تحقیقی از روش های تشخیص نفوذ در ابر

چکیده- رایانش ابری خدمات مورد تقاضای مقیاس پذیر و مجازی را برای کاربران نهایی با انعطاف‌پذیری بیشتر و سرمایه‌گذاری زیرساختی کمتر فراهم می‌کند. این خدمات با استفاده از اینترنتی که از پروتکل‌های شبکه‌ای شناخته ش ده، استانداردها و قالب بندی‌هایی با نظارت مدیریت های مختلف است. اشکالات و آسیب پذیری های موجود در تکنولوژی‌های پایه و پروتکل‌های برجا مانده سبب بازگشایی دروازه‌هایی برای اختلال می‌شود. این مقاله پیمایشی را بر تداخل های مختلف که بر دسترسی، محرمیت و انسجام منابع و خدمات ابری اثر گذار است انجام می‌دهد. پیشنهادات سیستم‌های شناسایی تداخل های مشترک (IDS) را در محیط ابری آزمون می‌کند و انواع و فنون مختلف IDS و سیستم‌های ممانعت از تداخل ها (IPS) را مورد بحث قرار می‌دهد و بر توزیع IDS/IPS در ساختار ابری توصیه‌هایی برای دستیابی به امنیت مطلوب در شبکه‌های نسل بعدی دارد.

کلمات کلیدی: راینش ابری، فایروال ها، سیستم تشخیص نفوذ، سیستم پیشگیری از نفوذ

۱- مقدمه

رایانش ابری با هدف تامین راحتی، تقاضا براساس نیاز، دسترسی به شبکه برای اشتراک منابع محاسباتی قابل پیکر بندی (مانند شبکه ها، سرورها، حافظه ها، برنامه های کاربردی کامپیوتری (اپلیکیشن ها) و خدمات) فراهم شده است، که می تواند به سرعت بازبینی شود و از حداقل فعالیت مدیریتی یا کنش های تامین کننده خدمات به دور باشد. محیط ابری خدمات را به شکل های مختلف ارائه می دهد: نرم افزار به عنوان یک سرویس SaaS (مثل Google Apps، اپلیکیشن های گوگل)، پلتفرم به عنوان یک سرویس PaaS (مثل موتور جستجوی اپلیکیشن گوگل Google App Engine)، Microsoft's Azure و زیرساخت به عنوان یک سرویس IaaS (Service-Iaas) مثل خدمات وبسایتی آمازون (AWS، اوکالیپتوس (Eucalyptus) ، Open Nebula.

همانگونه که خدمات ابری از طریق اینترنت بازرسی می شود، امنیت و حریم خصوصی خدمات ابری مسائل کلیدی هستند که باید مورد توجه باشند. بررسی موسسه داده های بین المللی (IDC) نشان داد که امنیت بزرگترین چالش رایانش ابری است. اوراق سفید اخیر امنیت محاسبات ابری توسط بخش امنیت سایبری لاکهید مارتین نشان می دهد که نگرانی عمده از امنیت بعد از امنیت اطلاعات، تشخیص و ممانعت از نفوذ در زیرساخت های ابری است. زیرساخت های ابری روش های مجازی سازی، فناوری های یکپارچه و اجرا از طریق پروتکل های استاندارد اینترنتی است. این موارد ممکن است سبب جذب مزاحم به دلیل آسیب پذیری های دخیل در آن باشد.

محاسبات ابری همچنین به سبب حملات قدیمی مختلف از قبیل جعل نشانی IP، جعل آرپ، حمله پروتکل اطلاعات مسیریابی، مسمومیت DNS، جریان، منع سرویس (DoS)، منع سرویس توزیع شده (DDoS) و غیره مثل حمله DoS به زیرساخت ابری آمازون سبب BitBucket.org شد که یک سایت در هاست AWS برای چند ساعت غیر قابل دسترس باقی می ماند. همانطور که در [۱۲] نشان داده شد، محاسبه هزینه با استفاده از روش های کنونی رمز نگاری نمی تواند بر محیط ابری غالب شود. فایروال (دیوار آتشین) می تواند گزینه خوبی برای ممانعت از حملات بیرونی باشد اما برای حملات داخلی کارایی ندارد. سیستم های تشخیص نفوذ (IDS) و سیستم های ممانعت از نفوذ (IPS) باید همراه با زیر ساخت ابری باشد تا این حملات را کاهش دهد.

ادامه مقاله به صورت ذیل سازماندهی شده است. بخش ۲ بر حملات تداخل قابل کاربرد در محیط ابری بحث می کند. فایروال های سنتی به عنوان راه حل امنیتی هستند که به طور مختصر در بخش ۳ بحث شد. بخش ۴ روش های مختلفی را برای IDS/IPS ارائه می دهد و بخش ۵ انواع IDS/IPS موجود و کار مشخص محیط ابری را در IDS بررسی می کند. بخش ۶ در انتها با مراجع به نتیجه گیری می پردازد.

۲- تداخل ها برای سیستم های ابری

این بخش چندین تداخل معمول را نشان می دهد که سبب دسترسی، محرمیت و مسائل منسجم برای منابع و خدمات ابری می شود.

A. حمله داخلی

کاربران ابری مجاز ممکن است برای به دست آوردن (و سوء استفاده) امتیازات غیر مجاز تلاش نمایند. مهاجم های داخلی ممکن است مرتکب کلاهبرداری و فاش نمودن اطلاعات به دیگران (یا تخریب عمدی اطلاعات) شوند. این برایند مسئولیتی جدی را در بر دارد. برای مثال، یک حمله DoS داخلی بر علیه ابر منعطف آمازون نشان داده شده است.

B. حملات طغیانی

در اینجا، مهاجم سعی بر آن دارد که طعمه را با ارسال تعداد بیشماری از بسته هایی از هاست بی ضرر (زامبی ها) در شبکه درگیر نماید. بسته ها می تواند در انواع TCP، UDP، ICMP یا ترکیبی از آنها باشد. این نوع حمله ممکن است به سبب اتصالات شبکه ای غیر قانونی باشد.

در محیط ابری تقاضا برای ماشین های مجازی ها توسط هر کسی از طریق اینترنت قابل دستیابی است که ممکن است سبب حمله DoS (یا DDoS) از طریق زامبی ها شود. حمله سیلابی بر دسترسی به خدمات توسط کاربر مجاز اثر می گذارد. با حمله به یک سرور تامین کننده خدمات خاص، مهاجم می تواند سبب کاهش دسترسی به خدمات مورد هدف شود. چنین حمله ایف حمله مستقیم DoS می شود. اگر منابع سخت افزاری سرور به طور کامل با پردازش تقاضاهای سیلابی تهی شود، جایگزین های خدماتی دیگر بر همان ماشین سخت افزاری به طور طولانی مدت قادر به وظایف هدف خود نیستند. این نوع حمله توزیع شده حمله غیر مستقیم نامیده می شود.

حمله سیلابی ممکن است به طور موثر صورت های مفید را افزایش دهد به طوریکه محیط ابری قادر به تشخیص بین کاربری معمول و جعلی نشود.

C- کاربر با حملات اساسی

در اینجا مهاجم به اکانت (حساب) کاربر مجاز با تشخیص پسورد دستیابی دارد و آن را قادر به استخراج اطلاعات محرمانه برای دستیابی به سطح روت (پایه) برای سیستم می کند. برای مثال بوفر (میانگیر) سابقا برای تولید پوسته های پایه از پردازش در حال اجرای روت ایجاد شده است. این وقتی اتفاق می افتد که کد برنامه کاربردی با میانگیر (بوفر) آماری پر می شود. مکانیزمهایی برای تامین پردازش تصدیقی استفاده می شود که هدف مکرری است از انجاییکه هیچ مکانیزم امنیت استاندارد جهانی وجود ندارد که بتواند برای ممانعت از خطرات امنیتی مثل جریان های کاری بازیابی ضعیف رمز، گزارشهای کلیدی و غیره.

در مورد محیط ابری، مهاجم نیاز به دستیابی به جایگزین های کاربری معتبر دارد که قادر باشد به دسترسی سطح روت (پایه) برای VM ها یا میزبان دست یابد.

D- اسکن پورت (مسیر یابی)

مسیریابی فهرستی از پورت های باز، پورت های بسته و پورت های فیلتر شده را فراهم می کند. از طریق مسیر یابی مهاجم می تواند پورت های باز را بیابد و به سرویس های در حال اجرا در این پورت ها حمله نماید. جزییات مربوط به شبکه از قبیل آدرس IP، آدرس MAC، روتر، فیلترینگ ورودی، دستورهای فایروال و غیره می تواند از این طریق این حمله شناخته شود. فنون مسیر یابی مختلفی مثل اسکن TCP، اسکن UDP، اسکن SYN، اسکن FIN، اسکن ACK، اسکن ویندوز (همانند اسکن ACK است اما هر تغییری را در زمینه ویندوز بسته بررسی می کند) و غیره وجود دارد. در مورد مساله محیط ابری مهاجم می تواند به سرویس های ارایه شده (با شناسایی پورتهای باز از طریق این سرویس های فراهم شده) از طریق اسکن پورت (مسیر یابی) حمله نماید.

E. حمله به ماشین مجازی (VM) یا فوق مجازی

با سازش کردن به فوق مجازی لایه های پایین تر، مهاجم می تواند VM های نصب شده را کنترل نماید مثل BLUEPILL، SubVir و DKSM که حملات به خوبی شناخته شده در لایه مجازی هستند. از طریق این حملات، هکرها می توانند با فوق مجازی نصب شده سازش نموده تا بر کنترل بر میزبان دست یابند.

آسیب پذیری های جدید از قبیل آسیب پذیری روز صفر در ماشین های مجازی (VMها) یافت شده است که مهاجم برای دستیابی به VM های فوق مجازی یا نصب شده آن را مورد حمله قرار می دهد. یک آسیب پذیری روز صفر وضعیتی است که تلاش می کند که آسیب پذیری های برنامه ای را استخراج کند که برای دیگران یا توسعه دهنده نرم افزار ناشناخته است. استخراج روز صفر توسط مهاجمان قبل از اینکه توسعه دهنده نرم افزار هدف در مورد آسیب پذیری آن بداند استفاده شده است. یک آسیب پذیری روز صفر در برنامه مجازی HyperVM استخراج شد که سبب تخریب سرورهای مجازی بر پایه وب سایت بسیاری گردید.

F. حملات کانالی پنهانی

حمله انفعالی به هکرها اجازه می دهد که به دسترسی کنترل شده برای گره های الوده شده دست یابند تا به اطلاعات محرمانه کاربر تراضی نمایند. با استفاده از کانالهای پنهانی، هکرهای می توانند منابع طعمه را کنترل

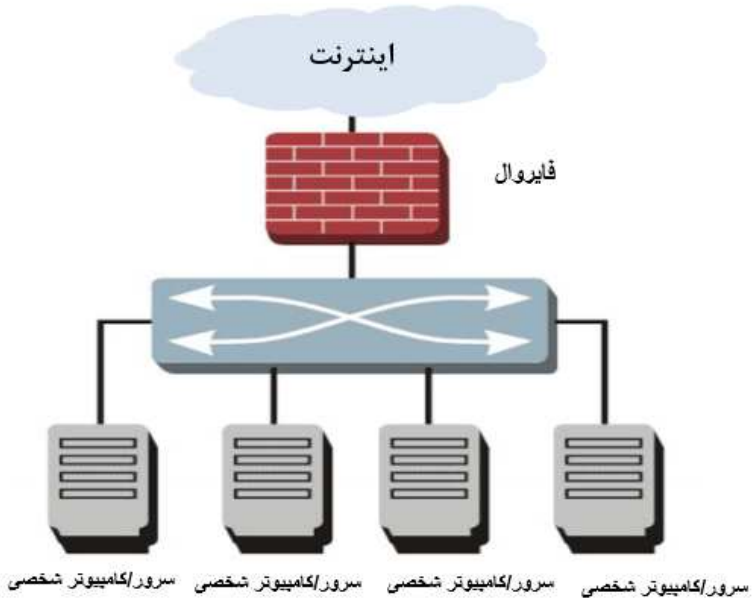
نمایند و می توانند آن را به عنوان یک زامبی بسازند تا به حمله DDoS تلاش نمایند. آن همچنین می تواند برای فاش سازی داده های محرمانه طعمه استفاده شود. به این دلیل سیستم های سازش شده به سختی با اجرای وظایف منظمشان مواجه می شوند. در محیط ابری، مهاجم می تواند به دسترسی و کنترل منابع کاربران ابری از طریق کانال پنهانی دست یابد و VM را به عنوان برای زامبی برای آغاز حمله DoS/DDoS می سازد.

