کنفرانس ملی چشم انداز ۱۴۲۰ و پیشرفت های
تکنولوژیک مهندسی برق، کامپیوتر و فناوری اطلاعات

تاثیر مجازی سازی در امنیت محاسبات ابری

احمد رستگارنژاد

a.rastegarnezhad@gmail.com

خلاصه

محاسبات ابری نتیجه تکاملی روش های محاسبات قبلی است، که نشان دهنده یک تغییر پارادایم برای ارائه منابع و خدمات است. در این تحقیق تمرکز اصلی بر روی امنیت ابر قرار گرفته و سعی شده است جزئیات مورد نیاز بررسی گردد. همچنین مجازی سازی که یکی از تکنیک‌های نوظهور در دنیای فن آوری اطلاعات است، را به عنوان پایه‌ای برای ساخت یک ابر به کار برد، بررسی کردیم. درضمن در این مقاله، ما نشان می دهیم که چگونه مجازی سازی می تواند امنیت محاسبات ابری، را با حفاظت از یکپارچگی ماشین های مجازی مهمان و اجزای زیرساخت ابر افزایش دهد.

کلمات کلیدی: محاسبات ابری، امنیت، مجازی سازی، معماری

۱. مقدمه

موسسه بین المللی استانداردها و تکنولوژی (NIST) محاسبات ابررایانه را به عنوان مدلی برای توانا سازی مناسب روی دستیابی به تقاضای شبکه برای به اشتراک گذاری محاسبات منابع گروهی قابل تنظیم مثل شبکه ها ، سرور ها ، ذخیره سازی ، کاربرد ها و خدمات تعریف کرده است که می توان با شروط سریع و با حداقل تلاش مدیریتی یا تعامل مهیا کننده خدمت منتشر کرد. واژه‌ی «ابر» واژه‌ای است استعاری که به اینترنت اشاره می کند و در نمودارهای شبکه‌های رایانه‌ای نیز از شکل ابر برای نشان دادن شبکه اینترنت استفاده می‌شود. دلیل تشبیه اینترنت به ابر در این است که اینترنت همچون ابری جزئیات فنی‌اش را از دید کاربران پنهان می‌سازد و لایه‌ای از انتزاع را بین این جزئیات فنی و کاربران به وجود می‌آورد.

گره های ابر ذاتاً به حملات cyber با راه حل های سنتی با توجه با اندازه شان و پیچیدگی اساسی مربوط به ارائه خدمات به مشتریان آسیب پذیری بیشتری دارند. ابر اینترنت با همه جوانب مثبت و منفی، سیستمی فراگیر است. در نتیجه، افزایش حفاظت از گره های ابر internetworked یک کار چالش برانگیز است. پس به رسمیت شناختن تهدیدات احتمالی و ایجاد فرآیندهای امنیتی برای محافظت از خدمات و پایگاه های اینترنتی از حملات بسیار مهم است. ابر رایانه در حال حاضر اهرم مجازی سازی برای حفظ تعادل بار از طریق تأمین پویا و مهاجرت از ماشین های مجازی در میان گره های فیزیکی است. VMS در اینترنت انواع بسیاری از فعل و انفعالات است که تکنولوژی مجازی سازی می تواند کمک کند به فیلتر کردن در حالی که اطمینان از درجه بالاتری از امنیت قرار گرفته است. به طور خاص، مجازی سازی همچنین می تواند به عنوان یک بخش امنیت مورد استفاده قرار گیرد، برای مثال، به منظور ارائه نظارت VMS، امکان مدیریت آسان تر از امنیت خوشه های پیچیده، مزارع سرور، و زیرساخت های محاسبات ابری. با این حال، فن آوری های مجازی سازی همچنین نگرانی بالقوه با توجه به امنیت ایجاد می کند[٦].

