نهمین همایش پژوهش های نوین در علوم و فناوری
تابستان ۱۳۹۶
Summer 2017
Conference on Recent Research in Science and Technology

بررسی سیستم تشخیص نفوذ و حمله های انکار سرویس در رایانش ابری

آزاده دانش پرور[۱]، مهدی جوانمرد[۲]

آزاده دانش پرور،کارشناسی ارشد مهندسی کامپیوتر نرم افزار ،دانشگاه پیام نور،صندوق پستی 19395-3697تهران، ایران
Azadehdaneshparvar@yahoo.com
مهدی جوانمرد،استادیار،گروه مهندسی کامپیوتر و فناوری اطلاعات،دانشگاه پیام نور،صندوق پستی 19395-3697تهران، ایران
info@javanmard.com

چکیده

رایانش ابری مفهومی انقلابی است که باعث دگرگونی فناوری اطلاعات و ارتباطات شده است ، این مفهوم منابع محاسباتی را در سراسر شبکه اینترنت در اختیار کاربران قرار می دهد . رایانش ابری در صورت نیاز سیستم منابع ارزان و قیاسی را فراهم می آورد و در نتیجه نیازی به سرمایه گذاری دریک سیستم عظیم کامپیوتری وجود نخواهد داشت . با این وجود در این فن آوری نوین امنیت یکی از بزرگترین دغدغه ها تلقی می شود در ابر ، سیستم های بیشتری برای حفاظت وجود دارد ، نقاط محتمل تری از ورودی ، درگاه های بیشتری برای اتصال و همچنین نقاط ارتباطی درونی بیشتری و متعاقبا امنیت در ابر در مقایسه با سیستم های قدیمی حیاتی تر خواهد بود . حمله DOS در ایمنی شبکه یکی از مشکلات شایع و متداول است .حمله DOS زمان بارگیری سرور را افزایش می دهد و باعث می شود سیستم خارج از دسترس قرار گیرد . جلوگیری کامل از بروز حملات DDOS که از شایع ترین انواع حملات DOS هستند ، امکان پذیر نیست ، بنابراین شناسایی این حملات گامی مهم در حفظ ایمنی سرور در برابر این نوع از تهدید امنیتی بسیار مرسوم است .

کلمات کلیدی: سیستم تشخیص نفوذ، DDOS، DOS، رایانش ابری، مجازی سازی

۱. مقدمه

امروزه رایانش ابری[۱] به دلیل خدمات انعطاف‌پذیر و ویژگی مبتنی بر پرداخت به ازای هر استفاده ، انتخاب هر سازمان فناوری اطلاعات و ارتباطات است. با این وجود امنیت و حریم شخصی سیستم‌های رایانش ابری به دلیل معماری توزیع شده‌ی آن‌ها و آسیب‌پذیری در برابر ورودی‌های ناخواسته مشکل اساسی رایانش ابری است. سیستم شناسایی ورودی ناخواسته، رایج‌ترین مکانیزم شناسایی در برابر حمله است[۱]. با پیشرفت فناوری اطلاعات انجام کارهای محاسباتی در هر زمان و مکانی اهمیت بیشتری پیدا کرده است. همچنین نیاز است که افراد بتوانند کارهای محاسباتی سنگین خود را بدون داشتن سخت‌افزارها و نرم‌افزارهای گران، از طریق خدماتی انجام دهند. رایانش ابری آخرین پاسخ فناوری به این نیازها است[۲]. معماری ابر، یک معماری توزیع‌شده و باز است که به عنوان هدف مناسب برای ورودهای ناخواسته در نظر گرفته می‌شود. بنابر این امنیت محیط

[1] **Cloud Computing**

ابری هنگامی‌که حمله‌های شبکه‌ای و حمله‌های خاص ابر، کاربران ابر را تهدید می‌کنند درخطر است. بیشترین حمله‌ها بر مبنای شبکه بر امنیت ابر در لایه‌ی شبکه تأثیر می‌گذارد.

پروتکل تفکیک آدرس، جعل کردن پروتکل آدرس اینترنت، اختلال سامانه نام دامنه یا اسکن پورت پروتکل اطلاعات مسیریابی، ارائه کردن خدمات حمله منع سرویس[1] و عدم دسترسی توزیع‌شده حملات مربوط به خدمات، سیستم‌های امنیتی شبکه‌ای سنتی مانند دیوار آتشین بهترین روش‌های متوقف کردن حملات بیرونی هستند اما حمله‌های درونی و حمله‌های پیچیده‌ی بیرونی نمی‌توانند به‌راحتی با این مکانیسم‌ها برطرف شوند. این روش که در آن سیستم‌های شناسایی حمله‌های ناخواسته وارد عمل می‌شود. نقش سیستم‌های شناسایی حمله‌های ناخواسته در امنیت ابر بسیار مهم است زیرا مانند یک لایه‌ی پیشگیرانه‌ی امنیتی عمل می‌کند و علاوه بر شناسایی حمله های شناخته شده می تواند بسیاری از حمله‌های ناشناخته را کشف کند [۳].

