اولین همایش ملی پیشرفت های تکنولوژی در مهندسی برق، الکترونیک و کامپیوتر

First National Conference of Technology Developments on Electronical, Electronics and Computer Engineering

. . . W W W . T D E C O N F . I R . . .

مقابله با حملات امنیتی به ابرها به کمک تکنیک های کاوش داده در شناسایی مزاحمت داده‌ای

فاطمه اسحقی، علی قوامی

دانشگاه پیام نور واحد تهران شمال،دانشگاه آزاد اسلامی واحد قزوین

نویسنده مسئول: فاطمه اسحقی

چکیده

رایانش ابری اصطلاحی است که برای ارائه خدمات میزبانی تحت اینترنت به کار رفته و به عنوان نسل بعدی معماری فناوری اطلاعات پیش بینی شده، پتانسیل بسیار خوبی را برای بهبود بهره وری و کاهش هزینه ها ارائه می‌دهد. در مقایسه با راه‌حلهای سنتی که در آن سرویسهای فناوری اطلاعات بر پایه کنترلهای فیزیکی و منطقی عمل میکنند؛ رایانش ابری، نرم افزارهای کاربردی و پایگاه داده‌ها را به سمت مراکز داده‌ای بزرگ سوق داده است. با این حال، ویژگیهای منحصر به فرد رایانش ابری، همواره با شمار بسیاری از چالشهای امنیتی جدید و شناخته نشده همراه بوده است. از دیگر سوی و در مبحث امنیت اطلاعات؛ شناسایی مزاحمت یا انحرافات داده‌ای، عبارتست است از شناسایی فعالیتهایی که تلاش می‌کنند یکپارچگی، قابلیت اطمینان و دسترس بودن یک منبع را به خطر بیندازند و شناسایی مزاحمت یا انحراف، در مجموع پیشگیری از مزاحمتهاست. در این مقاله، ضمن بررسی حملات امنیتی به ابرها از جمله: حملات بسته‌SOAP ، تزریق نرم افزارهای مخرب، حملات سیل آسا، سرقت اطلاعات و راه حل های مورد نیاز با توجه به این حملات؛ به ارائه راهکاری جدید در این خصوص به کمک سیستمهای تشخیص نفوذ داده کاو محور خواهیم پرداخت.

کلمات کلیدی: حملات امنیتی به ابر، سیستمهای تشخیص نفوذ، داده کاوی، شناسایی مزاحمت در سیستم.

۱- مقدمه

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

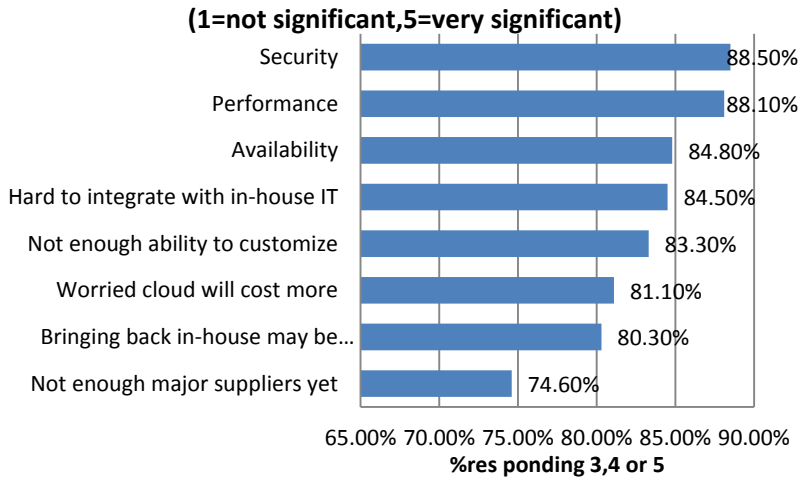
واضح است که رایانش ابری گام بعدی تکامل سرویس های فناوری اطلاعات برحسب تقاضا می‌باشد. با این حال مسئله امنیت در رایانش ابری یکی از مسائل پیچیده به شمار رفته که تمامی سه لایه ابر، مسئولیت هایی که بین کابران و ارائه دهندگان تقسیم می‌شود و حتی شخص ثالث را درگیر می‌کند. مشکلات امنیتی به عنوان یک مانع بزرگ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