۲. پرایمر مختصری در مورد امنیت:

هر چند که رایانش ابری در عصر حاضر یکی از کاربردی ترین تکنولوژهای ارائه شده توسط انسان می باشد، با این حال دغدغه امنیت بی شک قدم به قدم در کنار مزایای آن قابل طرح است. چیزی که بیش از پیش ذینفعان را در مورد استفاده از رایانش ابری دچار تردید می کند، امنیت این تکنولوژی می باشد. قبل از بحث امنیت در عرصه ابر به تعاریف پایه‌ای می پردازیم که ارتباط تنگاتنگی با امنیت دارند:

امنیت اطلاعات: واژه امنیت اطلاعات حجم وسیعی از فعالیت های یک سازمان را تحت پوشش قرار می دهد . امنیت اطلاعات به معنای واقعی یعنی با استفاده از یک سری فرآیند ها از دسترسی غیر مجاز به اطلاعات و یا محصولات و اعمال تغییرات یا حذف کردن آنها جلوگیری کنیم. این عمل را می توان به نحوی حفاظت از منابع موجود، در موقعیت های مختلف (مانند یک حمله هکری که معمولا خیلی انجام می شود) توسط افرادی که مسئول امنیت اطلاعات هستند در نظر گرفت .

زیر دامنه برای امنیت اطلاعات[1] از جمله اینها امنیت کامپیوتر، امنیت شبکه، امنیت پایگاه داده، و تضمین اطلاعات است. امنیت در ابر، ما را موظف می کند به طراحی هر یک از این موارد لازم برای پرداختن به مسائلی که با آن روبرو هستیم.

محرمانگی: محرمانگی یعنی جلوگیری از افشای اطلاعات به افراد غیر مجاز.

یکپارچگی: یکپارچه بودن یعنی جلوگیری از تغییر داده‌ها بطور غیرمجاز و تشخیص تغییر در صورت دستکاری غیر مجاز اطلاعات. یکپارچگی وقتی نقض میشود که اطلاعات در حین انتقال بصورت غیرمجاز تغییر داده میشود.

قابل دسترس بودن: اطلاعات باید زمانی که مورد نیاز توسط افراد مجاز هستند در دسترس باشند. این بدان معنی است که باید از درست کار کردن و جلوگیری از اختلال در سیستم‌های ذخیره و پردازش اطلاعات و کانال‌های ارتباطی مورد استفاده برای دسترسی به اطلاعات اطمینان حاصل کرد.

حداقل اصل امتیاز[2]: کاربران و فرآیندهای فعال از جانب آنان باید محدود به کار با حداقل مجموعه ای از امتیازات باشند. این اصل برای جلوگیری از استفاده فراگیر از حقوق امتیاز یا دسترسی در سیستم های فناوری اطلاعات است.

احراز هویت: به معنی ایجاد هویت یک کاربر، به طور معمول با ارائه اعتبار به عنوان نام کاربری و رمز عبور است.

مجوز: حقوق و مزایا که به یک فرد، کاربر، یا فرایند داده شده است.

رمزنگاری: رمزنگاری دانش تغییر دادن متن پیام به کمک کلید رمزنگاری و الگوریتم رمزنگاری است؛ کلمه Cryptography برگرفته از لغات یونانی «kryptos» به مفهوم «محرمانه» و «graphein» به معنای «نوشتن» است. قبل از هر چیز، لازم است بین رمز و کد تفاوت قایل شویم. رمز به مفهوم تبدیل کاراکتر به کاراکتر یا بیت به بیت، بدون تغییر محتویات زبان شناختی آن، است. در مقابل، «کد» تبدیلی است که کلمه‌ای را با کلمه یا نمادی دیگر جایگزین می کند.

بازرسی: شامل فعالیت‌های مختلف و گسترده‌ای از جمله، جمع آوری و بررسی رویدادهای شبکه، سیستم، و برنامه های کاربردی برای حفظ امنیت می‌باشد [۶].

۳. امنیت ابر: معماری

بی شک اولین گام در ارائه یک تکنولوژی، ایجاد چارچوب و ساختار برای آن تکنولوژی می‌باشد که با ارائه این چارچوب در قالب معماری، می‌توان جایگاه و عملکرد کلیه مولفه‌های معماری را ارائه و روابط و اهداف آن را تبیین نمود [۷].

۳,۱. نیازمندی های امنیتی برای معماری

یکی از اهداف معماری این است که باید برای پاسخگویی به نیازها مناسب باشد. در این بخش نظرسنجی‌هایی از نیازهای کلیدی معماری برای پیاده سازی ابر معمولی است. چند عامل به عنوان انگیزه اساسی مورد نیاز برای خدمت، عبارتند از:

[1] Subdomains to Information Security
[2] Least Privilege Principle

هزینه ها و منابع: منابع مالی ارائه دهنده باعث محدود کردن سرمایه گذاری در فن آوری و کنترل امنیت می شود. اما مهم این است که عدم وجود منابع نامحدود می تواند انگیزه بسیاری برای طرحان، معماران و سازندگان باشد. ماهیت این محدودیت ها به سمت توسعه خدمات با ویژگی های عملیاتی است که ایده آل برای تمام مصرف کنندگان نیست.

