نخستین کنگره بین المللی
چالش های الکترونیکی ۲۰۱۶-تهران
1st Tehran eChallenges
International Congress 2016
17-18 October 2016 / ۲۶و۲۷ مهرماه ۱۳۹۵

مروری بر امنیت محیط های رایانش ابری و انواع سیستم های تشخیص نفوذ ابری

نگین رادمنش
دانشجوی ارشد دانشگاه پیام نور قشم
negin.radmanesh@gmail.com

محمد ابراهیم شیری
استادیار دانشگاه صنعتی امیرکبیر
shiri@aut.ac.ir

سید سعید آیت
دانشیار دانشگاه پیام نور نجف آباد
dr.ayat@pnu.ac.ir

چکیده
با فراگیر شدن رایانش ابری[۱] و محبوبیت انواع نرم افزار بعنوان سرویس و اهمیت آن در انتقال اطلاعات روزانه، امنیت رایانش ابری مهم و مهم تر شده است. افزایش امنیت در هر یک از مدل های رایانش ابری از اهمیت بسزایی برخوردار است. بنابراین تشخیص نفوذ شبکه به عنوان یکی از چالش انگیزترین نیازهای امنیتی شبکه در سالهای اخیر درآمده است. سیستم های تشخیص نفوذ با تشخیص و یا پیشگیری از حملات در شبکه های کامپیوتری به افزایش امنیت کمک می کنند و نقش مؤثری در تامین امنیت دارند. پس لازم است سیستم های تشخیص نفوذ (IDS[۲]) توسعه داده شوند تا بتوانند حجم زیاد داده را در زمان قابل قبول برای انجام عکس العمل مناسب در مقابل حملات آنالیز کنند. با توجه به افزایش ویروسها و حملات، حجم هشدارهای سیستم های تشخیص نفوذ نیز بسیار زیاد شده است. از آنجا که محیط های رایانش ابری به دلیل ویژگی توزیع شدگی، به راحتی مورد حمله نفوذگرها قرار می گیرند، استفاده از سیستم تشخیص نفوذ در ابر یکی از مهمترین راهکارهای امنیتی برای کاهش این تهدیدها می باشد. بنابراین، بکارگیری تکنولوژیهای پیشرفته برای سهولت تشخیص ترافیک ناهنجار ضروری است. در این مقاله سعی شده است علاوه بر آشنایی با رایانش ابری، انواع حملات و راهکاری های مقابله با آن ها و برخی سیستم های تشخیص نفوذ بررسی شده و در پایان سیستم تشخیص نفوذ توزیع شده ای پیشنهاد شده است.

واژگان کلیدی: رایانش ابری، امنیت ابر، حملات در رایانش ابری، سیستم تشخیص نفوذ

---
۱ Cloud Computing
۲ Intrusion Detection System

۱- مقدمه

رایانش ابری نوعی سیستم موازی و توزیعی از رایانه های متصل بهم و مجازی است که به صورت پویا و بر اساس توافقات سطح سرویس و به عنوان یک یا چند منبع محاسباتی مجتمع ارائه می شود. رایانش ابری به معنای انتقال پویای منابع و قابلیتهای فناوری اطلاعات به عنوان سرویس روی اینترنت است. صنعت رایانش ابری، اکوسیستم بزرگی از مدل ها، فروشندگان و بازارهای مختلف است(Mell and Grance, ۲۰۱۱).

خدمات رایانشی پنج ویژگی کلیدی و چهار مدل استقرار و سه مدل خدمات دارد. پنج مشخصه اصلی شامل: تجمیع منابع، دسترسی وسیع از طریق شبکه، انعطاف پذیری سریع، سرویس خودکار مبتنی بر تقاضا و سرویس اندازه گیری شده می باشند. سه مدل خدمات عبارتند از : زیرساخت به عنوان سرویس (IaaS)، پلتفرم به عنوان سرویس (PaaS) و نرم افزار به عنوان سرویس (SaaS). انواع مدل عرضه شامل ابر خصوصی، ابر انجمنی، ابر عمومی و ابر هیبرید است(Mell and Grance, ۲۰۱۱).

در نمایش دیاگرام شبکه های کامپیوتری، بطور معمول از شکل یک ابر به عنوان روشی تلخیصی برای پنهان کردن زیر ساخت های پیچیده ای که درون شبکه وجود دارد، استفاده می گردد. در رایانش ابری نیز کلمه "ابر" از همین استعاره گرفته شده است و برای پنهان کردن اینترنت و زیرساخت ها در رایانش ابری نیز بکار می رود(Holtz et al, ۲۰۱۱).

آنچه که این مفهوم را مقیاس پذیر و کارآمد می سازد، معماری سرویس گرا است. به این ترتیب که منابع به جای اینکه بر روی سیستم های کاربران نصب شوند بر روی سرورهای ارائه دهندگان نگهداری می شوند. این تکنولوژی نوین برای آسان تر شدن استفاده از منابع اطلاعاتی سخت افزاری، برنامه های کاربردی شبکه ها و زیر ساخت ها اختراع شده است.

۲- محدوده تحقیق

موضوع این تحقیق امنیت در شبکه های رایانش ابری است. به همین منظور ابتدا به بررسی ساختار ابر پرداخته، سپس امنیت ابر و چالش های امنیتی آن مطرح شده است. حملات و راهکارهایی که تاکنون ارایه شده اند را شرح دادیم. سپس بمنظور حفظ امنیت و بالا بردن آن در این شبکه ها انواع سیستم های تشخیص نفوذ ابری بررسی و سیستم تشخیص نفوذ جدیدی پیشنهاد کرده ایم.

۳- آشنایی با مفهوم رایانش ابری

رایانش ابری مدل محاسباتی بر پایه شبکه های بزرگ کامپیوتری مانند اینترنت است، که الگویی تازه برای عرضه، مصرف و تحویل سرویس فناوری اطلاعات (شامل سخت افزار، نرم افزار، اطلاعات و سایر منابع اشتراکی محاسباتی) با بکارگیری اینترنت ارایه می کند. رایانش ابری راهکارهایی برای ارایه خدمات فناوری اطلاعات به شیوه های مشابه با صنایع همگانی (آب، برق ، تلفن و ...) پیشنهاد می کند. این بدین معنی است که دسترسی به منابع فناوری اطلاعات در زمان تقاضا و بر اساس میزان تقاضای کاربر به گونه ای انعطاف پذیر[۳] و مقیاس پذیر[۴] است که از راه اینترنت به کاربر تحویل داده می شود (Mell and Grance, ۲۰۱۱).

دلیل تشبیه اینترنت به ابر در این است که، اینترنت همچون ابری جزییات فنی اش را از دید کاربران پنهان می سازد و لایه ای از انتزاع را بین این جزییات فنی و کاربران به وجود می آورد. به عنوان مثال آنچه یک ارایه دهنده سرویس نرم افزاری رایانش ابری ارایه می کند، برنامه های کاربردی تجاری برخط[۵] است که از طریق مرورگر وب یا نرم افزارهای دیگر به کاربران ارایه می

---

[۳] Flexible
[۴] Scalable
[۵] On-Line

شود. نرم افزارهای کاربردی و اطلاعات روی سرورها ذخیره می گردند و بر اساس تقاضا[۶] در اختیار کاربران قرار می گیرند. جزییات از دید کاربر مخفی می ماند و کاربران نیازی به تخصص یا کنترل در مورد فناوری زیر ساخت ابری که از آن استفاده می کنند ندارد[۶].

در سالهای اخیر معرفی مفهوم رایانش ابری در کنار نیاز روز افزون برای پردازش داده ها تاثیر عمیق بر ارتباطات و نحوه محاسبات گذارده است. رایانش ابری زمینه را برای دسترسی مشترک به مجموعه ای از منابع، از طریق شبکه فراهم می کند که این منابع از انواع نرم افزارها تا کل ساختار یک ماشین مجازی را شامل می شود. به این ترتیب کاربران قادر خواهند بود بنا به تقاضا، به منابع دسترسی پیدا کرده و از آنها استفاده کنند و هزینه این استفاده را بر اساس مدل پرداخت بر اساس استفاده[۷] بپردازند.