۲. رایانش ابری

رایانش ابری به مدلی گفته می‌شود که دسترسی کاربران را بر اساس نوع تقاضایی که از منابع اطلاعاتی و رایانشی دارند، آسان می‌کند. این مدل سعی دارد با کمترین نیاز به منابع نیروی انسانی و کاهش هزینه‌ها و افزایش سرعت دسترسی به اطلاعات، پاسخگوی نیاز کاربران باشد. از آنجایی که این فناوری دوران ابتدایی خود را می‌گذراند، هنوز تعریف استاندارد علمی که مورد قبول عام باشد برای آن ارائه نشده است، اما بیشتر صاحب نظران بر روی قسمت‌هایی از تعاریف این مفهوم هم نظر می‌باشند. موسسه‌ی ملی فناوری و استانداردها[2]، رایانش ابری را این‌گونه تعریف می‌کند [۱]:

رایانش ابری مدلی است برای فراهم کردن دسترسی آسان بر اساس تقاضای کاربر از طریق شبکه به مجموعه‌ای از منابع رایانشی قابل‌تغییر و پیکربندی مثل: شبکه‌ها، سرورها، فضای ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها که این دسترسی بتواند با کمترین نیاز به مدیریت منابع و یا نیاز به دخالت مستقیم فراهم کننده سرویس به سرعت فراهم شده یا آزاد گردد[۴].

۳. سیستم تشخیص نفوذ در رایانش ابری

در محیط رایانش ابری به‌کارگیری سیستم‌های شناسایی و جلوگیری[3] از ورودهای ناخواسته نمی‌تواند به سطح مورد نظر امنیت و عملکرد دست یابد زیرا الگوی معماری رایانش ابری نیاز به گسترش یک سیستم تشخیص نفوذ و جلوگیری از حمله را دارد و بر اساس ویژگی‌های ابر طراحی شده است. هدف سیستم ها تشخیص نفوذ جلوگیری از آن نیست بلکه تشخیص‌نفوذ و البته ضعف های سیستم کلی و گزارش آن به مدیر سیستم است. در واقع سیستم های تشخیص نفوذ نخستین خط دفاعی در مقابل نفوذهای احتمالی می باشند[۵].

۳-۱ : نمونه هایی از حمله‌های مورداستفاده در سیستم‌های تشخیص نفوذ در رایانش ابری

- حمله‌های پهنای باند[4]

این نوع حمله‌ها تمامی پهنای باند هدف را با حجم‌های انبوهی از بسته‌های داده، مورد استفاده قرار می‌دهند و به دلیل آنکه درخواست‌های عادی نمی‌توانند پاسخ‌های سریع و عملکردی دریافت کنند منجر به رد پذیرش سرویس می‌شود. در این پژوهش از حمله HTTP به‌عنوان نماینده مناسبی برای EDOS[5] های مصرفی پهنای باند استفاده می‌کنیم.

---

[1] **Denial of Service attack**
[2] **National Institute of Standards and Technology (NIST)**
[3] **Detection Prevention System**
[4] **Bandwidth Consuming**
[5] **Economic Denial of Sustainability**

- حملاتی که اپلیکیشن‌های ویژه‌ای را مورد هدف قرار می‌دهند

این نوع حمله‌ها برنامه‌های کاربردی خاصی را در سرور هدف‌گیری می‌کند، در محیط رایانش ابری هر برنامه کاربردی می‌تواند در یک ماشین مجازی اجرا شود، بنابراین در یک سناریوی حمله، مهاجم تلاش می‌کند با حمله به VM[1] ویژه‌ای که حاوی برنامه کاربردی خاصی است به سرور آسیب برساند در پژوهش پیش رو از پایگاه‌داده به‌عنوان حمله‌ای که برنامه‌های کاربردی خاصی را هدف‌گیری می‌کند، انتخاب می‌شود. ماشین مجازی که به پایگاه‌داده اختصاص داده شده درخواست‌های پایگاه‌داده‌ای بسیاری را برای هر درخواست HTTP در مورد حمله‌های پایگاه‌داده دریافت می‌کند.