قابلیت اطمینان: قابلیت اطمینان را می توان به عنوان یک تضمین از تکنولوژی زیر بنایی که می تواند خدمات شرح داده شده را ارائه کند در نظر گرفت.

کارایی: نسبت بازده واقعی بدست آمده به بازدهی استاندارد و تعیین شده(مورد انتظار) یا نسبت مقدار کاری که انجام می‌شود به مقدار کاری که باید انجام شود.

اصول سه گانه امنیت: محرمانه بودن، یکپارچگی و در دسترس بودن

محدودیت های قانونی و نظارتی:[3] محدودیت های قانونی و نظارتی نیاز به انجام کنترل های امنیتی فنی، سیاست های دسترسی، و نگهداری از داده ها را دارد.

۳,۲. معماری امنیتی ابر

همان طور که در شکل ۱ مشاهده می کنید، در پشته امنیت یک شبکه امنیتی اختصاص داده شده است که توابع امنیتی فردی را به عنوان ترکیبی از تیغه های اختصاصی فیزیکی (بایگانی SYSLOG) و ماشین های مجازی بیان شده است. لیستی از توابع عبارتند از:

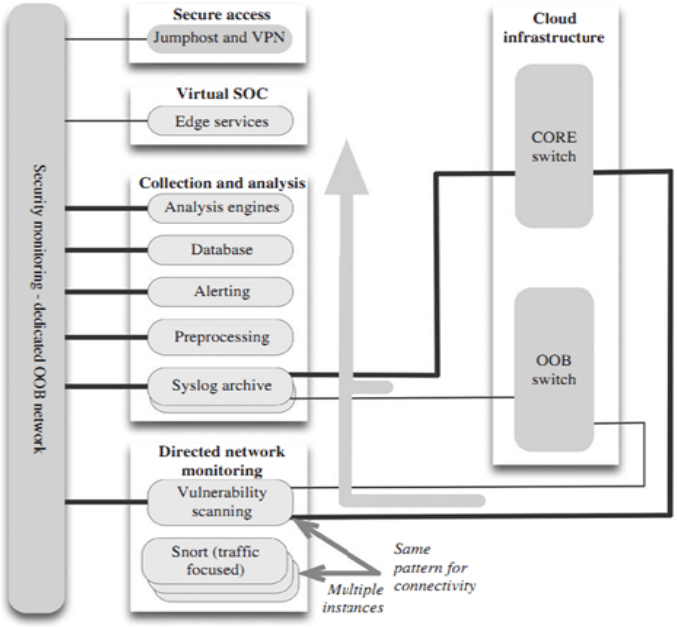
Jumphost و VPN: این فقط یک تیم امنیتی از مکانیسمی تعیین کننده، برای به دست آوردن دسترسی به شبکه‌ای امن است. یک مهندس امنیتی با توجه به نوع آدرس مبدأ می‌تواند وارد ابر شود، از طریق هسته و یا روترهای OOB ، که می تواند مستقیما متصل شود به jumphost امنیتی و یا VPN.

SOC مجازی: یک سری از رابط‌های کاربر به منظور نظارت بر کنسول ها و دیگر کنسول های امنیتی، برای اسکن، گزارش، تجزیه و تحلیل است.

جمع آوری و تجزیه و تحلیل: این یک مجموعه گسترده ای از قابلیت ها است که با مجموعه ای از SYSLOG و دیگر اطلاعات امنیتی از محاسبات SAN و سیستم های دیگر شروع می شود و از طریق شبکه های اصلی و OOB به آرشیو SYSLOG روت است. بعد از آن، منتقل می‌شود برای، تجزیه و تحلیل، هشدار، و اجزای IDS.

کارگردان مانیتورینگ شبکه:[4] شکل های دیگری از نظارت که در بخشی شامل بازرسی ترافیک شبکه و در بخش شامل آسیب پذیری تناوبی اسکن سیستم در محیط وجود دارد [۷].