این وضعیت می تواند موجب صرفه جویی بزرگی در هزینه های مصرف از جمله نگهداری و ارتقاء منابع، هزینه های اولیه در تهیه منابع، کاهش هزینه در اثر استفاده مشترک، و غیره گردد. با رشد پدیده رایانش ابری پیش بینی می شود این روند تمام صنعت IT، از سرویس های نرم افزاری که در قالب رایانش ابری به شکل سرویس های وب یا غیره ارایه می گردد، تا ماشین های خصوصی کاربران که می تواند به صورت کامل به عنوان یک ماشین مجازی، در صورت لزوم در هر نقطه و هر زمان توسط کاربران قابل دسترسی باشد، را در برگیرد(Tanenbaum and Wetherall, ۲۰۰۳).

رایانش ابری تکنولوژی است که از سوی شرکت های مختلفی که مهمترین آنها مایکروسافت، گوگل و آمازون می باشند، به جهان عرضه شده است. به بیان دیگر، این تکنولوژی همان بکارگیری منابع نرم افزاری و سخت افزاری موجود بر روی سرور توسط کاربر می باشد که کاربر را از به روز رسانی مداوم سخت افزار و نرم افزار سیستم خود بی نیاز می سازد. با استفاده از این فناوری تنها نیاز دارید از یک بستر با سرعت مناسب و امنیت بالا جهت دسترسی به سرور استفاده نمایید. در حال حاضر دنیای فناوری اطلاعات قسمت اعظمی از زندگی بشر را در بر می گیرد که در کنار آن این فناوری نیازهایی مانند امنیت اطلاعات، دسترسی سریع و آسان در هر لحظه، پردازش با قدرت بالا و مهمتر از آن استفاده از سرویس های با هزینه پایین می باشد(Sathya and Vasanthraj, ۲۰۱۳).

پیدایش محیط رایانش ابری، ویژگی ها و مزایای زیادی در اختیار کاربران قرار داده است. هرچند که بسیاری از کارشناسان معتقدند که رایانش ابری راه را بر آزادی های فردی خواهد بست و موجب نقض حریم های خصوصی افراد خواهد شد، زیرا دیگر اطلاعات مهم کاربران از دسترس و کنترل فیزیکی آنها خارج خواهد شد. از سوی دیگر با رشد سرویس دهنده های ابری عظیم سرویس دهنده های کوچک از بین خواهند رفت و پس از مدتی دنیایی خواهیم داشت به صورت شرکت های عظیم خدمات اطلاعاتی که می توانند بازار ارتباطات و اطلاعات را به صورت تک قطبی و انحصاری در اختیار خود بگیرند و آزادی عمل کاربران را بر اساس خواسته های خود نادیده بگیرند.

۳-۱ ساختار رایانش ابری

وقتی از پردازش به صورت یک ابر سخن می گوییم، بهتر است که ابررایانه ای را متشکل از دو قسمت ابتدایی و انتهایی فرض کنیم که توسط یک شبکه به یکدیگر متصل می گردند و بطور معمول این شبکه همان اینترنت می باشد. بخش ابتدایی قسمتی است که قابل مشاهده کاربران بوده و دربرگیرنده اطلاعات و شکل ظاهری نرم افزارها می باشد. بخش انتهایی نیز همان "ابررایانه ای" است که عملیات پردازش را دربرمی گیرد. نرم افزار مرتبط کننده دو بخش نیز جزئی از بخش ابتدایی می باشد. بخش انتهایی یا ابر، از چندین رایانه، مرورگر و واحدهای ذخیره کننده اطلاعات تشکیل شده است و از نظر نرم افزاری دارای

[۶] On-Demand
[۷] Pay-Per-Use

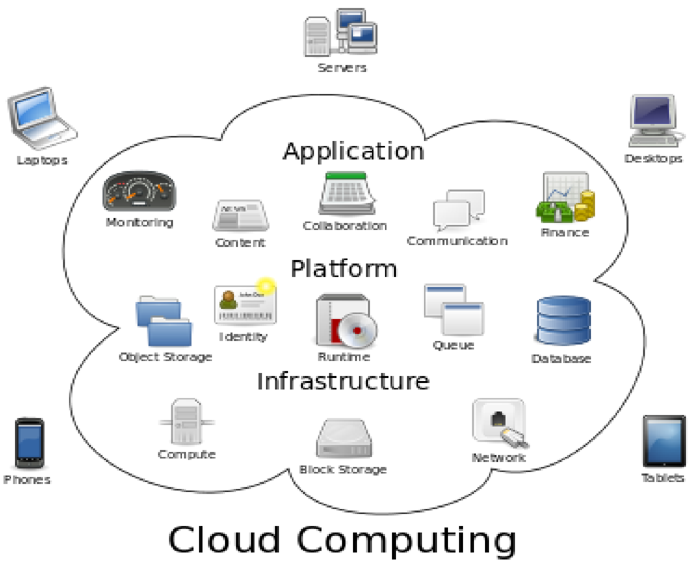
هرگونه نرم افزاری می تواند باشد. در این بین، رایانه نیز وظیفه مدیریت ابر و نظارت بر ترافیک و تبادل اطلاعات را بر عهده دارد. نرم افزارهای چند منظوره رابطی در داخل رایانه ها وظیفه تنظیم پردازش و ارسال اطلاعات به ابر را بر عهده دارند. با زیادتر شدن تعداد کاربران یک ابر، اطلاعات نیز بیشتر شده و برای ذخیره آنها در ابعاد کارهای یک شرکت، به واحدهای ذخیره سازی پیشرفته تر و پرحجم تری نیاز می باشد. در بعضی از ابرها از تمامی اطلاعات موجود در شبکه، کپی گرفته می شود و از آن به عنوان فایل پشتیبان (Backup) نگهداری می کنند تا در صورت ایجاد اخلال در ابر، بتوان از آن استفاده کرد.

۳-۲ انواع رایانش ابری

در حال حاضر طراحان مبحث "رایانش ابری" زمینه های مورد مطالعه در این حوزه را به سه بخش تقسیم می کنند (شکل ۱) (Boss et al, ۲۰۰۷).

۳-۲-۱ ارایه نرم افزار به عنوان سرویس

در این مدل یک نرم افزار از طریق ارتباطات شبکه ای روی کامپیوتر سرویس دهنده در حال اجرا است و از طریق شبکه فرمان های کاربر را دریافت کرده و با پردازش روی داده ها نتایج مورد نظر را به کاربر باز می گرداند. برای مثال در این حالت می توان انواع برنامه های کاربردی تحت وب و سرویس دهنده های ایمیل و غیره را نام برد.



شکل ۱ - تنوع سرویس ها در ابر [۶]

۳-۲-۲ ارایه پلتفرم [۸] به عنوان سرویس

در حال حاضر بسیاری از شرکتهای تولید کننده بسته های تولید کننده نرم افزار و اشکال زدایی آنها، در فکر این موضوع هستند که بتوانند برای کاربران محیطی را فراهم آورند که تیم های مختلف دست اندر کار پروژه بتوانند به صورت منظم و قانونمند روی پروژه های در دست ساخت، همکاری نموده و محیطی فراهم کنند که در آن تولید کنندگان نرم افزار بتوانند به

[۸] Platform

سهولت و بدون وجود دغدغه های مربوط به زیر ساخت های نرم افزاری و سخت افزاری و محیط تست به طراحی و تولید ایده های خود بپردازند. شرکت گوگل خدماتی از این دست را در قالب (Google App Engine) ارایه نموده است.