۲- امنیت رایانش ابری

براساس بررسی های انجام شده در سال ۲۰۰۸ میلادی که در شکل (۱) نشان داده شده است، امنیت به عنوان مهمترین چالش رایانش ابری از میان ۹ چالش موجود شناخته شده است.[Kazi, Aunnurhain, Susun, Vrbsky,2012] با این وجود نگرانی هایی در مورد عملکرد و قابلیت در دسترس بودن رایانش ابری جزء دیگر چالشها پس از امنیت مطرح شده است. جدیدترین بررسی ها در سال ۲۰۱۲ حاکی از کاهش ۳۳.۵ درصدی چالش امنیت و رسیدن این درصد به عدد ۵۵ می‌باشد.
[Manish Joshi, -Classification,2012]

تهدیدهای امنیتی بر روی کاربران ابر به دو دسته داخلی و خارجی تقسیم بندی می‌شود [Michael, M. J,2013]. تهدیدهای خارجی شامل تهدید مراکز داده بزرگ می‌باشد که این نگرانی امنیتی در میان کاربران ابر و فراهم آورندگان (که به عنوان شخص ثالث در نظر گرفته شده اند) در حصول اطمینان از نرم

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



شکل ۱: چالش‌های رایانش ابری (بررسی‌های IDC در سال ۲۰۰۸)

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

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

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

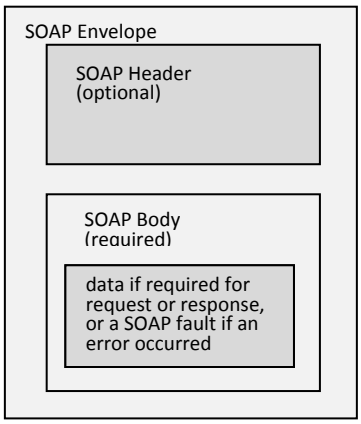
ج) به علت نفوذ کدهای مخرب در حال اجرا که توسط برنامه کاربردی کاربر یا تزریق اطلاعات ساختگی به برنامه توسط شخص ثالث صورت می گیرد. این رخداد در لایه پلتفرم به عنوان سرویس می‌تواند منجر به ایجاد نزاع و اختلاف بین ارائه دهنده و مشتری شود.

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

در ادامه مهمترین مسائل مربوط به امنیت رایانش ابری از جمله پیام SOAP[1] و حملات ابر که توسط دشمنان مزاحم آن صورت میگیرد مطرح می‌شود. وب سرویس، تکنولوژی‌ای است که اخیراً در معماری سرویس گرا (SOA) مورد استفاده قرار گرفته و به معنای ساده نوعی مولفه تحت وب است. این مولفه به برنامه های کاربردی که از آن استفاده می کنند این امکان را می دهد که بتوانند از متدهای این وب سرویس استفاده کنند. در سیستم ابر تبادل سرویس بین مرورگر وب کاربر و وب سرویس صورت می گیرد به طوری که درخواست های کاربر از طریق مرورگر خود به وب سرویس منتقل می‌شود. با این وجود سیستم امنیتی وب سرویس باید به اندازه کافی برای بهینه سازی امنیتی در برابر حملات دشمن مقاوم باشد. حملات امنیتی می‌تواند پیام های SOAP را مورد حمله قرار دهد. SOAP پیام های متنی مبتنی بر Xml است که برای تبادل اطلاعات کدگذاری شده بین وب سرویس و کاربر با استفاده از پروتکل های مختلف از جمله HTTP، SMTP و MIME به کار می رود. SOAP اجازه می دهد که یک برنامه رد حال اجرا در یک سیستم با یک برنامه در حال اجرا در یک سیستم دیگر بدون در نظر گرفتن مدل برنامه نویسی آن‌ها تماس برقرار کند.[Shetty M. and Shekokar N,2012]

[1] Simple Object Access Protocol

پیام SOAP به دو واحد سر پیام و بدنه همانند شکل (۲) تقسیم بندی می‌شود. که در آن سر پیام بسته SOAP از دو قسمت رمز امنیت دودویی و برچسب زمانی تشکیل شده است. که در آن قسمت رمز امنیت دودویی شامل مجوز برقراری ارتباط با وب سرویس و برچسب زمانی حاوی تاریخ ساخت و انقضای پیام SOAP می‌باشد.



در شروع ارتباط با وب سرویس، کاربر می‌بایست جهت ارسال درخواست و دریافت پاسخ خود از وب سرویس مجوزی را دریافت نماید. پس از دریافت مجور کاربر قادر به ادامه ارتباط با وب سرویس و دریافت پیام SOAP می‌باشد.همانگونه که قبلاً ذکر شد بسته SOAP می‌تواند مورد حمله Wrapping قرار بگیرد. حمله مذکور با حفظ شناسه بسته و تغییر در قسمت بدنه آن می‌تواند محتویات بسته در حال انتقال را دستخوش تغییر گرداند و با ایجاد یک بدنه ساختگی برای پیام به فعالیت بپردازد.

