

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



دانشگاه پیام نور تهران

شهری

سمینار، سمینار تحقیق و تتبع نظری

گرایش: نرم افزار

عنوان:

تشخیص و جلوگیری از نفوذ افراد غیرمجاز در سیستم مبتنی بر رایانش ابری با استفاده از
تجزیه و تحلیل الگوهای رفتاری

استاد راهنما:

جناب آقای دکتر سید علی رضوی ابراهیمی

نگارش:

احسان مخمی

زمستان ۱۳۹۹

فهرست مطالب

صفحه	عنوان
4	1-مقدمه.....
5	1-1-مقدمه.....
6	1-2-محاسبات. ابری.....
8	1-3-اهمیت و ضرورت مطالعه امنیت و تشخیص نفوذ در ابر.....
10	1-4-مدل پیشنهادی این مطالعه.....
11	1-5-نواوری و جنبه جدید بودن این تحقیق.....
12	1-6-ساختار سمینار.....
13	2-ادبیات پژوهش.....
14	2-1-مقدمه.....
15	2-2-ساختار محاسبات ابری.....
15	2-2-1-معماری.....
16	2-2-2-فراهم کننده سرویس ابر.....
16	2-2-3-انواع ارائه خدمت.....
17	2-2-4-کاربران محیط محاسبات ابری.....
17	2-3-امنیت در محیط محاسبات ابری.....
19	2-3-1-تهدیدات امنیتی محیط محاسبات ابری.....
19	2-3-1-1-حمله اخلال در خدمت رسانی.....
20	2-3-1-2-حمله شنود اطلاعات.....
20	2-3-1-3-دزدی اطلاعات شبکه.....
20	2-3-1-4-پویش درگاه.....
20	2-3-1-5-حمله دستورات SQL.....

- 20.....2-3-1-6-تزریق بدافزار به ابر
- 21.....2-3-1-7-نفوذ از طریق رابط کاربری ضعیف
- 21.....2-3-1-8-خودیهای مخرب
- 21.....2-3-1-9-حمله ربات ها
- 21.....2-4-سیستم های تشخیص نفوذ
- 22.....2-4-1-انواع حملات شبکه ای با توجه به حمله کننده
- 23.....2-5-انواع سیستم های تشخیصی نفوذ
- 23.....2-5-1-سیستم های تشخیص نفوذ مبتنی بر میزبان
- 24.....2-5-2-سیستم های تشخیص نفوذ مبتنی بر شبکه
- 24.....2-6-اجزای تشکیل دهنده سیستم های تشخیص نفوذ بر شبکه
- 25.....2-6-1-سیستم های توزیع شده
- 28.....2-7-انواع روش های تشخیص حمله
- 28.....2-7-1-روش های مبتنی بر امضاء
- 29.....2-7-2-روش های تشخیص حمله مبتنی بر ناهنجاری
- 31.....2-7-3-روش های مبتنی بر تحلیل حالت پروتکل ارتباطی
- 34.....3-ادبیات تحقیق
- 35.....3-1-مقدمه
- 35.....3-2-سیستم های تشخیص نفوذ و مدیریت ورودی چند سطحی در محاسبات ابری [29]
- 36.....3-3-جایگذاری یک NIDS در یک محیط محاسبات ابری [30]
- 37.....3-4-ابراهای دوقلو: یک معماری برای محیط ابری امن
- 38.....3-5-تشخیص نفوذ در سیستم با استفاده از منطق فازی
- 39.....3-6-تشخیص سلسله مراتبی نفوذ به روش ناهنجاری به وسیله شبکه های عصبی

فهرست شکل‌ها

شکل

صفحه

شکل 1: معماری محاسبات ابری در مجموعه سیستم‌های کامپیوتری [9]..... 15

شکل 2: معماری ساختاری محاسبات ابری 16

شکل 3: معماری IDS های توزیع شده با استفاده از حسگرهای بی اثر و با امکان توزیع بار 27

شکل 4: معماری پیشنهادی در [4]..... 37

فهرست جداول

صفحه	عنوان
19.....	جدول 1: حوزه‌های ریسک‌پذیر و بحرانی در مجازی‌سازی و محاسبات ابری.....
35-36.....	جدول 2: دسته‌بندی حملات با توجه به میزان خسارت.....

چکیده:

رایانش ابری، مدلی است که به ارائه دسترسی آسان، توزیع شده و فراگیر به منابع محاسباتی تجمیعی و مشترک قابل پیکربندی، می پردازد. در رایانش ابری، قابلیت های مبتنی بر فناوری اطلاعات به عنوان خدماتی که نیازی به دانش دقیق از فناوری های زیرساختی و کمترین تلاش مدیریتی داشته باشد، ارائه می شود. با توجه به این موضوع، یکی از مسائل مهم، تمرکز چالش های امنیتی بر فناوری های نوین است. مفیدترین جنبه های استفاده از ابر شامل: اجرای سریع و آسان مدل، پرداخت به میزان استفاده و کاهش هزینه های درون سازمانی است. با این وجود، با توجه به اینکه امنیت مهم ترین موضوعی است که به منظور استفاده گسترده از رایانش ابری باید مورد توجه قرار گیرد، ارائه دهندگان رایانش ابری نیاز دارند که چالش های امنیتی متداول سامانه های ارتباطی پیشین را برطرف نموده و همچنین آن ها باید هم زمان با آن به مباحث دیگری که توسط الگوی رایانش ابری معرفی می گردد، پردازند. در این سمینار هدف، معرفی یک سیستم تشخیص نفوذ کارا می شود به گونه ای که باعث بالا رفتن دقت سیستم و بالا رفتن سرعت تشخیص نفوذ می گردد و در نهایت با توجه به نتیجه به دست آمده می توان میزان و درصد احتمال آشکارسازی یا تشخیص نفوذ را تشخیص داد. عملکرد سیستم به این صورت است که با استفاده از روش درخت تصمیم C 4.5 نسبت به انتخاب ویژگی های تأثیرگذار در مجموعه داده اقدام نموده و پس از آن از شبکه های عصبی مصنوعی با استفاده از الگوهای رفتاری استخراج شده، جهت آموزش و نهایتاً جلوگیری از نفوذ استفاده شده است. برای ارزیابی روش پیشنهادی نیز مقایساتی با برخی از روش های موجود در این زمینه صورت گرفته است که ارزیابی ها بیان گر دقت روش پیشنهادی است.

کلمات کلیدی:

محاسبات ابری، ارتقای امنیت داده ها، شبکه عصبی مصنوعی، درخت تصمیم، تشخیص نفوذ

فصل اول

مقدمه

1-1- مقدمه

با پیشرفت فناوری اطلاعات نیاز به انجام کارهای محاسباتی در همه جا و همه زمان به وجود آمده است. همچنین نیاز به این هست که افراد بتوانند کارهای محاسباتی سنگین خود را بدون داشتن سخت افزارها و نرم افزارهای گران، از طریق خدماتی انجام دهند. محاسبات ابری آخرین پاسخ فناوری به این نیازها بوده است. محاسبات ابری مدلی است برای فراهم کردن دسترسی آسان، بر اساس تقاضای کاربر از طریق شبکه به مجموعه‌ای از منابع محاسباتی قابل تغییر و پیکربندی مثل شبکه‌ها، سرورها، فضای ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها که این دسترسی بتواند با کمترین نیاز به مدیریت منابع و یا نیاز به دخالت مستقیم فراهم‌کننده سرویس به سرعت فراهم‌شده یا آزاد گردد [۱]. محاسبات ابری، مدلی است که به ارائه دسترسی آسان، توزیع‌شده و فراگیر به منابع محاسباتی تجمیعی و مشترک قابل پیکربندی، می‌پردازد. در محاسبات ابری، قابلیت‌های مبتنی بر فناوری اطلاعات به عنوان خدماتی که بدون نیاز به دانش دقیق از فناوری‌های زیرساختی و کمترین تلاش مدیریتی در دسترس قرار می‌گیرد، ارائه می‌شود. درواقع محاسبات ابری توانایی بهره‌وری و صرفه‌جویی در منابع IT و افزایش توان محاسباتی را فراهم می‌کند، به‌طوری‌که توان پردازشی به ابزاری با قابلیت دسترسی همیشگی تبدیل می‌شود. اگرچه محاسبات ابری مزایای زیادی دارد؛ ولی امنیت در ابر بسیار حائز اهمیت است.

به دلیل فراگیر شدن پردازش ابری^۱ و افزایش حجم داده‌ها نیاز است که کار تحلیل داده‌ها در مقیاس بزرگ انجام شود، زیرا امروزه یکی از حیاتی‌ترین نیازهای یک سرویس‌دهنده ابری این است که کار تحلیل داده‌ها برای تمامی سطوح کاربران فراهم شود، بنابراین نیاز به داشتن یک سیستم مدیریت پایگاه داده کارا بیش‌ازپیش برای یک سرویس‌دهنده ابری اهمیت دارد. مدیریت منابع در ابر خصوصی می‌تواند بر روی طراح امنیتی ابر تأثیر بسیاری بگذارد. ازجمله مسائلی که در این زمینه مطرح است می‌توان به مسائل مربوط به استفاده مجدد منابع توسط برنامه‌های کاربردی مشتریان مختلف، مسائل مربوط به خدمات مشترکی که بر روی یک سرور متعلق به مشتریان مختلف است و مسائل مربوط به فرآیندهای خودکار که تخصیص یافتن و آزاد کردن منابع را مدیریت می‌کند، اشاره کرد [۲].

^۱ Cloud Computing

محاسبات ابری در کنار مزایا و فوایدی که فراهم می‌کند با چالش‌های نگران‌کننده‌ای پیرامون امنیت مواجهه است. حفظ امنیت و حریم خصوصی نیاز به سیاست‌ها و راهکارهایی دارد تا مورد اطمینان کاربر واقع شود. این بزرگ‌ترین مانع بر سر راه پذیرفتن این سبک است. اینکه کاربران و سازمان‌ها داده‌های خود را در محلی غیر از سازمان خود نگهداری و پردازش می‌کنند برای عده زیادی قابل‌پذیرش نیست و نمی‌توان مطمئن بود که افراد غیرمجاز قادر به دسترسی به داده‌هایشان نیستند. این نگرانی از دو جهت بررسی می‌شود، یکی جلوگیری از خواندن اطلاعات خصوصی توسط دیگران مانند مشتریان دیگر است، که یک نگرانی روشن و آشکار است که در سناریوهای مانند سرقت یا سایر حملات مخرب مستقیم نمایان است. مسئله دیگر موضوع خواندن اطلاعات خصوصی ارائه‌دهنده سرویس است. در حقیقت چالش بنیادی همان امنیت و حفظ حریم خواهد بود [۳].

1-2- محاسبات ابری

مفاهیم اساسی محاسبات ابری در سال ۱۹۶۰ میلادی توسط "جان مک کارتی" از بنیان‌گذاران هوش مصنوعی ارائه شد اما در آن زمان با استقبال چندانی مواجه نشد. محاسبات ابری نوعی فناوری است که با استفاده از اینترنت و سرویس‌دهنده (های) مرکزی، از داده‌ها و برنامه‌های نگهداری می‌کند و به مصرف‌کنندگان اجازه می‌دهد تا بدون آنکه هیچ‌یک از برنامه‌های کاربردی مورد نیاز خود را نصب یا آن‌ها را خریداری کنند، از آن‌ها استفاده کنند. پرواضح است که هر ایده یا روش جدید، دارای مزایا و معایبی است، از جمله مزایای محاسبات ابری می‌توان به عدم محدودیت مکانی و زمانی، اشتراک‌گذاری ساده منابع و همچنین کاهش هزینه‌های سرمایه‌ای و عملیاتی (مهم‌ترین مزیت) اشاره کرد، چراکه در واقع محاسبات ابری به صورت پویا منابع مقیاس‌پذیری را به عنوان سرویس بر روی اینترنت ارائه می‌دهد. از معایب محاسبات ابری نیز می‌توان به امنیت پایین، عدم حفظ حریم خصوصی، دسترسی محدود به سرویس‌دهنده، هزینه‌های بالای باند، مشکلات مربوط به تغییر سرویس‌دهنده و آسیب‌پذیری در شرایط بحران اقتصادی اشاره کرد [۳]. با گسترش روزافزون رایانه و همچنین وابستگی بشر به دنیای دیجیتال، محققان همواره به دنبال راهی به منظور سرعت بخشیدن و ارتقای خدمات به مشتریان خود بوده‌اند که امروزه پردازش ابری این امر را محقق می‌کند. پردازش ابری یک پدیده‌ی نوظهور در علم رایانه است و دلیل این نام‌گذاری آن

است که داده‌ها و برنامه‌ها در میان ابری از سرویس‌دهنده‌های وب قرار گرفته‌اند. به‌طور ساده، پردازش ابری یعنی استفاده اشتراکی از برنامه‌ها و منابع در محیط شبکه، بدون این‌که مالکیت و مدیریت منابع شبکه و برنامه‌ها برای ما مهم باشد. در حال حاضر تعریف استاندارد از محاسبات ابری ارائه نشده است اما با این حال تعریفی که بیشتر محققان روی آن اتفاق نظر دارند به این صورت است:

محاسبات ابری مدلی است برای دسترسی آسان به مجموعه‌ای از منابع محاسباتی، این منابع (همچون شبکه‌ها، سرویس‌دهنده‌ها، فضای ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها) قابل تغییر و پیکربندی هستند. در محاسبات ابری، مدیریت منابع و دخالت مستقیم تأمین‌کننده به حداقل می‌رسد و سرویس‌ها به سرعت فراهم یا آزاد می‌شوند. همواره یک ابررایانه‌ای در دو قسمت پیکربندی می‌شود. بخش انتهایی و بخش ابتدایی. بخش ابتدایی همان قسمتی است که کاربران مشاهده می‌کنند و درواقع شکل ظاهری نرم‌افزار است و بخش انتهایی همان "ابر" رایانه‌ای است که پردازش‌ها را در برمی‌گیرد و درواقع می‌توان گفت نرم‌افزاری که برای ارتباط با بخش انتهایی مورداستفاده قرار می‌گیرد نیز جزء بخش ابتدایی است [۴].