۳-۲-۳ ارایه زیر ساخت به عنوان سرویس

طراحان رایانش ابری پا را از این هم فراتر گذاشته و پیشنهاد نمودند که یک سیستم کامپیوتری کامل با سخت افزار شبیه سازی شده و همه امکانات یک ماشین را به صورت دسترسی راه دور در اختیار کاربران قرار دهند. به این ترتیب کاربر قادر خواهد بود که با اختیارات کامل به روی سخت افزار شبیه سازی شده، سیستم عامل و نرم افزارهای دلخواه خود را نصب نماید. و در هر کجایی از دنیا که قادر به دسترسی به شبکه باشند می توانند کل کامپیوتر و نرم افزارهای خود را در دسترس داشته باشند و فایل های خود را روی آن ذخیره و بازیابی نمایند.

همچنین قادرند در صورتیکه قابلیت های سخت افزاری فعلی پاسخگوی نیاز کاربران نباشد با ارایه درخواست خود به سرویس دهنده (ابر سرویس دهنده ماشین مجازی) درخواست قدرت بیشتری برای پردازنده مجازی خود کنند، یا پهنای باند یا میزان حافظه بیشتری طلب کنند و در قبال خدمات جدید هزینه معینی بپردازند. برای این کار دیگر نیاز نخواهد بود که سخت افزاری تعویض گردد و از این جهت در هزینه های کاربران صرفه جویی خواهد شد.

۳-۳ مزایای رایانش ابری

مزایای اصلی رایانش ابری عبارتند از :

- **هزینه** : ادعا می شود که این فناوری هزینه ها را به میزان زیادی کاهش می دهد و هزینه سرمایه ای را به هزینه عملیاتی تبدیل می کند. این به ظاهر موانع ورود به بازار را کاهش می دهد، زیرا رایانش ابری، مشتریان را از مخارج سخت افزار، نرم افزار و خدمات و همچنین از درگیری با نصب و نگهداری نرم افزارهای کاربردی به شکل محلی می رهاند. در عین حال، هزینه توسعه نرم افزاری را کاهش داده و فرآیند را مقیاس پذیرتر می نماید.
- **افزایش قابلیت اطمینان:** در حوزه اطلاعات می توان قالبیت اطمینان در دسترسی به اطلاعات را حیاتی ترین رکن در سیستم های اطلاعاتی عنوان نمود. بسیاری از کاربران بارها با مواردی مانند آسیب های فیزیکی و از دست رفتن اطلاعات، عدم دسترسی به اطلاعات مورد نیاز در شرایط حساس و موارد مشابه برخورد کرده اند. در دنیای امروز و در صورتیکه از تکنولوژی رایانش ابری استفاده گردد، برای دسترسی به هر گونه نیاز اطلاعاتی تنها یک ارتباط شبکه کافی خواهد بود. و سرویس دهنده ابر با هر تدبیر ممکن، سعی در ارایه اطلاعات و حفظ قابلیت اطمینان سرویس خواهد داشت و تدابیر لازم را به بهترین شکل و با کمترین هزینه انجام خواهد داد.
- **مقیاس پذیری[۹]:** کاربران می توانند در زمان تقاضا و به صورت پویا منابع را تدارک ببینند و نیازی به تدارک پیشین برای زمان های حداکثر بار مصرف منابع نمی باشد.
- **امنیت:** به دلیل تمرکز داده ها و منابع امنیتی بیشتر و پیچیده تر، امنیت افزایش می یابد. اما نگرانی ها به دلیل از دست دادن کنترل روی داده های حساس همچنان پابرجاست. امنیت در رایانش ابری اغلب بیشتر یا برابر با سیستم های سنتی می باشد، زیرا ارایه دهندگان رایانش ابری به منابع اختصاصی امنیتی دسترسی دارند، که بیشتر مشتریان از عهده خرید این منابع بر نمی آیند. مسلما در صورتی که حفظ امنیت نرم افزارها و سیستم

[۹] Scalable

های اطلاعاتی توسط متخصصان این زمینه تامین گردد، احتمال خرابکاری و ناامنی در سیستم کاهش یافته و برخورد با آن با سرعت و کیفیت بیشتری انجام خواهد پذیرفت.

- **نگهداری**: به دلیل عدم نیاز به نصب برنامه های کاربردی برای هر کاربر نگهداری آسان تر و هزینه کمتر انجام می شود شرکت هایی که پلتفرم های خودشان را پیاده سازی و اجرا می کنند، باید زیر ساخت های سخت افزاری و نرم افزارهای خودشان را خریداری، و نگهداری نمایند و کارمندانی را برای مراقبت از سیستم استخدام کنند، همه این ها می تواند پر هزینه و زمان بر باشد. در حالی که رایانش ابری نیاز به انجام این کارها را از میان می برد. هر دستگاه ساده که توانایی اتصال و برقراری ارتباط با سرور را داشته باشد برای استفاده از خدمات رایانش ابری کافی است، و می تواند نتایج را با دیگران به تشریک مساعی بگذارد. همچنین، مدیریت منابع اطلاعاتی به جای آنکه در دست کاربران باشد یا در محیط شرکت ها انجام شود، هزینه های سنگین نگه داری سیستم های اطلاعاتی و بروزرسانی آنها را ، از دوش کاربران سیستم های اطلاعاتی برداشته و در دست متخصصین خبره قرار خواهد گرفت و کاربران می توانند با خیال راحت و صرف کمترین هزینه بر کار اصلی خود تمرکز نمایند.
- **عدم وابستگی به تجهیزات خاص و مکان خاص:** کاربران می توانند در هر مکانی و با هر دستگاهی (مثل PC یا تلفن همراه) به وسیله یک مرورگر وب از اینترنت به سامانه ها دسترسی داشته باشند.
- **چند مستاجری**[۱۰]: این ویژگی، امکان به اشتراک گذاری منابع و هزینه ها، بین گروهی از کاربران را بوجود می آورد. و این امکان را فراهم می آورد که زیر ساخت ها در مکان هایی با هزینه کمتر (مثل مکان هایی با هزینه برق یا قیمت زمین کمتر) متمرکز شوند. همچنین باعث افزایش بکارگیری و کارایی برای سامانه هایی که در اغلب مواقع، درصد بسیار کمی از منابع اختصاصی را به کار می گیرند، می شود.
- **سنجش پذیری**: منابع در رایانش ابری باید قابل اندازه گیری باشند و لازم است که میزان مصرف منابع برای هر کاربر و هر منبع بر اساس واحد های ساعتی، روزانه، هفتگی، ماهانه اندازه گیری شود[۶].
- **صرفه جویی در مصرف منابع و هزینه ها:** واضح است که استفاده از منابع و در مواقع نیاز به آن منابع، همواره موجب کاهش هزینه ها و صرفه جویی در منابع می شود. بطور معمول کاربران در حدود ۱۰ تا ۱۵ درصد از ظرفیت قدرت پردازنده خود را در مدت استفاده از کامپیوتر خود استفاده می نمایند. یا همه ما معمولا بخش وسیعی از حافظه موقت یا هارد دیسکمان خالی است و مورد استفاده قرار نمی گیرد. حال اگر بتوان این فضای خالی را در صورت عدم استفاده از صاحب اصلی آن به کاربرانی که مایل به استفاده از آنها هستند، اجاره داد و از آنها بهره برداری نمود می توان در هزینه ها صرفه جویی فراوانی نمود. چرا که به علت کهنه شدن تکنولوژی یا افت قیمت، در صورت عدم استفاده از منابع، مالک دچار ضرر مالی خواهد شد.

۴- امنیت ابر

رایانش ابری از سال ۲۰۰۶ ایجاد شده و نسل بعدی محاسبات موازی، محاسبه توزیع شده و محاسبه شبکه ای و نتیجه ی توسعه ی مخازن شبکه، مجازی سازی و تعادل بار است. رایانش ابری تغییرات عمده ای در سبک زندگی و روش های کار افراد ایجاد کرده و فواید زیادی دارد. همانطور که شرکتها برای ساده کردن کارها و صرفه جویی در هزینه ها به سمت فناوری های رایانش ابری پیش می روند، امنیت این سیستم ها یک دغدغه اساسی خواهد بود. حملات در این سیستم ها می توانند بر روی

---
[۱۰] Multi-Tenancy

زیرساخت ها، شبکه ارتباطات، اطلاعات و خدمات متمرکز شوند. بنابراین امنیت رایانش ابری همیشه مورد توجه مشتریان بالقوه ابری و یک مانع بزرگ برای استفاده گسترده از آن است(Che and Duan, ۲۰۱۱).

