International Conference on
RESEARCH IN ELECTRICAL AND COMPUTER ENGINEERING
کنفرانس بین المللی پژوهش در مهندسی برق و کامپیوتر
15 December 2016 Singapore www.receconf.com سنگاپور ۲۵ آذر ۱۳۹۵

تشخیص نفوذ به صورت توزیع‌شده در سیستم‌های رایانش ابری

دنیا شعیبی
گروه فناوری اطلاعات، دانشکده برق و کامپیوتر، دانشگاه تحصیلات تکمیلی صنعتی و فناوری پیشرفته، کرمان، ایران.
d.shoeibi@kgut.ac.ir

دکتر حمیدرضا ناجی
گروه فناوری اطلاعات، دانشکده برق و کامپیوتر، دانشگاه تحصیلات تکمیلی صنعتی و فناوری پیشرفته، کرمان، ایران.
hamidnaji@ieee.org

چکیده

ساختار توزیع شده و باز محاسبات ابری و خدمات باعث شده اطلاعات موجود در ابر به هدف مناسبی برای پتانسیل حملات سایبری توسط مزاحمان باشد. با ظهور اینترنت، در طول زمان حملات نفوذ ، به پیچیدگی بسیاری دست یافته‌اند. سیستم تشخیص نفوذ سنتی تا حد زیادی در محیط محاسبات ابری به دلیل شفافیت و جوهر خاص، ناکارآمد می‌باشد. حملات پراکنده‌ی بسیاری وجود دارد که توسط سیستم‌های موجود تشخیص نفوذ ، قادر به شناسایی نمی‌باشند. در این مقاله، به بررسی اطلاع پژوهشگران در مورد انواع خاصی از سیستم‌های تشخیص نفوذ توسعه یافته و تکنیک‌های مدیریت آلارم با ارائه یک طبقه بندی جامع و بررسی روش‌های ممکن برای شناسایی نفوذ به سیستم رایانش ابری می پردازد. با توجه به ویژگی‌های مورد نظر سیستم تشخیص نفوذ و سیستم‌های رایانش ابری، یک لیست از الزامات وابسته شناسایی شده است و سه مفهوم تشخیص نفوذ توزیع شده، مدیریت و نظارت مرکزی و یکپارچگی اطلاعات، اهرمی برای برآوردن این نیازها هستند.

واژگان کلیدی: امنیت در شبکه ، تشخیص نفوذ ، توزیع شده ، رایانش ابری ، مدیریت مرکزی.

۱. مقدمه

در طول دهه گذشته، جامعه ما وابستگی بسیاری به تکنولوژی پیدا کرده است. مردم به شبکه‌های کامپیوتری برای دریافت اخبار، قیمت سهام، ایمیل و خرید آنلاین تکیه نموده‌اند. یکپارچگی و دردسترس بودن تمام این سیستم‌ها به دفاع در برابر تعداد زیادی از تهدیدات نیازمند است(Patel et al., 2013).

رایانش ابری ارائه دهنده‌ی محاسبات و فضای ذخیره‌سازی به‌عنوان یک سرویس به یک جامعه ناهمگن پایان‌گیرنده است که از اینترنت و سرورهای مرکزی از راه دور برای حفظ داده‌ها و برنامه‌های کاربردی استفاده می کند. برجسته‌ترین ویژگی رایانش ابری برای کسب دسترسی به داده‌ها از هر کامپیوتر از طریق اینترنت بدون هیچ گونه نصب و راه اندازی می‌باشد(Li And Wu, 2012.).