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

۲-۱- حمله به بسته SOAP[۲]

هنگامی که کاربر درخواست خود را از طریق مرورگر خود به سمت وب سرور می فرستد، در سمت سرور پیام SOAP که شامل اطلاعات ساختاری تبادل اطلاعات بین سرور و مرورگر می‌باشد، ساخته می‌شود. همانطور که گفته شد پیام SOAP دارای دو قسمت سر پیام حاوی امضا و بدنه جهت نگهداری اطلاعات می‌باشد.

[Meiko, Jenson, Jorg Schwenk,2012]

مهاجم در پی حمله خود به پیام SOAP، با نگهداری سر پیام یک بسته، قسمت بدنه آن را تغییر داده و بدنه ساختگی خود را در بسته جایگذاری نموده و با استفاده از IP معتبر به ابر حمله می‌کند حال چنانچه سرپیام بسته فوق علامتگذاری شود دیگر مهاجم نمی‌تواند با ارائه IP معتبر به سرور عمل کند. این کار با استفاده از تعریف کلید RSA از طرف فراهم آورنده برای کاربر صورت می گیرد. معمولترین و مشهورترین الگوریتم نامتقارن به عنوان RSA شناخته می‌شود که می توان از یک سیستم نامتقارن برای نشان دادن اینکه فرستنده پیام همان شخصی است که ادعا می‌کند، استفاده کرد. این عمل اصطلاحاً امضای دیجیتال نام دارد. امضا، متن اصلی را با استفاده از کلید اختصاصی رمز می‌کند، رمزگشایی عملیات مشابه ای روی متن رمز شده اما با استفاده از کلید عمومی است.

برای تأیید امضا بررسی می کنیم که آیا این نتیجه با اطلاعات اولیه یکسان است یا خیر. به بیان ساده تر چنانچه متنی از شخصی برای دیگران منتشر شود، این متن شامل متن اصلی و همان متن اما رمز شده توسط کلید اختصاصی همان شخص است. حال اگر متن رمز شده توسط کلید عمومی آن شخص که شما از آن مطلع هستید رمزگشایی شود، مطابقت متن حاصل و متن اصلی نشان دهنده صحت فرد فرستنده آن است، به این ترتیب امضای فرد تصدیق می‌شود. افرادی که از کلید اختصاصی این فرد اطلاع ندارند قادر به ایجاد متن رمز شده نیستند، به طوری که با رمزگشایی توسط کلید عمومی این فرد به متن اولیه

[2] Wrapping Attack

تبدیل شود. بدین ترتیب فرد فرستنده نمی‌تواند منکر فرستادن متن شود، زیرا کسی به جز او نمی توانسته آن متن را به شکل مطلوب امضا کند. در این صورت هر کاربر RSA منحصر به فرد خود را برای ارتباط با سرور در اختیار دارد.

۲-۲= حمله از طریق کدهای مخرب[3]

نوع دیگری از حمله که حقه بازی ابر داده[4] نیز نامیده می‌شود در ادامه بررسی می‌شود. در سیستم های ابری درخواست های کاربر براساس تشخیص هویت شناسایی و اجرا می‌شوند. چنانچه محتوای درخواستهای سمت سرور زیاد باشد سرور باید درخواست ها را زمان بندی کند. در برقراری ارتباط اولیه یک سری ابرداده بین کاربر و سرور جابجا می‌شود. در این مرحله است که مهاجم از فرصت استفاده کرده و با رسوخ در سرویس در حال اجرا، سرویس ساختگی خود را به صورت یک سرویس در حال اجرای معتبر درآورده و با ایجاد کدها یا سرویس های مخرب به استراق سمع اقدام می نماید. چنانچه مهاجم موفق به حمله به کاربری که درخواست خود را به سمت سرور فرستاده شود، باید برای زمان بندی درخواستی که خود منجر به تولید آن نشده است منتظر بماند. [IEEE Computer Society,2010]