برای ماجمان داخلی، راه حل های بازرسی گذرگاه های غیر مجاز تایید شده می تواند به طور بهینه استفاده شود. برای ممانعت از حمله بر VM/فوق مجازی، بر خلاف قاعده فنون بازرسی گذرگاه های غیر مجاز پایه می تواند استفاده شود. برای حمله ظغیانی و حمله کانالی پنهانی یا بازرسی گذرگاهیی غیر مجاز یا فنون بازرسی گذرگاهی غیر مجاز پایه می تواند مورد استفاده قرار گیرد. فایروال (در محیط ابری) می تواند راه حل معمول برای ممانعت از برخی حملات فهرست شده در بالا باشد. چندین فن بازرسی گذرگاهیی غیر مجاز در بخش ۴ بحث می شود.

۳- فایروال ها: راه حلی عام برای گذرگاه های غیر مجاز

فایروال از نقاط دسترسی رو به جلوی سیستم محافظت می کند و به عنوان خط مقدم دفاعی عمل می کند. فایروالها پیش از این پروتکل ها، پورت ها یا ادرس های IP را رد یا قبول می کردند. که آن ترافیک ورودی را بر اساس سیاست از پیش تعریف شده دایورت یا معطوف می کنند. نصف وایروال پایه در شکل ۱ نشان داده شده است که در نقطه ورودی سرورها نصب شده است. چندین نوع فایروال در منبع ۱۹ مورد بحث قرار گرفته است.

شکل ۲- نصب فایروال پایه



جدول ۱- خلاصه ای از فایروال ها	
نوع فایروال	خلاصه
بسته اماری فیلتر کننده فایروال ها	به بسته فقط اجازه یا رد بازرسی فقط اطلاعات اصلی از قبیل آدرس منبع و مقصد، تعداد پورت ها و غیره را می دهد. کد نادرست را در بسته ها شناسایی نمی کند نمی تواند در مقابل حقه بازی و حمله متلاشی کننده ممانعت کند.
بسته وضعی فیلتر کننده فایروال ها	استفاده شده در محیط سرور مشتری که مشتری تقاضا را آغاز می کند و سرور اجازه عبور احکام فایروال را می دهد نیاز به منابع اضافی مثل حافظه برای فهرست های کیفی حفظ شده در سخت افزار یا نرم افزار دارد
بازرسی کیفی فایروال ها	شکل ارتقا یافته بسته کیفی فیلتر کننده فایر وال ها برای برنامه هایی مثل FTP استفاده می شود که پورت های چند گانه را مورد استفاده قرار می دهد ظرفیت باری را آزمون می کند و پورت ها را در هر پروتکل باز یا بسته می کند
فایروال های پروکسی	میتواند شبکه داخلی را از اینترنت جدا کند ترکیب پروتکل را با شکست ارتباط مشتری/سرور تحلیل می کند نیاز به تعداد زیادی منابع شبکه دارد.

در جدول I ما خلاصه ای از فایروال های مختلف استفاده شده در شبکه را با هدف امنیتی فراهم نمودیم. وقتی که فایروال بسته های شبکه را در مرز شبکه شناسایی می کند، مهاجم های داخلی نمی تواند توسط فایروال های قدیمی شناسایی شود. تعدادی از ماجم های DoS یا DDoS همچنین پیچیدگی زیادی برای شناسایی با استفاده از فایروالهای قدیمی دارند. به عنوان مثال اگر مهاجمی در پورت ۸۰ وجود دارد (سرویس وب)، فایروال های نمی توانند ترافیک خوب را از ترافیک مهاجمی DoS تشخیص دهند.

راه حل دیگر پیوستن IDS یا IPS در محیط ابری است. اما کارامدی IDS/IPS بستگی به پارامترهایی مثل فنون استفاده شده در IDS ، موقعیتش در شبکه ، پیکربندی اش و غیره دارد.

۴- فنون IDS و IPS: سیر تکاملی

فنون IDS/IPS قدیمی همچون شناسایی بر پایه امضا، شناسایی غیر متعارف، شناسایی بر پایه جاسوسی جعلی (AI) و غیره می تواند برای محیط ابری استفاده شود.

A. شناسایی بر پایه امضا

شناسایی گذرگاه های غیر مجاز بر پایه امضا تلاش بر تعریف مجموعه قواعد یا تصدیق یا دانش پیش تعریف شده دارد که بتواند برای الگوی داده شده که یک مزاحم است تصمیم بگیرد. به عنوان یک نتیجه، سیستم های بر مبنای امضا قادر به دستیابی به سطوح بالای دقت و حداقل تعداد قطعیت های غیر مجاز در تشخیص هر گذرگاه های غیر مجاز قطعی هستند. تنوع اندک در مهاجم های شناخته شده ممکن است همچنین بر تحلیل اثر گذارد اگر سیستم شناسایی کاملا پیکره بندی نشده باشد. بنابراین شناسایی بر مبنای امضا راه حلی موثر برای شناسایی مهاجم های شناخته شده است اما برای شناسایی مهاجم های ناشناخته یا انواع مهاجم های شناخته شده ناقص است. یکی از دلایل محرک برای استفاده از شناسایی ببر پایه امضا راحتی در حفظ و به روز سازی احکام پیش پیکره بندی شده است. این امضاها مشتمل بر چندین جز است که ترافیک را تشخیص می دهد. برای مثال در SNORT بخشی از امضا در سر صفحه است (مثل آدرس منبع، آدرس مقصد، پورت ها) و گزینه هایش (مثل پی لود، متادیتا) که برای تعیین متناظرهای ترافیکی شیکه برای یک امضای شناخته شده استفاده می شود. داستاوان و همکارانش برخی برایندهای سیستم ممانعت گذرگاه های غیر مجاز را ارائه داده و چهرچوب های محتمل مختلفی نشان دادند.

در محیط ابری، فن شناسایی تداخل بر پایه امضا می تواند برای شناسایی مهاجم شناخته شده استفاده شود. آن می تواند در انتهای محیط ابری برای شناسایی گذرگاه های غیر مجاز خارجی با در ابتدای محیط ابری برای گذرگاه های غیر مجاز خارجی/داخلی استفاده شود. مثل شبکه قدیمی، آن نمی تواند برای شناسایی حملات ناشناخته در محیط ابری استفاده شود. شیوه های ارائه شده در منابع ۵۶، ۵۷، ۵۹ و ۶۲ سیستم شناسایی گذرگاه های غیر مجاز بر پایه امضا را برای شناسایی گذرگاه های غیر مجاز در VM ها ارائه می دهد (انتهای محیط ابری). این شیوه ها در بخش بعدی بحث شده است.

B. شناسایی غیر متعارف

شناسایی غیر متعارف (وضعیتی) مربوط به تشخیص وقایعی است که به نظر می رسد در رابطه با وضعیت سیستمی بهنجار غیر عادی باشد. انواع گسترده ای از فنون شامل دیتا یابی، مدلسازی آماری و مدل های مارکوف پنهان به عنوان روش های مختلف برای رسیدن به مشکلات شناسایی غیر متعارف بیان شده است. رسیدگی بر پایه غیر متعارف در جمع اوری داده های مربوط به وضعیت کاربران مجاز در یک دوره زمانی دخالت دارد و سپس آزمون های آماری را برای وضعیت مشاهده شده به کار می گیرد که تعیین می کند وضعیت مجاز است یا خیر. مزیت شناسایی مهاجم های این است که در گذشته یافت نشده است. جز کلیدی برای استفاده از این شیوه به طور موثر ایجاد احکامی است که بتواند میزان اخطار خطا را برای مهاجم های ناشناخته همانند شناخته شده ها پایین تر آورد.

دوتکویچ و همکارن راه حلی بر پایه غیر متعارف برای ممانعت از تداخل در سیستم فوری (ریل تایم) فراهم نمودند که پروتکلی را بر پایه ترافیک چند بعدی و حمله تحلیل می کند. اما یک شیب بهینه سازی برای کاهش تعداد IPS وجود دارد. ژگ بینگ و همکارانش سیستم شناسایی تداخل سیک برای شناسایی تداخل به صورت فوری ارائه داد، به طور موثر و کارامد. در این کار، فنون پروفایل وضعیتی و دیتاکاوی به طور خودکار برای شناسایی حملات مساعی حفظ شده است.

فنون شناسایی غیر متعارف می تواند برای محیط ابری برای شناسایی حملات ناشناخته در سطوح مختلف استفاده می شود. در محیط ابری، تعداد وقایع زیادی رخ می دهد (سطح شبکه یا سطح سیستم) که نمایش یا کنترل آنها

را با استفاده از فنون شناسایی غیر متعارف مشکل می سازد. در منابع ۲۶، ۵۵، ۶۰ و ۶۱ فنون شناسایی غیر متعارف برای شناسایی تداخل ها در لایه های مختلف محیط ابری پیشنهاد شده است.

توانایی فنون محاسباتی نرم استفاده از داده های واقعی جزیی یا غیر قطعی است که انها را برای شناسایی گذرگاه های غیر مجاز محبوب می سازد. فنون محاسباتی نرم زیادی وجود دارد از قبیل شبکه عصبی مصنوعی (ANN)، منطق فازی، پیوستگی احکام کاوی، ماشین برداری پشتیبانی (SVM)، الگوریتم ژنتیکی (GA) و غیره که برای اصلاح دقت شناسایی و کارامدی IDS بر پایه امضا یا IDS بر پایه سناسایی غیر متعارف استفاده شد.

C. IDS بر پایه شبکه عصبی مصنوعی

هدف از استفاده از ANN ها برای شناسایی گذرگاه های غیر مجاز توانایی برای تولید داده ها از داده های ناقص و توانایی برای دسته بندی داده ها به عنوان ورودی های طبیعی یا غیر مجاز اشت. انواع ANN استفاده شده در IDS عبارتند از: شبکه های عصبی بازخورد چند لایه (MLFF)، مشاهده چند لایه (MLP) و انتشار پی گشت (BP).

کندی یک شبکه عصبی سه لایه برای شناسایی سو استفاده در شبکه پیشنهاد کرد. ویژگی برداری استفاده شده مشتمل بر ۹ ویژگی شبکه ای بود (پروتکل ID، پورت منبع، پورت مقصد، آدرس IP منبع، آدرس IP مقصد، نوع ICMP، کد ICMP، طول داده های خام، داده های خام). اما دقت شناسایی تداخل خیلی پایین است. مولفان منبع ۳۸ IDS بر مبنای MLP را ارائه دادند. آنها نشان دادند که گنجایش لایه های پنهان بیشتر دقت شناسایی IDS را افزایش می دهد. این شیوه دقت شناسایی شیوه پیشنهاد شده در منبع ۳۷ را اصلاح می کند. گرادیاگا و همکاران سرعت یافتن متوالی تداخل با MLP و نقشه خود سازمان (SOM) را مقایسه کرد و نشان داد که SOM دقت شناسایی بالایی نسبت به ANN دارد. او ادعا کرد که شبکه عصبی زمان بر توزیع شده (DTDNN) دقت شناسایی بالاتری برای اغلب مهاجم های شبکه ای دارد. DTDNN راه حلی ساده و کارامد برای دسته بندی داده ها با سرعت بالا و سرعت تبدیل سریع دارد. اما دقت این شیوه می تواند با ترکیب آن با دیگر فنون محاسباتی ذکر شده در بالا اصلاح شود.