از آنجا که سیستم های فناوری اطلاعات رایانش ابری برای کاربران غیر مشهود است، قابل درک است که مشتریان می خواهند از اطلاعاتشان بطور کامل محافظت شود و خدمات ارائه شده پایدار باشند. پس نگرانی ها به ویژه در زمینه امنیت افزایش یافته است. در سال های اخیر تلاش های زیادی در جهت تأمین امنیت خدمات ابری شده است. بسیاری از تأمین کنندگان، دانشگاه ها و شرکت های بزرگ IT همکاری های وسیعی در این جهت داشته اند. در سال ۲۰۰۹ سازمانی غیرانتفاعی به نام Cloud Security Alliance (اتحاد امنیت ابری) با هدف ترویج و گسترش بهترین روش ها برای تأمین اطمینان از امنیت در عرصه رایانش ابری در جهت تأمین امنیت بیشتر تاسیس گردید. در حال حاضر بسیاری از تأمین کنندگان ابر عضو این سازمان هستند و به طور رسمی پژوهش های گسترده ای در زمینه امنیت فناوری رایانش ابری انجام می دهند(Okuhara et al, ۲۰۱۰).

محیط ابر مهمترین مثال از رایانش توزیع شده است، که همه انواع خدمات برای کاربر فراهم شده. ارائه دهندگان خدمات زیرساخت ابر اقدامات امنیتی اولیه در سطح زیرساخت مانند فایروال ها، حفاظت از انواع مختلف ویروسها را با توسعه و بروزرسانی نرم افزار آنتی ویروس بصورت منظم انجام می دهند. ماشین های مجازی نصب شده روی سیستم عامل، امنیت را به روشهای مختلف فراهم می کند. با اینحال، حملات شبکه در مواجه شدن با ماشین های مجازی شبکه، نمی توانند با فایروالها یا آنتی ویروسها رفع شوند. بنابراین یک بررسی در سیستم امنیتی شبکه جهانی در سطح مرکز داده لازم است. بسیاری چارچوب های زیرساخت ابر وجود دارد که خدمات رایانش ابری و خدمات مجازی سازی را برای کاربر فراهم می کند مانند OpenNode، Cloud Stack، Cloud Sigma، اکالیپتوس، EMOTIVE (مدیریت انعطاف پذیر وظایف در محیط های مجازی شده) و Archive. همانطور که منافع و مزایای قابل توجه و غیر قابل انکاری در رایانش ابری وجود دارد، این فناوری شامل ریسک ها و مخاطرات مربوط به خود هم می باشد. محرمانگی (قابلیت اعتماد)، جامعیت، قابلیت دسترسی، قابلیت اعتبار (تشخیص هویت) و حریم خصوصی اصلی ترین نگرانی ها برای ارائه دهندگان و مصرف کنندگان ابر هستند(Arora et al, ۲۰۱۲). ولی بزرگترین نگرانی در بکارگیری رایانش ابری، به امنیت مربوط است و پیوسته از مهمترین چالش های این فناوری بوده . بنابراین امنیت بیش از مزایای آن، ذینفعان را دچار تردید می کند.

امنیت یک چالش برجسته میان سایر چالش ها است. طبق تحقیق های انجام گرفته روی معماری های امنیتی رایانش ابری، کاربران احساس امنیت و اطمینان دارند، زمانیکه واقعا بدانند که عملیات چطور در حال انجام و اجرا شدن می باشد. گرچه، رایانش ابری آسایش زیادی برای کاربران به وسیله رهاسازی آنها از نیاز به دانستن جزئیات فرآیندها فراهم می کند، اما کاربران را مجبور می کند به ارائه دهنده سرویس های ابری اعتماد کنند. در بازار امروزه، آگاهی درباره مسائل رایانش ابری بیشتر به سمت مسائل قابلیت اطمینان و امنیت سوق دارد(Okuhara et al, ۲۰۱۰).

درک وابستگی لایه ای مدل های خدمات ابری برای آنالیز خطرات امنیتی رایانش ابری، بسیار حیاتی است. IaaS لایه پایه همه خدمات ابری است، PaaS روی IaaS و SaaS روی PaaS ساخته می شود. در نتیجه بین توانایی خدمات لایه های متفاوت در رایانش ابری رابطه ای وجود دارد. مشابه توانایی خدمات ابری، خطرات امنیتی رایانش ابری هم بین لایه های متفاوت خدمات، مشترک است(Che and Duan, ۲۰۱۱).

۴-۱ تهدیدها و حملات ابر

مشکلات امنیتی به عنوان یک مانع بزرگ در مقابل استفاده کاربران از سیستم های رایانش ابری قلمداد می شود. در اینجا به شناخت حملات امنیتی اولیه بر روی ابر و مسائل مطرح در آن پرداخته شده و برخی حملات امنیتی و راهکار مقابله با آنها را مورد بررسی قرار خواهیم داد.

هر یک از انواع مختلف خدمات رایانش ابری- مانند SaaS، PaaS، IaaS- چالش های امنیتی خودش را دارد. ولی IaaS همه انواع چالش مانند: حملات شبکه، حمله مبتنی بر رفتار، حمله مبتنی بر درخواست، کنترل درخواست ها از کاربران نامطمین، XSS و DDoS و بسیاری دیگر را در بر می گیرد. این حملات مستقل از یکدیگرند و در نتیجه کیفیت خدمات ارائه شده توسط ابر را به خطر می اندازند.

۴-۱-۱ حمله DoS

DoS یا از کار اندازی سرویس، نوعی حمله است که هدف آن از کاراندازی سیستم با استفاده از هدر دادن منابع آن است. بطوریکه سرویس دهنده توانایی سرویس دهی عادی به کاربران مجاز را از دست بدهد. محرومیت از سرویس یا DoS در دنیای کامپیوتر همانند هکر ها خیلی مشهور هستند و در طی سالیان به صورت های مختلف برای رد کاربران در استفاده از سرویس ها استفاده شده اند. هدف از حملات رد سرویس، غیر قابل دسترس کردن منابع کامپیوتر از کاربرانی که قصد دستیابی به آن را دارند، می باشد.

۴-۱-۲ DoS توزیع شده[۱۱]

حملات DDoS[۱۱] نیز مشابه DoS هستند با این تفاوت که حمله از طریق چندین سیستم و بصورت توزیع شده است. DoS توزیع شده حمله ای است که اغلب هزاران یا حتی میلیون ها کامپیوتر به یک هدف حمله می کنند. معمولا مهاجم از تعدادی کامپیوتر بدون اجازه مالکشان که botnet نامیده می شود، استفاده می کند. این botnet ها توسط یک مدیر کنترل می شوند و قدرتشان برای حمله به یک هدف به کار برده می شود.

۴-۱-۳ 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 بارگذاری 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 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.

۴-۱-۴ XSS[۱۲]: حملات کراس سایت اسکریپت روش نفوذ و گرفتن دسترسی غیرمجاز از یک وب گاه توسط هکرها می باشد.

۴-۱-۵ حملات ماسک : در این حملات تهدیدها نقش کاربران مجاز را بازی می کنند.

۴-۱-۶ حملات مبتنی بر میزبان: این حملات نتیجه حملات ماسک و عموما در ناهنجاری رفتاری کاربران قابل مشاهده است.