هنگامی که فراهم کننده سرویس ابر حسابی را به کاربر اختصاص می دهد فراهم آورنده نهایی یک تصویر از ماشین مجازی کاربر در منبع تصویری سیستم ابر برای کاربر ساخته می‌شود. پس از آن به هنگام ارسال درخواست سمت سرور از طریق کاربر برنامه های کاربردی کاربر به صورت چندین درخواست در حال اجرا و کاملاً یکپارچه بر روی ماشین مجازی قرار می گیرند. حال به دلیل دشوار بودن حمله به لایه زیرساخت به عنوان سرویس برای مهاجم، یکپارچگی فوق باید در سطح ماشین مجازی پیاده سازی شود. راه‌حل ارائه شده جهت مبارزه با ایجاد کدهای مخرب استفاده از جدول تخصیص فایل (FAT) است، که توسط همه سیستم عامل های موجود بر روی ماشین مجازی پشتیبانی می‌باشد. با کمک جدول تخصیص فایل می توان به برنامه در حال اجرای کاربر پی برد. با این کار تاریخچه برنامه در حال اجرای کاربر و مراحل قبل و بعد آن را می‌تواند مشخص نمود. جهت تحقیق این هدف به یک Hypervisor که روی سیستم نهایی پیاده سازی می‌شود نیاز خواهیم داشت.

۲-۳- حمله سیل آسا[5]

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

راه‌حل پیشنهادی برای مقابله با حملات سیل آسا، ایجاد ناوگانی از سرورها می‌باشد که در آن هر ناوگان جهت انجام کار خاصی در نظر گرفته شده است که با یکدیگر و سرور نام در ارتباط هستند. به طور مثال تعدادی از سرورها عمل مدیریت حافظه و تعدادی جهت مدیریت فایل در نظر گرفته می‌شوند. حال در این طراحی جدید چنانچه بار روی یک سرور بالا رود سرور جدید وارد عمل شده، بارگذاری جدید به آن منتقل شده و بدین ترتیب جهت جدول موجود در سرور نام به روز رسانی می‌شود.

۲-۴- سرقت اطلاعات[6]

یکی از راه های سنتی و معمول حمله به ابر سرقت اطلاعات از طریق به دست آوردن حساب کاربری و رمز عبور می‌باشد. در طی این نوع حمله که در محیط های خوشه ای، توری و ابری رخ می دهد، مهاجم به سرقت اطلاعات محرمانه یا تخریب داده های کاربر اقدام می‌کند که این امر موجب برهم زدن یکپارچگی داده ها و امنیت موجود در ابر می‌شود. در پایان هر استفاده کاربر از ابر، ارائه دهنده ایمیلی حاوی میزان استفاده و مانده حساب را به کاربر ارسال می‌کند.

---

[3] Malware– Injection
[4] Meta–Data Spoofing
[5] Flooding Attack
[6] Data Stealing

بدین ترتیب کاربر اطلاعات کاملی را از سرویس‌گیری خود دریافت کرده و چنانچه سرقت اطلاعات از طریق مهاجمی صورت گیرد وی با بررسی حساب خود می‌تواند به آن پی ببرد.

۳- سیستمهای تشخیص نفوذ

از آنجایی که از نظر تکنیکی، ایجاد سیستمهای کامپیوتری (سخت افزار و نرم افزار) بدون نقاط ضعف و شکست امنیتی عملاً غیرممکن است؛ تشخیص نفوذ در تحقیقات سیستمهای کامپیوتری با اهمیت خاصی دنبال می شود. سیستمهای تشخیص نفوذ (IDS) برای کمک به مدیران امنیتی سیستم در جهت کشف نفوذ و حمله به کار گرفته شده‌اند.

سیستمهای تشخیص نفوذ (IDS) وظیفه شناسایی و تشخیص هرگونه استفاده غیرمجاز از سیستم، سوء استفاده و یا آسیب رسانی توسط هر دو دسته ی کاربران داخلی و خارجی را بر عهده دارند. سیستم های تشخیص نفوذ به صورت سیستم های نرم افزاری و سخت افزاری ایجاد شده و هر کدام مزایا و معایب خاص خود را دارند .سرعت و دقت از مزایای سیستم های سخت افزاری است و عدم شکست امنیتی آن ها توسط نفوذگران، قابلیت دیگر این گونه سیستمها می باشد. اما استفاده آسان از نرم افزار، قابلیت انطباق پذیری در شرایط نرم افزاری و تفاوت سیستم های عامل مختلف، عمومیت بیشتری را به سیستمهای نرم افزاری می دهد و عموماً این گونه سیستم ها انتخاب مناسب‌تری هستند. به طور کلی سه عملکرد اصلی (IDS) عبارتند از: نظارت و ارزیابی، کشف و واکنش. بر همین اساس، هر IDS را میتوان بر اساس رو شهای تشخیص نفوذ، معماری و انواع پاسخ به نفوذ دسته بندی کرد. [IEEE Computer Society,2009]