[3] Legal and regulatory constraints
[4] Directed Network Monitoring



شکل ۱ - بررسی اجمالی از معماری مانیتورینگ امنیتی ابر

۴. مجازی سازی

مجازی سازی[5] یکی از تکنولوژی های نوظهور در دنیای IT می باشد، دانش و تکنیکی که با استفاده از آن می توان بر بسیاری از مشکلات و موانع موجود در عرصه زیر ساخت ها (نرم افزاری و سخت افزاری) فائق آمد و راه را برای توسعه پایدار و به وجود آوردن شرایط مناسب برای کسب و کار به بهترین نحو فراهم آورد.

کاربردهای مجازی سازی آنچنان گسترده است که نه تنها متخصصان و کارشناسان حوزه IT بلکه بسیاری از افراد در رشته های غیر مرتبط با کامپیوتر و IT نیز از آن بهره مند می گردند.

این روزها مجازی سازی تبدیل شده است به یک ضرورت فنی، که شامل مزایای بسیاری است از جمله موارد زیر:

۱. بهره وری هر چه بیشتر از سخت افزار و کاهش هزینه ها.

۲. مدیریت بهتر و آسانتر سرورها و سرویس ها و کاهش هزینه های مدیریتی.

۳. استفاده هر چه بهتر از فضای موجود در Data Center و کاهش هزینه های آن.

۴. پشتیبان گیری و بازیابی سرورها در حداقل زمان ممکن (Isaster Recovery And Backup).

۵. کاهش مصرف برق موجود در Data center که در شرایط کنونی حائز اهمیت بسیاری می باشد.

۶. در محیط های آموزشگاهی می توان با ایجاد ساخت چند ماشین مجازی به صورت بسیار مقرون به صرفه یک محیط آزمایشگاهی ایجاد نمود.

۷. صرفه جویی در انرژی برای زمین سبزتر [۹].

مجازی سازی ایجاد یک نسخه مجازی از چیزی مثل سیستم عامل، دستگاه محاسباتی (سرور)، دستگاه های ذخیره سازی و یا دستگاه های شبکه است. بسیاری مجازی سازی را با رایانش ابری یکسان می‌دانند که این اشتباهی بزرگ است. مجازی‌سازی معمولاً به عنوان یکی از فناوری‌های پایه‌ای رایانش ابری است

[5] Virtualization

(گرچه می‌توان از آن استفاده نکرد.). تفاوت اساسی بین ابر و مجازی‌سازی این است که هدف ابر خودکارسازی در اختیار گرفتن منابع است (این به هر سه نوع زیرساخت، بستر و نرم‌افزار به عنوان سرویس بر می‌گردد) و هدف مجازی‌سازی بهینه‌سازی استفاده از منابع است [۳].

۴,۱. انواع مجازی سازی

مجازی سازی می تواند باتوجه به نوع کاربرد، معانی زیادی برای بسیاری از مردم داشته باشد، که شامل موارد زیر است [۸]:

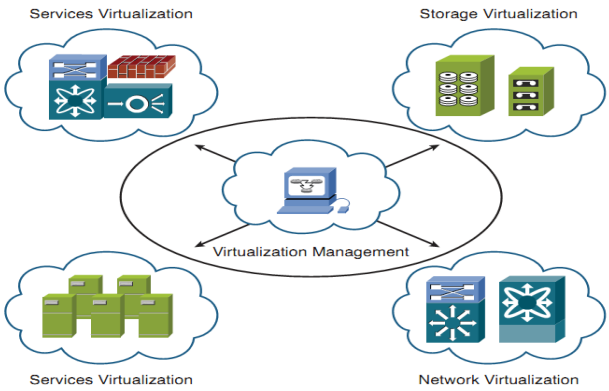
۱. مجازی سازی سرور[۶]

۲. مجازی سازی ذخیره سازی[۷]

۳. مجازی سازی شبکه[۸]

۴. مجازی سازی سرویس[۹]

شکل ۲ نشان می دهد که مجازی سازی سرور، مجازی سازی شبکه، مجازی سازی ذخیره سازی و مجازی سازی سرویس می تواند در یک مرکز داده وجود داشته باشد و با استفاده از مدیریت مجازی سازی اداره می شود. انواع دیگر از مجازی سازی می تواند وجود داشته باشد، اما این یک شروع برای تکنولوژی مجازی سازی در مراکز داده است.