۴-۲ راهکارهای امنیت ابر

[۱۱] Distributed DOS
[۱۲] Cross Site Scripting

شکست در امنیت رایانش ابری به چند دلیل رخ می دهد که یکی از دلایل آن، سخت افزاری است که در لایه زیرساخت به عنوان سرویس ابر بکار می رود. در جدول ۱ خلاصه ای از تهدیدها و راه حل های ارائه شده برای زیرساخت آورده شده است(Arora et al, ۲۰۱۲). سپس سایر راهکارهای امنیتی بطور خلاصه آورده شده است.

جدول۱- تهدیدها و راه حل های امنیت زیرساخت ابر

<table>
<tr><th>مؤلفه های IaaS</th><th colspan="2">تهدیدها / چالش ها</th><th colspan="2">راه حل ها</th></tr>
<tr><td>SLA
(موافقت نامه سطح خدمات)</td><td colspan="2">نظارت و اجرای SLA
نظارت ویژگیهای کیفیت خدمات</td><td colspan="2">چارچوب (WSLA) موافقت نامه سطح خدمات وب
نظارت SLA و اجرا در SOA</td></tr>
<tr><td>محاسبات سودمند</td><td colspan="2">اندازه گیری و صورتحساب ارائه دهندگان
دسترس پذیری سیستم صورتحساب بنابه تقاضا</td><td colspan="2">سیستم پرداخت آمازون</td></tr>
<tr><td>نرم افزار ابر</td><td colspan="2">حملات به XML
حملات به خدمات وب</td><td colspan="2">رمزگذاری XML و امضای آن</td></tr>
<tr><td>اتصالات اینترنت و شبکه ها</td><td colspan="2">کلاهبرداری IP
اسکن پورت
امنیت DNS</td><td colspan="2">دیوار آتش و بخش بندی شبکه منطقی
رمزگذاری ترافیک
نظارت بر شبکه
سیستم تشخیص نفوذ و ممانعت از نفوذ</td></tr>
<tr><td>مجازی سازی</td><td>تهدیدهای امنیتی از منبع میزبان:
• نظارت ماشین های مجازی از میزبان
• ارتباطات بین ماشین های مجازی و میزبان
• تغییرات ماشین های مجازی</td><td>تهدیدهای امنیتی از منبع ماشین مجازی:
• نظارت ماشین مجازی از ماشین مجازی دیگر
• ارتباطات بین ماشین های مجازی
• ماشین های مجازی سیار
• منابع انکار خدمات (DOS)
• مهاجرت ماشین های مجازی</td><td>تهدیدهای امنیتی از منبع میزبان:
• پلتفرم رایانش ابری مطمئن
• مراکز داده مجازی مطمئن (TVDc)
• کنترل دسترسی الزامی (MAC)</td><td>تهدیدهای امنیتی از منبع ماشین مجازی:
• رمزگذاری
• VPN
• امنیت Xen با جداسازی
• معماری LoBot برای تأمین امنیت و مهاجرت ماشین مجازی</td></tr>
<tr><td>سخت افزار کامپیوتر</td><td colspan="2">حمله فیزیکی به سخت افزار کامپیوتر
امنیت داده در دستگاههای ذخیره سازی از رده خارج شده یا جایگزین شده</td><td colspan="2">اتاق های قفل شده با امنیت بالا با دستگاههای نظارت
دسترسی چندگانه به مخازن رمزگذاری
سیستم فایل های مخفی شفاف</td></tr>
</table>

۴-۲-۱ ایجاد زیرساخت کلید عمومی (PKI) روی هر لایه.

۴-۲-۲ استفاده از سیستم تشخیص نفوذ شبکه در ابر: این کار با نصب ESX۴,۰، VCenter Server و VCenter Lab Manager در سخت افزار سرور امکان پذیر می باشد که به ایجاد و استقرار چندین سرور مجازی کمک می کند. سرورها، سیستم عامل و نرم افزار کاربردی دارند و حاوی اطلاعات با ارزش هستند که برای بدافزارها و مزاحم ها جلب توجه می کنند.

مزاحم ها به دنبال پیداکردن آسیب پذیری در نرم افزار و سیستم های شبکه شده برای دزدیدن و خراب کردن داده های حساس هستند. بمنظور کاهش این تهدیدها، سیستم تشخیص نفوذ شبکه منبع باز به نام Snort نصب می شود. Snort بر فعالیت شبکه نظارت کرده و هرزمان ترافیک خطرناکی پیدا کند، یک اعلان ارسال می کند. Snort قادر به تشخیص ترافیک های خطرناک و ذخیره آنها در فایل لاگ می باشد. از این روش می توان در هر مرکز داده مجازی برای کاهش خطرات احتمالی استفاده کرد. سیستم تشخیص نفوذ شبکه، قادر به ردیابی هکرها و تشخیص نقض های امنیتی و استفاده های غیرمجاز و حمله به یک رایانه، شبکه یا سیستم ارتباطی نیز می باشد. این سیستم سرورهای مجازی و نرم افزارها را نظارت کرده و هر زمان که فعالیت مخربی پیدا کند، اعلان می دهد. سیستم تشخیص نفوذ زمانی کارایی لازم را پیدا می کند که بتواند اعلان ها را اولویت بندی و یک پیام ارسال کند. از آنجا که فایل لاگ شامل مراحل مختلف همه حملات است، ارسال یک اعلان اولویت بندی شده بهتر از ارسال کل فایل است. در نتیجه سیستم تشخیص نفوذ باید با یک سیستم ممانعت از نفوذ شبکه ترکیب شود تا ترافیکهای غیرنرمال را شناسایی، متوقف و گزارش دهد.

۴-۲-۳ مجازی سازی: همانطور که در جدول ۱ نیز مشاهده کردیم، راهکار امنیتی دیگر مجازی سازی است. 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. مجازی سازی از دیدگاه امنیتی می تواند هم یک فرصت و هم یک تهدید باشد. از اینرو امنیت مجازی سازی از دو جهت اهمیت دارد: ۱ – ارتقاء امنیت سیستم ۲ – حملات جدید ناشی از حضور لایه مجازی سازی. دیدگاههای مختلفی که امنیت مجازی سازی را مورد بررسی قرار می دهند عبارتند از:

- سیستم های امنیتی مبتنی بر مجازی سازی:

ضعف امنیتی این سیستم ها، قابل رؤیت بودن سیستم، توسط نفوذگر است. راهکارهایی که می توان برای آن ارائه داد عبارتند از: کشف نفوذ، ممانعت از نفوذ، نظارت بر جامعیت و سیستم های ثبت.

- توسعه امنیت: شامل امنیت فوق ناظر، کاهش کد و کنترل دسترسی.
- امنیت با محاسبات مطمئن: این کار با استفاده از امکانات سخت افزاری نظیر ماژول پلتفرم مطمئن (TPM) و پردازنده های Intel وAMD میسر می باشد.

۴-۲-۴ راه حل حملات سیل آسا Flooding Attack

راه حل پیشنهادی برای مقابله با حملات سیل آسا ایجاد ناوگانی از سرورها 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 طراحی های جدید چنانچه بار روی یک سرور بالا رود سرور جدید وارد عمل شده، بارگذاری جدید به آن منتقل شده، در نتیجه بمنظور جدول موجود در سرور نام بروز رسانی می شود.

۵- مفهوم سیستم تشخیص نفوذ

سیستم تشخیص نفوذ ابزار امنیتی است که هدف آن تقویت امنیت اطلاعات و سیستمهای ارتباطی از طریق نظارت شبکه یا فعالیتهای سیستم، شناسایی نفوذها و تهیه گزارش می باشد(Jeong et al, ۲۰۱۲). سیستم های تشخیص نفوذ با مطالعه رفتار کاربران و اطلاعات موجود در حملات، رفتارهای غیر نرمال را تشخیص می دهند. این سیستم ها معایب و مزایای خاص خود را دارند که با تشخیص و یا پیشگیری از حملات نقش مؤثری در تامین امنیت دارند. IDSهای فعال[۱۳] سیستم های جلوگیری از

[۱۳] Active

نفوذ (IPS[۱۴]) هستند که علاوه بر نظارت ترافیک شبکه می توانند از ورود ترافیک ناهنجار به شبکه جلوگیری و تهدیدها را مسدود یا متوقف سازند. برخلاف IDS که فقط نفوذ را شناسایی می کند، IPSها قادر به جلوگیری از نفوذ، ارسال هشدار، کاهش بسته های مخرب و انسداد ترافیک IP معیوب نیز می باشد.