۳-۱- انواع روشهای تشخیص نفوذ

نفوذ به مجموعه اقدامات غیرقانونی که صحت و محرمانگی و یا دسترسی به یک منبع را به خطر می اندازد، اطلاق می گردد. نفوذ ها می توانند به دو دسته ی داخلی و خارجی تقسیم شوند. نفوذهای خارجی به آن دسته نفوذهایی گفته می شود که توسط افراد مجاز و یا غیرمجاز از خارج شبکه به درون شبکه ی داخلی صورت می گیرد و نفوذهای داخلی توسط افراد مجاز در سیستم و شبکه ی داخلی، از درون خود شبکه انجام می پذیرد.

نفوذگرها عموماً از عیوب نرم افزاری، شکستن کلمات رمز، استراق سمع ترافیک شبکه و نقاط ضعف طراحی در شبکه، سرویسها و یا کامپیوترهای شبکه برای نفوذ به سیستم ها و شبکه های کامپیوتری بهره می برند. به منظور مقابله با نفوذگران به سیستم ها و شبکه های کامپیوتری، روش های متعددی تحت عنوان رو شهای تشخیص نفوذ ایجاد گردیده است که عمل نظارت بر وقایع اتفاق افتاده در یک سیستم یا شبکه ی کامپیوتری را بر عهده دارد. روشهای تشخیص مورد استفاده در سیستم های تشخیص نفوذ به دو دسته: ۱) روش تشخیص رفتار غیرعادی و ۲) روش تشخیص سوء استفاده یا تشخیص مبتنی بر امضاء؛ تقسیم می شوند.[Manish Joshi,2012]

۱) روش تشخیص رفتار غیرعادی

در این روش، یک نما از رفتار عادی ایجاد می شود. یک ناهنجاری ممکن است نشان دهنده ی یک نفوذ باشد. برای ایجاد نماهای رفتار عادی از رویکردهایی از قبیل شبکه ها ی عصبی، تکنیک های یادگیری ماشین و حتی سیستم های ایمنی زیستی استفاده می شود که برای تشخیص رفتار غیرعادی، باید رفتارهای عادی را شناسایی کرده و الگوها و قواعد خاصی برای آن ها پیدا کرد. رفتارهایی که از این الگوها پیروی می کنند، عادی بوده و رویدادهایی که انحرافی بیش از حد معمول آماری از این الگوها دارند، به عنوان رفتار غیرعادی تشخیص داده می شود. نفوذهای غیرعادی برای تشخیص بسیار سخت هستند، چون هیچگونه الگوی ثابتی برای نظارت وجود ندارد. معمولاً رویدادی که بسیار بیشتر یا کمتر از دو استاندارد انحراف از آمار عادی به وقوع می پیوندد، غیرعادی فرض می شود. به عنوان مثال اگر کاربری به جای یک یا دو بار ورود و خروج عادی به سیستم در طول روز، بیست بار این کار را انجام دهد، و یا کامپیوتری که در ساعت ۲:۰۰ بعد از نیمه شب مورد استفاده قرار گرفته در حالی که قرار نبوده کامپیوتر فوق پس از ساعت اداری روشن باشد. هر یک از این موارد می تواند به عنوان یک رفتار غیر عادی در نظر گرفته شود. [Ye Qing,2010, Deepthy K Denatious and Anita John,2012]

۲) روش تشخیص سوءاستفاده یا تشخیص مبتنی بر امضاء

در این تکنیک که معمولاًبا نام تشخیص مبتنی بر امضاء شناخته شده است، الگوهای نفوذ از پیش ساخته شده (امضاء) به صورت قانون نگهداری می شوند. به طوری که هر الگو انواع متفاوتی از یک نفوذ خاص را در بر گرفته و در صورت بروز چنین الگویی در سیستم، وقوع نفوذ اعلام می شود. در این روشها، معمولاً تشخیص‌دهنده دارای پایگاه داده ای از امضاء ها یا الگوهای حمله است و سعی می کند با بررسی ترافیک شبکه، الگوهای مشابه با آن چه را که در پایگاه داده ی خود نگهداری می کند، بیابد. این دسته از روش ها تنها قادر به تشخیص نفوذهای شناخته شده می باشند و در صورت بروز حملات جدید در سطح شبکه،