برخی از ویژگی‌های محاسبات ابری برگرفته از مدل‌های محاسباتی دیگر (همچون محاسبات شبکه‌ای، محاسبات خودمختار، مدل مشتری/سرویس‌دهنده، محاسبات همگانی، محاسبات توزیع‌شده، نظیر به نظیر) است، اما تفاوت از آن‌ها است. پردازش شبکه‌ای، ترکیبی از پردازش موازی و پردازش ترکیب‌شده که در آن یک ابررایانه مجازی و تعدادی رایانه شبکه شده به‌صورت هماهنگ یک پردازش بزرگ را انجام می‌دهند. پردازش همگانی، مجموعه‌ای از منابع محاسباتی است و درواقع محاسبه و ذخیره‌سازی داده‌ها در مقیاس عمومی و به‌صورت خدمات اندازه‌گیری انجام می‌شود. در پردازش خودمختار نیز رایانه‌ها قابلیت خودگردان دارند. بنابراین همان‌طور که در بالا هم گفته شد واضح است که محاسبات ابری متفاوت از این محاسبات ذکرشده است. موضوع مهمی که اخیر در پردازش ابری موردتوجه قرار گرفته است امنیت است، اما با این حال هنوز هم امنیت در پردازش ابری یک چالش بزرگ محسوب می‌شود. از سوی دیگر برای برقراری و تأمین امنیت بایستی به بررسی و تشخیص تهدیدات احتمالی و محافظت از فرآیندهای امنیتی و پلتفرم‌های میزبان پرداخت.

1-3- اهمیت و ضرورت مطالعه امنیت و تشخیص نفوذ در ابر

مهم‌ترین نگرانی و چالش در خصوص استفاده از محاسبات ابری امنیت و حریم خصوصی افراد می‌باشد. سپردن اطلاعات محرمانه به یک شرکت، باعث تردید در حرکت به سمت محاسبات ابری است. ولی در نهایت کاربران مجبور به برون‌سپاری قسمتی از اطلاعات خود و نگهداری از سایر آن‌ها خواهند شد. همچنین میزبانی داده‌ها بر روی زیرساخت‌های به اشتراک گذاشته‌شده و برون‌سپاری شده در مکانی با سیستم قضایی متفاوت با مکان صاحبان این داده‌ها مستلزم ضمانت‌هایی در حوزه قانونی و مسائل حریم شخصی است. محاسبات ابری با وجود داشتن مزایای زیاد، همواره دارای تهدیدات امنیتی بی‌شماری برای اطلاعات در حال تبادل است که باعث می‌شود مشتریان از بهره بردن از مزایای ابر بازمانند. برخی از این تهدیدات در ادامه آورده شده است. تهدیدات داخلی از درون سازمان‌های ارائه‌دهنده سرویس به وجود می‌آیند. به این معنی که مشتریان داده‌های مهم و حیاتی خود را در فضای ابر میزبان ذخیره می‌کنند. اگر کارکنان سازمان به علت داشتن دسترسی به این داده‌ها، از اطلاعات مشتریان سوءاستفاده کنند، شرکت ارائه‌دهنده ابر شهرت خود را در بین مشتریان از دست خواهد داد. از روش‌های مقابله با این چالش می‌توان به اجرای دقیق مدیریت زنجیره تأمین، شفافیت شیوه‌های مدیریتی، امنیت اطلاعات و وجود یک سیستم گزارش‌گیری از نقص‌های امنیتی برای جلوگیری از انواع حمله‌ها اشاره کرد.

با وجود اینکه تهدیدات داخلی برای ارائه‌دهندگان ابر یک تهدید بزرگ است ولی تهدیدات خارجی هم می‌تواند تأثیر بسیار زیادی داشته و باعث بروز خسارت‌هایی به سیستم و فرآیندهای آن شود. نقاط ضعف یک سازمان ارائه‌دهنده می‌تواند راهی برای مهاجمان خارج از سازمان باز کرده و باعث حملات مخرب خارجی شود، به‌طور مثال مهاجمان می‌توانند از ضعف¹ API ها و کانال‌های ارتباطی استفاده کرده و سازمان را مورد حمله قرار دهند. برای حفاظت سازمان در برابر چنین تهدیداتی استفاده از فایروال‌ها و سیستم‌های تشخیص و پیشگیری از نفوذ بسیار ضروری است. همچنین پیاده‌سازی یک Honey Pot و استفاده از قانون² AAA ضروری است [۵].

¹ Application Program Interface

² Authentication & Authorization & Accounting

در محاسبات ابری داده‌های مشتریان در مکان ناشناخته‌ای که از دید کاربران پنهان است ذخیره می‌شود و مشتریان هیچ‌گونه کنترل و مدیریتی روی داده‌های حیاتی خود ندارند و هیچ‌گونه آگاهی از مکانیسم امنیتی که توسط ارائه‌دهنده پیاده‌سازی شده، ندارند. از دست دادن کنترل روی داده‌های حیاتی و سرویس‌های بحرانی و حساس می‌تواند در هر سازمانی اختلال ایجاد کند. عدم کنترل روی داده‌های حساس از سوی مشتریان ممکن است باعث از دست رفتن داده‌ها شود. این امر موجب از بین رفتن نام تجاری و شهرت سازمان‌های ارائه‌دهنده ابر شود. برای کاهش مشکلات کنترل دسترسی و افزایش دسترسی پذیری و کارایی، ایجاد یک توافق‌نامه در سطح سرویس بین سرویس‌دهنده و مشتری الزامی است. همچنین استفاده از یک احراز هویت بسیار قوی و فرآیند مجوز دهی، منجر به کاهش این چالش می‌شود. منظور از احراز هویت قوی این است که سازمان‌ها برای کاربران خود از روش Single Sign On استفاده کنند تا کاربران برای دسترسی به همه سرویس‌ها و برنامه‌های کاربردی موردنظر در هر قسمت از محیط ابراز یک احراز هویت واحد استفاده کنند.

ماهیت اصلی محاسبات ابری ارائه سرویس است، هرگونه اختلال در ارائه سرویس می‌تواند منجر به قطع سرویس و از بین رفتن شهرت سازمان ارائه‌دهنده ابر شود. اگر مهاجمان بتوانند به اعتبارنامه ورود سازمان سرویس‌دهنده و اعتبارنامه ورود مشتریان دسترسی پیدا کنند می‌توانند داده را تغییر داده، سرویس‌ها را مورد حمله قرار داده و آن‌ها را متوقف کنند. از جمله حمله‌هایی که می‌توان در این چالش‌ها برشمرد، حمله‌های DOS، DDOS، Phishing، Froud و... است. این تهدید در اثر وجود ثبت نام نسبتاً ضعیفی است که در محیط محاسبات ابری به وجود می‌آید که می‌تواند باعث حمله هکرها به سیستم شود. در واقع ثبت نام بدین معنی است که به هر مشتری برای دریافت سرویس‌ها یک حساب کاربری معتبر از سوی سرویس‌دهنده داده می‌شود. یکی از راه‌حل‌های موجود برای کاهش این چالش، عدم به اشتراک‌گذاری حساب کاربری بین مشتریان یک ارائه‌دهنده است که با استفاده از یک احراز هویت چندعاملی انجام می‌شود. ارائه‌دهنده ابر باید بتواند دائماً ترافیک شبکه مشتری را بازرسی کند و با یک سیستم پیشگیری از نفوذ بتواند از هر اقدام خرابکارانه‌ای جلوگیری کند [۶].

همان‌طور که گفته شد، محیط رایانش ابری معماری توزیع‌شده دارد، آسیب‌پذیر و مستعد حمله و نفوذ است. سیستم‌های تشخیص نفوذ سنتی برای این کار مناسب نیستند. یکی از چالش‌های رایانش ابری، قابلیت دسترسی است که حمله انکار سرویس (DOS) و دیگر حملات تهدیدی برای آن خواهد بود. برای شناسایی و جلوگیری از این‌گونه حملات از سیستم تشخیص نفوذ استفاده می‌شود. بعلاوه، متدلوژی‌های نفوذ و استراتژی‌های حمله به موازات تکنولوژی سیستم‌های تشخیص نفوذ در ابر تکامل یافته‌اند. از این‌رو IDS ی که چند سال پیش به خوبی کار می‌کرده، ممکن است امروزه نامناسب باشد. بنابراین عجیب نیست که اخیراً محققان در زمینه تشخیص نفوذ متمرکز شده‌اند. همچنین مسئله انتخاب ویژگی مناسب و دسته‌بندی در یک محیط چندعاملی¹، مسئله پیچیده‌ای است. از این‌رو تکنیک‌های یادگیری ماشین به‌طور گسترده‌ای مورد تحقیق و بررسی قرار گرفته‌اند. متدهای زیادی برای شناسایی حملات پیشنهاد شده‌اند، برخی از آن‌ها پیکربندی‌های مختلفی از سیستم‌های تشخیص نفوذ پیشنهاد کرده‌اند. در زمینه تحلیل هشدارها نیز تکنیک‌های متعددی مانند یادگیری ماشین، مدل‌سازی سری‌های زمانی² و استفاده از نمودارهای کنترل³ و غیره ارائه شده است. محدودیت‌ها و مشکلات محققان را به سمت استفاده و به‌کارگیری تکنیک‌های یادگیری ماشین برای حل مشکلات سوق می‌دهد و این فرصت را ایجاد می‌کند که یادگیری ماشین کمک و مشارکت مهمی در زمینه سیستم‌های تشخیص نفوذ داشته باشد. در این پژوهش قصد داریم یک راهکار جدید مبتنی بر یادگیری ماشین ارائه کنیم که هدف آن شناسایی و جلوگیری حملات مخرب و ایجاد امنیت در سطح قابلیت دسترسی برای کاربران ابر است.

4-1- مدل پیشنهادی این مطالعه

در دنیای محاسبات ابری در کنار مزایا و فوایدی که استفاده این سبک محاسباتی فراهم می‌کند با چالش‌های نگران‌کننده‌ای پیرامون امنیت مواجهه روبرو است. حفظ امنیت و تشخیص نفوذ نیاز به سیاست‌ها و راهکارهایی دارد تا مورد اطمینان کاربر واقع شود. این بزرگ‌ترین مانع راتبه‌گیر راه پذیرفتن این سبک است. اینکه کاربران و سازمان‌ها داده‌های خود را در محلی غیر از سازمان خود نگهداری و پردازش می‌کنند برای عده زیادی قابل پذیرش نیست و نمی‌توان مطمئن بود که افراد غیرمجاز قادر به دسترسی به داده‌هایشان نیستند. رایانش ابری⁴ را می‌توان توانایی اشتراک‌گذاری منابع محاسباتی فیزیکی در بین بسیاری از کاربران

¹ Multi-agent

² Modeling time series

³ Control charts

⁴ Cloud Computing

مختلف در نظر گرفت. رایانش ابری صرفه‌جویی در منابع فن‌آوری اطلاعات افزایش توان محاسباتی مانند شبکه‌ها، سرویس‌دهنده‌ها، ذخیره‌سازی داده و غیره را بدون دسترسی فیزیکی فراهم می‌کند. باوجود مزایای بی‌نظیر ابر^۱ نمی‌توان چالش‌های امنیتی آن را مانند افشای داده، حریم خصوصی و حمله به سرویس‌دهنده را نادیده گرفت [۷].