IDS بر پایه ANN راه حلی کارامد برای داده های شبکه ای ساختار بندی نشده است. دقت شناسایی گذرگاه های غیر مجاز این شیوه بر پایه تعداد لایه های پنهان و فار آموزش ANN است. اما نیاز به نمونه های آموزش و زمان برای یادگیری موثر ANN دارد.

استفاده از IDS بر پایه ANN به تنهایی نمی تواند راه حل موثری برای شناسایی تداخل برای محیط ابری باشد و نیاز به مکانیزم سریع شناسایی تداخل دارد. شیوه پیشنهاد شده در منبع ۵۵ استفاده از فنون شناسایی غیر متعارف بر مبنای ANN برای محیط ابری است مه نیازمند نمونه های آموزش بیشتر همچنین زمان بیشتر برای شناسایی موثر گذرگاه های غیر مجاز به طور موثر است.

D. IDS بر مبنای منطق فازی

منطق فازی می تواند برای بهره مندی از تفاسیر نادرست گذرگاه های غیر مجاز استفاده شود. مقداری انعطاف پذیری برای مسایل غیر قطعی شناسایی تداخل فراهم می کند.

تیلا پارت و همکارن IDS فازی (FIDS) را برای تداخل های شبکه ای مثل SYN و سیلاب های UDP، آهنگ مرگ، بمب E-mail، حدس زدن پسورد FTP/Talent و اسکن پورت پیشنهاد دادند. استنتاج از شبکه عصبی فازی (EFuNN) که در منبع معرفی شده است برای کاهش زمان آموزش ANN است. آن ترکیبی از آموزش پشتیبانی شده و غیر پشتیبانی شده را استفاده می کند. نتایج آزمایشی نشان می دهد که استفاده از تعداد کاهش یافته ورودی های EFuNN دقت دسته بندی بهتری برای IDS نسبت به استفاده از ANN به تنهایی دارد. شیوه های ۴۰ و ۴۱ نمی تواند به صورت فوری برای شناسایی گذرگاه های غیر مجاز شبکه همچون زمان آموزش که معنی دار است مورد استفاده قرار گیرد. احکام پیوستگی فازی در منبع ۴۲ ارائه شده است که برای شناسایی تداخل شبکه ای به صورت فوری استفاده شده است. دو مجموعه احکام بوجود آمده وجود دارد که به طور انلاین از آموزش داده ها استخراج شده است. ویژگی هایی برای مقایسه از سرفصل بسته شبکه ای استفاده شده است. این شیوه برای مهاجم های بزرگ مقیاس از قبیل DoS/DDoS استفاده شده است.

برای کاهش زمان آموزش ANN، منطق فازی یا ANN می تواند برای شناسایی سریع مهاجم های ناشناخته در محیط ابری استفاده شود.

E. IDS بر پایه احکام پیوسته

برخی از مهاجم های تداخلی بر پایه مهاجم های شناخته شده یا تنوع مهاجم های شناخته شده تشکیل شده اند. برای شناسایی چنین تصدیق ها یا مهاجم ها، الگوریتم استقرایی تصدیقی می تواند استفاده شود که می تواند مجموعه غالب از مجموعه حملات را بیابد (شامل برخی ویژگی های حمله اصلی).

هان و همکاران در منبع ۴۳ شناسایی تداخل را بر مبنای شبکه با استفاده از فن داده کاوی پیشنهاد کرد. در این شیوه، الگوریتم بر پایه امضا امضایی را برای شناسایی سو استفاده تولید می کند. اما اشکال الگوریتم پیشنهاد شده مصرف زمانی آن برای اسکن پایگاه داده برای تولید امضا می باشد. مولفان در منبع ۴۴ مساله زمانی اسکن پایگاه داده آزمون شده در منبع ۴۳ را مرتفع کردند. آنها اسکن کاهش الگوریتم را برای کاهش تعداد اسکن پایگاه داده برای تولید موثر امضا با حملات از مهاجم های از پیش شناخته شده پیشنهاد دادند. اما آن دارای میزان اخطار مثبت نادرست بالایی است از انجاییکه برخی الگوهای جال توجه حذف شده ات و الگوهای ناخواسته تولید شده است. لی و همکارانش الگوریتم استقرایی را بر پایه کاهش طول پشتیبانی برای شناسایی گذرگاه های غیر مجاز برای کاهش تولید الگوی کوتاه همانطور که در منابع ۴۳ و ۴۴ مشتق شده است پیشنهاد کردند و برخی الگوهای مورد توجه را پذیرفتند. آن نسبت به دیگر شیوه ها بر پایه استقرایی سریعتر است.

در محیط ابری احکام پیوسته می تواند برای تولید تصدیق های جدید استفاده شود. با استفاده از تصدیق های جدیدا ایجاد شده، انواع مهاجم های شناخته شده می تواند بلادرنگ شناسایی شود.

F. IDS بر پایه ماشینی برداری پشتیبانی (SVW)

SVW برای شناسایی تداخل ها بر پایه داده های نمونه محدود شده استفاده شده است که ابعاد داده ها دقت را تحت تاثیر قرار نمی دهد.

در منبع ۴۶ نشان داده شده است که نتایج در رابطه با میزان مثبت نادرستی در مورد SVW در مقایسه با ANN بهتر است، از آنجاییکه ANN نیاز به مقادیر بالاتری از نمونه های آموزش برای دسته بندی موثر دارد در حالیکه SVM با پارامترهای کمتری تنظیم می شود. اما SVM فقط برای داده های دو تایی استفاده می شود. با وجود این دقت شناسایی می تواند با ترکیب SVM با دیگر فنون اصلاح شود. لی و لوی یک مدل هوشمند برای سیستم ممانعت از تداخل شبکه ای با ترکیب SNORT و فایروال قابل پیکربندی طراحی کردند. طبقه بندی کننده ماشین

برداری پشتیبانی (SVM) همچنین با SNORT استفاده شده است تا میزان اخطار نادرست را کاهش دهد و دقت IPS را اصلاح کند. اما عملکرد نتایج هنوز ارزیابی نشده است.

در محیط ابری اگر داده های نمونه های محدود شده برای شناسایی تداخل ها داده شود نسبت به استفاده از SVM راه حل موثری نسبت به ANN است، از آنجاییکه ابعاد داده های به طور موثری بر دقت IDS بر پایه SVM اثر ندارد.

G. IDS بر پایه الگوریتم ژنتیکی (GA)

الگوریتم های ژنتیکی (GAها) برای انتخاب ویژگی های شبکه یا برای تعیین پارامترهای بهینه استفاده شده است که می تواند در فنون دیگر برای دستیابی به نتایج بهینه و اصلاح دقت IDS استفاده شود.

مولفان منبع ۵ هفت ویژگی را بسته محاسباتی دارای مقادیر قیاسی و عددی را مورد استفاده قرار دادند (دوره، پروتکل، پورت منبع، پورت مقصد، IP منبع، IP مقصد، نام مهاجم). آنها چهارچوبی را بر مبنای اطمینان پشتیبانی برای بزارش تابع استفاده کردند، که ساده و منعطف است. احکام ایجاد شده برای شناسایی تداخل های شبکه استفاده شده است. مقاله کمیت هایی را همچون ویژگی های قیاسی شبکه برای تولید احکام دسته بندی شده استفاده شده است. این میزان شناسایی را افزایش می دهد و دقت را اصلاح می کند. اما محدودیت این شیوه برای برازش مسایل بهتر است. لو و همکارانش شیوه ای بر پایه GP را برای ایجاد احکامی از ویژگی های شبکه ارائه دادند. آنها تایع برازش بر اساس اعتماد پشتیبانی را برای احکام مشتق شده استفاده نمودند که به طور موثری تداخل های شبکه را دسته بندی نمود. اما دوره آموزش برای تابع برازش زمان بیشتری می برد. در منبع ۵۲ تئوری اطلاعات و شیوه بر اساس GA برای شناسایی وضعیت ناهنجار استفاده شده است. آن تعداد کمتری ویژگی های شبکه را در ارتباط با مهاجم های شبکه بر مبنای اطلاعات متقابل بین ویزگی های شبکه و نوع تداخل تشخیص می دهد. اما این شیوه فقط ویژگی های مجزا را مورد توجه قرار می دهد. مولفان در منبع ۴۸ روشی را پیشنهاد کردند که برای شناسایی سو استفاده و غیر متعارف با ترکیب الگوریتم های فازی و زنتیکی استفاده شده است. الگوریتم فازی استفاده شده شامل پارامترهای کمی در شناسایی تداخل است در حالیکه الگوریتم ژنتیکی برای یافتن بهترین برازش پارامترها معرفی شده در تابع فازی رقمی مورد استفاده قرار گرفته است. این شیوه مساله برازش را بهتر حل می کند همانطور که در منبع ۴۹ نشان داده شده است در محیط ابری انتخاب پارامترهای بهینه

(ویزگی های شبکه) برای شناسایی تداخل دقت تحت IDS را افزایش خواهد داد. به این دلیل IDS بر مبنای الگوریتم ژنتیکی می تواند در محیط ابری استفاده شود.

H. فنون هیبرید

فنون هیبریدی از ترکیب دو یا تعداد بیشتری از فنون بالا استفاده می کند و دارای مزیت است از انجاییکه هر فن مزیت ها و اشکالاتی دارد.

NeGPAIM بر پایه فنون هیبرید ترکیبی از دو جز سطح پایین شامل منطق فازی برای شناسایی سواستفاده و شبکه های عصبی برای شناسایی موارد غیر متعارف است و یک جز سطح بالا که موتور مرکزی تحلیل کننده نتایج دو جز سطح پایین است. مزیت مدل این است که به بروز نمایی فعال احکام نیاز ندارد. برای اصلاح عملکرد IDS مولف در منبع ۵۴ شیوه ای ارایه می دهد که از ترکیب Naïve Bayes، ANN و دسته بندی کننده درخت تصمیم گیری (DT) بر سه مجموعه مجزا از ورودی داده استفاده می کند. خروجی مستقل از هر دسته بندی کننده ایجاد شده است و با استفاده از فن انتزاج چند گانه ترکیب شد. این شیوه از مزیت های هر دسته بندی کننده استفاده می کند و عملکرد کلی IDS را اصلاح می نماید.

مزیت استفاده از فنون محاسباتی نرم بر IDS قدیمی برای محیط ابری است. اما هر فن مزیت ها و محدودیت هایی دارد که بر عملکرد IDS اثر می گذارد. برای مثال مصرف زملنی بیشتر برای یادگیری شبکه ANN و انعطاف پذیری کمتر موانع عمده ANN هستند. ترکیب منطق فازی با فنون داده کاوی انعطاف پذیری را اصلاح می کند. GA با منطق فازی عملکرد IDS را ارتقا میدهد از آنجاییکه GA احکام برازش بهتری را برای IDS بر میگزینند. GA کارامدی بهتری برای تطبیق الگو ها دارد اما در شیوه ای خاص نسبت به کل. برای دستکاری تعداد زیادی از ویژگی های شبکه SVM ترجیح داده می شود. IDS بر اساس احکام پیوسته فقط برای مهاجم های وابسته موثر است. اما کارایی IDS بر اساس کارامدی احکام پیوسته بستگی به قاعده دانش استفاده شده دارد.

در جدول II خلاصه ای از فنون IDS/IPS موجود با قدرت و محدودیت هایشان ارائه داده شده است.