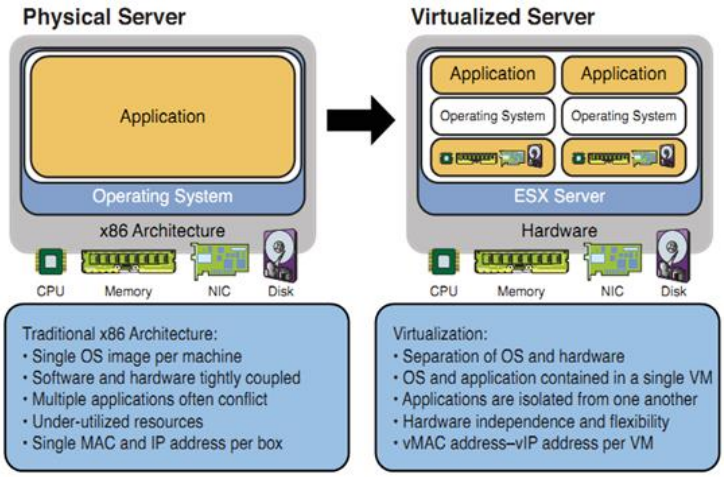
شکل ۲ - انواع مجازی سازی

۴,۱,۱. مجازی سازی سرور

مجازی سازی سرور (که همچنین به عنوان مجازی سازی سخت افزار نامیده می شود) بهترین و شناخته شده‌ترین روش کاربردی برای مجازی سازی سخت افزار است. سخت افزار کامپیوتر قدرتمند مبتنی بر x86 برای اجرای یک سیستم عامل تک و تنها یک برنامه طراحی شده بود. مجازی سازی به شما اجازه‌ی اجرای چندین ماشین مجازی بر روی یک ماشین فیزیکی منفرد را می‌دهد و همچنین می‌توانید منابع کامپیوتری در سراسر محیط های مختلف را به اشتراک بگذارید.

6 Virtualization Server
7 Storage virtualization
8 Network Virtualization
9 Service virtualization

ماشین‌های مجازی مختلف می تواند سیستم عامل‌های مختلف و برنامه های متعدد را بر روی همان کامپیوتر فیزیکی اجرا کنند. شکل ۳ یک سرور مجازی در مقابل یک سرور فیزیکی بدون مجازی سازی را نشان می دهد.



شکل ۳ - مجازی سرور

برخی از مزایای کلیدی مجازی سازی سرور به شرح زیر است:

جزء بندی: ۱. اجرای چندین سیستم عامل بر روی یک ماشین فیزیکی. ۲.تقسیم منابع سیستم فیزیکی در میان ماشین های مجازی است. ۳.یک VM از حضور دیگری اطلاعی ندارد.

مدیریت: ۱. شکست یک VM بر روی دیگر VMها تاثیر نمی گذارد. ۲. عوامل مدیریت را می توان در هر VM به طور جداگانه اجرا کرد.

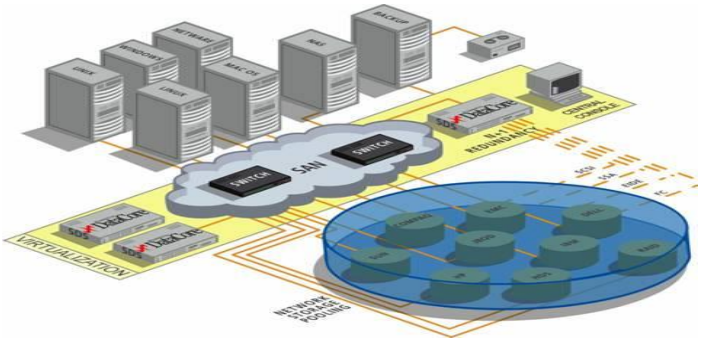
کپسوله کردن: ۱. کل حالت VM را می توان در یک فایل ذخیره کرد. ۲. انتقال و کپی کردن اطلاعات VM به آسانی کپی کردن فایل ها است

انعطاف پذیری: ۱. اجازه تأمین و مهاجرت هر VM به یک ماشین مشابه بر روی هر سرورو فیزیکی را می‌دهد. ۲. استفاده از چند سیستم عامل به عنوان مثال ویندوز، لینوکس. ۳. اجازه می دهد تا تغییرات پیکربندی VM انجام شود بدون اینکه VM واقعا از کار متوقف شود.