در ادامه بطور خلاصه به توضیح روشهای تشخیص نفوذ، تکنیک های بکار رفته در محیط های ابری و حملات قابل تشخیص توسط آنها می پردازیم.

۵-۱ روشهای تشخیص در IDS

روش تشخیص در سیستمهای تشخیص نفوذ برحسب تکنولوژیهای تحلیلی، به دو روش مختلف است: ۱- تشخیص ناهنجاری[۱۵] ۲- روش مبتنی بر امضا[۱۶]

در مدل مبتنی بر تشخیص ناهنجاری یک پروفایل معمولی با داده هایی درباره فعالیتهای سیستم ساخته شده و این پروفایل برای شناسایی الگوی فعالیتها استفاده می شود(Yang et al, ۲۰۱۱). همچنین تصمیم ها بر اساس پروفایل شبکه نرمال یا رفتار سیستم و با استفاده از تکنیکهای یادگیری ماشین[۱۷] یا آماری[۱۸] انجام می شود(Aljarah and Ludwing, ۲۰۱۳). از طرف دیگر اگر در این روش حمله ای رخ دهد با بررسی اینکه آیا انحراف بین رویداد رخ داده و رفتار نرمال، بیشتر از آستانه از پیش تعریف شده است یا نه تصمیم می گیرد. این رویکرد می تواند حملات دیده نشده قبلی را نیز تشخیص دهد(Jeong et al, ۲۰۱۲).

در روش مبتنی بر امضا، IDSها شبکه و فعالیت سیستم را با الگوی الگوریتم تطبیق، بررسی می کنند(Aljarah and Ludwing, ۲۰۱۳). این روش الگوهایی از حملات شناخته شده برای پیدا کردن حملات در نظر می‌گیرد. پس، لازم است پایگاه داده امضاها برای نمایش حملات شناخته شده پیشرفته ساخته شود. روش مبتنی بر امضا علیرغم کارایی، در مقابل حملات جدید و ناشناخته مؤثر نمی باشد(Jeong et al, ۲۰۱۲).

هر یک از این روشها ضعف ها و قوت های خود را دارند. سیستم های مبنی بر امضا نرخ FP[۱۹] خیلی پایینی دارند. یعنی نرخ خطاهای بدون نفوذی که اشتباها تشخیص داده شده در آنها بسیار کم است. همچنین این سیستمها در شناسایی حملات ناول و مبهم ناتوان هستند. الگوریتم الگوی تطبیق نیز در این مدل با رشد نمایی انواع مختلف حملات، قابل اعتماد نیست. از طرف دیگر، سیستم های مبنی بر ناهنجاری تعداد زیادی FP تولید می کنند. از اینرو پیشنهاد می شود از هر دو شیوه در یک IDS استفاده شود(Aljarah and Ludwing, ۲۰۱۳).

۵-۲ مدل های استقرار IDS

بر اساس مدل استقرار، IDSها به سیستم های بر اساس شبکه و میزبان[۲۰] تقسیم می شوند.

- NIDS (Network-based IDS): وظیفه نظارت شبکه را دارد و تشخیص در آن روی انواع دسترسی تمرکز دارد(Yang et al, ۲۰۱۱).

---

۱۴ Intrusion Prevention System
۱۵ Anomaly detection
۱۶ Signature based/misuse
۱۷ Machine Learning
۱۸ Statistical
۱۹ False-Positive
۲۰ host

- HIDS (Host-based IDS): برای تشخیص و نظارت فعالیتهای مخرب مانند تغییرات سیستم فایل و لاگ های برنامه استفاده می شود و از سیستم عامل جدا نیست(Yang et al, ۲۰۱۱).

سیستم های تشخیص نفوذ مبنی بر شبکه حملات را با تحلیل ترافیک بسته های شبکه در طول سگمنت یا سوییچ شبکه تشخیص و نظارت و حفاظت از چندین میزبان را با ماشین جداگانه ای انجام می دهند. این سیستم ها قادر به نظارت تعداد زیادی میزبان با هزینه استقرار نسبتا کم و شناسایی حملات به/ از چندین میزبان می باشند(Aljarah and Ludwing, ۲۰۱۳). NIDSها نمی توانند تشخیص و جلوگیری از حمله را- بخصوص در حملات روی بسته های رمز گذاری شده- تضمین کنند. از طرفی HIDSها قادرند تصمیم بگیرند آیا یک حمله با نیت سوء قصد در ماشین محلی موفق بوده است یا نه. همچنین سرور باید روی همه HIDSها نصب شده باشد. بنابراین حتی ساختار شبکه های در مقیاس کوچک هم معمولا لازم است بر پایه هر دو مدل باشد(Yang et al, ۲۰۱۱).

۶- مقایسه IDSهای اخیر

در جدول ۲ برخی IDSهای اخیر که پردازش اطلاعات یا تشخیص نفوذ را در ابر انجام می دهند، بهمراه ویژگیهای مهم، تکنیکها و حملات قابل تشخیص توسط آنها بررسی شده است.

جدول۲- مقایسه سیستم های تشخیص نفوذ مبتنی بر ابر

Ref.	IDS Name	IDS Type	IPS	Cloud	Snort	Scalable	Real Time	Log file Check	Behavior-based	Knowledge-based	Techniques					Attack Detection						Detection Type	
											Data mining	Neural Network	Machine learning	Profiling	Clustering	DoS / DDoS	XSS	TCP SYN Flooding	Packet Flooding	Masquerade	Host-based	Signature	Anomaly
(Holtz et al, ۲۰۱۱)		HIDS NIDS		✓		✓	✓	✓														✓	
(Taghavi Zargar et al, ۲۰۱۱)	DCDIDP	HIDS NIDS	✓	✓			✓	✓		✓	✓		✓	✓		✓						✓	✓
(Manavi et al, ۲۰۱۲)	SVL-IDS	HIDS	✓	✓												✓							✓
(Sathya and Vasanthraj, ۲۰۱۳)	MultiLevel-IDS	NIDS		✓				✓			✓												✓
(Kholidy and Baiardi, ۲۰۱۲)	CIDS	HIDS NIDS		✓	✓	✓		✓	✓	✓		✓								✓		✓	✓
(He et al, ۲۰۱۲)		HIDS NIDS		✓			✓	✓	✓				✓		✓							✓	✓
(Gupta and Kaliyar, ۲۰۱۳)	BIDS	HIDS NIDS		✓				✓	✓							✓	✓			✓	✓		✓
(Gupta et al, ۲۰۱۳)	PIDS	NIDS	✓	✓					✓					✓		✓		✓	✓			✓	✓

- DCDIDP[۲۱] سیستم تشخیص و جلوگیری از نفوذ است که هدف آن استفاده از منابع ابری و فراهم کردن یک IDPS برای همه ارائه دهندگان خدمات ابری است تا بتوانند در محیط توزیع شده و با معماری های مختلف به حملات پاسخ دهند. سطوح زیرساخت چارچوب این سیستم از سه لایه منطقی شبکه، میزبان و سراسری تشکیل شده است(Taghavi Zargar et al, ۲۰۱۱).