جدول II خلاصه فنون IDS/IPS		
فنون IDS/IPS	خصوصیات/ مزیت ها	محدودیت ها/ چالش ها

شناسایی سو استفاده	تداخل را با تطبیق الگوهای گرفته شده با مبنای دانش از پیش پیکربندی شده تشخیص می دهد دقت شناسایی بالا برای مهاجم های از پیش شناخته شده. هزین محاسباتی پایین	نمی تواند مهاجم های جدید یا انواع مهاجم های شناخته شده را شناسایی کند. مبنای دانش برای تطبیق باید به دقت بررسی شود. میزان اخطار نادرست زیاد برای مهاجم های ناشناخته
شناسایی غیر متعارف	آزمون های اماری را بر وضعیت جمع اوری شده برای تشخیص تداخل مورد استفاده قرار می دهد می تواند میزان اخطار نادرست را برای مهاجمهای ناشناخته کم نماید	زمان زیادی برای تشخیص مهاجم ها نیاز است تشخیص دقت بر اساس میزان وضعیت جمع آوری شده با ویژگی ها
IDS بر مبنای ANN	بسته شبکه ساختار بندی نشده را به طور موثر دسته بندی می کند لایه های پنهان چند گانه در ANN کارایی دسته بندی را افزایش می دهد	نیاز به زمان زیادی در مرحله آموزش دارد تعداد نمونه زیادی برای آموزش به طور موثر نیاز است دارای انعطاف پذیری کمتری است
IDS بر مبنای منطق فازی	برای ویژگی های کمی استفاده می شود انعطاف پذیری بهتری را برای مسائل غیر قطعی فراهم می کند	دقت شناسایی کمتر از ANN است
IDS بر مبنای احکام پیوسته	برای شناسایی تصدیق مهاجم شناخته شده با مهاجم های آشکار در شناسایی سو استفاده استفاده می شود	نمی تواند برای همه مهاجم های ناشناخته استفاده شود نیاز به تعداد بیشتری اسکن پایگاه داده برای ایجاد احکام دارد فقط برای شناسایی سو استفاده استفاده می شود.
IDS بر مبنای SVM	می تواند به درستی تداخل ها را دسته بندی کند، اگر داده های نمونه محدود شده فراهم شود. می تواند تعداد انبوهی از ویژگی ها را دستکاری کند.	می تواند فقط ویژگی های گسسته را دسته بندی کند. بنابراین پیش پردازش این ویژگی ها قبل از کاربرد نیاز است
IDS بر مبنای GA	برای انتخاب بهترین ویژگی ها برای شناسایی استفاده می شود کرایی بهتر ی دارد	روش پیچیده ای دارد در وضعیت ویژه نسبت به کل استفاده می شود.

فنون هیبرید	شیوه ای کارامد برای دسته بندی احکام به دقت را دارد	هزینه محاسباتی بالایی دارد

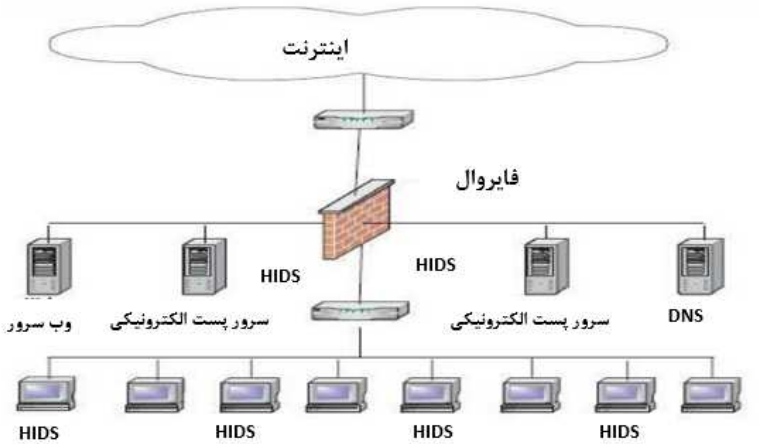
۵. انواع مختلف IDS/IPS مورد استفادع در محاسبات ابری

اساسا چهار نوع IDS استفاده شده در محیط ابری وجود دارد: سیستم شناسایی تداخل بر اساس هاست (HIDS)، سیستم شناسایی تداخل بر اساس شبکه (NIDS)، سیستم شناسایی تداخل بر اساس پشتیبانی گسترده (hypervisor) و سیستم شناسایی تداخل توزیع شده (DIDS).

A. سیستم های شناسایی تداخل بر اساس هاست (HIDS)

یک سیستم شناسایی تداخل بر اساس هاست (HIDS) سیستم شناسایی تداخلی است که اطلاعات جمع اوری شده از یک ماشین هاست ویژه را به نمایش گذاشته و تحلیل می کند. اجرای HIDS در یک ماشین هاست تداخل را برای ماشین با جمع اوری اطلاعاتی همچون سیستم فایل استفاده شده، وقایع شبکه، تماس های سیستم و غیره شناسایی می کند. HIDS تعدیل در هسته هاست، سیستم فایل هاست و وضعیت برنامه را مورد مشاهده قرار می دهد. بر اساس شناسایی انحراف از وضعیت مورد انتظار، آن وجود مهاجم را گزارش می کند. کارامدی HIDS به خصوصیات سیستم منتخب برای مانتیور بستگی دارد. در شکل ۳، برخی ماشین های هاست نصب شده با HIDS آمده است. هر HIDS تداخل برای ماشین های جایگزین شده را شناسایی می کند.

شکل ۳- سیستم شناسایی تداخل بر مبنای هاست (HIDS)

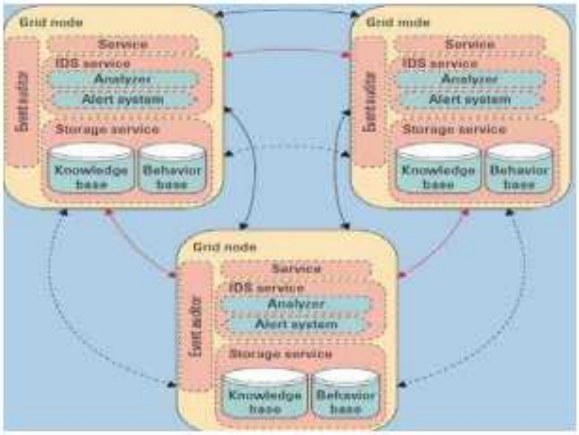


با توجه به محاسبات ابری، HIDS می تواند بر ماشین هاست، VM یا پشتیبانی گسترده قرار داده شود تا وضعیت تداخل از طریق مانیتورینگ و تحلیل log file، سیاستهای کنترل دسترسی امنیت و اطلاعات ورود کاربرمورد شناسایی قرار گیرد. اگر بر VM نصب شود ، HIDS باید با کاربر محیط ابری مانیتور شود در حالیکه در مورد نصب ان بر Hypervisor تامین کننده محیط ابری باید آن را مانتیور کند.

معماری بر اساس HIDS برای محیط ابری در منبع ۵۵ پیشنهاد شده است. در این معماری هر گره از درجه/ابری شامل IDS است که کنش بین سرویس های ارائه شده (مثل Iaas)، سرویس IDS و سرویس ذخیره را تامین می کند. همانطور که در شکل ۴ نشان داده است، سرویس IDS مشتمل بر دو جز است: سیستم تحلیل گر و سیستم اخطار. شونده واقعه داده ها را از منابع مختلف مثل لاگ های سیستم محاسبه می کند. بر پایه داده های دریافت شده توسط شنونده واقعه، سرویس IDS برای شناسایی تداخل با استفاده از فن بر پایه وضعیت یا فن بر پایه دانش استفاده شده است. فن بر پایه دانش برای شناسایی مهاجم های شناخته شده استفاده شده است در حالیکه فن بر پایه وضعیت برای شناسایی مهاجم های ناشناخته. برای شناسایی مهاجم های ناشناخته، شبکه عصبی مصنوعی (ANN) در این شیوه استفاده شده است. وقتی مهاجم یا تداخلی شناسایی شد، سیستم اخطار به دیگر گره ها اطلاع می دهد. بنابراین این شیوه برای شناسایی مهاجم های شناخته شده بر مبنای استفاده از دانش همچون مهاجم های ناشناخته با کاربرد ANN بازخوردی موثر است.

آزمایشات بیان شده در منبع ۵۵ نشان می دهد که نسبت اخطار مثبت و منفی نادرست وقتی تعداد بزرگی از نمونه های اموزش مهاجم تداخل برای روش تحلیل وضعیت استفاده می شود خیلی پایین است. محدودیت این شیوه این است که نمی تواند هر تداخل داخلی را شناسایی کند در حالیکه بر VM ها اجرا می شود.

شکل ۴- معماری IDS برای محیط صفحه/ابری



مولفان ایده ای را بر پایه نقطه تغییر برای شناسایی انواع مهاجم ها در فضای حمله پیشنهاد داده اند. این شیوه بر پایه تئوری امار و احتمال است. در این شیوه همه مهاجم ها به عنوان فضای نمونه در نظر گرفته می شوند. سپس مجموعه با استفاده از آمار بر پایه مجموعه های منحصر به فرد متقابل تجزیه می شوند. زیر مجموعه های ایجاد شده که متعلق به فضای نمونه هستند برای ایجاد الگوریتم شناسایی تداخل استفاده شده است. اما هیچ نتایج آزمایشی یا برایندهای بازبکارگیری هنوز گزارش نشده است.

B. سیستم شناسایی تداخل بر اساس شبکه (NIDS)

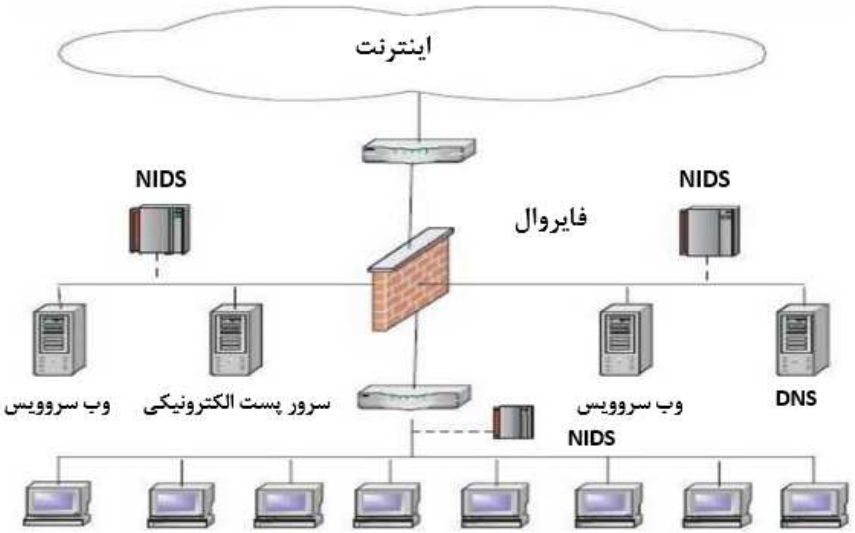
چنین سیستمی سیستم شناسایی تداخلی است که فعالیت های بد از قبیل حملات DoS، اسکن های پورت و یا حتی تلاش برای کرک به داخل کامپیوتر ها را با مانیتور نمودن ترافیک شبکه شناسایی می کند. اطلاعات جمع اوری شده از شبکه با مهاجم های شناخته شده برای شناسایی تداخل مقایسه شده است. NIDS مکانیزم شناسایی قوی تری برای شناسایی مزاحم های شبکه با مقایسه وضعیت فعلی با وضعیت مشاهده قبلی به صورت فوری دارد. NIDS اغلب IP و سر صفحه های لایه ناقل بسته را مانیتور می کند و فعالیت تداخلی را شناسایی می کند. NIDS از فنون شناسایی تداخل بر پایه غیر متعارف و بر پایه تصدیقی استفاده می کند. NIDS دارای وضوح بسیار محدود شده در ماشین های هاست است. اگر ترافیک شبکه کد شود، واقعا هیچ روش موثری برای رمز گشایی ترافیک برای تحلیل وجود ندارد.

هیمری و همکارانش درباره راه حل های امنیتی که می تواند برای شناسایی ARP فریب دهنده مهاجم ها از طریق آزمایشات و اجرا قابل کاربرد باشد پیمایشی انجام دادند. آنها به این نتیجه رسیدند که ابزار XArp 2 راه حل امنیتی قابل دسترس موثری است که می تواند به دقت ARP فریب دهنده مهاجم ها را در بین ابزارهای دیگر

شناسایی کند. با ترکیب ان با ARP تقاضا دهنده حمله ناگهانی ARP اسکن کننده مکانیزم شناسایی عملکرد ان می تواند در اینده اصلاح شود.