مجازی سازی سرور، نیروی محرکه اصلی در کاهش تعداد سرورهای فیزیکی و از این رو فضای فیزیکی، خنک کننده، کابل کشی، و هزینه های سرمایه در هر پروژه‌ی ترکیب مرکز داده است [۴].

۴,۱,۲. مجازی سازی ذخیره سازی

همان طور که در شکل ۴ نشان داده شده. مجازی سازی ذخیره سازی اشاره به ارائه منطقی و انتزاعی از دستگاه های ذخیره سازی فیزیکی است، که راه را برای بسیاری از کاربران و یا برنامه های کاربردی برای دسترسی به ذخیره سازی فراهم می کند بدون نیاز به دانستن اینکه کجا و چگونه ذخیره سازی فیزیکی انجام یا مدیریت می‌شود [۴].

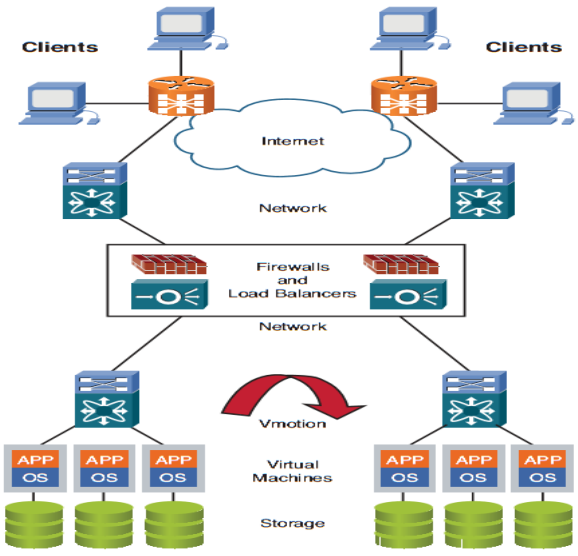


شکل ٤ - مجازی سازی ذخیره سازی

۴,۱,۳. مجازی سازی شبکه

به صورت خلاصه مجازی سازی شبکه را می‌توان به عنوان تکنیک‌هایی برای ایزوله کردن منابع شبکه و محاسباتی، برای تخصیص آنها به یک شبکه مجازی (منطقی)، جهت همساز کردن چندین شبکه مجازی قابل برنامه ریزی و مستقل، دانست.

شکل ۵ نشان می دهد که چگونه شبکه مجازی، محاسبه، و ذخیره سازی با یکدیگر در زیرساخت ارتباط برقرار کردند.



شکل ۵ - مجازی سازی شبکه

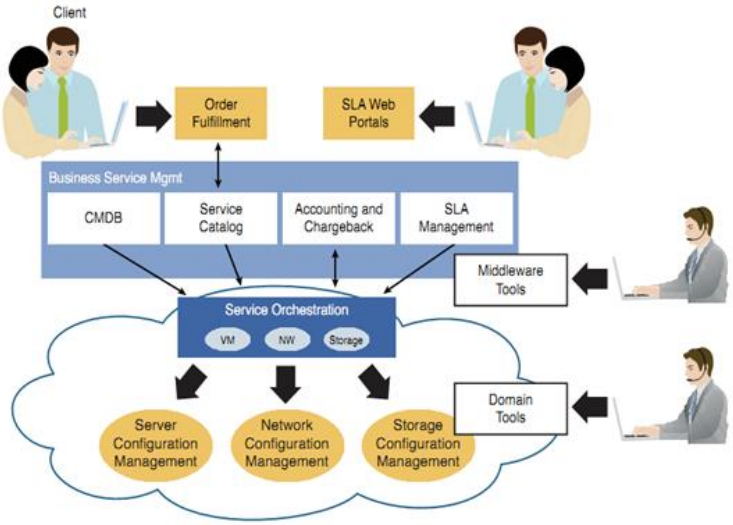
۴,۱,۴. مجازی سازی سرویس

خدمات مجازی سازی در مراکز داده، اشاره دارد به خدمات از جمله خدمات دیوار آتش برای امنیت بیشتر و یا خدمات متعادل کننده بار اضافی برای عملکرد و قابلیت اطمینان است [۳].