- حمله‌های مربوط به لایه اتصال

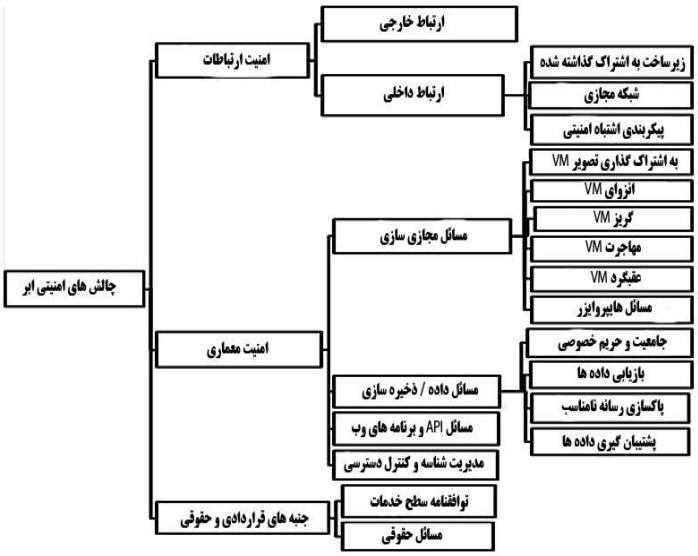
این نوع حمله‌ها سهمی در استفاده از جریان پروتکل دارد، حمله‌های جریان ICMP نمونه‌هایی از حمله‌های مربوط به لایه اتصال هستند. ازآنجایی‌که این حمله‌ها به هنگام برقراری ارتباط بین کاربر و سرور رخ می‌دهد، این گروه به حمله‌های مربوط به لایه اتصال نامیده می‌شوند و به‌عنوان نماینده حمله‌های مربوط به لایه اتصال در این پژوهش، حمله جریان TCP SYN نام‌گذاری می‌شوند که یکی از مهم‌ترین موضوعات در حوزه امنیت است. حمله‌های جریان DNS برای نمونه ای از حملات DDOS در نظر گرفته می‌شوند که باعث از کار افتادن سیستم و یا بالا رفتن پردازش می‌گردد. حمله کنندگان تعداد زیادی از بسته های پرس‌وجو را به DNS در زمان کوتاه می فرستند. سرور باید به تمام درخواست های پرس و جو پاسخ دهد. درنتیجه DNS نمی‌تواند سرویس را برای کاربران مجاز فراهم کند[۶].

۳-۲ : چالش‌های امنیتی رایانش ابری

خصوصیات و مدل‌های رایانش ابری مزبور سرویس‌های بهبودیافته، بهینه‌شده و کم‌هزینه‌ای را در اختیار مشتریان قرار می‌دهند. مدل‌های عنوان‌شده فوق که خصوصیات مزبور رادارند با فناوری‌های مختلفی مثل مجازی‌سازی و چند مالکیتی اجرا و پیاده‌سازی می‌شوند. فناوری‌های سرویس ابری و مدل‌های گسترش آسیب‌پذیری‌ها و ریسک‌های خاص ابری را به همراه داشته بعلاوه ریسک و خطرات مشترکی با زیرساخت سنتی فناوری اطلاعات. ریسک‌های امنیتی در محیط ابری با ریسک‌های سنتی زیرساخت IT چه ازلحاظ ماهیت و چه ازلحاظ شدت و یا هردو متفاوت است[۷]. ادغام منبع امکان استفاده از یک مجموعه توسط چند کاربر را از طریق فناوری‌های مجازی‌سازی و چند مالکیتی میسر می‌سازد. علیرغم آنکه فناوری‌ها الاستیسیته سریع و مدیریت بهینه منابع دارند، ریسک‌های خاصی نیز در سیستم ایجاد می‌کنند. چند مالکیتی به ریسک قابلیت رؤیت داده‌ها برای سایر کاربران و دنباله و رد عملیات ختم می‌شود. به‌واسطه واسط‌های کاربری مدیریت تحت وب که احتمال دسترسی غیرمجاز به واسط کاربری مدیریت در آن بیشتر از سیستم‌های سنتی است، خصیصه خودیاوری برحسب تقاضا را ارائه می‌دهد. محیط مجازی نیز مجموعه‌ی خاص خود از خطرات و آسیب‌پذیری‌ها را داشته که شامل تبانی بین ماشین‌های مجازی و رهایی و گریز ماشین‌های مجازی می‌شود. مدل‌های سرویس از منظر مدل سرویس ابری به یکدیگر وابسته‌اند. اپلیکیشن های SaaS در PaaS ساخته و گسترش‌یافته و PaaS به IaaS بنیادین وابسته است. این وابستگی عملیاتی مدل‌های سرویس به یکدیگر منجر به وابستگی امنیتی نیز می‌شود. مثلاً اگر مهاجمی موفق شود که کنترل IaaS را به دست گیرد، نتیجه PaaS به خطر افتاده‌ای خواهد بود که از IaaS استفاده می‌کند.PaaS به خطر افتاده به SaaS به خطر افتاده ختم می‌شود. درمجموع، تمام مدل‌های سرویس به خطر افتاده امکان دسترسی به لایه دیگری از مدل سرویس را میسر می‌سازند. مدل گسترش ابر خصوصی همین مجموعه از آسیب‌پذیری‌های زیرساخت سنتی IT را دارد؛ که دلیلش این است که ابر خصوصی برای کاربرد یک تک سازمان است. ابرهای عمومی، اجتماعی و ترکیبی به خاطر حضور کاربرانی با منشأهای مختلف و کنترل اجرایی یک شخص ثالث ریسک‌ها و آسیب‌پذیری‌ها خاص ابری بیشتری دارند. حضور چند مالک با استفاده از منابع مجازی معادل همان منابع فیزیکی دغدغه‌ها و نگرانی‌های امنیتی زیادی به همراه دارد. تفکیک کامل مالکین مختلف و منابع تخصیص‌یافته کار پیچیده‌ای است و میزان امنیت

[1] **Virtual Machine**

به‌مراتب بیشتری می‌طلبد. برخی از فناوری‌های رایانش ابری تأثیری بر هیچ‌کدام از مدل‌های سرویس نمی‌گذارند. بلکه بیشتر از یک مدل تحت تأثیر قرار می‌گیرد، مانند مجازی‌سازی که هم بر IaaS تأثیر گذاشته و هم بر PaaS؛ بنابراین به‌طور خلاصه و صرف‌نظر از مدل سرویس به چالش‌های موجود می‌پردازیم[۷]. دسته بندی چالش‌های امنیتی رایانش ابری در شکل۳-۱ مشاهده می‌شود[۸].