یکی از چالش‌هایی که در این تحقیق به آن می‌پردازیم، قابلیت دسترسی است که در شرایط ساده قابلیت دسترسی به این معنی است که مجموعه کامل از منابع سازمان در تمام اوقات قابل دسترسی و قابل استفاده باشد. دسترسی می‌تواند موقتی یا همیشگی باشد و از دست دادن دسترسی می‌تواند به صورت جزئی یا کامل باشد. حمله انکار سرویس (DOS)، قطعی برق تجهیزات و بلایای طبیعی همه تهدیدی برای وقفه سرویس‌دهی رایانش خواهد بود.

از آنجایی که محیط رایانش ابری معماری توزیع شده دارد، آسیب‌پذیر و مستعد حمله و نفوذ است. با توجه به پیچیدگی فرایند کشف نفوذ در ابر و از طرفی کارآمدی تکنیک‌های یادگیری ماشین، این تحقیق بنا دارد با تلفیق تکنیک‌های یادگیری ماشین به صورت لایه‌ای به ساخت مدل تشخیص نفوذ در ابر بپردازد. روش پیشنهاد شده که هشدارها را به پنج کلاس Normal، DOS، Probe، R2L، U2R^۲ تقسیم می‌کند.

این روش از چندین لایه تشکیل شده که هر لایه وظیفه تشخیص یک نوع حمله را بر عهده دارد. لایه‌ها در این سیستم به صورت مستقل از یکدیگر عمل می‌کنند. هر لایه به صورت مجزا آموزش داده می‌شود. روش پیشنهادی از تلفیق الگوریتم شبکه‌های عصبی مصنوعی و ماشین بردار پشتیبان برای شناسایی حملات استفاده می‌کند. و همچنین برای تست و ارزیابی از مجموعه داده‌های مربوط به NSL_KDD استفاده خواهیم کرد.

1-5- نوآوری و جنبه جدید بودن این تحقیق

در این پژوهش تلاش می‌شود تا با به کارگیری ترکیبی از الگوریتم‌های یادگیری ماشین، حملات مخرب شناسایی و سرکوب گردند. اگرچه تحقیقات زیادی در این زمینه انجام شده است اما مشکلات به طور کامل برطرف نشده‌اند. از طرفی راهکارهای ارائه شده دارای برخی نواقص و مشکلات هستند که در عمل باعث

¹ Cloud

² Remote to Local

³ User to Root

تضعیف عملکرد سیستم تشخیص نفوذ خواهد شد. روش پیشنهادی از تلفیق الگوریتم شبکه‌های عصبی مصنوعی و ماشین بردار پشتیبان برای شناسایی حملات استفاده می‌کند. و همچنین برای تست و ارزیابی از مجموعه داده‌های مربوط به NSL_KDD استفاده خواهیم کرد.

1-6- ساختار سمینار

مطالب این سمینار در سه فصل گردآوری شده است که فصول بعدی به شرح زیر می‌باشند.

فصل دوم: ادبیات پژوهش

در این فصل به بیان جزییات مسئله امنیت و تشخیص نفوذ در محاسبات ابر پرداخته می‌شود و این مسئله از دیدگاه‌های متفاوتی مورد بررسی قرار می‌گیرد. علاوه بر این در این فصل الگوریتم‌های یادگیری ماشین و الگوریتم شبکه عصبی همراه با جزییات هر یک مورد مطالعه قرار می‌گیرد.

فصل سوم: ادبیات تحقیق

در این فصل برخی از بهترین و جدیدترین روش‌های ارائه شده برای حل مسئله تشخیص نفوذ در ابر معرفی می‌گردد. علاوه بر آن جزییات هر یک از این روش‌ها بیان گردیده و از نظر روش کار و نتایج مورد انتظار با روش معرفی شده در این تحقیق مورد مقایسه قرار می‌گیرد.

فصل دوم

ادبیات پژوهش

2-1- مقدمه

رایانش ابری نامی است که به روند اخیر ارائه سرویس محاسبه، داده‌شده است. این روند به‌عنوان یک گذر در آماده بودن سرویس محاسبه از محلی به محل دیگر از راه دور و به‌یک‌باره توسط سرویس‌دهندگان شخص ثالث دیده می‌شود. قابلیت‌هایی از قبیل فضای ذخیره‌سازی، پردازش و سایر قابلیت‌ها، مثل یک سرویس و به‌صورت آزاد و به‌صرفه اکنون برحسب تقاضا پیشنهاد داده می‌شوند.

داده‌ها که زمانی تحت مدیریت شخصی مصرف‌کنندگان و دامین امنیتی قرار داشتند، اکنون استخراج شده و تحت دامین سرویس‌دهنده ابری^۱ قرار گرفته است. مصرف‌کننده به‌طور مؤثر کنترل روی اینکه داده‌هایشان چگونه ذخیره، اشتراک‌گذاری و استفاده می‌شوند و همچنین کنترل روی امنیت به‌کاررفته برای حفاظت داده‌هایشان را از دست داده است. به‌علاوه، می‌تواند موردی به وجود بیاید که یک کارمند از سرویس‌دهنده به داده‌های شما برای مقاصد مشروع و قانونی دسترسی محرمانه داشته باشد اما از آن دسترسی برای مقاصد شخصی خود سوءاستفاده کند. زمانی که کاربران نهایی از خدمات ابری استفاده می‌کنند و داده‌های خود را در زیرساخت ارائه‌دهندگان، ذخیره می‌کنند، مهم‌ترین جنبه‌های امنیتی مربوط به حریم خصوصی و محرمانگی داده‌های کاربران می‌باشد. کاربران نهایی می‌خواهند بدانند که اطلاعات آن‌ها در کجا ذخیره می‌شود و چه کسانی بر اطلاعات آن‌ها کنترل و دسترسی دارند و همچنین کاربران تمایل دارند تا تضمینی به آن‌ها در این راستا داده شود که حتی دسترسی غیرقانونی به داده‌های حساس و مهم آن‌ها توسط ارائه‌دهندگان خدمات صورت نگیرد.

کاربران نهایی بدون آگاهی دقیق از این‌که منابع چنین خدماتی در کجا واقع شده‌اند از خدمات ارائه‌شده توسط ارائه‌دهندگان ابری استفاده می‌کنند. زمانی که رخداد امنیتی روی می‌دهد این‌یک مشکل بالقوه را نشان می‌دهد که گاهی از کنترل ارائه‌دهندگان ابری فراتر می‌رود. داده‌های ذخیره‌شده توسط ارائه‌دهندگان خدمات ابری تنها تحت تأثیر خط مشی‌های ارائه‌دهندگان قرار ندارد بلکه تحت تأثیر قانون کشورهای مقیم ارائه‌دهنده قرار می‌گیرد. کاربران دیگر روی امنیت داده‌های خود کنترل کامل ندارند و حفاظتی که از سوی سرویس‌دهنده پیشنهاد می‌شود کامل و مطلق نیست. نیازی برای کاربران وجود دارد مبنی بر اینکه

^۱ Cloud Service Provider (CSP)

کنترل بیشتری روی حفاظت داده‌هایشان در ابر داشته باشند: کاربران نیاز دارند قدرتمند شوند. در این فصل محیط ابر و مسائل و چالش‌های موجود در آن را به تفصیل بررسی نموده و سپس مسائل مربوط به حوزه یادگیری ماشین و شبکه عصبی را با جزئیات مورد مطالعه قرار خواهیم داد.

2-2- ساختار محاسبات ابری

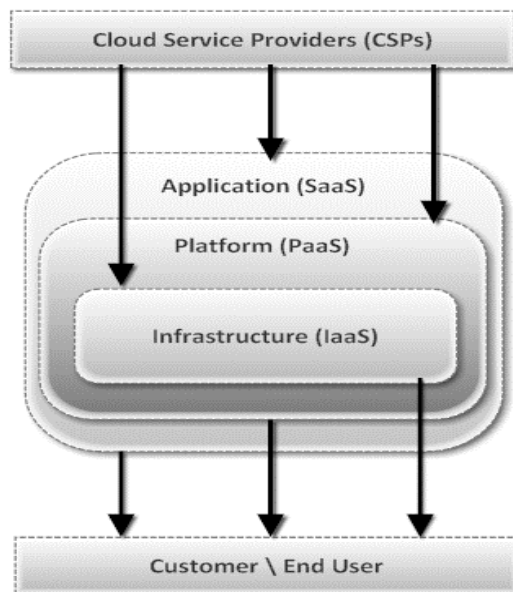
2-2-1- معماری

معماری محاسبات ابری به گونه است که معماری‌های دیگر همچون معماری نرم‌افزاری، معماری میان‌افزاری، معماری فن‌آوری اطلاعات و معماری خدمات گرا را در خود جای داده و آن‌ها را به عنوان منابع مدیریت می‌کند [۱۲]. نحوه قرارگیری محاسبات ابری در سیستم را می‌توانید در شکل ۳ ببینید.



شکل 1: معماری محاسبات ابری در مجموعه سیستم‌های کامپیوتری [9]

اما معماری کل محاسبات ابری از لحاظ پیاده‌سازی را می‌توان در شکل ۴ مشاهده نمود که به شرح زیر آن‌ها را توضیح خواهیم داد.



شکل 2: معماری ساختاری محاسبات ابری

2-2-2- فراهم‌کننده سرویس ابر

فراهم‌کننده سرویس کسانی هستند که بستری برای استفاده از منابع موجود فراهم می‌کنند. سرویس‌دهندگان می‌توانند یک یا چند سرویس که در میانه شکل ۴ نشان داده شده را فراهم کند؛ بنابراین می‌تواند سه دسته سرویس‌دهندگان نرم‌افزار، سرویس‌دهندگان بستر و سرویس‌دهندگان زیرساخت را معرفی نمود.

2-2-3- انواع ارائه خدمت

در محیط محاسبات ابری عموماً سه خدمت عمده را به‌عنوان ساختار خدمات‌رسانی به‌صورت اولویت‌بندی شده ارائه می‌دهد؛ که به ترتیب ارائه نرم‌افزار به‌عنوان خدمت، ارائه بستر به‌عنوان خدمت و ارائه زیرساخت به‌عنوان خدمت نام دارند. در ابتدای این زنجیره نیز فراهم‌کنندگان قرار دارند و در انتها نیز کاربران می‌باشند.

ارائه نرم‌افزار به‌عنوان خدمت در بالاترین و ساده‌ترین لایه محاسبات ابری مجموعه نرم‌افزارها به‌عنوان یک خدمت ارائه می‌گردد. تمام نرم‌افزارهای موجود را می‌تواند در این بخش ارائه نمود. پایگاه داده نیز می‌تواند در این بخش ارائه گردد. یکی از اولین ساده‌ترین نرم‌افزارها خدمات ایمیل می‌باشد که می‌توانید

در آن‌ها پیام‌های خود را نگهداری و مدیریت کنید؛ اما امروزه برنامه‌هایی همچون مدیریت ارتباط با مشتری، مدیریت منابع سازمانی، مدیریت زنجیره چرخه و... نیز در این لایه ارائه می‌گردند [۱۳].

2-2-4- کاربران محیط محاسبات ابری

کاربران این محیط را می‌تواند به دودسته تقسیم کرد: یکی استفاده‌کنندگان خدمات‌ها که تنها برای استفاده از خدمات درخواست می‌دهند و از آن‌ها استفاده می‌کنند و بر اساس مصرف خود هزینه پرداخت می‌کنند. کاربران دیگر محیط محاسبات ابری اعضای آن می‌باشند که می‌توانند در تهیه خدمات همکاری کنند.

2-3- امنیت در محیط محاسبات ابری

با توجه به روند روبه‌پیشرفت و توسعه استفاده از محاسبات ابری بسیاری از شرکت‌ها همچون eBay، Amazon، Google، Microsoft و... با صرف میلیاردها دلار به خدمات‌دهی به مشتریان و کاربران خود در این زمینه پرداخته‌اند. با توجه به این سرمایه‌گذاری‌ها مطمئناً ایجاد امنیت برای اطلاعات مهم کاربران بسیار مهم می‌باشد. دو بخش بسیار مهم در محیط محاسبات ابری وجود دارد که می‌بایست از لحاظ امنیتی موردتوجه قرار گیرند. یکی آسیب‌های ماشین‌های مجازی و دیگری جامعیت پیام‌ها می‌باشد.