۴٫۱٫۵. مدیریت مجازی سازی

مدیریت مجازی سازی به تأمین هماهنگی و تنظیم منابع مجازی، و همچنین هماهنگی زمان اجرا از مخزن منابع و نمونه مجازی اشاره دارد . این ویژگی شامل نقشه برداری استاتیک و دینامیک از منابع مجازی به منابع فیزیکی، و همچنین به طور کلی قابلیت های مدیریت از قبیل ظرفیت، تجزیه و تحلیل، صدور صورت حساب، و SLAs است.

شکل ۶ نشان می دهد که چگونه شبکه، کامپیوتر، ذخیره سازی، با لایه مدیریت / تنظیم ارتباط برقرار کرده‌اند، بنابراین خدمات می توانند در زمان نزدیک به واقعیت ارائه شوند.



شکل ٦- مدیریت مجازی سازی

۵. امنیت در مجازی سازی

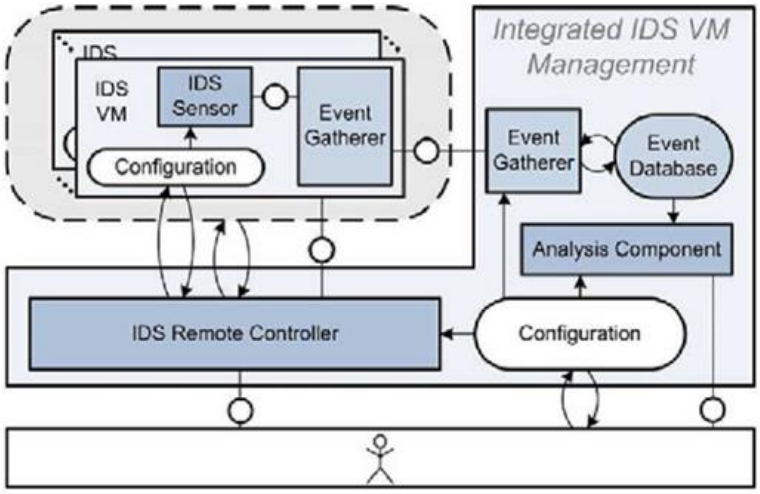
تکنولوژی نرم افزاری است که به دسترسی به اجزای مختلف در محیط مجازی سازی را کنترل کرده و از دسترسی غیر مجاز و خرابکارانه جلوگیری می کند. امنیت محیط مجازی اشاره به ابزاری دارد که برای کنترل دستیابی به لایه های مختلف تکنولوژی مجازی لازم است. امنیت مجازی سازی را از سه دیدگاه مختلف مورد بررسی قرار می‌دهیم.

۵٫۱. سیستم های امنیتی مبتنی بر مجازی سازی

سیستم های امنیتی در یک ماشین معمولی به گونه ای هستند که یک نفوذگر پس از نفوذ به سیستم می تواند به سادگی سیستم های امنیتی را متوقف کرده،کنترل ماشین را به دست گیرد و حضور خود را در سیستم مخفی می کند. یکی از دلایل بروز این مشکل این است که سیستم امنیتی در همان ماشینی اجرا می شود که می

خواهیم آن را نظارت کنیم. شکل ۷ نشان می دهد که ماشین های مجازی مزایایی دارند که آنها را برای فراهم کردن سرویس های امنیتی نسبت به ماشین های فیزیکی مناسب تر کرده است [۵].

تشخیص نفوذ: عبارت است از تحلیل بی‌درنگ داده‌های شبکه به منظور تشخیص و ثبت و اخطار به هنگام بروز حملات و یا اقدامات مخرب امنیتی. سیستم تشخیص نفوذ[1](IDS)، یک دستگاه یا برنامه نرم افزاری است که بر فعالیت های شبکه یا سیستم برای فعالیت های مخرب و یا ناقص سیاست نظارت می‌کند جهت تولید گزارش برای ایستگاه مدیریت. همانطور که در شکل نشان داده شده است، ماشین مجازی سازگار با معماری سیستم تشخیص نفوذ به طور کلی شامل دو جزء می‌باشد: واحد مدیریت سیستم تشخیص نفوذ و سنسور سیستم تشخیص نفوذ [۱].