۳-۱ چالش‌های امنیتی ابر[۸].

۴. شبکه مجازی

فعالیت‌های ارتباطی در سیستم‌های محاسبات ابری نه‌فقط در شبکه‌های واقعی بلکه در شبکه‌های مجازی نیز نقش مهمی در ارتباط ایفا می‌کنند. شبکه مجازی شبکه منطقی است که در یک شبکه فیزیکی ساخته می‌شود. شبکه‌های مجازی مسئول ارتباط بین ماشین‌های مجازی (VM ها) هستند. مؤلفه‌های نرم‌افزاری شبکه مانند پل‌ها، مسیریاب‌ها و پیکربندی‌های تحت نرم‌افزار شبکه از شبکه کردن VM ها در یک هاست پشتیبانی می‌کنند. شبکه‌های مجازی چالش‌های امنیتی زیر را در محیط ابری به وجود می‌آورند. مکانیسم‌های امنیتی و محافظ در شبکه فیزیکی امکان مانیتور کردن ترافیک در شبکه مجازی را ندارند؛ که چالش جدی بشمار می‌آید از آن نظر که فعالیت‌های مخرب VM ها فراتر از مانیتورینگ ابزار امنیتی می‌رود. مکانیسم‌های تشخیص حمله و تجاوز و پیشگیری معمولاً به الگوهای ترافیک و فعالیت‌های قضاوت ناهنجاری‌ها و تشخیص احتمال حمله بستگی دارد. شبکه مجازی مانعی سر راه هدف این قبیل اقدامات پیشگیرانه ایجاد می‌کند. شبکه مجازی میان چند ماشین مجازی به اشتراک گذاشته‌شده و احتمال حملات خاصی مانند رد سرویس (DoS)، کلاه‌برداری شبکه مجازی می‌شود. نرخ ترافیک برای اهداف بدطینتانه پایش می‌گردد. کلیدهای رمزنگاری نسبت به درز اطلاعات آسیب‌پذیر هستند. داده‌های متعلق به کاربران که در حال انتقال هستند از رخنه‌ها و نقض‌های پرهزینه‌ای رنج می‌برند[۹].

خلاصه‌ای از فنون IDS/IPS موجود باقدرت و محدودیت‌هایشان ارائه داده‌شده است[۱۰]

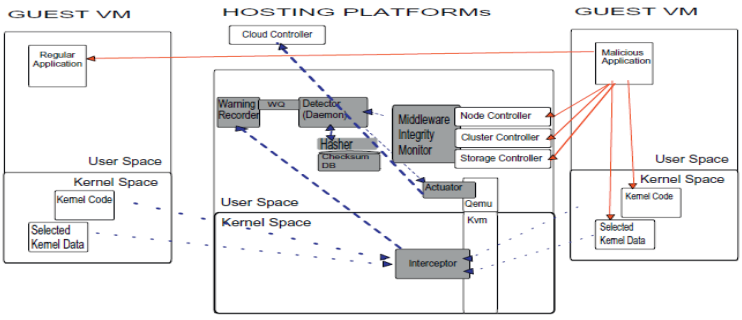
خلاصه فنون IDS/IPS		
فنون IDS/IPS	خصوصیات/ مزیت‌ها	محدودیت‌ها/ چالش‌ها
شناسایی سو استفاده	تداخل را با تطبیق الگوهای گرفته‌شده با مبنای دانش از پیش پیکربندی‌شده تشخیص می‌دهد دقت شناسایی بالا برای مهاجم‌های از پیش شناخته‌شده. هزینه محاسباتی پایین	نمی‌تواند مهاجم‌های جدید یا انواع مهاجم‌های شناخته‌شده را شناسایی کند. مبنای دانش برای تطبیق باید به‌دقت بررسی شود. میزان اخطار نادرست زیاد برای مهاجم‌های ناشناخته
شناسایی غیرمتعارف	آزمون‌های آماری را بر وضعیت جمع‌آوری‌شده برای تشخیص تداخل مورداستفاده قرار می‌دهد می‌تواند میزان اخطار نادرست را برای مهاجم‌های ناشناخته کم نماید	زمان زیادی برای تشخیص مهاجم‌ها نیاز است تشخیص دقت بر اساس میزان وضعیت جمع‌آوری‌شده با ویژگی‌ها
IDS بر مبنای ANN	بسته شبکه ساختاربندی نشده را به‌طور مؤثر دسته‌بندی می‌کند لایه‌های پنهان چندگانه در ANN کارایی دسته‌بندی را افزایش می‌دهد	نیاز به زمان زیادی در مرحله آموزش دارد تعداد نمونه زیادی برای آموزش به‌طور مؤثر نیاز است دارای انعطاف‌پذیری کمتری است
IDS بر مبنای منطق فازی	برای ویژگی‌های کمی استفاده می‌شود انعطاف‌پذیری بهتری را برای مسائل غیرقطعی فراهم می‌کند	دقت شناسایی کمتر از ANN است

