بالاترین لایه نرم افزار کاربردی به عنوان سرویس (SaaS)است که دسترسی به این خدمات از طریق وب سرویس ها و مرورگرهای وب صورت می گیرد. Amazon Ec2، Google App و Salesforce به ترتیب نمونه های لایه های ارائه شده رایانش ابری می باشند.

واضح است که رایاش ابری گام بعدی تکامل سرویس های فناوری اطلاعات بر حسب تقاضا می باشد. با این حال مسئله امنیت در رایانش ابری یکی از مسائل پیچیده به شمار رفته که تمامی سه لایه ابر، مسئولیت هایی که بین کاربران و ارائه دهندگان تقسیم می شود و حتی شخص ثالث را درگیر می کند. مشکلات امنیتی به عنوان یک مانع بزرگ در مقابل استفاده کاربران از سیستم های رایانش ابری قلمداد می شود. هدف از ارائه این مقاله شناخت حملات امنیتی اولیه بر روی ابر می باشد. در ادامه به معرفی کوتاه امنیت ابر و مسائل مطرح در آن پرداخته شده و سه حمله امنیتی و راه کار مقابله با آن مورد بررسی قرار خواهد گرفت.

۲. امنیت ابر

براساس بررسی های انجام شده در سال ۲۰۰۸ میلادی همانگونه که در شکل (۱) نشان داده شده است، امنیت به عنوان مهم ترین

چالش رایانش ابری از میان ۹ چالش موجود شناخته شده است[5]. با این وجود نگرانی هایی در مورد عملکرد و قابلیت دردسترس بودن رایانش ابری جزء دیگر چالش ها پس از امنیت مطرح شده است. جدیدترین بررسی ها در سال ۲۰۱۲ حاکی از کاهش ۳۳,۵ درصدی چالش امنیت و رسیدن این درصد به عدد ۵۵ می باشد.[7]



شکل ۱: چالش های رایانش ابری (بررسی های IDC در سال ۲۰۰۸)

تهدیدهای امنیتی بر روی کاربران ابر به دو دسته داخلی و خارجی تقسیم بندی می شود[1]. تهدیدهای خارجی شامل تهدید مراکز داده بزرگ می باشد که این نگرانی امنیتی در میان کاربران ابر و فراهم آورندگان (که به عنوان شخص ثالث در نظر گرفته شده اند) در حصول اطمینان از نرم افزارهای امن وجود امکان‌پذیر است.

مسئولان امنیت رایانش ابری در سه لایه بیان شده متفاوت هستند به گونه ای که در لایه نرم افزار کاربردی به عنوان سرویس ارائه دهنده سرویس مسئول امنیت فیزیکی است و وظیفه اجرای سیاست های خارجی دیوار آتش را به عهده دارد. در برقراری امنیت لایه پلتفرم به عنوان سرویس کاربر و ارائه دهنده سرویس هر دو سهیم می باشند. در پایین ترین سطح یعنی لایه زیرساخت به عنوان سرویس بیشترین مسئولیت بر عهده کاربر می باشد. علاوه بر مسائل مربوط به امنیت خارجی ابر دارای برخی از مسائل مربوط به امنیت داخلی نیز می باشد که در آن کاربران باید در مقابل حملات از یکدیگر محافظت شوند.

مجازی سازی یکی از مکانیزم های اصلی است که در مقابل تلاش های کاربران برای حمله به یکدیگر و متعاقباً حمله به زیرساخت رایانش ابری، دفاع قدرتمندی را از خود نشان می دهد. البته در پی گفته قبلی باید به این نکته توجه داشت که منابع مجازی ومحیط های مجازی سازی عاری از ایراد نیستند و نرم افزارهای کاربردی مجازی سازی شامل اشکالاتی در زمینه کدها می باشند. مجازی سازی شبکه هایی که نادرست طراحی شده اند اجازه دسترسی یک کاربر به زیرساخت ارائه کننده و منابع دیگر کاربران را می دهند. همچنین ابر باید از ارائه دهندگان که پایین ترین لایه زیرساخت به عنوان سرویس را در دست دارند هم محافظت شود زیرا این مهم می تواند در از دست دادن داده های ناخواسته سهیم باشد.