نمی توانند آن ها را شناسایی کنند و مدیر شبکه باید همواره الگوی حملات جدید را به سیستم تشخیص نفوذ اضافه کند. از مزایای این روش دقت در تشخیص نفوذهایی است که الگوی آن ها عیناً به سیستم داده شده است. [D. Zhao, Q. Xu and Z. Feng,2013]

۳-۲ انواع معماری سیستم های تشخیص نفوذ

۱- سیستم تشخیص نفوذ مبتنی بر میزبان (HIDS)

این سیستم، شناسایی و تشخیص فعالیت های غیرمجاز بر روی کامپیوتر میزبان را بر عهده دارد. سیستم تشخیص نفوذ مبتنی بر میزبان می تواند حملات و تهدیداتی را روی سیستم های بحرانی تشخیص دهد (شامل دسترسی به فایل ها، اسب های تروا و غیره که توسط سیستم های تشخیص نفوذ مبتنی بر شبکه قابل تشخیص نیستند). HIDS.ها به واسطه ی مکان شان روی میزبانی که باید نظارت شود، از همه ی انواع اطلاعات محلی اضافی با پیاده سازی‌های امنیتی (شامل فراخوانی های سیستمی، تغییرات فایل های سیستمی و اتصالات سیستم) مطلع می باشند. این مساله هنگام ترکیب با ارتباطات شبکه‌ای، داده های خوبی را برای جستجوی رویداد های ممکن فراهم می کند. [Y. Qing, W. Xiaoping and H. Gaofeng,2012]

۲- سیستم تشخیص نفوذ مبتنی بر شبکه (NIDS)

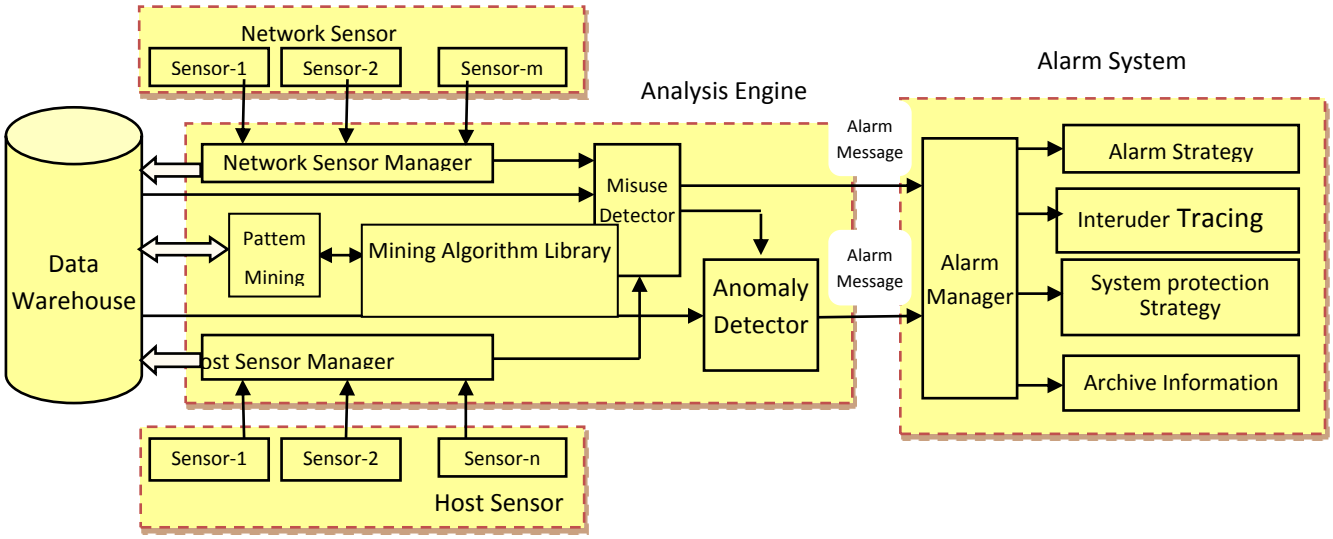
نام NIDS از این حقیقت مشتق شده است که از منظر محلی که قرار گرفته، بر تمام شبکه نظارت دارد. شناسایی و تشخیص نفوذهای غیرمجاز قبل از رسیدن به سیست مهای بحرانی، به عهد هی سیستم تشخیص نفوذ مبتنی بر شبکه استNIDS ها اغلب از دو بخش ناظر (حسگر) و عامل تشکیل شده اند. این دو بخش اغلب در پشت دیواره ی آتش و بقی هی نقاط دسترسی برای تشخیص هر نوع فعالیت غیرمجاز نصب می شود .عامل های شبکه می توانند جایگزین زیرساختار شبکه شوند تا ترافیک شبکه را جستجو کنند. نصب عام لها و ناظرها این مزیت را دارد که هر نوع حمله ای را در ابتدا از بین می برد. ضمناً دنباله های بررسی یک یا چند میزبان می توانند برای جستجوی علائم حملات، مفید باشند. [G. Xiaoqing, G. Hebin and C. Luyi,2012]