برای ارائه هر خدمتی می‌بایست یک ماشین مجازی به کاربر ارائه گردد تا در محیط کاملاً کنترل‌شده‌ای بتواند از خدمات استفاده نماید. این باعث می‌شود تا هم کاربر در محیط خود احساس امنیت کند و از در امان بودن اطلاعات خود مطمئن باشد؛ و هم اینکه کاربر نتواند به محیط‌های غیرمجاز دسترسی داشته باشد و یا اینکه از محتویات سرور باخبر گردد؛ بنابراین ایجاد امنیت در این محیط بسیار مهم می‌باشد تا از سوءاستفاده دیگران و خرابکاری و یا دزدی اطلاعات و دیگر خطرات جلوگیری شود.

نکته دوم و مهم برای حفظ امنیت، راه‌های ارتباطی تبادل اطلاعات بین ماشین‌های مجازی با یکدیگر و یا با سرور و هرگونه محیط دیگر می‌باشد؛ تا از نشت اطلاعات و یا سرقت اطلاعات شخصی کاربران جلوگیری شود؛ بنابراین می‌بایست در ارسال اطلاعات از روش‌های مختلفی برای جلوگیری از دزدی استفاده شود. در این راستا از روش‌هایی همچون رمزنگاری اطلاعات، استفاده از پروتکل‌های امن و نشانه‌گذاری پیام‌ها و یا تأیید صحت کاربران استفاده می‌شود.

هرچند امروزه گره‌های ابر بسیار مورد توجه مردم قرار گرفته‌اند اما با این حال یکی از چالش‌های عمده‌ای که محاسبات ابری با آن روبرو است، چگونگی حفاظت از داده‌ها و برقراری امنیت فرآیندهای کاربران است، امنیتی که در محیط ابر فراهم می‌شود، برای سازمان‌ها و افراد بسیار حائز اهمیت است، چراکه برخی سازمان‌ها انتقال برنامه‌های کاربردی مهم و داده‌های حساس خود را به یک محیط ابر عمومی، یک ریسک بزرگ تلقی می‌کنند، بنابراین برای کاهش این نگرانی‌ها، یک ارائه‌دهنده ابر باید این اطمینان را ایجاد کند که مشتریان می‌توانند امنیت و کنترل حریم خصوصی خود را روی برنامه‌های کاربردی حفظ کنند، پس ارائه‌دهندگان ابر برای متقاعد کردن مشتریان خود در مورد مسائل امنیتی بایستی اقداماتی را انجام دهند، از جمله می‌توان به " موافقت‌نامه سطح سرویس اشاره نمود. این موافقت‌نامه سندی است که ارتباط بین ارائه‌دهنده و دریافت‌کننده را مشخص می‌کند و در حقیقت یک توافق حقوقی بین ارائه‌دهنده سرویس و مشتری است.

مواردی که در خصوص جلب رضایت و اطمینان مشتری در موافقت‌نامه مطرح می‌شود، به شرح زیر می‌باشد.

- شناسایی و تعریف نیازهای مشتری
- ساده‌سازی مسائل پیچیده
- کاهش زمینه‌های تعارض بین کاربران تشویق به گفت‌وگو در مورد برخوردها و اختلافات
- حذف انتظارات غیرواقعی
- ارائه چارچوبی برای درک راحت

همان‌طور که در جدول ۳ نشان داده شده است، برای پیاده‌سازی رویه و کنترل محاسبات ابری، اهمیت "امنیت" در حوزه‌های ریسک‌پذیر و بحرانی، برابر ۷/۹۱ درصد است. در [۱۴] نشان داده شده است که محیط مجازی ابرها به اندازه کافی ایمن و قابل اعتماد هستند.

جدول 1: حوزه‌های ریسک‌پذیر و بحرانی در مجازی‌سازی و محاسبات ابری

درصد عدم (%)	درصد اهمیت (%)	درصد بحرانی بودن (%)	حوزه ریسک‌پذیر
۰	۸,۳	۹۱,۷	امنیت
۰	۵۸,۳	۴۱,۷	مدیریت عملیات
۸,۳	۵۰	۴۱,۷	مدیریت تغییرات
۰	۳۳,۳	۶۶,۷	حوادث و سوانح
۱۶,۷	۴۱,۷	۴۱,۷	مدیریت سطح سرویس
۴۱,۷	۵۰	۸,۳	مدیریت واسط
۲۵	۴۱,۷	۳۳,۳	آیین‌نامه و قوانین

2-3-1- تهديدات امنیتی محیط محاسبات ابری

با توجه به تحت اینترنت بودن محیط محاسبات ابری می‌تواند گستره بزرگی از حملات را برای آن در نظر گرفت به‌گونه‌ای که می‌تواند گفت تمامی حملات موجود در گونه‌های دیگر شبکه‌ها را در این محیط پیدا خواهیم نمود. در زیر برخی از این حملات را شرح خواهیم داد.

2-3-1-1- حمله اخلاص در خدمت‌رسانی

یکی از رایج‌ترین حملات در این محیط حمله اخلاص و یا انکار خدمت است که باعث مختل شدن سرویس‌دهنده می‌شود. حمله‌کننده در زمان مناسبی شروع به ارسال مداوم و سریع درخواست به سرویس‌دهنده می‌کند. در این حمله سیل آسا اگر تعداد درخواست‌کننده‌ها و درخواست‌های آن بیش از اندازه باشد باعث می‌شود تا میزان پردازش سرویس‌دهنده بالا برود و باعث اخلاص در کار آن می‌گردید و می‌تواند باعث هنگ کردن پردازشگر و یا پر شدن حافظه آن و یا گم‌شدن درخواست‌ها و غیره گردد.

2-3-1-2 - حمله شنود اطلاعات

اگر لایه امنیتی SSL به خوبی استفاده نشود حمله شنود اطلاعات انجام می پذیرد. در این حمله شخصی می تواند در بین افراد قرار گیرد و به شنود پردازد و در نتیجه اطلاعات افراد را به سرقت ببرد؛ بنابراین می بایست لایه های امنیتی را به خوبی تنظیم نمود تا از این گونه حملات جلوگیری شود.

2-3-1-3 - دزدی اطلاعات شبکه

اگر داده ها به خوبی رمزنگاری نشوند و از آن ها محافظت نگردد به راحتی به وسیله متهاجمان مورد حمله و دستبرد قرار می گیرند. در این حمله مهاجم به کپی برداری از اطلاعات تبادل شده و یا نفوذ به فضای نگهداری اطلاعات به سرقت آن ها می پردازد.

2-3-1-4 - پوش درگاه

گاهی مهاجمان به شنود و پوش درگاه های سیستم می پردازند تا از طریق آن ها در سیستم کاربران نفوذ کنند؛ مثل درگاه های عمومی همچون درگاه ۸۰ یا ۸۰۸۰ همواره باز هستند و از طریق آن ها می توان به نفوذ پرداخت. برای نمونه مهاجم می تواند از راه این درگاه ها به نشر وب سرویس در سیستم کاربران پردازد و در زمان مناسب آن ها را اجرا نماید و به تخریب و یا دزدی اطلاعات دست بزند.

2-3-1-5 - حمله دستورات SQL

یعنی اینکه درجهایی که مثل نام کاربری و رمز عبور خواسته می شود به SQL تزریق دستورات راحتی یک دستور پایگاه داده را قرارداد تا در زمان اجرا اطلاعات مورد نیاز را از پایگاه داده واکنشی نمود. این یکی از ساده ترین راه های نفوذ در شبکه می باشد که با انجام چند عمل پیشگیرانه می توان آن را برطرف نمود.

2-3-1-6 - تزریق بدافزار به ابر

همان طور که در بخش قبل گفته شد ماشین های مجازی از مهم ترین بخش های ابر می باشد که همواره می تواند مورد حمله قرار گیرد. در این راستا مهاجم می تواند بدافزار مورد نظر خود را در ماشین مجازی

تزریق نماید و پس از آن به اجرای آن دست بزنند. آنگاه می‌تواند از طریق آن به ماشین مجازی و یا سخت‌افزار و حتی سرورها صدمه‌های شدید وارد نماید.

7-1-3-2- نفوذ از طریق رابط کاربری ضعیف

اگر رابطی که برای ایجاد ارتباط با برنامه‌ها در سرور و ماشین‌های مجازی طراحی کردیم از لحاظ، امنیتی ضعیف و دارای رخنه‌های امنیتی باشند می‌تواند با استفاده از آن‌ها در سیستم نفوذ نمود. در اینجا نیز می‌تواند اطلاعات مورد نیاز خود را از نشست‌ها و کوکی‌ها دریافت نمود و یا حتی فایل‌های مخرب را در آن‌ها قرارداد.

8-1-3-2- خودی‌های مخرب

کاربران ابر نیز می‌توانند خود باعث خرابی شوند. گاه این خرابکاری آگاهانه و گاهی ناخودآگاه می‌باشد؛ مثل با سهل‌انگاری توسط کاربران زمینه برای نفوذ و یا سرقت اطلاعات برای مهاجمان فراهم می‌شود. کاربران باید در این زمینه آموزش‌های مناسب را فراگیرند تا از سرقت اطلاعات جلوگیری شود.

9-1-3-2- حمله ربات‌ها

یکی از مهم‌ترین و رایج‌ترین حملات در محیط محاسبات ابری که بیشتر مربوط به ماشین‌ها مجازی می‌باشد، حمله ربات‌ها می‌باشد. در این نوع از حمله می‌تواند کنترل یک یا چند سیستم کاربر را به عنوان سیستم قربانی به دست گرفت و از طریق آن‌ها به انجام حمله پرداخت. به سیستم‌های قربانی در اصطلاح زامبی گفته می‌شود چراکه دیگر کنترل آن‌ها در دست کاربر نیست.

4-2- سیستم‌های تشخیص نفوذ

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. در عمل انواع مختلفی از روش‌های تشخیص حمله وجود دارد که با توجه با انواع مختلف اقدامات درون شبکه قادر هستند اقدامات مخرب و نفوذی را کشف کنند. در عین این دستگاه‌ها از بخش‌های مختلفی تشکیل شده‌اند و به طرق مختلفی این اجزا می‌توانند در کنار هم

قرار گیرند و عملکرد خاصی را ایجاد کنند. در این بخش به ارائه چارچوب کلی در مورد امنیت شبکه و سیستم‌های کامپیوتری می‌پردازیم. ابتدا انواع حملات و تهدیدهای موجود در شبکه‌های کامپیوتری را طبقه‌بندی می‌کنیم. سپس به طبقه‌بندی سیستم‌های تشخیص نفوذ از حیث ساختار می‌پردازیم. در نهایت هم در مورد تکنولوژی‌های تشخیص نفوذ و کارکردهای مختلف این ابزارها در مدیریت و حفظ امنیت و نظارت بر شبکه‌های کامپیوتری بحث می‌کنیم.

1-4-2- انواع حملات شبکه‌ای با توجه به حمله‌کننده

حملات شبکه‌ای را می‌تواند با توجه به حمله‌کننده به چهار گروه تقسیم کرد:

حملات انجام‌شده توسط کاربر مورد اعتماد داخلی: این حمله یکی از مهم‌ترین و خطرناک‌ترین نوع حملات است، چون از یک طرف کاربر به منابع مختلف شبکه دسترسی دارد و از طرف دیگر سیاست‌های امنیتی معمولاً محدودیت‌های کافی درباره این کاربران اعمال نمی‌کنند.

حملات انجام‌شده توسط افراد غیر معتمد خارجی: این معمول‌ترین نوع حمله است که یک کاربر خارجی که مورد اعتماد نیست شبکه را مورد حمله قرار می‌دهد. این افراد معمولاً سخت‌ترین راه را پیش رودارند زیرا بیشتر سیاست‌های امنیتی درباره این افراد تنظیم شده‌اند.

حملات انجام‌شده توسط مهاجم‌های بی‌تجربه: بسیاری از ابزارهای حمله و نفوذ بر روی اینترنت وجود دارند. درواقع بسیاری از افراد می‌توانند بدون تجربه خاصی و تنها با استفاده از ابزارهای آماده برای شبکه ایجاد مشکل کنند. حملات انجام‌شده توسط کاربران مجرب: مهاجم‌های باتجربه و حرفه‌ای در نوشتن انواع کدهای خطرناک متبحرند. آن‌ها از شبکه و پروتکل‌های آن و همچنین از انواع سیستم‌های عامل آگاهی کامل دارند. معمولاً این افراد ابزارهایی تولید می‌کنند که توسط گروه اول به کار گرفته می‌شدند. آن‌ها معمولاً پیش از هر مرحله، آگاهی کافی درباره هدف خود و آسیب‌پذیری‌های آن کسب می‌کنند.