شکست در امنیت رایانش ابری به دلایل زیر رخ می دهد:

الف)به علت سخت افزاری که در لایه زیرساخت به عنوان سرویس ابر رخ می دهد.

ب)به علت نفوذ کدهای مخرب در نرم افزار که در لایه نرم افزار کاربردی به عنوان سرویس رخ می دهد.

ج)به علت نفوذ کدهای مخرب در حال اجرا که توسط برنامه کاربردی کاربر یا تزریق اطلاعات ساختگی به برنامه توسط شخص ثالث صورت می گیرد. این رخداد در لایه پلتفرم به عنوان سرویس می تواند منجر به ایجاد نزاع و اختلاف بین ارائه دهنده و مشتری شود.

با توجه به دلایل ذکر شده شکست در امنیت ابر می تواند نزاع میان ارائه دهنده سرویس و کاربران آن را به همراه داشته باشد. از طرفی از دیدگاه کاربر از دست رفتن اطلاعات یا قطعی در ارائه سرویس ها می تواند هزینه های مالی هنگفتی را در پی داشته باشد. و از طرفی از دیدگاه ارائه دهنده سرویس ارائه خدمات با کیفیت مختل شده و بدین ترتیب توافقات سطح سرویس (SLA) محقق نمی شود.

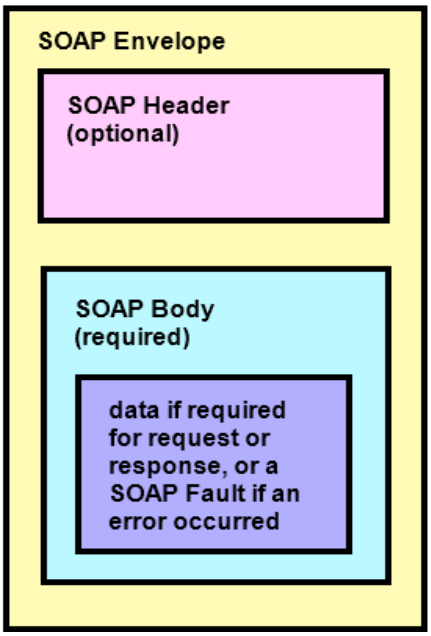
۲,۱. مسائل مرتبط با امنیت ابر

در ادامه مهم ترین مسائل مربوط به امنیت رایانش ابری از جمله پیام SOAP و حملات ابر که توسط دشمنان مزاحم آن صورت می گیرد مطرح می شود.

وب سرویس تکنولوژی است که اخیراً در معماری سرویس گرا (SOA) مورد استفاده قرار گرفته است. یک وب سرویس به معنای ساده نوعی مولفه تحت وب است.این مولفه به برنامه های کاربردی که از آن استفاده می کنند این امکان را می دهد که بتوانند از متدهای این وب سرویس استفاده کنند. در سیستم ابر تبادل سرویس بین مرورگر وب کاربر و وب سرویس صورت می گیرد به طوری که درخواست های کاربر از طریق مرورگر خود به وب سرویس منتقل می شود. با این وجود سیستم امنیتی وب سرویس باید به اندازه کافی برای بهینه سازی امنیتی در برابر حملات دشمن مقاوم باشد. حملات امنیتی می تواند پیام های SOAP را مورد حمله قرار دهد. SOAP (Simple Object Access Protocol) پیام های متنی مبتنی بر Xml است که برای تبادل اطلاعات کد گذاری شده بین وب سرویس و کاربر با استفاده از پروتکل های مختلف از جمله HTTP، SMTP و MIME به کار می رود. SOAP اجازه می دهد که یک برنامه در حال اجرا در یک سیستم با یک برنامه در حال اجرا در یک سیستم دیگر بدون در نظر گرفتن مدل برنامه نویسی آن ها تماس برقرار کند.