شکل ۵ موقعیت NIDS را در نوعی شبکه با هدف هدایت ترافیک از طریق NIDS نشان می دهد. NIDS بین فایروال و هاست های مختلف شبکه قرار داده شد.

شکل ۵- سیستم شناسایی تداخل بر مبنای شبکه

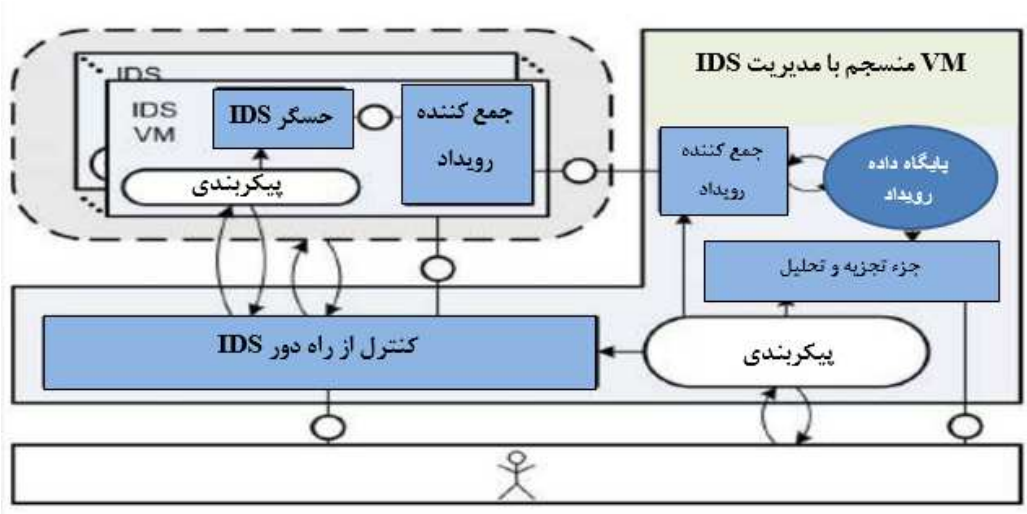


NIDS می تواند در تقابل با شبکه خارجی بر سرور محیط ابری گسترش داده شود. تا مهاجم های شبکه را بر VM ها و هایپرویژور شناسایی کند. اما چندین محدودیت دارد.NIDS نمی تواند کمک کند وقتی شروع به حمله می کند در یک شبکه مجازی که به طور کامل درون هایپرویژر است. در محیط ابری نصب NIDS مسئول تامین ابری است.

VM سازگار با معماری IDS در منبع ۵۶ پیشنهاد شده است که در شکل ۶ نمایش داده شده است. اساسا دو جز مورد استفاده در این شیوه وجود دارد: واحد مدیریت IDS و حسگر IDS. واحد مدیریت IDS مشتمل بر گرد اورنده واقعه، پایگاه داده واقعه، جز تحلیل و کنترل کننده از راه دور است. گرد اورنده واقعه وضعیت های ناجور تشخیص داده شده با حسگر IDS را جمع آوری می کند و در پایگاه داده ذخیره می کند. پایگاه داده واقعه اطلاعات را در رابطه با وقایع گرفته شده ذخیره می کند. جز تحلیلی به پایگاه داده واقعه دسترسی پیدا می کند و وقایع را

تحلیل می کند که توسط کابران پیکربندی شده است. IDS-VMs با کنترل کننده از راه دور IDS مدیریت شده است که می تواند با IDS-VMs و حسگرهای IDS ارتباط بر قرار می کند. حسگرهای IDS بر VM وضعیت بد را شناسایی و گزارش می کند و واقعه را به گرد اوورنده واقعه منتقل می کند. حسگرها می توانند با کنترل کننده از راه دور IDS، NIDS پیکر بندی کند. در این شیوه حسگرهای جدید می تواند به آسانی منسجم شود که فقط به جفت شدن فرستنده/گیرنده برای ارتباط با گرد اورنده واقعه دارد. مدیریت IDS-VM نقش کنترل، مانیتور و پیکربندی VM را دارد. مدیریت VM همچنین می تواند VM ها را بازیابی کند. این شیوه در محیط مجازی برای ممانعت از تراضی استفاده شده است. اما این شیوه نیاز به نمونه های چند گانه IDS دارد.

شکل ۶-معماری VM منسجم با مدیریت IDS



در شیوه پیشنهاد شده در منبع ۵۷، برای شناسایی حمله DDoS در VM سیستم های IDS در سوئیچ مجازی نصب شده اند تا ترافیک ورودی یا خروجی به پایگاه داده را گزارش کنند. برای شناسایی مهاجم های شناخته شده، بسته های گزارش شده تحلیل شده و بلافاصله توسط IDS با تصدیق شناخته شده مقایسه شود. IDS ماهیت مهاجم ها را تعیین می کند و به سرور مجازی اطلاع می دهد. سپس سرور مجازی بسته ها را از آدرس IP ویژه دریافت می کند. اگر نوع حمله DDoS است همه ماشین های زامبی بلوکه می شوند. سرور مجازی سپس برنامه های مورد هدف را به ماشین های دیگر هاست شده توسط مرکز داده های مجزا منتقل می کند و فهرست های در حال مسیریابی فورا به روز می شوند. فایروال در سرور جدید همه بسته ها را که از آدرس IP تشخیص داده شده

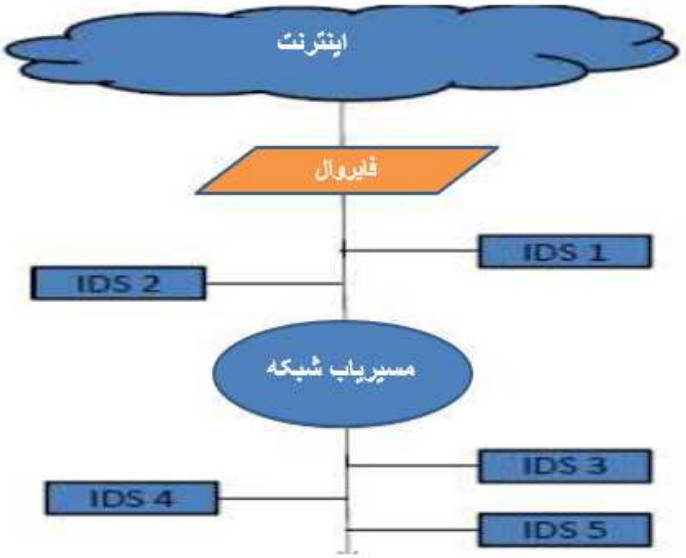
می آید بلوکه (متوقف) می کند. این شیوه می تواند حمله DDoS را در محیط مجازی بوکه نماید و می تواند سرویس های در حال اجرا در ماشین های مجازی را ایمن کند. اما نمی تواند همه انواع حملات را به صورت ابزاری که در اینجا فقط حملات شناخته شده را تشخیص می تواند شناسایی کند (SNORT).

مازارلو و همکاران شناسایی خطا را بر اساس SNORT در محیط ابری منبع eucalyptus باز ارایه دادند. در این شیوه SNORT در کنترل کننده ابری (CC) همچون ماشین های فیزیکی (هاست کردن ماشین های مجازی) برای شناسایی تداخل ها امده از شبکه خارجی گسترش یافته است. این شیوه مشکل گسترش نمونه های چند گانه IDS را همچون در منبع ۵۷ حل می کند. آن راه حلی سریع و هزینه بر است. اما می تواند فقط مهاجم های شناخته شده را شناسایی کند از انجاییکه فقط SNORT درگیر شده است.

C. سیستم توزیع شده شناسایی تداخل (DIDS)

یک IDS توزیع شده (DIDS) مشتمل بر چندین IDS است (مثل HIDS، NIDS و غیره) در یک شبکه بزرگ که همگی در ارتباط با یکدیگر هستند یا با سرور مرکزی در ارتباطند که قادر به مانتیور کردن شبکه می شود. اجزای شناسایی تداخل اطلاعات سیستم را شناسایی می کند و ان را به شکل استاندارد شده تبدیل می کند تا از تحلیلگر مرکزی بگذرد. تحلیلگر مرکزی ماشینی است که اطلاعات را از IDS چندگانه گرد آوری می کند و به صورت یکسان تحلیل می کند. ترکیب شیوه های شناسایی بر مبنای تصدیقی و غیر متعارف برای تحلیل منظور استفاده می شود. DIDS می تواند برای شناسایی مهاجم های شناخته شده و ناشناخته استفاده شود از انجاییکه دارای مزیت های NDIS و HIDS با هم است که جزیی از هر یک از انهاست. شکل ۷ نحوه کار DIDS را بیان می کند. در محیط ابری DIDS می تواند در ماشین هاست یا در پردازش سرور قرار گیرد.

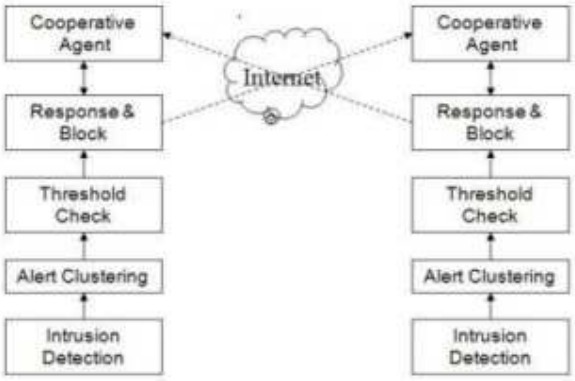
شکل ۷- سیستم شناسایی تداخل توزیع شده (DIDS)



در شیوه بر اساس عامل مشترک ، حوزه هر NIDS در هر محیط ابری در حال محاسبه منطقه گسترش یافته است که در شکل ۸ نشان داده شده است. اگر هر منطقه ابری تداخل ها را تشخیص دهد به منطقه دیگر هشدار می دهد. هر ID اخطار را به دیگری می فرستد تا شدت اخطار را تشخیص دهد. اگر مهاجم جدید شناسایی شود، حکم بلوکه کننده جدید به لیست بلوکه اضافه می شود. بنابراین این نوع شناسایی و ممانعت به مقاومت به مهاجم ها در منطقه محاسباتی ابری کمک می کند.

معماری سیستم مشتمل بر شناسایی تداخل، خوشه بندی اخطار، بررسی استانه ، پاسخ به تداخل و بلوکه کردن و عامل مشترک است. در مورد شناسایی تداخل، ان بسته مهاجم را قطع می کند، سپس پیام اخطار درباره مهاجم شناخته شده به حوزه دیگر میفرستد. حوزه خوشه بندی اخطار ، اخطار تولید شده توسط حوزه های دیگر را جمع آوری می کند. تصمیم گیری در مورد اخطار اینکه آیا درست یا نادرست است بعد از محاسبه شدت اخطارهای جمع اوری شده تشخیص داده می شود. این شیوه برای ممانعت سیستم ابری از نقطه منفرد نقص سبب شده با حمله DDoS مناسب است. اما فعالیت محاسباتی افزایش یافته است.

شکل ۸- دیاگرام بلوکه شیوه بر اساس عامل مشترک



دستجردی و همکاران روشی موثر قابل اندازه گیری و منعطف و هزینه بر را برای شناسایی تداخل برای برنامه های ابری صرفنظر از موقعیت شان با استفاده از عامل موبایل پیشنهاد دادند. این روش با هدف حمایت از VM ها است که خارج از سازمان است. عامل موبایلی اسناد یک حمله را از همه VM مورد حمله واقع شده برای تحلیل بعدی و بازرسی جمع اوری می کند. این شیوه پیش از این برای شناسایی تداخل در VM بیرون از سازمان استفاده شده است. اما بار شبکه ای بیشتری تولید می کند، اگر تعداد VM ها رسیده به عامل موبایلی افزایش یابد.