سه نوع از محاسبات ابری وجود دارد:

- زیرساخت به عنوان یک سرویس (IaaS) مانند خدمات وب آمازون، ابر، Rackspace و غیره
- بستر های نرم افزاری به عنوان یک سرویس (PaaS) مانند خدمات وب آمازون، گوگل نرم افزار موتور، مایکروسافت آزور و غیره
- نرم افزار به عنوان خدمات (SaaS) مانند گوگل ، مایکروسافت آفیس ۳۶۵ و غیره

حتی اگر رایانش ابری دارای مزایای بسیاری باشد، محدودیت‌های امنیتی باعث می شود که کاربر نهایی و یا مشتریان قبل از اجرای محیط ابر در سازمان خود تردید نمایند. امنیت یکی از مسائل مهم در همه نوع از شبکه هاست، به خصوص در اینترنت مسائل امنیتی بسیاد حائز اهمیت است(Xin et al., 2010). در همین‌جاست که موضوع تشخیص نفوذ به میان می آید. سیستم تشخیص نفوذ وظیفه‌ی شناسایی و تشخیص هر گونه استفاده‌ی غیرمجاز به سیستم، سوء استفاده و یا آسیب رسانی توسط هر دو دسته‌ی کاربران داخلی و خارجی را بر عهده دارند. تشخیص نفوذ امروزه به عنوان یکی از مکانیزم‌های اصلی در برآوردن امنیت شبکه‌ها و سیستم‌های رایانه‌ای مطرح است. این سیستم دارای روش‌های متعددی تحت عنوان روش‌های تشخیص نفوذ می باشد که عمل نظارت بر وقایع اتفاق افتاده در یک سیستم یا شبکه‌ی رایانه‌ای را بر عهده دارد. روش‌های تشخیص مورد استفاده در سامانه‌های تشخیص نفوذ به دو دسته تقسیم می‌شوند:

- روش تشخیص رفتار غیر عادی anomaly detection
- روش تشخیص سوءاستفاده یا تشخیص مبتنی بر امضاء misuse detection

هان‌لی و همکاران (Li .And Wu, 2012) به پیشنهاد ارایه ی یک مدل تشخیص نفوذ توزیعی مبتنی بر ساختار ابر پرداختند. که دارای زیر سیستم‌های جمعاوری داده‌ی مرکزی و عامل‌های توزیع شده می‌باشد که یک گزارش یکپارچه از طریق بخش جمعاوری داده، ارائه می‌نماید. در مقاله‌ای دیگر روشکه و مینل(Roschke et al., 2009) به تشخیص نفوذ در ابر (IDC) برای معرفی مفهوم مدیریت سیستم تشخیص نفوذ با مشتقات جزئی برای کاربران ابر پرداخته اند. معماری ارائه شده متشکل از چندین حسگر به‌صورت توزیع‌شده و یک واحد مدیریت مرکزی می باشد. پاراگ و همکاران (Shelke et al., 2012)به ارائه‌ی مدل تشخیص نفوذ چند رشته‌ای که به‌دلیل مدل توزیع شده ی ابری، باعث آسیب پذیری بسیار و مستعد ابتلا به حملات پیچیده نفوذ توزیع شده می‌باشد. این سیستم دارای مدیریتی مرکزی، در خارج از شبکه و عامل‌های توزیع‌شده می‌باشد. جی ساتیا در مقاله (Sathya .And Vasanthraj, 2013)، یک سیستم تشخیص نفوذ با سیستم بازرسی لاگ برای تشخیص حملات و حفظ سطح امنیت و اثربخشی با سیستم چند سطح مختلف سیستم را پیشنهاد نموده است که می‌تواند گزارش هشدار به کاربران ابر و مشاوره برای ارائه دهندگان خدمات ابر را با توجه به اولویت حساس بودن، فراهم نماید. ایساکوف و همکاران(Balasubramaniyan et al., 1998) در مورد عامل‌های سیستم تشخیص نفوذ توزیع شده مبتنی‌بر میزبان (AAFID)و به‌صورت خودمختار وبر اساس زمان واقعی برای سیستم تشخیص نفوذ، پرداخته‌اند. در مقاله‌ی افضلی و عظیمی(Seresht .And Azmi, 2014) یک رویکرد مبتنی بر عامل با استفاده از پارادایم های سیستم ایمنی مصنوعی (AIS) به عنوان یک مکانیسم موفق برای یک سیستم تشخیص نفوذ توزیع (IDS) پیشنهاد می کند. این