پیام SOAP به دو واحد سرپیام و بدنه همانند شکل (۲) تقسیم بندی می شود. که در آن سر پیام بسته SOAP از دو قسمت

رمز امنیت دودویی و برچسب زمانی تشکیل شده است. که در آن قسمت رمز امنیت دودویی شامل مجوز برقراری ارتباط با وب سرویس و برچسب زمانی حاوی تاریخ ساخت و انقضای پیام SOAP می باشد.



شکل ۲: بسته SOAP[۳]

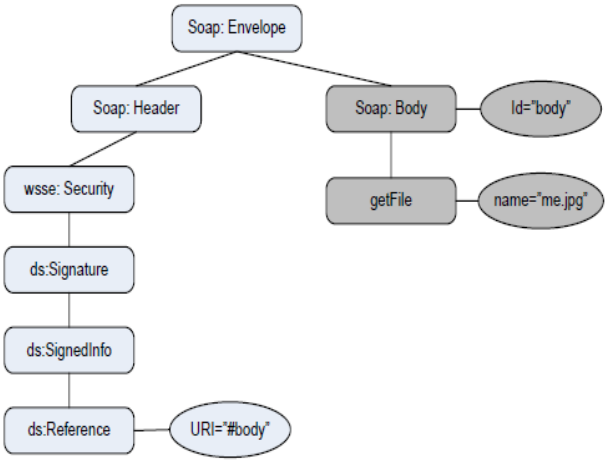
در شروع ارتباط با وب سرویس کاربر می بایست جهت ارسال درخواست و دریافت پاسخ خود از وب سرویس مجوزی را دریافت نماید. پس از دریافت مجوز کاربر قادر به ادامه ارتباط با وب سرویس و دریافت پیام SOAP می باشد.

همانگونه که قبلاً ذکر شد بسته SOAP می تواند مورد حمله Wrapping قرار بگیرد. حمله مذکور با حفظ شناسه بسته و تغییر در قسمت بدنه آن می تواند محتویات بسته در حال انتقال را دستخوش تغییر گرداند و با ایجاد یک بدنه ساختگی برای پیام به فعالیت بپردازد.

در ادامه حملات امنیتی ممکن به ابر از جمله حمله به بسته SOAP، تزریق کدهای مخرب، حملات سیل آسا، سرقت اطلاعات و پس از آن راه حل مقابله با هر کدام مورد بررسی قرار خواهد گرفت. لازم به ذکر است از میان چهار حمله فوق تنها دو حمله سیل آسا و سرقت اطلاعات در محیط های رایانش خوشه ای و توری نیز رخ می دهند.

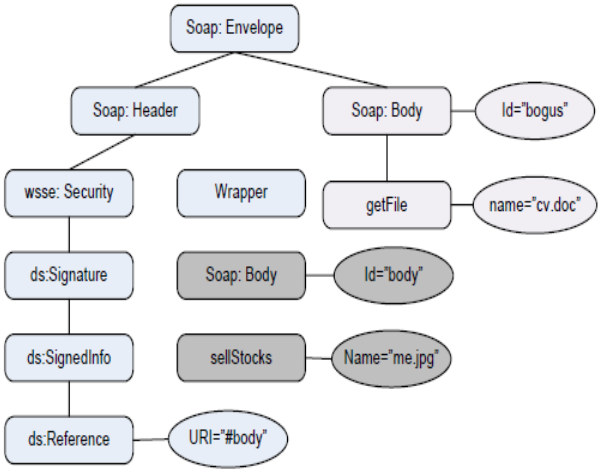
الف: حمله به بسته SOAP (*Wrraping Attack*)

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. همانطور که گفته شد پیام SOAP دارای دو قسمت سر پیام حاوی امضا و بدنه جهت نگهداری اطلاعات می باشد. شکل (۳) یک پیام SOAP ایده آل قبل از حمله بسته را نشان می دهد که در آن کاربر فایل me.jpg را از سرور درخواست نموده است.[4]