D. سیستم های شناسایی تداخل بر مبنای هایپرویژر

این سیستم یک سیتم شناسایی تداخل است که به طور ویژه برای هایپرویژر طراحی شده است. برای اجرا در لایه هایپرویژر، این نوع IDS به کاربر اجازه می دهد تا مکاتبات بین VM ها ، بین هایپرویژر و VM و درون شبکه مجازی بر اساس هایپر ویژر را مانیتور و تحلیل کند. دسترسی یه اطلاعات یکی از فواید IDS بر اساس هایپرویژر است. تازگی در تکنولوژی و فقدان تجربه چالش های ان است.

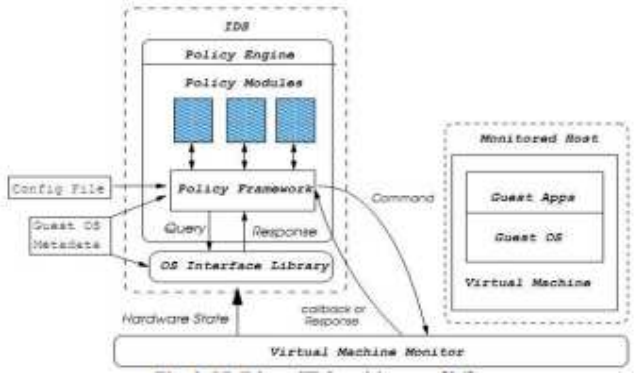
IDS بر مبنای درون گرایی VM یکی از مثالهای سیستم شناسایی تداخل بر مبنای هایپرویژر است. اخیرا پژوهش IBM به استفاده از شیوه درون گرایی ماشین مجازی برای ایجاد یک مجموعه لایه بندی شده از سرویس های امنیتی در VM حمایت شده در حال اجرای بر همان ماشین فیزیکی تشویق کرده است چنانچه گمان نماید VM در حال اجرا در سیستم ابری است.

چنانچه محاسبه ابری به عنوان مخزنی از منابع کامپیوتری مجازی تعریف شود و ماشین های مجازی مختلفی را مدیریت نماید، هایپرویژر (همچنین به عنوان یک مدیریت ماشینی مجازی شناخته شده است) استفاده می شود.

IDS بر مبنای هایپرویژر یکی از تکنیک های مهم استف به ویزه در محاسبه ابری برای شناسایی تداخل در محیط مجازی.

مولفان منبع ۲۶ معماری IDS بر مینای درون گرایی ماسین مجازی (VMI-IDS) را همانند شکل ۹ پیشنهاد کردند. VMI-IDS متفاوت از HIDS قدیمی است از انجاییکه مستقیما وضعیت سخت افزاری، وقایع و وضعیت نرم افزاری هاست را مشاهده می کند و نظر قوی تری از سیستم نسبت به HIDS ارائه می دهد. مانیتور ماشین مجازی (VMM) مسئول مجازی سازی سخت افزای است و همچنین جداسازی، مانیتور نمودن و خصوصیات میانجی است. VMI-IDS دسترسی بیشتری نسبت به اجرای کد در VM مانیتور شده دارد. تداخل VMM برای VMI-IDS استفاده می شود تا با VMM مکاتبه کند، که به VMI-IDS برای دریافت اطلاعات وضعی VM ، مانیتور کردن وقایع خاص و کنترل VM ها اجازه دسترسی دهد. این تداخل VMM ترکیبی از سوکت Unix برای فرستادن دستورها یا دریافت پایخ ها بهو از VMM است. آن همچنین از دسترسی حافظه فیزیکی به VM مانتیور شده پشتیبانی می کند. کتابخانه رابط OS برای تامین وضعیت های ماشینی سطح پایین از VMM در موراد ساختار OS سطح بالا استفاده می شود. موتور خط مشی برای ساخت سالات سطح بالا درباره OS هاست مانیتور شده مشارکت دارد. موتور خط مشی به شویه ای مقتضی پاسخ می دهد حتی اگر سیستم تراضی شده باشد. VMI-IDS شناسایی غیر متعارف پیچیده ای را اجرا می کند. برای شناسایی کذب، شناسایی تایید، شناسایی انسجام برنامه و شناسایی سوکت خام استفاده می شود. بر اساس نتایج نشان داده شده در منبع ۲۶، عملکرد موتور خط مشی در رابطه با میزان کار و زمان دستگاهه خوب است.

شکل ۹- معماری IDS بر مبنای VMI



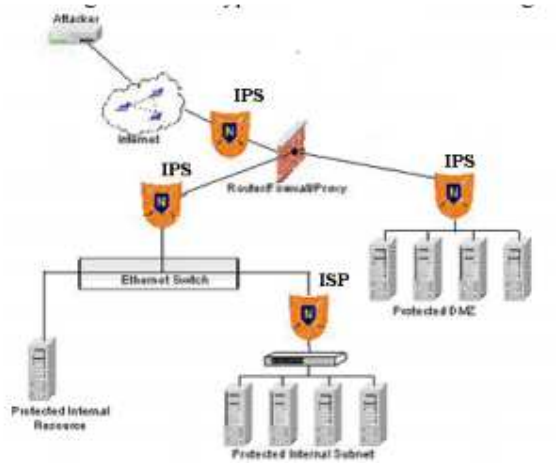
E. سیستم ممانعت از تداخل (IPS)

با کمک IDS، IPS ترافیک شبکه و فعالیت های سیستم را برای شناسایی تداخل های ممکن و پاسخ فعال به تداخل ها برای بلوکه نمودن ترافیک یا قرنطینه آن را مانیتور می کند . IPS باید به دقت برای نتایج مورد انتظار پیکره بندی شودف وگرنه جریان بسته ها را متوقف می کند و در نتیجه باعث عدم دسترسی به شبکه می شود. برای ممانعت از تداخل اغلب فایروال همراه با IDS استفاده می شود که محتوی احکام ترافیکی شبکه ویژه تصدیقی است. بر پایه احکام از پیش پیکره بندی شده، HPS تصمیم می گیرد که آیا باید ترافیک شبکه عبور نماید یا متوقف شود. در پاسخ به مهاجم شناسایی شده، IPS می تواند خودش مانع مهاجم شود، می تواند محتوی حمله را تغییر دهد یا محیط امنیتی را تغییر دهد.

احمد و همکاران شناسایی تداخل بر مبنای شبکه موثر و شیوه ممانعتی را پیشنهاد کردند که نیاز به نصب IDS بر روی هر گره ندارد. این شیوه مشکلات واقعی و انتقال پیام اخطار مشکل را حل می کند. آن مخارج کلی کمتری دارد و هیچ میزان اخطار اشتباهی ندارد. لیو و لی سیستم ممانعت از تداخل بر مبنای جمع تجمعی (CSIPS) برای ممانعت از DoS با مهاجم های DDoS پیشنهاد دادند. در این کار مولفان از الگوریتم طبقه بندی بسته و سه الگوریتم شناسایی (به نام درون مرزی، برون مرزی و پیش رو) استفاده کردند که به طور مشارکتی حمله DDoS را شناسایی کردند و به گزارش های خود برای کنترل از راه دور ماشین IPS ارسال کردند.

IPS ها اساسا به دو دسته تقسیم بندی می شوند: IPS بر مبنای هاست (HIPS) و IPS بر مبنای شبکه (NIPS). موقعیت ممکن IPS در یک نوع شبکه در شکل ۱۰ آورده شده است.

شکل ۱۰- سیستم ممانعت از تداخل بر مبنای شبکه



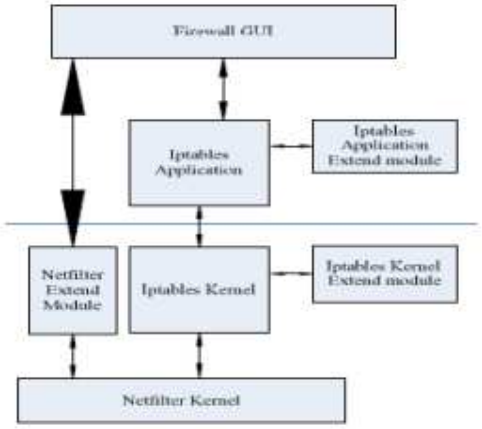
در معماری محاسباتی ابری HIPS می تواند برای شناسایی و ممانعت از تداخل بر VM ،هایپرویژر یا سیستم هاست که گسترده شده است استفاده شود. NIPS می تواند برای محافظت از شبکه (یا بخشی از شبکه) برای محاظت از سیستم های چند گانه (مثل VM ها) در یک زمان استفاده شود.

مولفان در منبع ۵۸، فایروال سیستمی هاست بر مبنای Xen و گستره ان را ارائه دادند. در این شیوه فلتر شبکه و جدول Ip برای ساخت فایروال بر سیستم لینوکس هاست که به داده های شبکه رسیدگی می کند استفاده شد. جدول Ip (Iptables) برنامه مدیریتی فایروال بر مبنای چهارچوب فیلتر شبکه (Netfilter) است. همانطور که در شکل ۱۱ نشان داده می شود، گستره Iptables مشتمل بر د بخش است: بخش اول در ارتیاط با لایه برنامه Iptables است که به عنوان کتابخانه به اشتراک گذاشته ایجاد شده است و بخش دوم هسته Iptable است که به عنوان کتابخانه پویای هسته توسعه یافته است. کتابخانه پویای هسته در زمان اجرا بارگذاری شده است. علاوه بر این GUI فایروال برای پیکربندی احکام فایروال استفاده می شود.

گستره برنامه Iptables برای تصدیق احکام پیکربندی شده توسط کاربران و برای تجزیه پارامترهای احکام استفاده می شود. هر حکم تکمیل شده در ساختار داده توسط Iptables تامین شد. گستره هسته Iptable به طور پپویا بارگذاری می شود وقتی فایروال در حال اجرا است. آن بر اساس فیلتر شبکه یا Iptables ایجاد شده است. وقتی بسته شبکه از طریق HOOK می رود ، تابع HOOK نامیده می شود. تابع HOOK مشخص می کند آیا بسته داده ها با احکام از پیش پیکره بندی شده تطابق دارد یا خیر و نتیجه را به هسته بر می گرداد که برای قبول یا رد

بسته تصمیم گیری کند. ساختار کلی داده سپس به تابع HOOK منتقل می شود که ساختار داده را به ساختار تعریف شده توسط حوزه برنامه Iptable تبدیل می کند. همچنین اشاره گر به بوفر skb که در حال ذخیره اطلاعات بسته است به تابع HOOK منتقل می شود تا احکام را بدون توجه به همسازی با داده ها تشخیص دهد. بوفر (میانبر) skb داده های بسته را ذخیره می کند ، همچون آدرس IP منبع، تعداد پورت مقصد که وقتی به HOOK می رود مورد محاسبه قرار گیرد. اما مهاجم های ناشناخته با این شیوه نمی تواند شناسایی شوند.