۳- سیستم تشخیص نفوذ توزیع شده (DIDS)

این سیستم ها از چندین NIDS یا HIDS یا ترکیبی از این دو نوع همراه یک ایستگاه مدیریت مرکزی تشکیل شده است. بدین صورت که هر IDS که در شبکه موجود است گزارش های خود را برای ایستگاه مدیریت مرکزی ارسال میکند. ایستگاه مرکزی وظیفه بررسی گزارشهای رسیده و آگاه سازی مسئول امنیتی سیستم را برعهده دارد. [L. Wenjun,2013]

۳-۳- سیستم تشخیص نفوذ داده کاو محور با استفاده از تکنولوژی انبار داده

در ادامه مدل دیگری موسوم به سیستم تشخیص نفوذ ترکیبی ارائه میگردد که از ترکیب سیستم‌های تشخیص نفوذ مبتنی بر میزبان و مبتنی بر شبکه بوده و از تشخیص براساس امضا و آنومالی استفاده میکند. تکنولوژی انبار داده به این جهت مفید است که اجزای مختلف به صورت غیرهمزمان قسمت‌های مشابه‌ای از داده‌های ذخیره شده در پایگاه داده را دستکاری می‌کنند. بنابراین انبار داده قلب داده‌ها و مدل‌ها در تمام سیستم است. در این مقاله، سنسورها بطور نزدیکی مرتبط با سیستم عامل هستند و سنسورهای میزبان اطلاعات مشاهده در هاست‌ها را با گسترده‌ای از روش‌ها نظیر Application Logs و Security Logsو Event Logs و تغییرات رجیستری و نرم افزارهای در حال اجرا جمع‌آوری می‌کنند.



شکل ۳: انبار داده شامل اعمال مدیریت پروسه تصمیم گیری، جمع آوری داده‌های یکپارچه و نهادگرا و ... جهت پشتیبانی از تکنولوژی‌های چند نخی و چند پردازشی

بعد از تنظیم ویژگی‌های حسابرسی، ویندوز سرور حالت‌های مختلف سیستم را نظارت می‌کند و آنها را در فایل‌های log ذخیره می‌کند. با کمک توابع API ویندوز می‌توان برنامه‌ای را توسعه داد تا System log ها و تغییرات رجیستری و کاربردهای در حال اجرا را بگیرد و آنها را به Host sensor manager مربوط به موتور تحلیل ارسال کند تا در آنجا تحلیل شود. قبلاً در مورد استفاده از توابع هوک برای این منظور توضیح داده شده است. در سنسورهای شبکه به کمک ابزار ویندوزی netstat، سنسورهای شبکه می‌توانند اطلاعاتی راجع به اتصالات شبکه جمع آوری کنند. فرمان netstat می‌تواند اطلاعاتی راجع به پورتهای باز سیستم جمع آوری کند. می‌توانیم یک برنامه طراحی کنیم تا فرمان netstat را در فواصل منظم اجرا کند و خروجی را به یک فایل منتقل کند. می‌توان این برنامه را به گونه‌ای بهینه کرد تا تنها اطلاعات مورد نیاز را بگیرد، برای اینکار ابتدا تمام پورت‌های باز لیست می‌شوند و پورت هایی نظارت می‌شوند که تازه باز شدند و تازه بسته شده اند. رکوردهای اطلاعات به Network sensor manager ارسال می‌شود. رکوردهای اطلاعات شامل Port services، Port number، Activation time، Time stamp و غیره میشوند. Analysis Engine شامل سه قسمت است: مدیر سنسورهای هاست/ شبکه، شناساگر آنومالی و امضا، کتابخانه الگوریتم‌های پویش و پویش الگو.

۱) مدیرهای سنسور، داده‌ها را از سنسورها دریافت می‌کنند، سپس داده‌ها را تحلیل می‌کنند آنگاه آنها را به شکلی از رکوردهای پایگاه داده ترجمه می‌کنند و آنها در انبار داده‌ها ذخیره می‌کنند.