[۲۱] Distributed Collaborative and Data-driven Intrusion Detection and Prevention

- در SVL-IDS[۲۲] مدل امن برای لایه مجازی بنام SVL، محیط ابر را از تهدیدها و حملات حفاظت می کند و از معماری ابر برای ایجاد IaaS روی ماشین های مجازی استفاده می کند. استفاده از معماری ناول در این IDS، کنترل فروشنده ها را روی زیرساخت بهبود می بخشد. این سیستم از ناظر ماشین مجازی[۲۳] برای امنیت ماشین های مجازی و انتقالات بین آنها استفاده می کند. در این مدل به جای پیاده سازی مدل نرمال ابر، یک لایه جدید بنام V-Basement برای مجازی سازی ارائه شده. این لایه، مجازی سازی را به دو مؤلفه نظارتی مجزا تقسیم می کند. این مدل که از ترکیب مجازی سازی و IDS استفاده می کند، اگرچه هزینه پیاده سازی بالایی دارد ولی نرخ تشخیص را افزایش و از حملات به مجازی سازی محافظت می کند(Manavi et al, ۲۰۱۲).
- MultiLevel-IDS سیستم تشخیص نفوذ چند سطحی براساس تحلیل فایل لاگ می باشد. این مدل یک طرح تأیید اعتبار برای کاربر ارائه می دهد تا هر زمان کاربر درخواست داده می دهد، ابتدا کاربر در سطح مرکز داده/گره تأیید اعتبار شده و سپس تنها داده تأمین شود. این مدل برای زیرساخت ابر با استفاده از مجازی سازی و ماشین های مجازی ارائه شده. همچنین هشدارهای نفوذ را در سه سطح پایین ، متوسط و بالا تقسیم می کند(Sathya and Vasanthraj, ۲۰۱۳).
- CIDS[۲۴] چارچوبی برای سیستم تشخیص نفوذ ابری است که همه انواع حملات را پوشش می دهد:
    - حملات ماسک (حمله PaaS)
    - حملات بر اساس میزبان (حملات Paas وSaaS با تحلیل لاگ و تکنیکهای داده کاوی)
    - حملات بر اساس شبکه (حملات IaaS): با تحلیل بسته‌های شبکه با استفاده از snort بعنوان NIDS انجام می شود.

CIDS هشدارهای IDS مبنی بر شبکه را بر اساس امضای حمله خلاصه و رویدادها و محاسبات را از ماشین مجازی جمع آوری می‌کند. در معماری CIDS هر نود دارای ۲ تشخیص دهنده IDS است، CIDS و HIDS. با این کار هر نود، رویدادهای محلی را شناسایی و نقض های امنیتی را نشان می دهد. CIDS شامل سیستم حسابرسی برای کشف حملاتی است که NIDS و HIDS ها نمی توانند تشخیص دهند(Kholidy and Baiardi, ۲۰۱۲).

- BIDS[۲۵] امکان تشخیص ناهنجاری کاربران مطمئن را فراهم و درخواستهای غلط را که ممکن است به فریب کاری، حملات DoS یا XSS و بسیاری حملات دیگر منجر شوند را شناسایی می کند. علاوه بر آن مواردی که در آن نام کاربری و کلمه عبور کاربر به خطر می افتد را تشخیص می دهد. BIDS می تواند در تشخیص این حملات و نگهداری کیفیت خدمات ارائه شده برای کاربر در زیرساخت ابر مفید باشد. BIDS رفتار و درخواستها و فعالیتهای کاربر را در ابر که بر اساس بررسی فایل های لاگ می باشد، ردیابی می کند ولی بلادرنگ نمی باشد. BIDS هم حمله مبنی بر رفتار شبکه و هم حملات مبنی بر ناهنجاری را در برمی گیرد و پیشرفته تر است(Gupta and Kaliyar, ۲۰۱۳).
- PIDS[۲۶] سیستم تشخیص نفوذ شبکه مبتنی بر پروفایل است که از معماری ناول برای تشخیص نفوذ در ماشین مجازی (موجودیتهای داخلی مثل کاربران مخرب ابر) و موجودیتهای خارجی (مهاجمان خارجی) در زیرساخت ابر استفاده می کند. PIDS بمنظور امنیت ابر با حداقل هزینه اعم از هزینه های توان محاسباتی، مخازن ذخیره سازی و ارتباطات ساخته شده و با ایجاد پایگاه داده پروفایل ماشین مجازی، الگوهای حملات را شرح می دهد. PIDS برای تشخیص حملات سیل

---
[۲۲] Secure model for Virtualization Layer- IDS
[۲۳] Virtual Machine Monitor
[۲۴] Cloud based Intrusion Detection System
[۲۵] Behavior based Intrusion Detection System
[۲۶] Profile based Intrusion Detection System

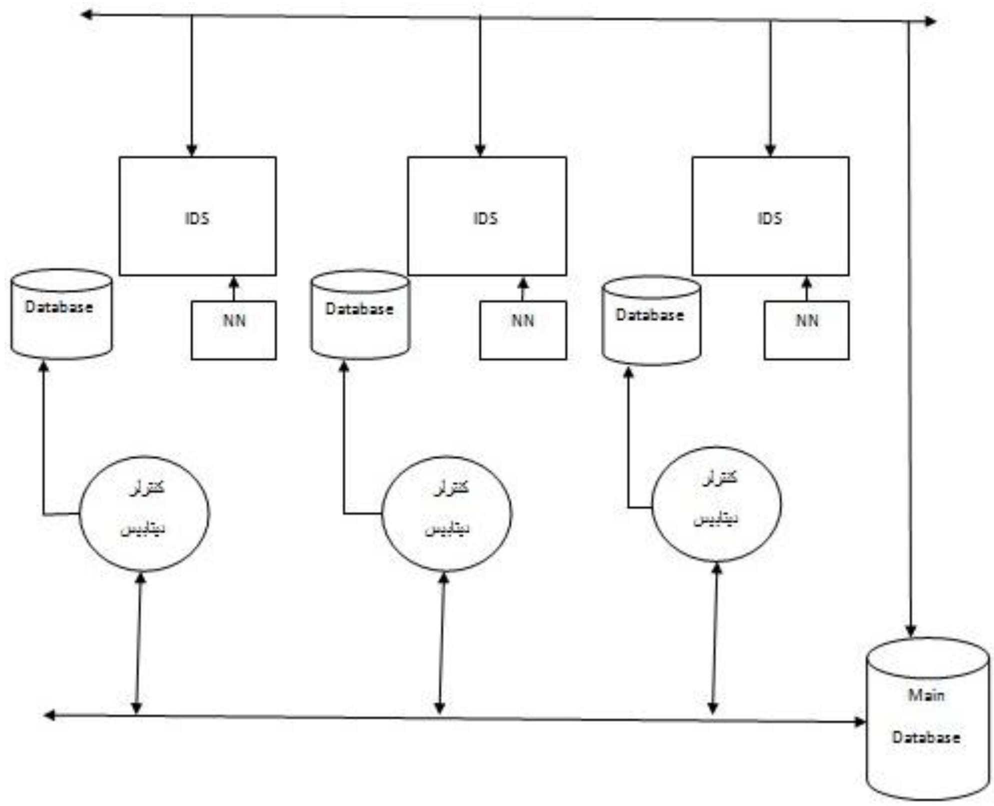
آسای بسته مانند حملات DoS و یافتن الگوهای شامل سایر حملات ماشین مجازی در ابر استفاده می شود. PIDS ترافیک ورودی و خروجی را تقسیم و رفتار ناهنجار شبکه را – برای یافتن حملات بر اساس پروفایلهای شخصی ماشین های مجازی خاص – تحلیل می کند. نتایج نشان می دهد PIDS برای تشخیص همه انواع حملات شناخته شده شبکه مبتنی بر ناهنجاری و امضا بکار می رود(Gupta et al, ۲۰۱۳).