2-5- انواع سیستم‌های تشخیص نفوذ

سیستم‌های تشخیص نفوذ با توجه به نحوه کاربری و محل نصب و میزبان یا شبکه‌ای که از آن محافظت می‌کند، می‌تواند مبتنی بر میزبان، شبکه یا به صورت توزیع شده عمل کند.

2-5-1- سیستم‌های تشخیص نفوذ مبتنی بر میزبان

این دستگاه‌ها از یک میزبان در مقابل عملیات نفوذی و مخرب محافظت می‌کند. این سامانه محافظتی بر روی سیستم اجرا می‌شود و تمام فعالیت‌ها و فرآیندهای درون سیستم را کنترل می‌کند. HIDS می‌تواند واسط شبکه‌ای را نیز پوشش دهد و بر دسترسی‌هایی که از خارج به سیستم می‌شود، نظارت کند. این نوع از سیستم تشخیص نفوذ بر روی خود سیستم اجرا می‌شود و از منابع خود سیستم مثل حافظه و پردازنده و... استفاده می‌کند. HIDS عمل کنترل دسترسی‌ها را انجام می‌دهد و بررسی می‌کند که چه پردازش‌هایی از چه منابعی استفاده می‌کنند. برای مثال دسترسی یک برنامه با عنوان پردازشگر متن به اطلاعات حساس سیستم مثل رمز محل ذخیره عبور، یک اقدام مشکوک است. همچنین به بررسی مداوم وضعیت سیستم می‌پردازد و منابع سخت‌افزاری و اطلاعاتی سیستم را در مورد دسترسی و ویرایش توسط عوامل مشکوک بررسی می‌کند. امروزه بسیاری از برنامه‌های امنیتی تحت عنوان ضدویروس برای حفظ امنیت سیستم کامپیوتری به کار می‌روند. این دستگاه‌ها بیشتر وقت خود را صرف کنترل دسترسی پردازش‌ها می‌کنند. این‌که هر کدام از پردازش‌ها به چه منابعی می‌تواند و یا نمی‌تواند دسترسی داشته باشد. یک HIDS می‌تواند سیاست‌های امنیتی خاص را بر روی سیستم اعمال کند و در مقابل حملات منجر به اشباع شدن منابع سیستم از آن حفاظت کند.

در بسیاری از موارد حمله‌کننده عملیات نفوذ را در چند مرحله صورت می‌دهند. مهاجم‌ها در بیشتر موارد هدف چنین مهاجم‌هایی تصاحب منابع سیستم است، به نحوی نرم‌افزار خاصی بر روی سیستم نصب کنند و یا تغییر موردنظر خود را در اطلاعات سیستم ایجاد کنند. از نظر تئوری تمام اقدامات نفوذی به این نحو امکان‌پذیر است بسیاری از این اقدامات توسط سیستم‌های تشخیص نفوذ تحت شبکه (NIDS) کشف می‌شوند. سیستم‌های HIDS در تکمیل کار NIDS سعی در کشف نفوذهای کشف نشده توسط NIDS دارند. به لحاظ تکنیکی راه‌حل‌های نرم‌افزاری برای ایجاد همکاری بین این دو سیستم امکان‌پذیر است.

عمل نظارت معمولاً به این صورت انجام می‌شود که از تمام اشیاء سیستمی مهم به‌طور معمول اشیاء سیستم فایل) یک نمونه درهم‌سازی شده تولید می‌شود و در یک پایگاه داده مطمئن ذخیره می‌شود. به‌مرور زمان با بررسی آن می‌تواند فهمید که کدام یک از اشیاء سیستم می‌تواند دسترسی به نقاط حساس سیستم را کنترل HIDS دچار تغییر ناخواسته شده‌اند. به‌عنوان مثال قسمت‌های خاصی از فضای حافظه یا جدول فراخوانی‌های سیستمی مربوط به سیستم عامل.

2-5-2- سیستم‌های تشخیص نفوذ مبتنی بر شبکه

این سیستم‌ها در بستر شبکه فعالیت می‌کنند و با پوشش ترافیک شبکه و تحلیل آن در تمام لایه‌های مختلف شبکه، به دنبال کشف نشانه‌های اقدامات نفوذی و یا حملات هستند. انواع حملاتی که در سطح شبکه می‌توانند وجود داشته باشند شامل حملات DoS، حملات پوشش درگاه هستند. معمولاً این سیستم‌ها از چندین حسگر نقاط مختلف برای دریافت ترافیک شبکه برخوردارند. ویژگی‌های دریافت شده از این ترافیک به پایگاه مرکزی تحلیل فرستاده می‌شود تا بر اساس روش‌های مختلف تشخیص نفوذ، اقدامات نفوذی آشکار شوند.

2-6- اجزای تشکیل دهنده سیستم‌های تشخیص نفوذ مبتنی بر شبکه

اجزای اصلی این دستگاه‌ها عبارت‌اند از حسگر، سرور مدیریت و تحلیل، سرور پایگاه داده، چندین واسط کاربری و سرورهای پایگاه داده. حسگر جزئی است که ترافیک شبکه مربوط به یک یا چند بخش را پوشش می‌کند. واسط شبکه‌ای حسگرها طوری پیکربندی شده‌اند که تمام بسته‌های دریافتی را بدون در نظر گرفتن آدرس مقصد دریافت می‌کند. تمام حسگرها در یکی از این دو نوع هستند:

- نوع مبتنی بر سخت‌افزار: این نوع حسگر شامل سخت‌افزار خاص منظوره طراحی شده که به همراه نرم‌افزار اجرا شوند بر روی آن است. سخت‌افزار برای استفاده جهت کاربرد حسگر بهینه‌سازی شده است و کارت‌های واسط شبکه‌ای خاصی بر روی آن‌ها قرار گرفته که تمام ترافیک عبوری را دریافت می‌کند. این افزارها معمولاً شامل سیستم عاملی هستند که به‌صورت مستقیم توسط مدیر سیستم مورد دسترسی نیست، ولی واسط نرم‌افزاری مناسب امکان ارتباط با کاربر و بخش‌های دیگر سیستم تشخیص نفوذ را فراهم

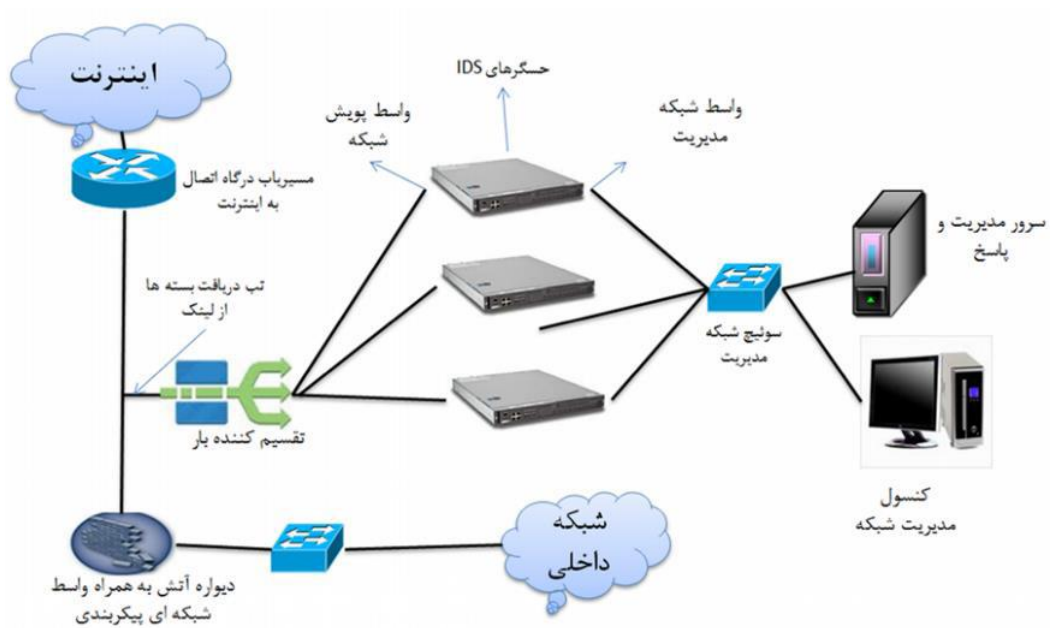
می‌کند.

- نوع مبتنی بر نرم‌افزار: ابزار تشخیص نفوذ به‌عنوان یک نرم‌افزار عرضه می‌شود. در این حالت ممکن است نرم‌افزار به همراه سیستم‌عامل مربوط به آن ارائه شود یا آنکه نرم‌افزار قابل نصب بر روی سیستم‌عامل‌های همه‌منظوره باشد. بسیاری از ابزارهای تشخیص نفوذ در این حالت قابل پیکربندی هستند.

1-6-2- سیستم‌های توزیع شده

امروزه با روند افزایش پهنای باند شبکه‌ها و نیاز به پویایی و وقفه این داده‌ها، سیستم‌های تشخیص نفوذ تحت شبکه هم باید همگام با آن‌ها توسعه پیدا کنند. امروزه روش‌های معماری‌های متمرکز مبتنی بر شبکه، جوابگوی شبکه‌های امروزی نیست. این روش‌ها برای تشخیص حملات چندمرحله‌ای و نگهداری وضعیت انواع ارتباطات و نیز مراودات پروتکلی در جریان، به خاطر وجود یک نقطه سرویس‌دهی، سیستم دچار کوییدگی^۱ و افت گذردهی می‌شود. الگوریتم‌های تشخیص نفوذ مبتنی بر یک سری قوانین هستند که به‌سرعت در حال بزرگ شدن هستند. ایجاد IDS های توزیع شده نیاز به تمهیداتی برای معماری شبکه‌ای، نرم‌افزار مناسب برای عملکرد توزیع شده و تقسیم ترافیک شبکه بین بخش‌های موازی دارد.

^۱ Thrashing



شکل 3: معماری IDS های توزیع شده با استفاده از حسگرهای بی اثر و با امکان توزیع بار

برای عملکرد IDS های توزیع شده، دو نوع تکنیک مطرح وجود دارد: تقسیم ترافیک و متعادل کردن بار. روش های مبتنی بر تقسیم ترافیک بیشتر بر اساس جریان های داده ای و سیاست های امنیتی و ساختار IDS و با این هدف ها کار می کنند:

بسته های مربوط به هر کدام از حمله کننده های احتمالی به یک حسگر وارد شود.

بر اساس سرعت و پهنای باند شبکه عملکرد و بهره وری حفظ شود.

تطابق پذیری سیستم در شرایطی با ترافیک های مختلف.

روش های مبتنی بر تعادل بار در هر زمان مقدار بار مناسبی برای هر کدام از حسگرها در نظر می گیرد به نحوی که از ظرفیت سیستم به نحو بهینه استفاده شود. تعادل بار می تواند به دو صورت برآورده شود:

استفاده از تسهیم کننده بار: این ابزار در ورودی شبکه قرار می‌گیرد و کل ترافیک شبکه باید از آن عبور نماید. به همین دلیل بایستی ابزار مورد استفاده توانمندی بالایی داشته باشد تا به گلوگاه عبور ترافیک تبدیل نشود.

هرکدام از حسگرها با استفاده از چندین الگوریتم تسهیم بار و انجام محاسبات خاص، حسگرهایی را که دچار بار بیش از حد شده‌اند را تعیین کرده و با انجام تنظیم‌های خاص، باعث می‌شود که بار ورودی به آن‌ها کاهش یابد. این عملیات با روش‌های مختلفی می‌تواند صورت پذیرد. از جمله فیلتر کردن زودرس که بعضی از بسته‌ها در خود تسهیم کننده بار پردازش می‌شدند. روش دیگر استفاده از یک گره مرکزی است که از دیگر گره‌ها پیغام‌هایی را دریافت می‌کند و بار زیاد بر روی هرکدام از حسگرها و یا بروز حملات توزیع شده در شبکه یا حملات چندمرحله‌ای را متوجه می‌شود. بعد از این مرحله این گره با ارسال فرمان‌های کنترلی باعث می‌شود که جریان بسته‌ها در حسگرها به نحو پویا تنظیم شود. این الگوریتم‌ها پیچیدگی بالایی دارند ولی در صورت پیاده‌سازی موفق، بهره‌وری قابل توجهی دارند.