IDSبرمبنای قوانین پیوسته	برای شناسایی تصدیق مهاجم شناخته‌شده با مهاجم‌های آشکار در شناسایی سو استفاده می‌شود	نمی‌تواند برای همه مهاجم‌های ناشناخته استفاده شود نیاز به تعداد بیشتری اسکن پایگاه داده برای ایجاد احکام دارد فقط برای شناسایی سو استفاده، استفاده می‌شود.
IDS بر مبنای SVM	می‌تواند به‌درستی تداخل‌ها را دسته‌بندی کند، اگر داده‌های نمونه محدودشده فراهم شود. می‌تواند تعداد انبوهی از ویژگی‌ها را دست‌کاری کند.	می‌تواند فقط ویژگی‌های گسسته را دسته‌بندی کند؛ بنابراین پیش‌پردازش این ویژگی‌ها قبل از کاربرد نیاز است
IDS بر مبنای GA	برای انتخاب بهترین ویژگی‌ها برای شناسایی استفاده می‌شود ویژگی بهتری دارد	روش پیچیده‌ای دارد در وضعیت ویژه نسبت به‌کل استفاده می‌شود.
فنون هیبرید	شیوه‌ای کارآمد برای دسته‌بندی احکام به‌دقت را دارد	هزینه محاسباتی بالایی دارد

۵. پیشینه و بررسی حمله های صورت گرفته بر روی سیستم های تشخیص نفوذ :

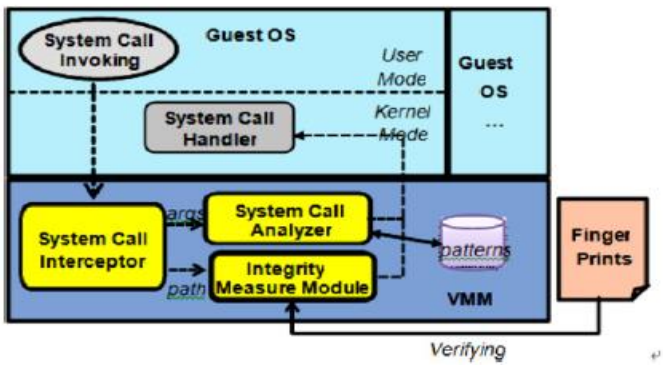
لومباردی و همکاران سیستم پیشرفته محافظت ابری (ACPS) را پیشنهاد کرده که معماری روش پیشنهادی در شکل ۵-۱ نشان داده شده است. هدفش ایجاد امنیت بیشتر برای منابع ابری است. سرویس‌های امنیتی مختلفی برای منابع CSP توسط ACPS ارائه شده است که حملات علیه کاربر و داده‌های CSP از جمله این سرویس‌ها می‌باشد. حملات چند مالکی نیز با مانیتورینگ پایدار VM های اجراشده در پلتفرم میزبان خنثی می‌گردد. افزون بر آنکه، ACPS قابلیت حسابرسی برای عملیات ماشین‌های مجازی نیز دارد. در پلت فرم میزبان ACPS به چند ماژول تقسیم می‌گردد. ماژول جداکننده مسئول شناسایی فعالیت‌های مشکوک در پلت‌فرم میزبان است. فعالیت‌های مشکوک شناسایی‌شده با ماژول ثبت‌کننده هشدار ثبت شده و درمجموعه هشدار ذخیره می‌شوند. ارزیابی فعالیت‌های ثبت‌شده بر عهده ارزیاب است. افزایش نرخ تولید هشدارها به عنوان خطر امنیتی تلقی شده که ماژول محرک را برای واکنش نشان دادن مطابق با سیاست‌های امنیتی فعال می‌کند. مجموعه‌های مقابله‌ای برای زیرساخت بحرانی و شاخص از جمله شبکه در زمان شروع توسط ACPS مشخص می‌شود. وضعیت و حالت زیرساخت

به‌صورت ناهم‌زمان توسط محاسبه مجدد مجموعه مقابله‌ای برای اهداف بررسی‌شده مشخص می‌گردد. در صورت وجود ناهنجاری‌ها، هشدارها برای ارزیاب فرستاده می‌شوند. بررسی دوره‌ای و متناوب مجموعه مقابله‌ای نیز نقاط ورودی ابری را تحت پایش پایدار و ثابت نگه می‌دارد. جهت جلوگیری از حمله در زیرساخت شبکه، ACPS از متد ریستنپارت و همکاران استفاده کرده که در آن جستجوی شبکه با جدول‌های IP و هشدارهای ثبت‌شده درمجموعه هشدار شناسایی می‌گردد. علاوه بر تأمین امنیت شبکه و زیرساخت حیاتی، ACPS امنیت در مقابل حملات داده‌ای و ماشین‌های مجازی مخرب را نیز تأمین می‌کند. یکی از مهم‌ترین خصیصه‌های ACPS این است که برای VM ها شفاف و غیرقابل تشخیص باقی می‌ماند. ماژول جداساز برای جلوگیری از شناسایی‌اش هیچ درخواست فراخوانی سیستمی را مسدود نمی‌کند. هرچند اگر فعالیت حمله تایید شود، آنگاه اقدامی صورت می‌گیرد. امکان اجرای فرمان فراخوانی سیستم اولیه حملات زمان‌بندی را برای شناسایی سیستم‌های مانیتورینگ خنثی می‌سازد. نمونه اولیه ACPS در Eucalyptus و OpenECP پیاده‌سازی شده که سیستم‌های ابری منبع باز هستند [۱۱].