شکل ۱۱- معماری فایروال و Xen گسترده آن

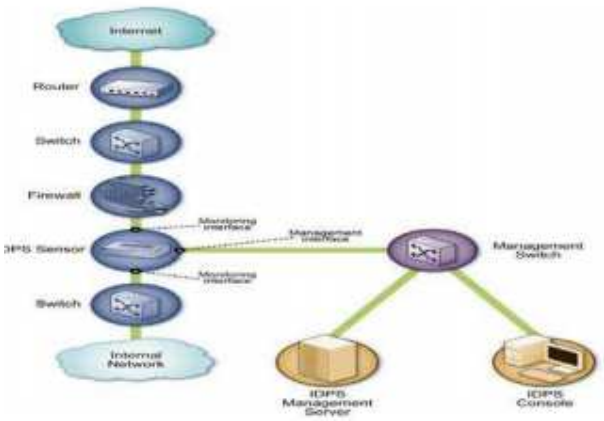


F. سیستم ممانعت و شناسایی تداخل (IDPS)

یا داشتن نقاط قوت و ضعف، IDS و IPS به تنهایی قادر به تامین امنیت کامل نیستند. روش بهینه استفاده ترکیبی از IDS و IPS است که IDPS نامیده می شود. صرفنظر از تشخیص تداخل های ممکن، IDPS متوقف می کند و آنها را به مسئولین شبکه امنیتی گزارش می دهد. پیکربندی و مدیریت مناسب ترکیب IDS و IPS می تواند امنیت را اصلاح کند. NIST چگونگی شناسایی و ممانعت از تداخل را که می تواند با یکدیگر برای افزایش امنیت استفاده شود توضیح می دهد، و همچنسن در مورد روش های مختلف طراحی، پیکربندی و مدیریت IDPS بحث می نماید. IDPS به سه دسته گسترده طبقه بندی می شود: برمبنای تصدیقی، بر مینای غیر متعارف، تحلیل پروتکل توضیحی. انواع زیادی از تکنولوژی IDPS وجود دارد. IDPS به چهار گروه بر مینای نوع وقایعی که مانیتور می کنند و روشی که بکار میگیرند تقسیم می شوند: a) بر مبنای شبکه b) بی سیم c) تحلیل وضعیت

شبکه (NBA) d) بر مبنای هاست. IDPS بر مبنای موقعیت شبکه نوعی شبکه است که در شکل ۱۲ نشان داده شده است.

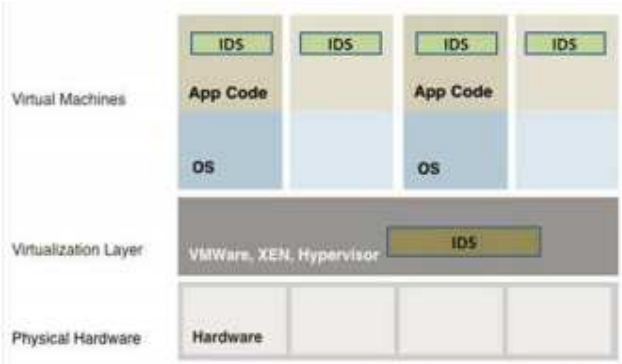
شکل ۱۲- موقعیت IDPS در شبکه



با توجه به موضوع ابری، IDPS بر مبنای شبکه می تواند برای حمایت از VM های چند گانه از نقطه نظر شبکه مورد استفاده قرار گیرد. IDPS بر مبنای هاست می تواند در VMها یا هایپرویژر برای حمایت از ماشین هایی که در آن قرار داده شده اند به کار روند.

نتیجه گیری این بخش این است که ما هم اکنون از نظر گرافیکی موقعیت انواع مختلف IDS/IPS (که در بالا ذکر شد) را در لایه های مختلف معماری ابری ارائه می دهیم. شکل ۱۳ به همین ضورت آن را به صورت خلاصه بیان می کند.

شکل ۱۳- قراردادن IDS بر روی VMS و سیستم هایپرویژر/هاست



مشارکت IDS بر VM اجازه به مانیتور نمودن فعالیت توسط خود VM می دهد. کاربر ابری باید مسئول حفظ گسترش ، مدیریت و مانیتور IDS بر VM باشد. جاگذاری IDS بر هایپرویژر توانایی برای شناسایی فعالیت تداخلی شامل ارتباط بین VM ها را بر هایپرویژر فراهم می کند. اما مقادیر زیاد ارتباط بین داده ها عملکرد IDS را کاهش می دهد یا سبب افت بسته می شود. گسترش، مدیریت و مانیتور نمودن IDS باید با تامین کننده ابری انجام شود. شبکه مجازی (تثبیت شده در سیستم هاست) به VM ها اجازه مکاتیه به طور مستقیم بدون استفاده از شبکه خارجی را می دهد. IDS می تواند درون چنین شبکه ای برای مانیتور ترافیک بین VM ها همچون بین VM و هاست قرار داده شود.

جدول III خلاصه ای انواع IDS/IPS

نوع IDS/IPS	خصوصیات/ توانایی ها	محدودیت ها/چالش ها	موقعیت در محیط ابری	گستردگی و مانیتور کردن قدرت
HIDS	تداخل ها را با مانتیور کردن سیستم فایل هاست، تماس های سیستم یا وقایع شبکه تشخیص می دهد هیچ سخت افزار اضافی نیاز نیست	نیاز به نصب بر روی یک ماشین مثل VM ها، هایپرویژر یا ماشین هاست می تواند حملات را فقط بر روی هاست که گسترش یافته مانیتور کند	بر هر VM، هایپرویژر یا سیستم هاست	بر VMها: کاربران ابری بر هایپرویژر: تامین کننده ابری
NIDS	تشخیص تداخل ها برای مانیتور نمودن ترافیک شبکه	مشکل در شناسایی تداخل ها از ترافیک کد شده	در شبکه خارجی یا در شبکه مجازی	تامین کننده ابری

	نیاز به قرار گرفتن فقط بر شبکه تحت نظر می تواند سیستم های چند گانه را در یک زمان مانتیور کند.	فقط به شناسایی مهاجم های خارجی کمک می کند مشکل در شناسایی تداخل های شبکه در شبکه مجازی		
IDS بر مبنای هایپرویژر	به کاربر برای مانتیور و تحلیل مکاتبات بین VM ها، بین هایپرویژر و VM و با شبکه مجازی بر اساس هایپرویژر	جدید و مشکل برای فهمیدن	در هایپرویژر	تامین کننده ابری
DIDS	از هر دو خصوصیات NIDS و HIDS استفاده می کند و بنابراین فوایدی از هر دو را نشان می دهد	سرور مرکزی ممکن است دارای بار اضافی باشد و برای مدیریت در DIDS مرکزی شده دارای مشکل است مکاتبات بالا و هزینه محاسباتی	در شبکه خارجی، بر روی هاست، بر هایپرویژر یا بر VM	بر VM ها: کاربران ابری. برای موارد دیگر : تامین کننده ابری
IPS	ممانعت از تداخل مهاجم ها NIPS از مهاجم های شبکه ممانعت می کند HIPS از مهاجم های سطح سیستم ممانعت می کند	دقت شناسایی برای ممانعت از حمله پایین تر از IDS است	برای NIPS: در شبکه خارجی/داخلی برای HIPS: بر VM یا هایپرویژر	NIPS: تامین کننده ابری HIPS بر VM: کاربر ابری HIPS بر هایپرویژر: تامین کننده ابری
IDPS	به طور کارامدی حملات تداخلی را شناسایی و ممانعت می کند	ساختار پیچیده	IDPS بر مبنای شبکه: در شبکه خارجی/داخلی.	IDPS بر مبنای شبکه: تامین کننده ابری

			IDPS بر مبنای هاست: بر VM یا هایپرویژر	IDPS بر مبنای هاست (بر VM): کاربر ابری IDPS بر مبنای هسا (بر هایپرویژر): تامین کننده ابری

تامین کننده ابری می تواند وظیفه مدیریت IDS را بر عهده بگیرد. IDS می تواند در شبکه خارجی گسترش داده شود، که دروازه ای برای سیستم ابری براب کاربران است. ان به مانیتور نمودن ترافیک شبکه در شیکه قدیمی می دهد. تامین کننده ابری باید برای ذخیره در اینجا کامل باشد. خلاصه ای از IDS ها در جدول III نشان داده شده است.

تاکنون ما از برخی شیوه های موجود بحث کردیم که مشارکت دهنده IDS در ابری است. اما هیچ راه حل کارامد جهانی هنوز یافت نشده است. هر کدام محدودیت هایی دارد. در جدول IV ما خلاصه ای از شیوه ها را با نوع، فن، موقعیت در ابری، جنبه های منفی و مثبت ارائه دادیم. این چندین چالش مکاتباتی پژوهش امنیت را برای ردیابی قبل از یک چهارچوب امنیتی استاندارد برای ابری که می تواند پیشنهاد شود را فراهم می کند.

جدول IV خلاصه ای از شیوه های IDS موجود در ابری

عنوان	نوع IDS	فن مورد استفاده	قرارگیری	جنبه های مثبت	جنبه های منفی
ساختار IDS برای محیط ابری	HIDS	شناسایی تصدیقی و شناسایی غیر متعارف با استفاده از ANN	بر هر گره	میزان اشتباه برای مهاجم ناشناخته پایین تر از ANN استفاده شده است	نیاز به زمان آموزش بیشتر برای شناسایی دقت دارد
ساختار HDS سازگار با VM	NIDS	شناسایی تصدیقی	بر هر VM	امنیت VM بر اساس پیکر بندی کاربر	نمونه های چند گانه IDS نیاز به درجه بندی

					مجدد عملکرد دارد
شناسایی حمله DDoS در ماشین مجازی	NIDS	شناسایی تصدیقی	بر هر VM	VM را از حملات DDoS ایمن می کند	می تواند فقط مهاجم های شناخته شده را شناسایی کند از انجاییکه فقط اندک استفاده می شود
NIDS در ابری منبع باز	NIDS	شناسایی تصدیقی	بر شبکه قدیمی	می تواند چندین مهاجم شناخته شده را شناسایی کند	نمی تواند مهاجم های داخلی را همچون مهاجم های شناخته شده شناسایی کند از آنجائیکه به طور ضعیف استفاده می شود.
شیوه بر اساس عامل مشترک	DIDS	شناسایی تصددیقی	بر هر حوزه ابری	سیستم ممانعت از نقص هر نقطه	نمی تواند برای همه انواع مهاجم ها استفاده شود هزینه کلی محاسباتی بالا
شیوه بر اساس عامل موبایل	DIDS	شناسایی غیر متعارف	بر هر VM	IDS را برای برنامه ابری صرفنظر از موقعیت انها تامین می کند	ایجاد بار شبکه با افزایش VM ها ارسال شده به MA
ساختار بر اساس VMI-IDS	بر مبنای هایپرویژر	شناسایی غیر متعارف	بر هایپرویژر	شناسایی مهاجم ها بر VM ها	VMI-IDS می تواند مورد حمله واقع

					شوند. روش خیلی پیچیده
فایروال بر اساس هاست بر مبنای Xen		ممانعت	بر هر هاست	ممانعت با استفاده از احکام پیکربندی شده کاربر	برای ممانعت از مهاجم های ناشناخته استفاده نمی شود
شیوه بر اساس CP		شناسایی غیر متعارف	-	برای شناسایی همه انواع مهاجم ها استفاده می شود. محدودیت زمان محاسباتی را حل می کند	هیچ نتیجه ازمایشی نشان داده نشده است

VI. نتیجه گیری

این پژوهش بر چندین تداخل بحث نمود که می تواند انسجام، محرمیت و دسترسی سرویس های ابری در آینده اثر بگذارد. یکی از راه حل های موجود به طور مختصر این است که فایروال ممکن نیست برای حل برایندهای امنیتی ابری کافی باشد. فرضیه مقاله استفاده از گزینه های پیشنهادی برای مشارکت در فنون شناسایی با ممانعت از تداخل در محیط ابری است و موقعیت های کشف شده در محیط ابری است که IDS/IPS می تواند برای شناسایی و ممانعت موثر تداخل قرار داده شود. یافته های پژوهشی اخیر به طور ویژه مشارکت IDS/IPS را در محیط ابری مورد بحث قرار داده اند و مزیتها و معایب آنها را مشخص نمودند. سازگاری فنون محاسباتی نرم در IDS/IPS می تواند به طور بهینه امنیت را اصلاح نماید. مقاله سرانجام چندین چالش امنیتی را تشخیص داد که نیار به توجه در پژوهش محیط ابری دارد قبل از اینکه محیط ابری بتواند به صورت قالب ایمن و مطمئن برای تحویل اینترنتی موارد آینده شود.

REFERENCES

[1] P. Mell, and T. Grance. (2011). The NIST Definition of Cloud Computing (Draft). *NIST* [Online]. Available: http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

[2] Google apps. [Online]. Available: http://www.google.com/apps/business

[3] "Google apps engine." [Online]. Available: URL http://code.google.com/appengine.