نمونه‌ها برای سیستم تشخیص نفوذ ناهنجاری بسیار موفق بوده‌اند. پیشنهاد عوامل بر اساس پارادایم های سیستم ایمنی مصنوعی قادر به یادگیری، خود-تنظیم، استقلال و همکاری می‌باشد و با استفاده از این عامل‌های توزیع شده‌ی قدرتمند و مشترک طراحی شده‌اند. در مقاله‌ی هالر و همکاران (Genge et al., 2016) یک چارچوب جدید برای طراحی سیستم های تشخیص نفوذ توزیع شده‌ی انعطاف پذیر معرفی کرده‌اند. چارچوب قدرتمند خروجی، یک متدولوژی ارزیابی ریسک برای شناسایی و رتبه بندی جریان ارتباطات حیاتی است. چارچوب طراحی یک الگوریتم تشخیص نفوذ انعطاف پذیر توزیع شده با پیش‌بینی احتمال به‌خطر افتادن یا شکست سیستم‌های تشخیص نفوذ است. نتایج تجربی نیز، اثربخشی طراحی تشخیص نفوذ در چارچوب توزیع شده‌ی را نشان داده است.

هدف اصلی ما برای کاهش تاثیر حملات شبکه بر روی رایانش ابری، در حالی که اطمینان از تشخیص زودهنگام فعالیت‌های مخرب و نرخ تشخیص بالاتر و میزان مثبت کاذب کمتر می‌باشد. همچنین دارای سیستمی که دیدی سراسری بر روی شبکه داشته تا بتواند بهتر نظارت شده و حملات جدید به کل سیستم اعلام شود.

بخش‌های بعدی مقاله عبادتند از:

بخش ۲ به تشخیص نفوذ توزیع شده در زیرساخت ابر می‌پردازد ، بخش۳ تشخیص نفوذ توزیع‌شده در لایه‌های ابر ، بخش ۴ تشخیص نفوذ چند رشته‌ای توزیع‌شده در ابر، در بخش ۵ سیستم تشخیص نفوذ چند سطحی، در بخش ۶ سیستم تشخیص نفوذ خودمختار توزیع‌شده و در بخش ۷ به مقایسه و جمع‌بندی و در بخش ۸ به نتیجه گیری و کارهای آیندگان و منابع در پایان پرداخته شده است.

۲. تشخیص نفوذ توزیع‌شده در زیر ساخت و لایه‌های ابر

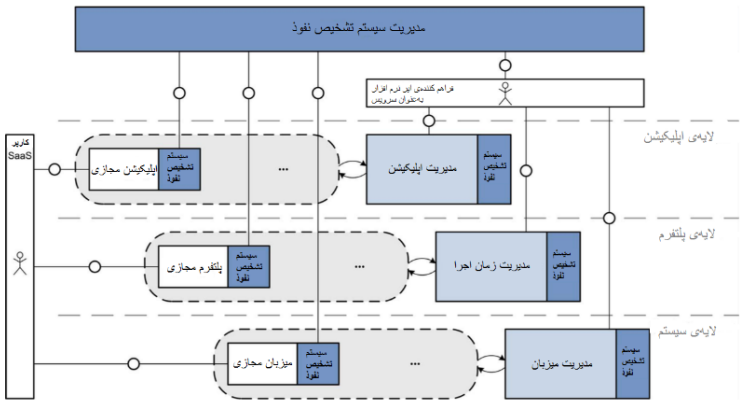
در این نوع ساختار از دو زیر سیستم کلی استفاده شده، و از زیر سیستم‌های تشخیص نفوذ عامل توزیع شده و زیر سیستم داده‌های تجمعی، تشکیل شده است. که خود تشخیص نفوذ عامل نیز دارای ۳ بخش، اطلاعات ماژول مجموعه، ماژول تصمیم‌گیری ابر و ماژول ارتباطات می باشد.