شکل (۳) : پیام SOAP قبل از حمله

مهاجم در پی حمله خود به پیام SOAP ، با نگهداری سر پیام یک بسته قسمت بدنه آن را تغییر داده و بدنه ساختگی خود را در بسته جایگذاری می کند. در شکل (۴) پیام SOAP پس از حمله نشان داده شده است همانگونه که مشاهده می شود مهاجم با تغییر قسمت بدنه پیام و ارسال درخواست به سمت سرور اقدام به حمله نموده است. چنانچه تغییر در بدنه به صورتی باشدکه منجر به تغییر تمام ساختار بدنه شود وب سرور این حمله را تشخیص داده و از قبول بسته خودداری خواهد کرد.



شکل (۴) : پیام SOAP بعد از حمله

ب: حمله از طریق کدهای مخرب (*Malware-Injection*)

نوع دیگری از حمله که حقه بازی ابرداده (Meta-Data Spoofing) نیز نامیده می شود در ادامه بررسی می شود. در

سیستم های ابری درخواست های کاربر بر اساس تشخیص هویت شناسایی و اجرا می شوند. چنانچه محتوای درخواست های سمت سرور زیاد باشد سرور باید درخواست ها را زمان بندی کند. در برقراری ارتباط اولیه یک سری ابرداده بین کاربر و سرور جابجا می شود در این مرحله است که مهاجم از فرصت استفاده کرده و با رسوخ در سرویس در حال اجرا، سرویس ساختگی خود را به صورت یک سرویس در حال اجرای معتبر درآورده و با ایجاد کدها یا سرویس های مخرب به استراق سمع اقدام می نماید.

چنانچه مهاجم موفق به حمله به کاربری که درخواست خود را به سمت سرور فرستاده شود، باید برای زمان بندی درخواستی که خود منجر به تولید آن نشده است منتظر بماند.

ج: حمله سیل آسا (*Flooding Attack*)

یکی از اقداماتی که مهاجم برای دسترسی به سرور انجام می دهد محرومیت کاربران مجاز از سرویس های درخواستی می باشد. حملات سیل آسا نه تنها در محیط ابری بلکه در رایانش های خوشه ای و توری نیز رخ می دهد. در سیستم های ابری سرورهایی که از طریق ارتباطات داخلی با هم در ارتباطند به انجام کار خاصی می پردازند و هنگامی که درخواست های سمت یک سرور زیاد می شود و سرور پربار می شود قسمتی از کارهای خود را به سرور خاص شبیه به خود از لحاظ کاری می دهد و اینگونه لود جانبی صورت می گیرد. هنگامی که مهاجم با مجوز و داده های ساختگی درخواست های خود را به سمت سرور گسیل می کند، مهاجم درخواست ساختگی خود را به سمت سرور می فرستد در سمت سرور درخواست های ارسالی کنترل شده، مجوز آن ها بررسی می شود و مشخص می گردد که درخواست فعلی نامعتبر بوده است. در طی این فرآیند کنترل کردن درخواست های فوق به مصرف پردازشگر و حافظه زیادی نیاز دارد که و این امر باعث بالا رفتن بار روی سرور شده و سرور مجبور به بارگذاری جانبی به سرور دیگر می شود. در نتیجه مهاجم با ایجاد اختلال در فرآیندهای معمول و عادی سرور موفق به انجام حمله خود شده است.

د : سرقت اطلاعات (Data Stealing)

یکی از راه های سنتی و معمول حمله به ابر سرقت اطلاعات از طریق به دست آوردن حساب کاربری و رمز عبور می باشد. در طی این نوع حمله که در محیط های خوشه ای، توری و ابری رخ می دهد، مهاجم به سرقت اطلاعات محرمانه یا تخریب داده های کاربر اقدام می کند که این امر موجب برهم زدن یکپارچگی داده ها و امنیت موجود در ابر می شود.

۲,۲. رویکردهای امنیتی ممکن

در ادامه راه حل های ممکن جهت حملات فوق مورد بررسی قرار خواهد گرفت.