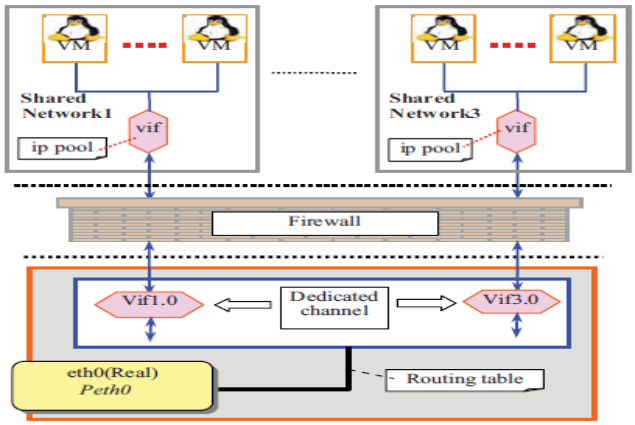
شکل۵-۱: معماری روش پیشنهادی لومباردی و همکاران [۱۱].

جیانگسن و همکارانش ابزار امنیتی را برای محاسبات ابری پیشنهاد داده به نام سایبرگاردر (CyberGuarder) که از طریق گسترش ادوات شبکه مجازی امنیت شبکه مجازی را تأمین می‌کند. معماری داخلی روش پیشنهادی در شکل ۵-۲ نشاد داده شده است.افزون بر آنکه، با استفاده از تونل دولایه شبکه خصوصی مجازی (VPN) بین پل‌های مجازی تفکیک شبکه مجازی مطرح می‌گردد. داده‌ها بین VM ها به شیوه نظیر به نظیر (P2P) و بدون عبور از سرور مرکزی ارسال می‌شوند. هرچند متاداده‌ها در گره مرکزی برای ترافیک بهینه‌شده بین VMM ها ذخیره می‌گردند. پورت‌های نرم‌افزاری برای مانیتور نمودن ترافیک شبکه طراحی‌شده‌اند. سیستم‌های سنتی امنیت شبکه مانند سیستم تشخیص تهاجم (IDS) برای تأمین امنیت اپلیکیشن های اجرایی در شبکه مجازی گسترش می‌یابند. ضمن آنکه سایبرگاردر از طریق بررسی جامعیت اپلیکیشن ها و مانتیورینگ فراخوانی سیستم توسط اپلیکیشن ها امنیت VM را تأمین می‌کند. نتایج تجربی سربارى ۱۰ درصدی در عملکرد (بازده) ناشی از سایبرگاردر و افزایش ۵ درصدی در مصرف انرژی را نشان دادند[۱۲].



شکل ۵-۲: معماری داخلی CyberGuarder VM [۱۲].

دینگ و همکاران مدل شبکه مجازی را ارائه نموده که از شبکه‌های مجازی درمقابل حملات جعل و کلاه‌برداری محافظت می‌کند. هایپروایزر Xen مدل پیشنهادی را نشان می‌دهد و مدل پیشنهادی از هردو حالت پل و روت هایپروایزر Xen برای پیکربندی شبکه مجازی استفاده می‌کند. در حالت پل،Xen مستقیماً VM را به پل اترنت مجازی متصل می‌کند. پل در عوض به شبکه فیزیکی متصل می‌شود. حالت روت لینک P2P بین ماشین مجازی و دامین 0 ایجاد می‌کند. مدل پیشنهادی به سه لایه الف. روتینگ (مسیریابی)، ب. دیوار آتش و ج. لایه شبکه مشترک (به اشتراک گذاشته‌شده) تقسیم می‌شود. لایه روتینگ کانال منطقی اختصاصی بین شبکه مجازی و فیزیکی ایجاد می‌کند. برای هر کانال یک ID منطقی منحصربه‌فرد تعیین‌شده که برای مانیتور کردن منبع بسته‌هایی بکار می‌رود که از شبکه مشترک نشأت می‌گیرند. لایه دیوار آتش مسئول حفظ امنیت درمقابل حملات جعل شبکه به اشتراک گذاشته شده است. این لایه تضمین می‌کند که هر واسط مجازی متصل شده به شبکه مجازی مشترک با هیچ‌کدام از شبکه‌های مشترک مجازی ارتباط برقرار نکند. مانیتورینگ بر اساس ID های منطقی انجام‌گرفته که لایه روتینگ تعیین می‌کند. ثانیاً، لایه دیوار آتش امکان به روز رسانی بسته‌های داده در جدول روتینگ را ندارد. تمامی این بسته‌ها حذف می‌شوند. لایه شبکه به اشتراک گذاشته از ارتباط بین VM های متعلق به کانال‌های شبکه مجازی ممانعت به عمل می‌آورد [۱۳].معماری مدل ارائه شده در شکل ۵-۳ آورده شده است.