زیر سیستم تشخیص نفوذ عامل بصورت توزیع شده در سیستم پراکنده است و اطلاعات را جمعاوری کرده و رکورد های غیر طبیعی را شناسایی کرده و به زیر سیستم تجمع داده‌ها انتقال داده و در آنجا تصمیم گیری نهایی انجام می شود. این سیستم، سیستمی یکپارچه، دارای عامل های تشخیص نفوذ توزیع شده در سراسر رایانش ابری، دارای دیدی سراسری و مدیریت متمرکز می‌باشد. معماری سیستم تشخیص نفوذ توزیع شده را می‌توانید در شکل شماره‌ی ۱ مشاهده نمایید.

شکل ۱. معماری تشخیص نفوذ توزیع شده در زیرساخت ابر

تشخیص نفوذ درلایه‌های ابر، متشکل از چندین حسگر و یک واحد مدیریت مرکزی می باشد و تشخیص نفوذها به‌صورت توزیع شده در هر ۳ لایه رایانش ابری (لایه کاربردی، لایه بستر های نرم افزاری و لایه سیستم) اجرا شده‌اند، که شامل ترکیبی از هر دو سیستم تشخیص نفوذ مبتنی بر میزبان (HIDS) و سیستم تشخیص نفوذ مبتنی بر شبکه (NIDS) می باشند. سنسورهای سیستم تشخیص نفوذ مبتنی بر شبکه‌ی قرار داده شده در هر لایه‌ی ابر، برای نظارت بر مدیریت ماژول آن لایه است. در واحد مدیریت سیستم تشخیص نفوذ مرکزی دیدی سراسری از کل سیستم را دار ا می‌باشد و اجازه‌ی دسترسی به پایگاه داده‌ها و کانال های ارتباطی بین ماشین‌های مجازی و تحویل گزارش از زیر سیستم‌های مدیریت تشخیص نفوذ می‌باشد.

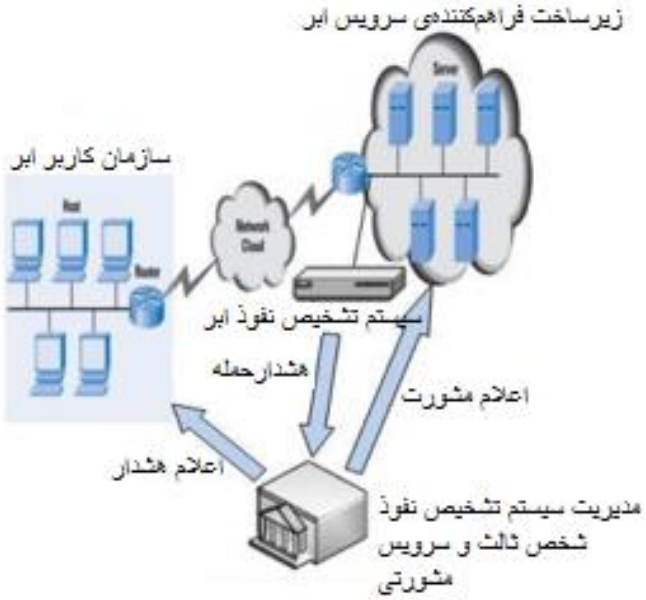
کاربران ابر کاملا بر زیرساخت سیستم تشخیص نفوذ ارائه دهنده وابسته هستند اما آنها هنوز هم تا حدی با قابلیت‌های محدود به کنترل واحد مدیریت سیستم تشخیص نفوذاند. علاوه بر این، حریم خصوصی نگرانی‌های جدی ناشی از ادغام اجزا سیستم تشخیص نفوذ که توسط ارائه‌دهندگان ابر بر روی هر دستگاه مشتریان مجازی نصب شده، وجود دارد.
شکل ۲ سیستم تشخیص نفوذ توزیع شده در لایه‌های ابر می‌باشد که می‌توانید در صفحه‌ی بعد مشاهده فرمایید.