الف: راه حل حمله بسته *SOAP* (*WrappingAttack*)

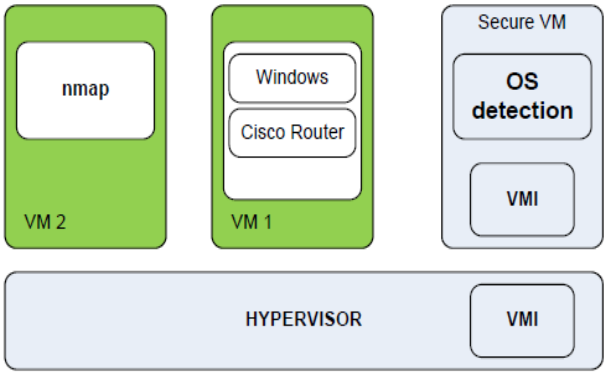
همانطور که در حمله Wrap بیان شد مهاجم از طریق دستکاری بدنه بسته SOAP یا استفاده از IP معتبر به ابر حمله می کند. حال چنانچه سر پیام بسته فوق علامت گذاری شود دیگر مهاجم نمی تواند با ارائه IP معتبر به سرور عمل کند. این کار با استفاده از تعریف کلید RSA از طرف فراهم آورنده برای کاربر صورت می گیرد. معمول ترین و مشهورترین الگوریتم نامتقارن به عنوان RSA شناخته می‌شود.

RSA مخفف حروف اول نام پدیدآورندگان آن است. می‌توان از یک سیستم نامتقارن برای نشان دادن اینکه فرستنده پیام همان شخصی است که ادعا می‌کند، استفاده کرد. این عمل اصطلاحاً امضای دیجیتال نام دارد. امضا، متن اصلی را با استفاده از کلید اختصاصی رمز می‌کند، رمزگشایی عملیات مشابه‌ای روی متن رمزشده اما با استفاده از کلید عمومی است. برای تایید امضا بررسی می‌کنیم که آیا این نتیجه با اطلاعات اولیه یکسان است یا خیر. به بیان ساده‌تر چنانچه متنی از شخصی برای دیگران منتشر شود، این متن شامل متن اصلی و همان متن اما رمز شده توسط کلید اختصاصی همان شخص است. حال اگر متن رمز شده توسط کلید عمومی آن شخص که شما از آن مطلع هستید رمزگشایی شود، مطابقت متن حاصل و متن اصلی نشان دهنده صحت فرد فرستنده آن است، به این ترتیب امضای فرد تصدیق می‌شود. افرادی که از کلید اختصاصی این فرد اطلاع ندارند قادر به ایجاد متن رمز شده نیستند، به طوری که با رمزگشایی توسط کلید عمومی این فرد به متن اولیه تبدیل شود. بدین ترتیب فرد فرستنده نمی‌تواند منکر فرستادن متن شود، زیرا کسی به جز او نمی‌توانسته آن متن را به شکل مطلوب امضا کند. در این صورت هر کاربر RSA منحصر به فرد خود را برای ارتباط با سرور در اختیار دارد.

ب: راه حل حمله از طریق کدهای مخرب (*Malware-Injection*)

هنگامی که کاربر حسابی را از طریق فراهم کنندگان سرویس ابر به خود اختصاص می دهد فراهم آورنده نهایی یک تصویر از ماشین مجازی کاربر در منبع تصویری سیستم ابر برای کاربر ساخته می شود. پس از آن به هنگام ارسال درخواست سمت سرور از طریق کاربر برنامه های کاربردی کاربر به صورت چندین درخواست در حال اجرا و کاملا یکپارچه بر روی ماشین مجازی قرار می گیرند. حال به دلیل دشوار بودن حمله به لایه زیرساخت به عنوان سرویس برای مهاجم، یکپارچگی فوق باید در سطح ماشین مجازی پیاده سازی شود. راه حل ارائه شده در این مقاله جهت مبارزه با ایجاد کدهای مخرب استفاده از