بحث

امروزه با نرخ بالای دسترسی به شبکه، ارائه خدمات زیاد و آسیب های حملات توزیع شده، به یک IDS کارآمد و قابل اطمینان نیاز داریم. IDSهای امروزی برای حجم زیاد ترافیک در شبکه های با مقیاس بزرگ مناسب نبوده و طبیعت شبکه هـای ابـری، ناهمگون و توزیع شده می باشد. لذا IDSها باید مقیاس پذیر باشند تا بصورت کارآمد حجم زیـاد گـره هـای شـبکه را مـدیریت کنند و با اضافه شدن نودها در ابعاد بزرگ مقیاس پذیر باشند. جدول ۲ نشان می دهـد کـه در سیسـتم هـای تشـخیص نفـوذ مقیاس پذیر از روش تشخیص مبتنی بر امضا استفاده شده است. علاوه بر این روش مبتنی بر امضا دارای ویژگی های زیـر مـی باشد:

- سیستم های تشخیص نفوذ مبتنی بر امضا درصد خطا و اشتباه کمی در یافتن حملات دارند.
- تصمیم گیری در سیستم های تشخیص نفوذ مبتنی بر امضا علایم هشدار را بر حسب تشخیص امضاها انجام می دهد و نیازی به مطالعه ترافیک شبکه ندارد.
- در سیستم های تشخیص نفوذ مبتنی بر امضا, هر امضا نیاز به یک مکان در دیتابیس دارد و هر بسته باید با تمامی این امضاها در دیتابیس مقایسه شود. بنابراین هزینه پردازشی و حافظه ای بالا یکی از مشکلات این سیستم ها است.

در این مقاله با بهره گیری از سیستم های تشخیص نفوذ مبتنی بر امضا و مطالعه و بررسی نقاط ضعف آنها و بهبود این مدل, سیستم تشخیص نفوذ نوین توزیع شده ای را پیشنهاد داده ایم. در سیستم پیشنهادی سعی شده راهکار های کارا و مناسب برای مشکلات سیستم های قبلی ارایه داده شود. در مورد مساله ذخیره سازی امضا ها در دیتابیس و هزینه های پردازشی بالای آن از تکنیک تشخیص ناهمگون بهره خواهیم برد. به هر سیستم تشخیص نفوذ یک دیتابیس کوچک امضا اختصاص داده شده است که با دیتابیس مرکزی که شامل تمامی امضاها است در ارتباط است. در این ساختار نحوه انتخاب امضاها و قوانین در دیتابیس با توجه به دفعات تکرار استفاده از آنها است. امضاهایی که دفعات تکرار استفاده آنها کم است با امضاهای پرتکرار جایگزین می شوند.



شکل۲ – روش ساختار پیشنهادی

نتیجه گیری

همانطور که قبلاً اشاره شد مهمترین چالش رایانش ابری تضمین امنیت داده های موجود می باشد . در حال حاضر حفاظت از کارکرد ابر در اینترنت یک چالش بزرگ محسوب می شود و راه حل های بسیاری برای امنیت داده ها در رایانش ابری به کار

گرفته می شود. همانطور که در جدول ۱ مشاهده شد روش های گوناگونی جهت مقابله با حمله های احتمالی ابداع شده اند به نحوی که ارائه دهندگان ابر از بابت حفاظت داده های شخصی و سازمانی کاربران آسوده باشند. اما این روش ها کامل نیستند. سیستمی که بتواند در مقیاس های بزرگتر به طرز مناسب و کارآمد کار کند، مقیاس پذیر است. این ویژگی باعث می شود عملکرد کلی با افزودن منابع سخت افزاری افزایش یابد. IDSهای مقیاس پذیر می توانند در محیط های بزرگتر و با سخت افزار بیشتر نیز کار کنند. در سیستم تشخیص نفوذ پیشنهادی با بهره گیری از تکنیک تشخیص ناهمگون هزینه پردازشی و حافظه ای کاهش یافته و به دلیل مقیاس پذیر بودن از سرعت بالایی نیز برخوردار خواهد بود.

منابع

Aljarah, I. And Ludwig, S. A. (۲۰۱۳). MapReduce Intrusion Detection System based on a Particle Swarm Optimization Clustering Algorithm. ۲۰۱۳ IEEE Congress on Evolutionary Computation Conference (IEEE CEC'۱۳).

Arora, P. , Wadhawan, R. C. And Ahuja, S. P. (۲۰۱۲). Cloud Computing Security Issues in Infrastructure as a Service. International Journal of Advanced Research in Computer Science and Software Engineering.

Boss, G. , Malladi, P. , Quan, D. , Leregni, L. And Hall, H. (۲۰۰۷). Cloud Computing, " IBM Corporation, White Paper.

Che, J. , Duan, Y. , Zhang, T. And Fan, J. (۲۰۱۱). Study on the security models and strategies of cloud computing. ۲۰۱۱ International Conference on Power Electronics and Engineering Application. pp. ٥٨٦ – ٥٩٣.

Gupta, P. And Kaliyar, P. (۲۰۱۳). History Aware Anomaly Based IDS for Cloud IaaS. INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY. pp. ۱۷۷۹-۱۷۸٤.

Gupta, S. , Kumar, P. And Abraham, A. (۲۰۱۳). A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment. International Journal of Distributed Sensor Networks.

Hassan, Q. F. , Riad, A. M. And Hassan, A. E. (۲۰۱۲). Software reuse in the emerging cloud computing era. pp. ۲۰٤–۲۲۷. doi:۱۰,٤۰۱۸/۹۷۸-۱-٤٦٦٦-۰۸۹۷-۹.ch۰۰۹. ISBN ۹۷۸-۱-٤٦٦٦-۰۸۹۷-۹. Retrieved ۲۰۱٤.

He, J. , Tang, Ch. , Yang, Y. And Qiao, Y. (۲۰۱۲). ۳D-IDS: IaaS user-oriented Intrusion Detection System. ۲۰۱۲ Fourth International Symposium on Information Science and Engineering (ISISE). pp. ۱۲-۱٥.

Holtz, M. D. , David, B. M. , Timoteo, R. And Junior, S. (۲۰۱۱). Building Scalable Distributed Intrusion Detection Systems Based on the MapReduce Framework. pp. ۲۲-۳۱.

Jeong, H. J. , Hyun, W. , Lim, J. And You, I. (۲۰۱۲). Anomaly Teletraffic Intrusion Detection Systems on Hadoop-Based Platforms : A Survey of Some Problems and Solutions. ۲۰۱۲ ۱٥th IEEE International Conference on Network-Based Information Systems(NbiS). pp. ۷٦٦-۷۷۰.

Kholidy, H. A. And Baiardi, F. (۲۰۱۲). CIDS: A framework for Intrusion Detection in Cloud Systems. ۲۰۱۲ Ninth International Conference on Information Technology- New Generations (ITNG). pp. ۳۷۹-۳۸٥.

Manavi, S. , Mohammadalian, S. , Udzir, N. I. And Abdullah, A. (۲۰۱۲). Secure Model for Virtualization Layer in Cloud Infrastructure. International Journal of Cyber-Security and Digital Forensics (IJCSDF) ۱(۱). pp. ۳۲-٤۰.

Mell, P. And Grance, T. (۲۰۱۱). The NIST Definition of Cloud Computing. National Institute of Standards and Technology (NIST), Standard Definition ۲۰۰۸.

Okuhara, M. , Shiozaki, T. And Suzuki, T. (۲۰۱۰). Security Architecture for cloud computing. pp. ۳۹۷-٤۰۲.

Sathya, A. And Vasanthraj, K. (۲۰۱۳). Network Activity Classification Schema in IDS and Log Audit for Cloud Computing. ۲۰۱۳ International Conf. on Information Communication and Embedded Systems (ICICES). pp. ٥۰۲-٥۰٦.

Taghavi Zargar, S. , Takabi, H. And Joshi, J. B.D. (۲۰۱۱). DCDIDP: A Distributed, Collaborative, and Data-driven Intrusion Detection and Prevention Framework for Cloud Computing Environments. CollaborateCom ۲۰۱۱, Orlando, Florida, USA.

Tanenbaum, A. S. and Wetherall, D. J. (۲۰۰۳). Computer Networks, ٤th ed.:Prentice Hall.

Yang, Sh. , Chen, W. And Wang, Y. (۲۰۱۱). ICAS: AN INTER-VM IDS LOG CLOUD ANALYSIS SYSTEM. ۲۰۱۱ IEEE International Conference. pp. ۲۸٥-۲۸۹.