موازی‌سازی در سطح بسته‌ها: در این حالت یک تسهیم کننده بار با سیاست گردشی، بسته‌ها را بین حسگرها تقسیم می‌کند. در این صورت تعادل بار به نحو مناسبی صورت می‌گیرد. با این حال برای ایجاد حالت مندی و حفظ اطلاعات جریان‌های مختلف و مراودات پروتکلی مختلف و همین‌طور داشتن اطلاعات کامل از هر ارتباط، نیاز به عنصری تحت عنوان تحلیل‌گر ارتباطات هستیم. این عنصر تمام داده‌های مورد نیاز خود را از طریق پیش پردازنده‌ها به دست می‌آورد. در ساختار چنین سیستمی باید هریک از حسگرها با این تحلیل‌گر ارتباطات، ارتباط مناسب و امنی داشته باشند. همچنین در پیاده‌سازی آن باید دقت بسیاری شود، چون به سادگی می‌تواند به گلوگاه بهره‌وری تبدیل شود.

موازی‌سازی در سطح ارتباطات و مراودات پروتکلی: در این روش در تسهیم کننده بار، توزیع بسته‌ها به روشی صورت می‌گیرد تا بسته‌های مربوط به هرکدام از ارتباطات به یک حسگر وارد شوند. در این حالت وجود جدول‌ها و اطلاعات مربوط به هرکدام از جریان‌ها در هریک از حسگرها ضروری است. در این ساختار باید توجه شود که باید برای تشخیص حملات چندمرحله‌ای و حملات مربوط به چندین ارتباط، نیاز به عنصری تحت عنوان تحلیل‌گر شبکه داریم. این عنصر باید توانایی تحلیل رویدادهای مربوط

به جریان‌های مجزا و ایجاد ارتباط بین این رویدادها را داشته باشد. این روش موازی‌سازی هیچ تضمینی در مورد تقسیم عادلانه بار ارائه نمی‌دهد.

موازی‌سازی در سطح قوانین: در این روش قوانین موجود در IDS بین حسگرهای مختلف تقسیم می‌شود. عنصری در ابتدای مسیر تحت عنوان Traffic Duplicator یک کپی از ترافیک را برای هرکدام از بسته‌ها می‌فرستد. به این ترتیب هرکدام از حسگرها مسئول اعمال تعداد محدودی از قوانین بر روی بسته‌ها می‌باشد. در صورت تقسیم مناسب قوانین بین حسگرها و اعمال قوانین از یک کلاس و دسته به یک حسگر خاص، عمل تشخیص به بهترین نحو صورت گرفته و تعادل بار صورت می‌گیرد. با این حال، هرکدام از حسگرها باید جداگانه عملیات پیش‌پردازش و حذف بسته‌های زائد را انجام دهد که اتلاف منابع را نسبت به روش‌های دیگر در پی دارد.

2-7- انواع روش‌های تشخیص حمله

ابزارهای تشخیص نفوذ از روش‌های مختلفی برای تشخیص انواع مختلف حملات استفاده می‌کنند. این روش‌ها را می‌تواند در سه کلاس مبتنی بر امضا، تشخیص ناهنجاری و مبتنی بر تحلیل حالت پروتکل ارتباطی دسته‌بندی کرد.

2-7-1- روش‌های مبتنی بر امضا

امضا یا ویژگی عبارت است از الگوی مربوط به یک عملیات مشخص. وجود یک فرمان اجرایی در بسته که برای افزایش سطح دسترسی به سیستم موردنظر ممکن است مورد استفاده قرار گیرد؛ مانند فرمان دسترسی root روش تشخیص مبتنی بر امضا عبارت است از مقایسه الگوی رفتارهای در جریان در شبکه با نمونه‌های مشاهده‌شده به منظور مشخص کردن امکان بروز حملات. این روش تشخیص حملات در برابر طیف حملات شایع و شناخته‌شده بسیار مؤثر و نتیجه‌بخش است. لکن با توجه به انواع مختلف حملات و الگوهای رفتاری متنوعی که می‌تواند توسط مهاجمین به کار گرفته شود، بازدهی این روش محدود می‌شود. به عنوان نمونه در مثال ایمیل‌هایی که ضمیمه فایل اجرایی داشتند، چنانچه نام فایل اجرایی ضمیمه به "FREEPics.exe" تغییر یابد، این روش قادر به تشخیص این نوع نفوذ نخواهد بود.

روش تشخیص مبتنی بر امضا ساده‌ترین روش تشخیص حملات به شبکه‌های کامپیوتری می‌باشد، زیرا در این روش فقط فعالیت در جریان فعلی مورد بررسی قرار می‌گیرد؛ مانند فرآیند آخرین بسته دریافتی یا گزارش آخرین فعالیت صورت گرفته. در این عملیات با استفاده از روش‌های مقایسه رشته‌های حرفی، مقایسه‌ای با فهرستی از الگوهای موجود صورت می‌گیرد. این روش کار آیی اندکی در مقابل ارتباطات پیچیده‌تری که طی چند مرحله صورت می‌گیرند و در هر مرحله در وضعیت خاصی به سر می‌برند، دارد. این روش‌ها قادر نیستند درخواست ارسال‌شده را با پاسخ مربوط به آن کنار هم ارسالی را با پاسخ مربوط به HTTP قرار دهند. برای مثال قادر نیستند در یک ارتباط وب درخواست آن باهم در نظر بگیرند. این روش‌ها همچنین قادر نیستند درخواست‌های قبلی یک کاربر را با درخواست‌های فعلی او باهم در نظر بگیرند. حفظ نکردن وضعیت، محدودیت‌های جدی به همراه دارد. این روش‌ها در مقابل حملاتی که از چند مرحله تشکیل شده‌اند و مبتنی بر یک سری رخداد پیاپی هستند ناکام‌اند، مگر اینکه هرکدام از مراحل شامل نشانه و یا الگوی مشخصی، دال بر بروز حمله داشته باشند.

2-7-2- روش‌های تشخیص حمله مبتنی بر ناهنجاری

روش‌های مبتنی بر تشخیص ناهنجاری عبارت است از مقایسه شرایط عادی سیستم با شرایط مشاهده‌شده، به‌منظور تشخیص تفاوت‌های جدی که معمولاً در صورت بروز حملات رخ می‌دهد. دستگاه‌هایی که بر اساس این روش‌ها عمل می‌کنند، دارای سابقه‌های مستندی هستند که نمود وضعیت اجزای مختلف سیستم در وضعیت عادی است. وضعیت ارتباطات، تعداد مشترکین، وضعیت رفتاری و درخواست‌های معمول مشترکین و نیز مناسبات نرم‌افزاری و سخت‌افزاری در جریان از آن جمله‌اند. این سابقه‌ها با بررسی و ثبت عملکرد کاربران و وضعیت سیستم در یک دوره زمانی مشخص به دست می‌آیند. برای مثال این مستندات ممکن است نشان دهند که استفاده از وب در حدود ۴۰ درصد فعالیت کاربران شبکه و نیز پهنای باند در دسترس را نشان می‌دهد. ابزار تشخیص نفوذ بر اساس روش‌های ایستایی ویژگی‌های وضعیت فعلی را اندازه‌گیری می‌کند و با حدود آستانه‌ای که در سابقه سیستم ثبت شده است مقایسه می‌کند. برای مثال ممکن است نسبت ترافیک وب از حد بالای آستانه بیشتر شود. همچنین پارامترهای دیگری می‌توانند مورد بررسی قرار بگیرند. از آن جمله می‌تواند تعداد ایمیل‌های ارسالی و یا دریافتی، تعداد دفعات تلاش

برای وارد کردن رمز و ورود به سیستم و یا درصد به کارگیری پردازنده در یک دوره زمانی اشاره کرد. به عنوان یک نمونه دیگر از به کارگیری این روش ها می توان به تشخیص حملات سرریز اشاره کرد. در حالت عادی بعد با توجه به مراحل دست دهی سه گانه TCP، به طور معمول باید تعداد بسته های درخواست ایجاد ارتباط با پرچم SYN با بسته های پاسخ ارتباط TCP که دارای پرچم های SYN و Ack هستند، برابر باشند. در صورتی که تعداد بسته های نوع نخست افزایش فرآیندهای نسبت به نوع دوم داشته باشد، این نشانه می تواند دلیلی بر بروز حملات DoS باشد.

مزیت عمده روش های مبتنی بر تشخیص ناهنجاری این است که می تواند با صرف کمترین هزینه، انواع مختلف و ناشناخته ای از حملات را که الگوی آن ها قبل مشاهده نشده را تشخیص دهد. برای مثال حملاتی که در آن ها پردازنده سرور مشغول می شود، یا آنکه تعداد زیادی ایمیل فرستاده می شود، یا تعداد زیادی ارتباط بی مورد برای مشغول نگه داشتن سرور به سمت آن ایجاد می شود، با این روش قابل تشخیص اند.

سابقه سیستم مورد استفاده در این دستگاه ها در یک فاز آموزش که ممکن است روزها و یا هفته ها ادامه داشته باشد، ثبت و بررسی می شود. این پرونده ها می توانند به صورت ثابت باشند، یا در طول زمان به صورت تطبیقی تغییر داده شوند. در روش اول اطلاعات ثابت باقی می ماند مگر آنکه به طور صریح از طرف مدیر سیستم، فاز آموزش از سرگیری شود. به این دلیل که رفتارها و پارامترهای وضعیتی دستگاه ها دارای توزیعی نرمال هستند و در طول زمان تغییر می کنند. در روش پروفایل های تطبیقی مشکل کمتری به مرور زمان پیش می آید. لکن این امکان وجود دارد که حمله کننده با صرف زمان، به مرور و مرحله به مرحله تغییرات مورد نظر را ایجاد کند و با گذشت زمان این رفتار برای سیستم تشخیص نفوذ تغییر رفتار عادی جلوه کند. از دیگر مشکلات سیستم های مبتنی بر ناهنجاری این است که ممکن است در فاز آموزش، سیستم حمله کننده وضعیت مطلوب خود را در سابقه سیستم ثبت کند. باید پذیرفت که رفتارهای این چنینی با احتمال زیاد در سابقه سیستم ثبت می شدند.

از دیگر مسائل مربوط به روش های تشخیص مبتنی بر ناهنجاری این است که به خاطر پیچیدگی و تنوع رفتارهای مختلفی که در یک شبکه ممکن هستند، اولاً ایجاد این سابقه به دقت زیادی نیاز دارد، ثانیه

تشخیص دقیق علت بروز ناهنجاری ممکن نیست. ممکن است عملیات بروز رسانی سیستم که نیازمند انتقالات داده و ارتباطات زیادی است در فاز آموزش دیده نشود. به این ترتیب در زمان کار سیستم راه اندازی چنین تغییراتی به خودی خود موجب اختارت بی مورد و غلط می شود. در حالاتی که سیستم اختار تولید می کند، بررسی اینکه اختار، دلیل درست ووجهی دارد دشوار است.

از سوی دیگر تعیین نوع حمله و روزه امنیتی آسیب پذیر در مقابل حمله، بر اساس پارامترهای اندازه گیری شده کاری دشوار است. بسیاری حملات ممکن است بدون نیاز به تغییرات اساسی در وضعیت سیستم، به نقاط ممنوعه آن وارد شده و اطلاعات را تخریب یا سرقت کنند. لکن با توجه به اینکه تغییرات اساسی در وضعیت سیستم رخ نداده است، تشخیص این حملات بر اساس این روش ها دشوار و یا ناممکن است.

3-7-2- روش های مبتنی بر تحلیل حالت پروتکل ارتباطی

این روش به فرآیندی گفته می شود که طی آن روند رخدادهایی که در جریان ارتباط های مختلف به وقوع می پیوندند، با نمونه های سلسله رخداد مربوط به پروتکل های مناسب و غیر مهاجم مقایسه می شدند تا در صورتی که مجموعه رخداد های در جریان، ناشناس و یا مشکوک تشخیص داده شود، سیستم آن را تشخیص دهد. برخلاف روش مبتنی بر تشخیص ناهنجاری که بر سابقه رفتارهای شبکه خاص تکیه داشت، در اینجا پروفایل های مورد بررسی مربوط به پروتکل های خوش تعریف، جامع و مشخصی است که کاملاً شناخته شده هستند و روند اجرای آنها مشخص است و هرگونه تخطی از کاربرد درست آنها می تواند یک رخداد مشکوک به تجاوز به شبکه باشد. کاربرد روش های مبتنی بر پروتکل به این معنی است که ابزار تشخیص نفوذ قادر به فهم و تشخیص و پیگیری روند اجرای پروتکل های لایه انتقال و کاربرد هست.