شکل ۲. مدل پیشنهادی تشخیص نفوذ توزیع شده در لایه‌های ابر

۳. تشخیص نفوذ چند رشته‌ای توزیع‌شده

مدل توزیع شده ی ابری، بسیار آسیب پذیر و مستعد ابتلا به حملات پیچیده نفوذ توزیع شده می‌باشد. برای رسیدگی به مقیاس بزرگ ترافیک دسترسی به شبکه و کنترل داده‌ها و برنامه‌ها در ابر، یک مدل جدید ابر سیستم تشخیص نفوذ چند رشته‌ای مبتنی بر شبکه‌ی توزیع شده (Shelke et al., 2012)ارائه شده است. به پیشنهاد سیستم تشخیص نفوذ ابری، که دسته جریان بزرگی از بسته‌های داده را تجزیه و تحلیل می‌کند و تولید گزارش‌های کارآمدی با یکپارچه‌سازی آگاه و عملکرد آنالیز، به تشخیص نفوذ می‌پردازد که سیستمی یکپارچه و با تشخیص نفوذ توزیع شده می‌باشد. سیستم مانیتورینگ شخص ثالث (Third Party IDS monitoring) یک سخت‌افزار در خارج از شبکه می‌باشد و همه‌ی درخواست‌های ورود به شبکه را چک می‌کند .
وجود قسمتی از سیستم در خارج از شبکه، خود می‌تواند یک ضعف امنیتی بزرگی برای سیستم باشد (Rajendran et al., 2015) ، از آنجا که قطعات سخت‌افزاری تشخیص نفوذ در خارج از شبکه قرار دارند ، می‌توان به آسانی توسط مهاجمان، قابل نفوذ باشد و امنیت شبکه را به شدت تحت تاثیر قرار می‌دهد.
معماری مدل رایانش ابری سیستم تشخیص نفوذ چند رشته‌ای توزیع شده در شکل شماره‌ی ۳ نمایش داده شده است.



شکل ۳. مدل پیشنهادی ابر سیستم تشخیص نفوذ چند رشته‌ای توزیع شده

۴. تشخیص نفوذ چند سطحی

سیستم تشخیص نفوذ چند سطحی و سیستم بازرسی لاگ، برای تشخیص حملات و حفظ سطح امنیت و اثربخشی سیستم، می‌توان گزارش هشدار به کاربران ابر و مشاوره برای ارائه دهندگان خدمات ابر فراهم کند (Sathya .And Vasanthraj, 2013). این سیستم‌های تشخیص نفوذ بر پایه‌ی تکنیک‌های داده کاوی و روش تشخیص ناهنجاری می‌باشند. پس از طی نمودن رکوردهای سطوح مختلف جهت شناسایی، سطح ناهنجاری نیز اولویت‌بندی شده و با توجه به درجه‌ی سطح امنیتی، اولویت‌دهی می‌شود و منجر به استفاده از منابع موثر با توجه به سطح متفاوتی از قدرت امنیتی مطابق با درجه‌ی ناهنجاری متصل می‌شود. به همین جهت با دسته‌بندی شدن ترافیک به سطوح و طبقه‌های مختلف، به کاهش ترافیک در ابر کمک می نماید. از آنجا که سیستم تشخیص نفوذ می‌تواند هر ماشین مجازی را نظارت نموده و داده‌های هشدار را تولید نماید، می‌تواند رایانش ابری را در سطح سراسری (Global) مدیریت نماید. این روش می‌تواند در مواقع رویارویی با حملات احتمالی که ممکن است خطرناکتر از حملات هم‌زمان دیگر باشد، بسیار موثر باشد.