[4] Azure services platform. [Online]. Available: http://www.microsoft.com/azure

[5] Amazon web services. [Online]. Available: http://aws.amazon.com

[6] Eucalyptus. [Online]. Available: http://eucalyptus.cs.ucsb.edu/.

[7] Opennebula. [Online]. Available: http://www.opennebula.org

[8] International Data Corporation. 2009. [Online]. Available: http://blogs.idc.com/ie/wpcontent/uploads/2009/12/idc_cloud_challenges_2009.jpg, 2009.

[9] Lockheed Martin White Paper: Available: http://www.lockheedmartin.com/data/assets/isgs/documents/CloudComputingWhitePaper.pdf

[10] C. Brooks. Amazon EC2 Attack Prompts Customer Support Changes. *Tech Target*. [Online]. Available: http://searchcloudcomputing.techtarget.com/news/article/0,289142,sid201_gci1371090,00.html

[11] M. Slaviero, "BlackHat presentation demo vids: Amazon." [Online]. Available: http://www.sensepost.com/blog/3797.html

[12] Y. Chen, and R. Sion, "On securing untrusted clouds with cryptography," *In WPES '10*, pp. 109–114, 2010.

[13] J. Rutkowska, "Subverting VistaTM Kernel for Fun and Profit," *Black Hat Conference*, 2006.

[14] S. King, P. Chen, and Y-M. Wang, "SubVirt: Implementing malware with virtual machines," *2006 IEEE Symposium on Security and Privacy*, 2006, pp.314-327.

[15] S. Bahram, X. Jiang, Z. Wang, and M. Grace, "DKSM: Subverting Virtual Machine Introspection for Fun and Profit," *Proceedings of the 29th IEEE International Symposium on Reliable Distributed Systems*, 2010.

[16] NIST: National vulnerability database. [Online]. Available: http://web.nvd.nist.gov/view/ vuln/detail?vulnId=CVE-2009-3733

[17] D. Goodin, "Webhost Hack Wipes Out Data for 100,000 Sites." [Online]. Available: http://www.theregister.co.uk/2009/06/08/webhost_attack/

[18] S. Beg, U. Naru1, M. Ashraf, and S. Mohsin, "Feasibility of Intrusion Detection System with High Performance Computing: A Survey," *International Journal for Advances in Computer Science*, vol. 1, no. 1, 2010.

[19] Dinesh Sequeira, "Intrusion Prevention Systems- Security's Silver Bullet?", SANS Institute InfoSec Reading Room 2002.http://www.sans.org/reading_room/whitepapers/detection/intrusion_prevention_systems_securitys_silver_bullet_366?show=366.php&cat=detection

[20] Denial-of-service attack. [Online]. Available: http://en.wikipedia.org/wiki/Denial-of-service_attack

[21] Phil cox, "Intrusion detection in a cloud computing environment." [Online]. Available: http://searchcloudcomputing.techtarget.com/tip/Intrusion-detection-in-a-cloud-computing-environment

[22] "Snort-Home page." [Online]. Available: https://www.snort.org/

[23] D. stiawan, A. H. Abdullah, and M. Y. Idris, "The Trends of Intrusion Prevention System Network," 2nd International Conference on Education Technology and Computer (ICETC), vol. 4, 2010, pp. 217-221.

[24] M. A. Hemairy, S. Amin, and Z. Trabelsi, "Towards more sophisticated ARP Spoofing detection/prevention systems in LAN networks," *International Conference on the Current Trends in Information Technology (CTIT)*, 2009, pp. 1-6.

[25] XArp 2.2.2. [Online]. Available: http://www.filecluster.com/Network-Tools/Network-Monitoring/Download-XArp.html
[26] T. Garfinkel, and M. Rosenblum, "A Virtual Machine Introspection Based Architecture for Intrusion Detection," *In Proc. Network and Distributed Systems Security Symposium*, pp. 191-206, 2003.
[27] IBM Research-Zurich. [Online]. Available: http://www.zurich.ibm.com/csc/security/securevirt.html#top
[28] A. K. Jones, and R. S. Sielken. Computer System Intrusion Detection: A Survey. [Online]. Available: http://www.cs.virginia.edu/~jones/IDSresearch/ Documents/jones-sielken-survey-v11.pdf
[29] M. Ahmed, R. Pal, H. M. Hossain, M. Bikas, and M. K. Hasan, "NIDS: A Network Based Approach to Intrusion Detection and Prevention," *Computer Science and Information Technology - Spring Conference*, 2009, pp. 141-144.
[30] F. Y. Leu, and Z. Y. Li, "Detecting DoS and DDoS Attack Using an Intrusion Detection and Remote Prevention System," *Fifth International Conference on Information Assurance and Security*, Vol. 2, 2009, pp. 251-254.
[31] K. Scarfone, and P. Mell. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). Recommendations of the National Institute of Standards and Technology. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
[32] D. J. Brown, B. Suckow, and T. Wang. *A Survey of Intrusion Detection Systems*. Department of Computer Science, University of California, San Diego.
[33] T. Dutkevyach, A. Piskozub, and N. Tymoshyk, "Real-Time Intrusion Prevention and Anomaly Analyze System for Corporate Networks," *4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2007. IDAACS 2007*, 2007, pp. 599-602.
[34] H. Zhengbing, S. Jun, and V. P. Shirochin, "An Intelligent Lightweight Intrusion Detection System with Forensic Technique," *4th IEEE Workshop on Intelligent Data Acquisition and Advanced ComputingSystems: Technology and Applications, 2007. IDAACS*, 2007, pp. 647-651.
[35] J. Han and M. Kamber. *Data Mining Concepts and Techniques 2nd edition*. Morgan Kaufmann Publishers, 2006
[36] L. M. Ibrahim, "Anomaly Network Intrusion Detection System Based On Distributed Time-Delay Neural Network," *Journal of Engineering Science and Technology*, vol. 5, no. 4, pp. 457 – 471, 2010.
[37] J. Cannady, "Artificial Neural Networks for Misuse Detection," *National Information Systems Security Conference*. 1998.
[38] M. Moradi, and M. Zulkernine, "A Neural Network Based System for Intrusion Detection and Classification of Attacks," *Proceedings of the 2004 IEEE International Conference on Advances in Intelligent Systems - Theory and Applications*, 2004.
[39] Grediaga, F. Ibarra, F. García, B. Ledesma, and F. Brotons, "Application of neural networks in network control and information security," *LNCS*, pp. 208–213, 2006.
[40] P. Tillapart, T. Thumthawatworn, and P. Santiprabhob, "Fuzzy intrusion detection system," *Assump University J Technology (A.U. J.T.)*, vol. 6, no. 2, pp.109–114, 2002.
[41] S. Chavan, K. Shah, N. Dave, and S. Mukherjee, "Adaptive neuro-fuzzy intrusion detection systems," *IEEE international conference on information technology: coding and computing (ITCC'04)*, 2004, pp 70–74.
[42] M-Y. Su, G-J. Yu, and C-Y. Lin, "A real-time network intrusion detection system for large-scale attacks based on an incremental mining approach," *Computer Security*, pp.301–309, 2009.
[43] H. Han, X. L. Lu, and L. Y. Ren, "Using Data Mining To Discover Signatures In Network-Based Intrusion Detection", *Proceedings of the First International Conference on Machine Learning and Cybernetics*, Beijing, vol. 1, 2002.
[44] H. Zhengbing, L. Zhitang, and W. Jungi, "A Novel Intrusion Detection System (NIDS) Based on Signature Search of DataMining," *WKDD First International Workshop on Knowledge discovery and Data Ming*, 2008, pp. 10-16.
[45] L. Lei, D-Z Yang, and F-C Shen, "A Novel rule based Intrusion Detection system using Data Ming," *3rd IEEE International Conference on Computer Science and Information Technology*, vol. 6, pp. 169-172, 2010.

[46] W-H. Chen, S-H. Su, and H-P. Shen, "Application of svm and ann for intrusion detection," *Computer Oper Res*, vol. 32, no.10, pp. 2617–2634, 2005.
[47] H. Li, and D. Liu, "Research on Intelligent Intrusion Prevention System Based on Snort," *International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE)*, vol. 1, pp. 251-253, 2010.
[48] Y. Dhanalakshmi, and I. Ramesh Babu, "Intrusion detection using data mining along fuzzy logic and genetic algorithms," *International Journal of Computer Science & Security*, vol. 8, no.2, pp. 27–32, 2008.
[49] W. Lu, and I. Traore, "Detecting new forms of network intrusion using genetic programming," *Computational Intelligence*, vol. 20, no. 3, pp. 475-494, 2004.
[50] W. Li, "A Genetic Algorithm Approach to Network Intrusion Detection", SANS Institute, USA, 2004.
[51] R. H. Gong, M. Zulkernine, and P. Abolmaesumi, "A software implementation of a genetic algorithm based approach to network intrusion detection," *In Proceedings of the sixth international conference on software engineering, artificial intelligence, networking and parallel/distributed computing and first ACIS international workshop on self-assembling wireless networks (SNPD/SAWN'05)*, 2005.
[52] T. Xiao, G. Qu, S. Hariri, and M. Yousif, "An Efficient Network Intrusion Detection Method Based on Information Theory and Genetic Algorithm," *Proceedings of the 24th IEEE International Performance Computing and Communications Conference (IPCCC '05)*, Phoenix, AZ, USA. 2005.
[53] M. Botha, R. Solms, K. Perry, E. Loubser, and G. Yamoyany, "The utilization of Artificial Intelligence in a Hybrid Intrusion Detection System", *SAICSIT*, 2002, pp. 149-155.
[54] C. Katar, "Combining multiple techniques for intrusion detection," *International Journal of Computer Science & Network Security*," vol. 6, no.2B, pp. 208–218, 2006.
[55] C. B. W. C. M. W. K. M. VIEIRA, A. SCHULTER, "Intrusion detection techniques in grid and cloud computing environment," *IEEE IT Professional Magazine*, 2010.
[56] S. Roschke, C. Feng, and C. Meinel, "An Extensible and Virtualization Compatible IDS Management Architecture," *Fifth International Conference on Information Assurance and Security*, vol. 2, 2009, pp. 130-134.
[57] A.bakshi, and B. Yogesh, "Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine," *Second International Conference on Communication Software and Networks*, 2010, pp. 260-264
[58] L. Fagui Liu, S. Xiang Su, and L. Wenqianl, "The Design and Application of Xen-based Host System Firewall and its Extension," *in The 2009 International Conference on Electronic Computer Technology*, 2009, pp. 392-395.
[59] C. C. Lo, C. C. Huang, and J. Ku, "Cooperative Intrusion Detection System Framework for Cloud Computing Networks," *First IEEE International Conference on Ubi-Media Computing*, 2008, pp. 280-284.
[60] K. A. B. A. V. Dastjerdi, and S. G. H. Tabatabaei, "Distributed intrusion detection in clouds using mobile agents," *in Third International Conference on Advanced Engineering Computing and Applications in Sciences*, 2009. ADVCOMP '09, 2009, pp. 175 – 180.
[61] Y. Guan, and J. Bao, "A CP Intrusion Detection Strategy on Cloud Computing," *In International Symposium on Web Information Systems and Applications (WISA)*, pp. 84–87, 2009.
[62] C. Mazzariello, R. Bifulco, and R. Canonoco, "Integrating a network IDS into an Open source Cloud computing," *Sixth International conference on Information Assurance and Security (IAS)*, 2010, pp. 265-270.
[63] The concept of Intrusion Detection System. [Online]. Available: http://maltainfosec.org/archives/26-The-concept-of-Intrusion-Detection-Systems.html
[64] IPS:Intrusion Prevention System. *Javvin*. [Online]. Available: http://www.javvin.com/networksecurity/IPS.html
[65] Firewall. *Telecom-Network Tech*. [Online]. Available: http://teleco-network.blogspot.com/