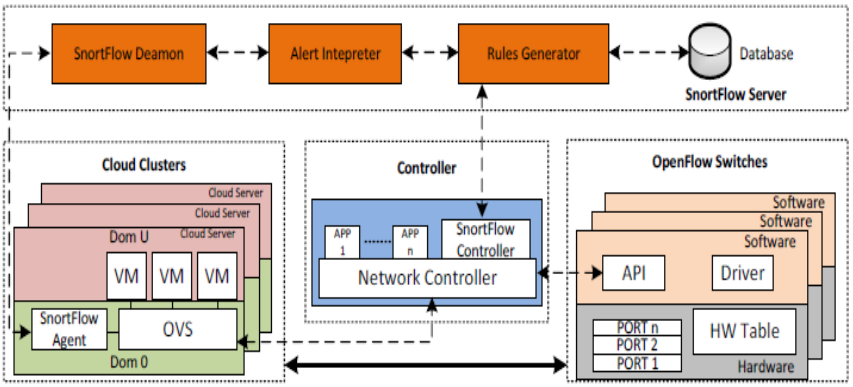


شکل ۵-۳ مدل شبکه مجازی ارائه‌شده[۱۳].

مورائزو همکاران تکنیکی بنام DCPortalsNg را برای تفکیک شبکه‌های مجازی در انواع ماشین‌های مجازی (VM ها) ارائه نمود. تکنیکی که از متد شبکه تعریف‌شده توسط نرم‌افزار (SDN) برای تفکیک شبکه مجازی استفاده می‌کند. DCPortalsNg از طریق plug in نوترونی با مجموعه انباشته باز تعامل برقرار نموده و به تمام اطلاعات موردنیاز شبکه مجازی دست می‌یابد. سپس داده‌های خود را از شبکه‌های ترسیم برای مالکین شبکه ایجاد می‌کند. درنتیجه شناسه منحصربه‌فردی برای تمام ماشین‌های مجازی تعیین می‌شود. مفهوم بازنویسی بسته داده در تفکیک شبکه استفاده‌شده که بسته اصلی را بازکرده و آدرس‌های مبدأ و مقصد را از بسته استخراج می‌کند. بسته‌های داده‌ای که مقصد یک شبکه هستند بیشتر پردازش‌شده درحالی‌که سایر بسته‌ها حذف می‌شوند. درصورتی‌که انتقال و ارسالی معتبر باشد پیام OpenFlow به سوئیچ مجازی درست ارسال‌شده تا بسته را با آدرس‌های مبدأ/مقصدی بازنویسی کند که با شناسه‌ها جایگزین شدند. افزون بر آنکه، آدرس‌های فیزیکی میزبان جایگزین آدرس‌های MAC دیگر می‌شوند. این امر از حمله چند مالک در شبکه مجازی جلوگیری می‌کند. ترافیک تنها در تکنیک پیشنهادی توسط آدرس‌های MAC کنترل می‌شود. تکنیک پیشنهادی از حمله DoS جلوگیری می‌کند[۱۴].

ژینگ و همکاران سیستمی بنام SnortFlow برای جلوگیری حمله در محیط ابری ارائه نمودند. در شکل ۵-۴ معماری سیستم SnortFlow نشان داده شده است. سیستم SnortFlow از ویژگی‌های سیستم‌های Snort و OpenFlow بهره می‌برد. نمونه اولیه SnowFlow در ابر تحت Xen ساخته و تست می‌شود. ترافیک مشکوک با مؤلفه‌ای بنام snortFlow جمع‌آوری می‌شود. آژیر در مفسر هشدار قرارگرفته که آن را آنالیز کرده و مولد قوانین را می‌طلبد. مولد قوانین، قوانین را برای ترافیک مشکوک

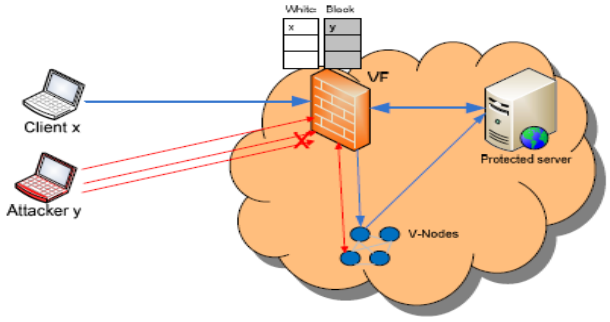
توسعه داده و آن‌ها را به ابزار openflow می‌فرستد. سیستم Openflow شبکه را مطابق با قوانین توسعه‌یافته مجدد پیکربندی می‌کند. ارزیابی SnowFlow عملکرد خوبی برحسب تحلیل ترافیک و پیشگیری علیه تهاجم نشان می‌دهد[۱۵].