شکل ۷ - معماری مدیریت یکپارچه سیستم تشخیص نفوذ ماشین مجازی

ممانعت از نفوذ: سیستم‌های جلوگیری نفوذ[1]که با نام سیستم‌های تشخیص و جلوگیری از نفوذ هم شناخته می‌شوند، ابزاری برای امنیت شبکه هستند که فعالیت‌های موجود در شبکه و یا سیستم را برای تشخیص و جلوگیری از فعالیت‌های مخرب تحت نظر می‌گیرند. وظایف اصلی یک سیستم جلوگیری نفوذ شامل شناسایی فعالیت‌های مخرب، ثبت اطلاعات در مورد این فعالیت‌ها، اقدام به بلوکه و متوقف کردن این فعالیت‌ها و ثبت گزارش کارهای انجام شده توسط خود سیستم می‌شوند.

سیستم‌های جلوگیری از نفوذ حالت ارتقاء یافته سیستم‌های تشخیص نفوذ محسوب می‌شوند چرا که هر دو این سیستم‌ها فعالیت‌های شبکه و یا سیستم را برای یافتن فعالیت‌های مخرب نظارت می‌کنند. تفاوت اصلی این سیستم‌ها با سیستم‌های تشخیص نفوذ در این است که این سیستم‌ها می‌توانند به صورت فعال مانع فعالیت‌های مخرب شده و یا آنها را متوقف کنند. به طور دقیق‌تر می‌توان گفت که یک سیستم جلوگیری نفوذ توانایی انجام کارهایی مانند ارسال هشدار، دور ریختن بسته‌های مخرب، بازنشاندن و یا بلوکه کردن ارتباط از طرف آدرس‌های متخاصم [۶].

نظارت بر جامعیت فایل: فایل‌های سیستمی معمولا از اهداف حملات مخرب هستند، زیرا حاوی مقدار زیادی از داده های حساس، از جمله برنامه های اجرایی، پیکربندی و اطلاعات مجوز است. فایل های نظارت بر جامعیت یک روش موثر برای کشف رفتارهای تهاجمی با تشخیص اعمال تغییر بر روی این فایل ها حساس است [۲].

1 Intrusion Detection System 0
1 Intrusion prevention system 1

۶. نتیجه‌گیری

مجازی‌سازی را می‌توان به عنوان پایه‌ای برای ساخت یک ابر بکار برد ولی الزامی نیست و آن را می توان به عنوان یک لایه انتزاعی تعریف کرد، و مجازی سازی می‌تواند در بخش هایی و یا در سراسر پشته IT وجود داشته باشد. مجازی سازی هم یک فرصت است و هم یک تهدید، از آنجایی که ماشین‌های مجازی در لایه زیرساخت محاسبات ابری قرار گرفته‌اند تضمین امنیت در این ماشین‌ها می‌تواند گام مؤثری در فراهم کردن اعتماد مشتریان باشد.

مراجع

1. *Habib, S. M., S. Hauke, and S. Ries, "Trust as a facilitator in cloud computing a survey," Journal of Cloud Computing: Advances, Systems and Applications, 1:19, 2012.*
2. *Huang, J. and D. M. Nl, "Trust mechanisms for cloud computing," Journal of Cloud Computing: Springer open Journal Advances, Systems and Applications, 2:9, 2013.*
3. *Li, J. B. Li, T. Wo and C. Hu, "CyberGuarder: A virtualization security assurance architecture for green cloud computing," FutureGenerationComputerSystems28(2012)379–390.*
4. *Lombardi, F. and R. Di Pietro, "Secure virtualization for cloud computing," Journal of Network and Computer Applications 34 (2011) 1113 –1122, 2011.*
5. *Modi, C. "A survey of intrusion detection techniques in Cloud," Journal of Network and Computer Applications 36 (2013) 42 – 57, 2012.*
6. *Patel, A. M. Taghavi, K. Bakhtiyari and J. C. Ju´ nior, "An intrusion detection and prevention system in cloud computing A systematic review," Journal of Network and Computer Applications 36 (2013) 25 –41*
7. *V. (J.R.) W. ler, Securing the Cloud: Cloud Computer Security Techniques and Tactics, 2012.*
8. *V. Josyula, M. Orr and G. Page, Cloud Computing: Automating the Virtualized Data Center, Paul Boger, 2011.*
9. *D. Kusnetzky, Virtualization: A Manager's Guide, O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2011*