برای مثال در یک ارتباط FTP که در دو مد قابل انجام است، در مد کاربران غیرمجاز فقط اقداماتی از قبیل مشاهده لیست راهنما و وارد کردن نام کاربری و شناسه عبور مجاز است. در این وضعیت ابزار تشخیص نفوذ می تواند زوج درخواست کاربر و پاسخ سرور را باهم مطابقت دهد و مشخص کند که آیا هر کدام از درخواست های کاربر برای وارد شدن به سیستم موفق بوده است یا نه. به محض اینکه شناسه

کاربر تأیید شد و کاربر به سیستم وارد شد، کاربر قادر به انجام اقدامات مختلف هست. صدور هر یک از فرامین مربوط به کاربران وارد شده به سیستم از سوی کاربری که هنوز وارد سیستم نشده است می‌تواند مشکوک به یک فعالیت مخرب در جهت نفوذ به سیستم باشد.

در روش تشخیص نفوذ مبتنی بر پروتکل امکان پیگیری روند ارسال فرمان‌ها از کاربران وجود دارد؛ به این ترتیب فرامین نامربوط قابل تعقیب‌اند. برای مثال صدور فرمان‌هایی خارج از روند پروتکل و یا ارسال پیغام‌های مربوط به یک‌فاز پروتکل به دفعات متعدد. این دستگاه‌ها همچنین قادرند بر اساس رده‌های کاربری مختلف و تعیین سطح دسترسی آن‌ها، فعالیت آن‌ها را پیگیری کنند. همچنین روند بررسی طول دستورات و آرگومان‌ها می‌تواند به صورت مجزا بر روی هر کدام از دستورات پروتکلی لایه کاربرد صورت گیرد. هر کدام از دستورات تعداد آرگومان‌های مشخص دارند که طول آن‌ها مشخص است. برای مثال دستوری می‌تواند ۲ آرگومان با حداکثر طول ۲۰ کاراکتر داشته باشد. در صورتی که تعداد آرگومان‌ها و یا طول آن‌ها مثلاً دستوری با طول از این حد تخطی کند، می‌تواند نشانه یک اقدام مشکوک باشد.

روش‌های مبتنی بر تحلیل پروتکل بر اساس مدل‌های پروتکلی استاندارد که توسط توسعه‌دهندگان نرم‌افزارهای شبکه معرفی می‌شدند و یا استانداردهای اینترنتی مشخص ثبت شده صورت می‌گیرد. در بسیاری از موارد جزئیات دقیق پروتکل به طور دقیق در مستندات مربوطه آورده نمی‌شود. در بسیاری از موارد، توسعه‌دهندگان نرم‌افزار با تخطی از مستندات پروتکل، در پیاده‌سازی‌های مختلف ویژگی‌های خاصی بر اساس نیاز به پیاده‌سازی پروتکل اضافه می‌شود. در بعضی موارد در مورد پروتکل‌هایی که کاربرد خصوصی دارند و در انحصار مالک هستند اطلاعات دقیقی در دسترس نیست. در تمام موارد ذکر شده، بعد از بروز رسانی پروتکل‌ها و یا معرفی پروتکل‌های جدید مدل پروتکلی ابزار تشخیص نفوذ باید بر اساس تغییرات صورت گرفته بروز رسانی شود. با این حال مهم‌ترین ایراد روش‌های مبتنی بر پروتکل این است که این روش‌ها به منابع سخت‌افزاری و نرم‌افزاری زیادی نیاز دارند. پیچیدگی تحلیل پروتکل‌های متعدد و نگهداری وضعیت و پیگیری روند اجرای مربوط به هر کدام از مراودات پروتکلی در جریان، سربار زیادی را به سیستم تحمیل می‌کند. مشکل جدی دیگر این است که این روش‌ها برای تشخیص حملاتی که بر اساس الگوهای پروتکلی استاندارد عمل می‌کنند دچار مشکل هستند؛ مانند

حملاتی که با ایجاد تعداد زیادی ارتباط پروتکلی صورت می‌گیرند و با مشغول کردن سرور و گرفتن منابع آن در وضعیت انتظار صورت می‌گیرند. حملات جلوگیری از سرویس‌گیری، گذشته از این‌ها در مواردی که ارتباط خدمتگذار و مشتری بر اساس پیاده‌سازی خاص پروتکل صورت گیرد یا آنکه پیغام‌ها رمز شده باشند، علاوه بر اینکه سیستم در تشخیص حملات واقعی ممکن است دچار اشتباه شود، ممکن است در بعضی موارد هشدارهای بی‌مورد تولید کند.

فصل سوم

ادبیات تحقیق

3-1- مقدمه

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. در عمل انواع مختلفی از روش‌های تشخیص حمله وجود دارد که با توجه با انواع مختلف اقدامات درون شبکه قادر هستند اقدامات مخرب و نفوذی را کشف کنند. در عین این دستگاه‌ها از بخش‌های مختلفی تشکیل شده‌اند و به طرق مختلفی این اجزا می‌توانند در کنار هم قرار گیرند و عملکرد خاصی را ایجاد کنند. در این بخش به ارائه چارچوب کلی در مورد امنیت شبکه و سیستم‌های کامپیوتری می‌پردازیم.

در این فصل به بررسی تکنولوژی‌های تشخیص نفوذ و برخی از بهترین مطالعات انجام شده در این زمینه خواهیم پرداخت و هریک از آن‌ها را به همراه مزایا و معایب آن‌ها مورد بررسی قرار می‌دهیم.

3-2- سیستم‌های تشخیص نفوذ و مدیریت ورودی چند سطحی در محاسبات ابری [۲۹]

روش دیگری که برای محافظت از محیط ابری طراحی شد در این مقاله می‌باشد. در این مقاله حملات با توجه به میزان خسارت و همچنین سطح حملات آن‌ها در محیط ابری دسته‌بندی شدند بر این اساس برای هر حمله یک ریسک خطر تهیه و به آن‌ها داده شد و بر اساس آن روشی برای مقابله با آن در نظر گرفته شده است. در جدول ۳ می‌توانید این دسته‌بندی و شماره‌های سطح داده شده به برخی حملات مهم را ببینید.

جدول ۲: دسته‌بندی حملات با توجه به میزان خسارت

میزان ریسک	نوع ترافیک فعالیت ناهنجاری
۸	تلاش برای دسترسی به دستورات مدیریتی خارج از محدوده
۷	اختصاص فضای حافظه سیستم عامل کاربران
۶	اختصاص کارت شبکه از طریق غیرمعمول
۶	بالا رفتن ترافیک کاربر بیش از ۵۰۰ برابر معمول
۶	کاربر در هنگام استفاده از محیط ابری IP تغییر
۵	تلاش برای دسترسی به سیستم کاربران از سوی مدیر محیط
۵	دخالت سیستم عامل کاربری در سیستم عامل کاربر دیگر

۴	بالا رفتن ترافیک کاربر بیش از ۳۰۰ برابر معمول
۴	دسترسی مدیر به سیستم عامل میزبان بدون اعلام
۳	شکست بیش از ۵ بار در ورود به محیط
۳	IP نامعتبر
۳	استفاده از شماره درگاه نامعقول
۳	انجام جستجو و کنکاش های مخرب در محیط
۲	به روز نبودن سیستم عامل کاربر
۲	ایجاد نشست ارتباط بین سیستم عامل کاربران در سیستم عامل میزبان همسان
۲	خاموش شدن غیر معمولی سیستم عامل کاربر
۱	بالا رفتن ترافیک کاربر بیش از ۱۵۰ برابر معمول

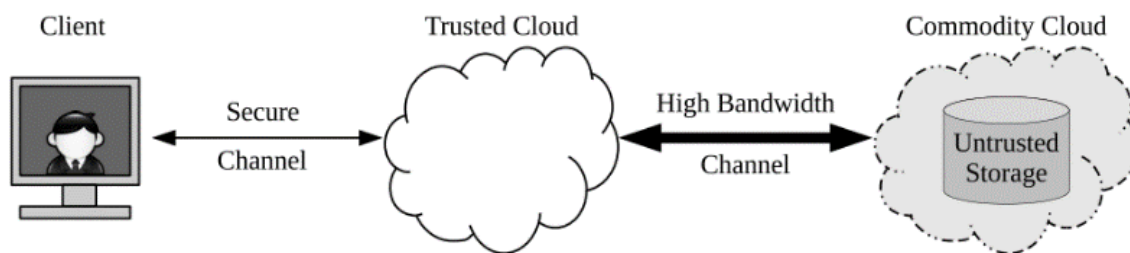
مشکل این سیستم تهیه این قوانین و همین طور تعیین ریسک های مربوط به آنها می باشد. حتی در برخی موارد نمی توان برای هر کاربری همه موارد را به کاربرد و یا میزان ریسک همسانی را به آنها داد. همچنین تهیه این قوانین نیاز به داشتن آگاهی هایی از زمینه کاربرد کاربر و برنامه های آنها دارد که خود باعث انجام پردازش هایی سنگین و پیچیده و گاه زمان بر می گردد؛ اما در نوع خود دارای مزیت هایی است. از آن جمله اینکه بیشتر به مباحث درون شبکه ای، به ویژه منابع، پرداخته است و از انجام پردازش هایی بر روی عوامل خارجی پرهیز می کند و این یعنی صرفه جویی در انجام پردازش های مازاد؛ اما همین خود باعث نقص در سیستم می باشد.

3-3- جایگذاری یک NIDS در یک محیط محاسبات ابری [۳۰]

در این مقاله نیز همانند [۳۰] از روش تعیین میزان ریسک برای منابع استفاده شده است و در سیستم از یک IDS مرکزی استفاده گردیده است. این سیستم نیز بر اساس مکانیزم استفاده شده مزایا و معایبی دارد. از جمله معایب آن فرایند تشخیص طولانی و هزینه بر می باشد و کنترل کننده بخش ها خود می تواند یک گلوگاه باشد که باعث کند شدن سیستم و حتی بن بست می شود.

3-4- ابرهای دوقلو: یک معماری برای محیط ابری امن

مقاله [۴] به طراحی یک سیستم امنیتی برای تبادل امن اطلاعات با استفاده از احراز هویت و رمزنگاری پرداخته است. در سیستم پیشنهادشده دو ابر دوقلو (در نظر گرفته شده است. یک ابر معتبر و یک ابر ارتباطی؛ بنابراین برای تبادل اطلاعات با کاربر به طور مستقیم از ابر معتبر استفاده می شود که به صورت بسیار امن طراحی شده است و کاربر برای درخواست هرگونه سرویسی باید درخواست خود را به ابر معتبر بدهد و ابر معتبر نیز به ابر ارتباطی در تماس است و سرویس ها را از آن گرفته و به کاربر تحویل می دهد. به این ترتیب هرگونه ارتباط که از قوانین امنیتی طراحی شده تبعیت نکند حمله تشخیص داده شده و با آن مقابله خواهد شد. در شکل ۴ این سیستم را مشاهده می کنید.



شکل 4: معماری پیشنهادی در [4]

هماهنگی بین این دو ابر می تواند یکی از مسائل مهم باشد که به دقت و ریزه کاری نیاز دارد. پس از آن تبادل اطلاعات بین این دو ابر زمان بر خواهد بود؛ بنابراین با تغییر در روند ورودی و خروجی و سیاست های هر یک از این دو ابر باعث اجبار در تغییر ابر دیگر می شود تا همچنان این دو ابر هماهنگ کار کنند؛ اما اگر سیستم به خوبی پیاده سازی گردد که در عمل بسیار سخت می باشد می تواند به خوبی از منابع اصلی و بسیار حیاتی سیستم محافظت نماید چراکه کاربر هیچ گاه به طور مستقیم با منابع در تماس نخواهد بود و همین باعث می شود تا هکرها نتوانند به راحتی حمله خود را طراحی نمایند.

3-5- تشخیص نفوذ در سیستم با استفاده از منطق فازی

توجه به افزایش حملات اینترنتی، ایجاد یک سیستم تشخیص نفوذ برای امنیت سیستم‌ها به یک امر ضروری تبدیل شده است. در بیشتر سیستم‌های تشخیص نفوذ ارائه شده یک دیتابیس برای ذخیره الگوهای مربوط به حملات وجود دارد که با کمک آن مراقبت از سیستم انجام می‌گیرد. در روش FC-ANN ارائه شده [۷] الگوها به صورت خودکار یافت می‌شوند و این الگوها در دیتابیس‌های سیستم تشخیص نفوذ ذخیره و مورد استفاده قرار می‌گیرد.