۵. تشخیص نفوذ خودمختار توزیع‌شده

عامل‌های سیستم تشخیص نفوذ خودمختار توزیع شده (AAFID)، مبتنی‌بر میزبان و زمان واقعی برای سیستم تشخیص نفوذ ، توسط ایساکوف و همکاران (Balasubramaniyan et al., 1998) ارائه شده است. این اساسا خطاب به نواقص معماری سیستم‌های تشخیص نفوذ، معمولا یکپارچه‌ی واحد اند، بیشتر از جمع آوری داده ها و پردازش، ساخته شده است. از این رو، معماری عامل‌های سیستم تشخیص نفوذ خودمختار توزیع شده با واحد های مستقل متعددی، بر انجام کار گروهی استوار است. این نهادها، عامل های خودمختار نامیده می شوند. معماری با استفاده از عامل‌ها به عنوان پایین‌ترین سطح عناصر برای جمع آوری داده‌ها و تجزیه و تحلیل، یک ساختار سلسله مراتبی مقیاس‌پذیری بوجود می آید. معماری عامل‌های سیستم تشخیص نفوذ خودمختار توزیع شده شامل سه قسمت اصلی است: عوامل، فرستنده و گیرنده، و مانیتور.

یک عامل، یک موجودیت مستقل در حال اجرا است که بر رویدادهای میزبان برای رویدادهای مشکوک نظارت دارد و گزارش چنین رویدادهایی را به فرستنده و گیرنده مناسب انتقال می‌دهد. هر یک از میزبان ها می توانند هر تعداد از عوامل و همه عوامل در یک میزبان یافته های خود را تنها به فرستنده و گیرنده گزارش کنند. عامل فاقد این صالحیت است که به طور

مستقیم تولید آلارم در مواجه با رویدادی مشکوک نماید. علاوه بر این، عوامل با یکدیگر در معماری عامل‌های سیستم تشخیص نفوذ خودمختار توزیع شده ارتباط برقرار نمی کند.

فرستنده و گیرنده در هر میزبان شخصیست که نظارت بر عملیات تمام عوامل در حال اجرا بر روی میزبان و ارسال دستورات پیکربندی به عامل مربوطه می باشند. در نهایت، فرستنده و گیرنده نتایج را به یک یا چند سیستم ناظر، گزارش می دهند.

سیستم نظارت ، بالاترین سطح موجودیت‌ها، در معماری عامل‌های سیستم تشخیص نفوذ خودمختار توزیع شده هستند. هر مانیتور ناظر بر عملیات چند فرستنده و گیرنده است و اطلاعات کاهش یافته‌ی تمام فرستنده و گیرنده ها را به رابطه سطح بالا ارایه داده و تشخیص نفوذ می‌کند. سیستم نظارت با یک رابط کاربری که به عنوان نقطه دسترسی بر تمامی سیستم‌های عامل‌های تشخیص نفوذ خودمختار توزیع شده اعمال شده، ارتباط برقرار کند.

سیستمی Real-time تشخیص نفوذ مبتنی بر شبکه، با عامل های توزیع شده می باشد.

۶. مقایسه و جمع‌بندی

با توجه به مطالعات انجام شده، بر روی مقاله‌های اشاره شده، می توان به این دید دست یافت که سیستمی دارای امنیت بالاتری می‌باشد که مدیریت ناظر دارای دید یکپارچه و سراسری از کل ترافیک شبکه، با سیستم های تشخیص نفوذ توزیع شده که بتوانند به صورت همزمان قسمت‌های مختلف سیستم را نظارت کرده و در صورت برخورد با رفتار مشکوک ، آن را به ناظر خود گزارش داده و مدیریت ناظر مرکزی و سراسری برای جلوگیری احتمال نفوذ اقدام نمایند. در زیر یک جدول مقایسه ۱ آمده است.