۲) در شناسایی آنومالی و امضا، نفوذها را براساس الگوها تطبیق دهنده ذخیره شده در انبار داده، تشخیص می‌دهند.

۳) کاوش کتابخانه الگوریتم‌ها و کاوش الگو برای شناسایی حملات ناشناخته از الگوریتم‌های تحلیل مانند تحلیل انجمنی و تحلیل الگوی توالی و تحلیل طبقه بندی می‌شود که در تحلیل طبقه بندی از لگوریتم طبقه بندی بیز استفاده شده است.

۴- بحث و نتیجه‌گیری

رایانش ابری انقلابی در نحوه استفاده، مدیریت سرویس ها و منابع می‌باشد. اما این تحول با مشکلات جدید همراه شده است. در این مقاله برخی از مشکلات مهم و حملات امنیتی و راه‌حل‌های مبارزه با آن‌ها از جمله جدول تخصیص فایل و یکHypervisor شرح داده شد. مفهوم و چارچوبی که در این مقاله مورد بحث قرار گرفت به ایجاد یک ساختار امنیتی قوی در شاخه رایانش ابری کمک خواهد کرد. این امنیت ساختار بندی شده با دسترسی از طریق VPN تا حد بالایی قادر به بهبود رضایت مشتریان و جذب سرمایه گذاران بیشتری در این مفهوم از رایانش خواهد بود. ساختن یک سیستم تشخیص نفوذ داده کاو محور به صورت بلادرنگ واقعی کاری بسیار دشوار است برای نیل به این هدف باید حجم داده‌های اولیه را کاهش دهیم زیرا که الگوریتم‌های محاسباتی در داده کاوی بار محاسباتی زیادی دارد بنابراین تشخیص بلادرنگ واقعاً بلادرنگ نخواهد بود. از سوی دیگر یکی از مسئله‌های اساسی در مورد سیستم‌های تشخیص نفوذ این است که آنها فقط نفوذ در سطح شبکه را تشخیص می‌دهند اما اگر نفوذ بر روی یک نرم افزار خاصی باشد قادر به تشخیص نیست زیرا که بسیاری از حمله‌ها ممکن است در سطح نرم افزار باشد به گونه‌ای که تأثیری بر ترافیک شبکه مدنظر نداشته باشد.

۵- منابع مورداستفاده

- Michael, M. J., A view Of Cloud Computing, Communications of the ACM, April 2013.
- Kazi, Aunnurhain, Susun, Vrbsky, SecurityIn Cloud Computing, University of Albama, 2012.
- Shetty M. and Shekokar N., "Data Mining Techniques for Real Time Intrusion Detection Systems", International Journal of Scientific & Engineering Research Volume 3, Issue 4, April 2012.
- Meiko, Jenson, Jorg Schwenk. On Technical. Security Issued in Cloud Computing. IEEE International Conference On Cloud Computing, 2012.
- IEEE Computer Society, 2010 Sixth International Conference on Semantics, Knowledge and Grids, Security and Privacy in Cloud Computing: A Survey, 2010.
- Kazi, Aunnurhain, Susun, Vrbsky, Security Attacks and Solutions in Clouds, University of Albama, 2009.
- Manish Joshi, -Classification, Clustering and Intrusion Detection System‖, International Journal of Engineering Research and Applications (IJERA), pp.961-964, ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2, Mar-Apr 2012.
- Ye Qing, Wu Xiaoping and Huang Gaofeng. An Intrusion Detection Approach based on Data Mining‖, 2nd International Conference on Future Computer and Communication, pp. No. 695 – 698, 2010 IEEE.
- Deepthy K Denatious and Anita John, ―Survey on Data Mining Techniques to Enhance Intrusion Detection‖, International Conference on Computer Communication and Informatics, Jan 2012.
- D. Zhao, Q. Xu and Z. Feng, "Analysis and Design for Intrusion Detection System Based on Data Mining", IEEE Second International Workshop on Education Technology and Computer Science, pp 339-342, 2013.
- Y. Qing, W. Xiaoping and H. Gaofeng," An Intrusion Detection Approach based on Data Mining", 2nd International Conference on Future Computer and Communication, Volume 1, pp 695-698, 2012.
- G. Xiaoqing, G. Hebin and C. Luyi, "Network Intrusion Detection Method Based on Agent and SVM", 2010.
- L. Wenjun, "A Security Model: Data Mining and Intrusion Detection", 2nd International Conference on Industrial and Information Systems, pp 448-450, 2013.