روش پیشنهادی مبتنی بر سه ماژول زیر می‌باشد:

1. مشاهده و صف کردن: این ماژول بسته‌های داده‌ای را دریافت می‌کند. سپس داده‌ها را به صف مشترک ماژول آنالیز می‌سپارد.
 2. آنالیز و پردازش
 3. گزارش
- کنترل صف به صورت چند نخه انجام می‌گیرد. سپس در این صف بسته‌ها مورد بررسی قرار می‌گیرند و هشدارهای لازمه تولید می‌گردد.
- هدف این پژوهش [۷] طراحی و تحلیل انواع مختلفی از سیستم‌های فازی است که برای تشخیص نفوذ می‌تواند مورد استفاده قرار بگیرد. در نهایت نیز مقاله یک معماری برای کنار هم قرار دادن طبقه بندها ارائه کرده است

روش یادگیری قوانین با تکرار

مراحل پردازشی روش به شرح زیر است:

- تولید یک جمعیت اولیه فازی از قوانین if-then
- تولید قوانین جدید فازی if-then به وسیله عملیات فازی سازی
- جانشین کردن بخشی از جمعیت موجود با قوانین جدید
- افزودن دوباره جمعیت

- اگر شرایط توقف ملاقت شده پردازش را متوقف کن در غیر این صورت به مرحله ۲ برو

در این سیستم از روش تسریع شده نیز بهره برده شده است. انقدر مراحل یادگیری در این چرخه تکرار می‌گردد تا به نتایج موردنظر برسیم. قوانین فازی در این روش در هر فاز اضافه می‌شوند تا دقت دریافتن جواب افزایش یابد. بخش تسریع دهنده روش ارائه شده وزن مثال‌های آموزشی که به درستی طبقه‌بندی شده‌اند را کاهش می‌دهد تا پردازش چندباره بر روی بخشی از داده‌ها صورت نگیرد.

3-6- تشخیص سلسله مراتبی نفوذ به روش ناهنجاری بوسیله شبکه‌های عصبی

همراه با رشد سریع شبکه‌های کامپیوتری در طی چند سال اخیر، امنیت در سیستم‌های کامپیوتری مدرن به صورت موضوعی بسیار حیاتی و مهم درآمده است. در طی دو دهه اخیر تلاش‌های تحقیقاتی فراوانی در زمینه امنیت شبکه صورت گرفته و تکنیک‌های مختلفی برای ساختن شبکه‌های امن ارائه شده‌اند. تکنیک‌هایی نظیر فایروال، کنترل دستیابی و تشخیص نفوذ از این قبیل هستند. تمرکز پژوهش انجام شده در [۲۷] بر روی تشخیص نفوذ و طراحی و پیاده‌سازی یک سیستم تشخیص نفوذ می‌باشد. سیستم‌های تشخیص نفوذ از دو رویکرد برای تشخیص حملات استفاده می‌کنند: تشخیص ناهنجاری و تشخیص سوءاستفاده. سیستم‌های تشخیص ناهنجاری نفوذ را بر اساس رفتار ناهنجار کاربران یا پرده‌ها تشخیص می‌دهند، درحالی‌که سیستم‌های تشخیص سوءاستفاده نفوذ را بر اساس الگوهای تعریف شده از حملات کشف می‌کنند. سیستم‌های تشخیص سوءاستفاده، تشخیص حملات را تضمین می‌کنند اما برخلاف سیستم‌های تشخیص ناهنجاری قادر به شناسایی حملات جدید یا ناشناخته نیستند. از لحاظ منبع اطلاعات نیز می‌توان سیستم‌های تشخیص نفوذ را به دودسته سیستم‌های مبتنی بر میزبان و سیستم‌های مبتنی بر شبکه دسته‌بندی کرد. سیستم‌های مبتنی بر میزبان بر روی اطلاعات جمع‌آوری شده در داخل یک سیستم کامپیوتری مجزا عمل می‌کنند، در حالیکه سیستم‌های مبتنی بر شبکه بر ترافیک شبکه نظارت می‌کنند. در این پژوهش یک سیستم تشخیص نفوذ سلسله مراتبی طراحی و پیاده‌سازی شده است که قادر است حملات مبتنی بر شبکه را با روش تشخیص ناهنجاری و به وسیله شبکه‌های عصبی تشخیص دهد. شبکه‌های عصبی به دلیل دارا بودن توانایی دسته‌بندی بالا و قدرت تعمیم می‌توانند در سیستم‌های تشخیص نفوذ به کاربرده شوند. شبکه نمونه از سه سطح سلسله‌مراتب استفاده می‌کند که هر سیستم

تشخیص نفوذ در سطح پایین، گزارشی را به سیستم تشخیص نفوذ در سطح بالا ارسال می‌کند. این سیستم تشخیص نفوذ با دریافت بسته‌ها از شبکه، ویژگی‌های اتصالات شبکه را استخراج کرده و پس از پیش‌پردازش آماری بر روی اتصالات با استفاده از دسته‌بندی شبکه‌های عصبی رفتارهای غیرعادی را در سطح شبکه تشخیص می‌دهد. سیستم تشخیص نفوذ پیاده‌سازی شده از شبکه‌های عصبی در ساختار خود به‌عنوان دسته‌بندی کننده استفاده می‌کند که سیستم‌های تشخیص نفوذ سلسله مراتبی و توزیع‌شده کنونی فاقد چنین ویژگی هستند. شبکه‌های عصبی مورد استفاده شده BP و PBH می‌باشند که شبکه عصبی PBH تاکنون در یک محیط واقعی مورد آزمایش قرار نگرفته است و الگوریتم یادگیری شبکه PBH در پیاده‌سازی سیستم تشخیص نفوذ پیشنهادی استخراج شده است. هدف این پژوهش [۲۷] بررسی و مقایسه کارایی و هزینه دو شبکه عصبی BP و PBH برای تشخیص نفوذ در محیطی عملی و واقعی می‌باشد. نتایج تست شبکه‌های عصبی BP و PBH نشان داد که شبکه PBH با داشتن تعداد نورون‌های مخفی کمتر دارای نرخ اعلان خطای پایین‌تری می‌باشد و در نتیجه کارایی بالاتری نسبت به شبکه BP دارد و همچنین با کاهش تعداد نورون‌های مخفی در شبکه PBH هزینه محاسبات نیز در این شبکه کاهش می‌یابد.

منابع و مراجع

- [1] Rasheed, Hassan. "Data and infrastructure security auditing in cloud computing environments." *International Journal of Information Management* 34.3 (2014): 364-368.
- [2] Bose, Ranjit, Xin Luo, and Yuan Liu. "The Roles of Security and Trust: Comparing Cloud Computing and Banking." *Procedia-Social and Behavioral Sciences* 73 (2013): 30-34.
- [3] Kshetri, Nir. "Privacy and security issues in cloud computing: The role of institutions and institutional evolution." *Telecommunications Policy* 37.4 (2013): 372-386.
- [4] Sood, Sandeep K. "A combined approach to ensure data security in cloud computing." *Journal of Network and Computer Applications* 35.6 (2012): 1831-1838.
- [5] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." *Future Generation Computer Systems* 28.3 (2012): 583-592.
- [6] Che, Jianhua, et al. "Study on the security models and strategies of cloud computing." *Procedia Engineering* 23 (2011): 586-593.
- [7] A .H. Sung, S. Mukkamala. " Feature Selection for Intrusion Detection using Neural Networks and Support Vector Machines." *Future Generation Computer Systems* 32 (2014): 27-40.
- [8] Shin, Dong-Hee. "User centric cloud service model in public sectors: policy implications of cloud services." *Government Information Quarterly* 30.2 (2013): 194-203.
- [9] Rong Chunming, Nguyen Son T. Cloud trends and security challenges. In: *Proceedings of the 3rd international workshop on security and computernetworks (IWSCN 2011)*; 2011.
- [10] Zhao Gansen, Rong Chunming, Li Jin, Zhang Feng, Tang Yong. Trusted data sharing over untrusted cloud storage providers. In: *Proceedings of the 2nd IEEE international conference on cloud computing technology and science (CloudCom 2010)*; 2010.
- [11] Pearson Siani. Toward accountability in the cloud. *EEE Internet Comput* 2011;15(4):64–9.
- [12] Brian Hayes. 'Cloud computing'. In: *Commun. ACM* 51.7 (2008).
- [13] Tim Mather, Subra Kumaraswamy and Shahed Latif. *Cloud Security and Privacy: An Enterprise Perspective on Risk and Compliance*. Editor Mike Loukides. O'Reilly, 2009.

- [14] Graham Kirby, Alan Dearle et al. An Approach to Ad hoc Cloud Computing. Tech. rep. St Andrews Cloud Computing Initiative, School of Computer Science, University of St Andrews, Feb. 2009.
- [15] Cloud Computing: Benefits, risks and recommendations for information security. Tech. rep. European Network and Information Security Agency (ENISA), 2009.
- [16] Dan Hubbard, Michael Sutton et al. Top Threats to Cloud Computing v1.0. Tech. rep. v1.0. Cloud Security Alliance, Mar. 2010.
- [17] Meiko Jensen, Nils Gruschka and Norbert Lüttenberger. 'The Impact of Flooding Attacks on Network-based Services'. In: ARES '08: Proceedings of the 2008 Third International Conference on Availability, Reliability and Security. Washington, DC, USA: IEEE Computer Society, 2008, pp. 509-513.
- [18] Ken Birman, Gregory Chockler and Robbert van Renesse. 'Toward a cloud computing research agenda'. In: SIGACT News 40.2 (2009), pp. 68{80.
- [19] The Cross-Site Request Forgery (CSRF/XSRF) FAQ. English. CGI Security. Apr. 2010.
- [20] [XSS02] The Cross-Site Scripting (XSS) FAQ. English. CGI Security. May 2002.
- [21] H. Güneş Kayacık, A. Nur Zincir-Heywood, Malcolm I. Heywood," Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets", Dalhousie University, Faculty of Computer Science, 6050 University Avenue, Halifax, Nova Scotia. B3H 1W5.
- [22] B.B.Sujitha and R.R. Ramani, "Intrusion Detection System using Fuzzy Genetic Approach", International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 10, December 2012.
- [23] M. Sadiq and Ali Khan,"Rule based Network Intrusion Detection using Genetic Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 18– No.8, March 2011.
- [24] J.R. Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics, Technical Editor Bill Meine, Elsevier Publishing, 2011.
- [25] Y. Jadeja and K. Modi, "Cloud computing - concepts, architecture and challenges," in Computing, Electronics and Electrical Technologies(ICCEET), 2012 International Conference on, 2012, pp. 877-880.

- [26] A. Soule, K. Salamatian, and N. Taft, "Combining filtering and statistical methods for anomaly detection," in Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement, pp. 31-31, 2005.
- [27] A. Kannan, G. Q. Maguire, " Genetic Algorithm based Feature Selection Algorithm for Effective Intrusion Detection in Cloud Networks," 2012 IEEE 12th International Conference on Data Mining Workshops, 2012.
- [28] Y. Li, J. Xia, S. Zhang, J. Yan, X. Ai, K. Dai, " An efficient intrusion detection system based on support vector machines and gradually feature removal method ",in Expert Systems with Applications 39 (2012) 424–430, 2012.
- [29] J.-H. Lee, M.-W. Park, J.-H. Eom, and T.-M. Chung, "Multi-level Intrusion detection system and log management in cloud computing," in Advanced Communication Technology (ICACT), 2011 13th International Conference on, pp. 552-555, 2011.
- [30] C. Mazzariello, R. Bifulco, and R. Canonico, "Integrating a network ids into an open source cloud computing environment," in Information Assurance and Security (IAS), 2010 Sixth International Conference on, pp. 265-270, 2010.

ABSTRACT

Cloud computing model to provide easy access, distributed and pervasive computing resources and shared collective configurable deals. In cloud-based IT capabilities as services that do not require detailed knowledge of infrastructure technologies and have minimal management effort, is provided. Due to this, one of the important issues is the focus of security challenges on modern technology. The most useful aspect of the cloud include: quick and easy implementation model, payments to the amount of use and reduce costs within organizations. Other topics that will be presented by cloud computing paradigm to pay. To evaluate the proposed approach and comparisons with some of the approaches taken in this field assessments indicate that the proposed method is accurate.

Key words:

Cloud Computing, Data Security Improvement, Artificial Neural Networks, Decision Tree