جدول تخصیص فایل (FAT) است، که توسط همه سیستم عامل های موجود برروی ماشین مجازی پشتیبانی می باشد. با کمک جدول تخصیص فایل می توان به برنامه در حال اجرای کاربر پی برد. با این کار تاریخچه برنامه در حال اجرای کاربر و مراحل قبل و بعد آن را می توان مشخص نمود. جهت تحقق این هدف به یک Hypervisor که روی سیستم نهایی پیاده سازی می شود نیاز خواهیم داشت. همانطور که در شکل (۵) نشان داده شده است Hypervisor قرار گرفته شده برروی سیستم انتهایی مسئول زمان بندی همه درخواست های در حال اجرای کاربر می باشد. باید به این نکته توجه داشت که قبل از زمان بندی درخواست ها کنترل یکپارچگی آنها از طریق جدول تخصیص فایل صورت می پذیرد. بنابراین با توجه به مطالب بیان شده می توان نتیجه گرفت که جدول تخصیص فایل جهت کنترل یکپارچگی یک برنامه در حال اجرای کاربر به کار برده می شود.



شکل (۵) : برنامه کاربردی کاربر

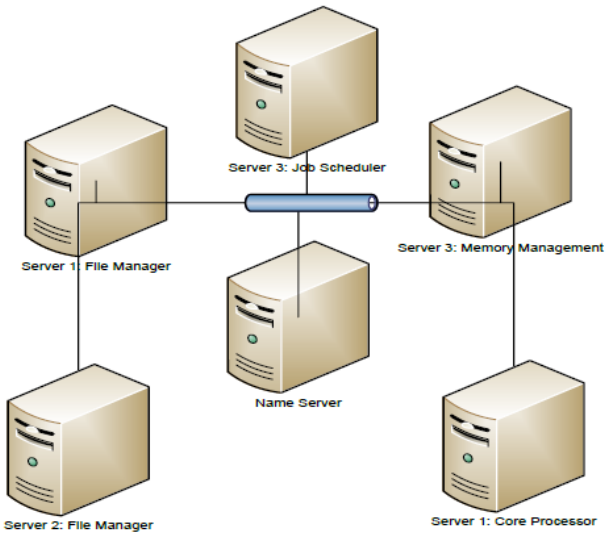
ج : راه حل حملات سیل آسا (*Flooding Attack*)

راه حل پیشنهادی برای مقابله با حملات سیل آسا ایجاد ناوگانی از سرورها همانند شکل(۶) می باشد که در آن هر ناوگان جهت انجام کار خاصی در نظر گرفته شده است که با یکدیگر و سرور نام در ارتباط هستند. به طور مثال تعدادی از سرورها عمل مدیریت حافظه و تعدادی جهت مدیریت فایل در نظر گرفته می شوند.

حال در این طراحی جدید چنانچه بار روی یک سرور بالا رود سرور جدید وارد عمل شده، بارگذاری جدید به آن منتقل شده و بدین ترتیب جهت جدول موجود در سرور نام به روز رسانی می شود.

د : راه حل سرقت اطلاعات (*Data Stealing*)

در پایان هر استفاده کاربر از ابر، ارائه دهنده ایمیلی حاوی میزان استفاده و مانده حساب را به کاربر ارسال می کند. بدین ترتیب کاربر اطلاعات کاملی را از سرویس گیری خود دریافت کرده و چنانچه سرقت اطلاعات از طریق مهاجمی صورت گیرد وی با بررسی حساب خود می تواند به آن پی ببرد.



شکل (۶) : پیام بین سرورها

۳. معرفی یک ساختار امنیتی

نحوه پرداخت در سیستم ابری براساس میزان استفاده کاربر می باشد. هنگامی که کاربر سرویس مورد تقاضای خود را درخواست می کند در طی اجرا مواردی از قبیل مدت زمان سرویس گیری، میزان داده منتقل شده در شبکه و چرخه های کاری پردازشگر در ثانیه همگی ثبت خواهد شد و پس از اتمام اعتبار، کاربر می بایست به شارژ مجدد اقدام نماید. در این صورت هنگامی که مهاجم به حمله خود از طریق کدها یا سرویس مخرب اقدام نماید به صورت فزاینده ای از اعتبار کاربر کم کرده و در نتیجه این امر، در خوش نامی و سرویس دهی فراهم آورنده اختلال ایجاد می کند.