شکل ۵-۴: معماری سیستم SnortFlow [۱۵].

اسکوآلی و دیگران رویکردی را به نام EDOS-Shield برای کاهش حمله‌های EDOS در رایانش ابری پیشنهاد داده‌اند. در شکل ۵-۵ معماری روش را ملاحضه می‌نمایید.

آن‌ها درخواست‌های دریافتی از جانب کاربر را به دو گروه طبقه‌بندی کرده‌اند: درخواست کاهش و درخواست افزایش با درخواست BOT ها. آن‌ها از یک تغییردهنده استفاده می‌کنند و اولین درخواست از یک IP جدید را به این تغییردهنده ارسال می‌کنند. تغییردهنده روندی از تغییرات را انجام داده و آدرس مورد نظر را علاوه بر لیست سیاه در لیست سفید نیز قرار می‌دهد. این فهرست‌ها مربوط به درخواست‌های مجاز و درخواست‌های کلیBOT ها هستند. درخواست‌های متعاقب که از IP آدرس‌های موجود در لیست سیاه آمده‌اند با یک دیوار امنیتی مجازی بلاک می‌شوند و درخواست‌های متعاقب از IP آدرس‌های لیست سفید می‌توانند با سرویس‌های ابر ارتباط برقرار کنند تا بتوانند خدمات مورد نیازشان را دریافت کنند [۱۶].



شکل ۵-۵: پیشنهاد معماری EDoSسپر برای کاهش EDoS [۱۶].

۶. نتیجه‌گیری

در این مقاله روش های شناسایی حمله انکار سرویس در رایانش ابری مورد بررسی قرار گرفت و روش های جلوگیری آن ها نیز گفته شد. با برر سی این گونه حمله ها و آ سیب پذیری رایانش ابری در برابر حمله های DOS و DDOS که حتی به صورت حمله هایی از نوع اقتصادی نیز می گردد که EDOS نام دارند. مورد بررسی قرار گرفت . با استفاده از این روشها و تحقیق های صورت گرفته می توان برای جلوگیری از انواع حمله ها بر روی رایانش ابری استفاده نمود. مجازی سازی یکی از بهترین روشها در رایانش ابری میباشد که با بررسی حمله ها کارایی آن بیشتر مورد تایید بوده است .

مراجع

[1] Y. Mehmood, M. A. Shibli, U. Habiba, and R. Masood, "Intrusion detection system in cloud computing: Challenges and opportunities," in *Information Assurance (NCIA), 2nd National Conference on*, pp. 59-66, 2013.

[2] P. Mell and T. Grance, "The NIST definition of cloud computing," *Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg*, 2011.

[3] C. N. Modi, D. R. Patel, A. Patel, and R. Muttukrishnan, "Bayesian Classifier and Snort based network intrusion detection system in cloud computing," in *Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on* pp. 1-7, 2012.

[4] S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in cloud computing," in *2010 Information Security for South Africa*, pp. 1-7, 2010.

[5] R. Bace and P. Mell, "NIST special publication on intrusion detection systems," DTIC Document,2001

[6] H. Debar, "An introduction to intrusion-detection systems," *Proceedings of Connect*, 2000.

[7] M. D. Ryan, "Cloud computing security: The scientific challenge, and a survey of solutions," *Journal of Systems and Software*, vol. 86, pp. 2263-2268, 2013.

[8] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Information Sciences*, vol. 305, pp. 357-383, 2015

[9] F. Durao, J. F. S. Carvalho, A. Fonseka, and V. C. Garcia, "A systematic review on cloud computing," *The Journal of Supercomputing*, vol. 68, pp. 1321-1346, 2014.

[10] S. K. Mohiddin and S. B. Yalavarthi, "Research Challenges in the Emerging trends of Cloud Computing." International Journal of Advances in Computer Science and Technology (IJACST), Vol. 4 No.1, Pages : 01 – 07, 2015.

[11] F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," *Journal of Network and Computer Applications*, vol. 34, pp. 1113-1122, 2011.

[12] J. Li, B. Li, T. Wo, C. Hu, J. Huai, L. Liu, *et al.*, "CyberGuarder: A virtualization security assurance architecture for green cloud computing," *Future Generation Computer Systems*, vol. 28, pp. 379-390, 2012.

[13] H. Wu, Y. Ding, C. Winer, and L. Yao, "Network security for virtual machine in cloud computing," in *Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on*, pp. 18-21, 2010.

[14] H. M. Moraes, R. V. Nunes, and D. Guedes, "DCPortalsNg: Efficient isolation of tenant networks in virtualized datacenters," *Proc. 13th ICN*, 2014.

[15] T. Xing, D. Huang, L. Xu, C.-J. Chung, and P. Khatkar, "Snortflow: A openflow-based intrusion prevention system in cloud environment," in *Research and Educational Experiment Workshop (GREE), 2013 Second GENI*, pp. 89-92, 2013.

[16] M. H. Sqalli, F. Al-Haidari, and K. Salah, "Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing," in *Utility and cloud computing (UCC), 2011 Fourth IEEE International Conference on*, pp. 49-56, 2011.