در این مقاله حملات که می تواند از طریق مهاجم رخ دهد به همراه راه حل های آنها مطرح شد. ایجاد یک ساختار امنیتی قوی می تواند در بالابردن ضریب امنیت و همچنین کاهش خطر حملات احتمالی موثر واقع شود. چارچوب ذکر شده محیطی امن را جهت دسترسی کاربران مجاز به سرویس های مورد نیاز از طریق شبکه خصوصی مجازی (VPN) فراهم می آورد. در این چارچوب پس از شناسایی کاربران مجاز داده ها رمزگذاری شده و در سمت فراهم آورنده رمزگشایی و سپس ذخیره خواهد شد. مراحل کار در چارچوب فوق عبارتند از:

۱. سیاست های امنیتی

- امکان تنظیم تغییر رمز عبور کاربران به صورت اجباری در زمان های مشخص
- تامین کننده رمز عبور سرور

۲. پشتیبان گیری، بازیابی، ثبت وقایع

- پشتیبان گیری از داده ها باید در فواصل زمانی منظم صورت گیرد.
- تدابیر لازم جهت بازگردانی داده ها توسط فراهم آورندگان باید صورت بگیرد.
- به روز رسانی ها به صورت منظم باید صورت بگیرد.

۳. تست نفوذ

- برای اطمینان از سیستم ارائه دهنده باید در فواصل منظم زمانی تست سیستم صورت پذیرد.

۴. دیوار آتش و امنیت شبکه

- فایروال نصب شده و تنظیمات آن انجام شود.
- نرم افزار ضد ویروس نصب و به روز رسانی شود.

۵. زیرساخت های فیزیکی امن

- محل فیزیکی سرور امری حیاتی است، ارائه دهندگان ابر باید از دستگاه های ذخیره سازی در مکان های امن با حفاظت فیزیکی مناسب نگه داری کنند.

البته باید توجه داشت که چارچوب فوق شاید خیلی ساده به نظر برسد اما می تواند به عنوان کمکی در گسترش امنیت در ابر باشد.

۴. نتیجه‌گیری

رایانش ابری انقلابی در نحوه استفاده، مدیریت سرویس ها و منابع می باشد. اما این تحول با مشکلات جدید همراه شده است. در این مقاله برخی از مشکلات مهم و حملات امنیتی و راه حل های مبارزه با آنها از جمله جدول تخصیص فایل و یک Hypervisor شرح داده شد .

مفهوم و چارچوبی که در این مقاله مورد بحث قرار گرفت به ایجاد یک ساختار امنیتی قوی در شاخه رایانش ابری کمک خواهد کرد. این امنیت ساختار بندی شده با دسترسی از طریق VPN تا حد بالایی قادر به بهبود رضایت مشتریان و جذب سرمایه گذاران بیشتری در این مفهوم از رایانش خواهد بود.

۵. مراجع

[1] Michael, M. J., A view Of Cloud Computing, Communications Of The ACM,April 2010.
[2] Kazi,.Aunnurhain,*Susun,.Vrbsky,SecurityInCloudComputing* ,University of Albama,2009.
[3] SOAP, http://www.w3.org/TR/soap/.
[4] Meiko,Jenson,Jorg Schwenk.On Technical.Security Issued in Cloud Computing.IEEE International Confrence On Cloud Computing,2009.
[5] IEEE Computer Society ,2010 Sixth International Conference on Semantics, Knowledge and Grids, Security and Privacy in Cloud Computing: A Survey ,2010.
[6] Kazi,.Aunnurhain,Susun,.Vrbsky,Security Attacks and Solutions in Clouds,University of Albama,2009.
Cloud Computing Survey,http://northbridge.com/2012-cloud-computing-survey