جدول ۱. مقایسه‌ی روش‌های تشخیص نفوذ توزیع‌شده در رایانش ابری

روش مقاله	نحوه‌ی شناسایی	عکس‌العمل	نحوه‌ی مدیریت	انواع سیستم تشخیص نفوذ
تشخیص نفوذ توزیع‌شده در زیر ساخت و لایه‌های ابر	یکپارچه	برون‌خط	مرکزی	ترکیبی
تشخیص نفوذ چند رشته‌ای	چندرشته‌ای یکپارچه	برون‌خط	سوم شخص-مرکزی	مبتنی‌بر شبکه
تشخیص نفوذ چندسطحی	چندسطحی	اولویت‌دار	مرکزی	مبتنی‌بر شبکه
تشخیص نفوذ خودمختار	یکپارچه	برخط	مرکزی	مبتنی‌بر میزبان

همان‌طور که در جدول بالا قابل مشاهده می‌باشد، در مقاله‌ی تشخیص نفوذ توزیع‌شده در زیر ساخت ابر دارای یک سیستم تشخیص نفوذ توزیع شده توزیع شده با مدیریت مرکزیست، اما حجم زیادی از ترافیک از چندین عامل توزیع شده، در حال انتقال به سیستم جمعاوری دادهاست.

در مقاله تشخیص نفوذ توزیع‌شده در زیر ساخت ابر نیز به یک سیستم ترکیبی تشخیص نفوذ توزیع شده‌ی یکپارچه در هر سه لایه‌ی ابر و با حجم ترافیک بالا در مدیریت مرکزی می‌باشد.

در مقاله‌ی تشخیص نفوذ چند رشته‌ای توزیع‌شده از یک سیستم مدیریت مرکزی چند رشته استفاده شده تا در اثر ترافیک بسته‌ای از دست نرود که در خارج از ابر قرار دارد و در صورتی که خود سیستم مدیریت مورد نفوذ قرار گیرد کل امنیت سیستم از کار می‌افتد.

در مقاله‌ی سیستم تشخیص نفوذ چند سطحی از یک سیستم تشخیص نفوذ توزیع شده‌ی چند سطحی استفاده شده و در هر سطح یا مرحله از شناسایی حمله انجام می‌شود و با تخصیص وزن و اولویت به حملات با وزن بالاتر ، اولویت جهت رسیدگی از نظر اختصاص منابع و زمانی می‌دهد. این کار به کمتر شدن ترافیک در مدیریت مرکزی کمک می‌کند.

در مقاله‌ی سیستم تشخیص نفوذ خودمختار توزیع‌شده به گزارش یکپارچه و تشخیص نفوذ توزیع شده با مدیریت مرکزی و تشخیص حملات مبتنی بر میزبان بصورت Real-time با روش تشخیص حملات سلسله مراتبی و مقیاس‌پذیر می‌باشد.

با توجه به مقاله‌های متناسب با موضوع به این نتیجه می‌توان رسید که در صورتی که دارای گزارشات سراسری از قسمت های مختلف رایانش ابری به وسیله‌ی سیستم تشخیص نفوذ توزیع شده، داشته باشیم و گزارشات مفیدی را بتوان بصورت Real-

time با توجه به اولویت حیاتی بودن حملات به مدیریت مرکزی رسانده تا هشدار و تدابیرلازم جهت امنیت سیستم را بعمل آورد.

۷. نتیجه‌گیری

با توجه به مطالعات انجام شده، بر روی مقاله‌های اشاره شده، به این نتیجه می‌توان رسید که در صورتی که دارای گزارشات سراسری از قسمت های مختلف رایانش ابری به وسیله‌ی سیستم تشخیص نفوذ توزیع شده و به صورت همزمان، داشته باشیم و در صورت برخورد با رفتار مشکوک ، آن را به ناظر خود گزارش داده و گزارشات مفید را با توجه به اولویت و اهمیت حیاتی بودن حملات بتوان بصورت Real-time به مدیریت مرکزی رسانده تا هشدار لازم را اعلام کرده و تدابیرلازم جهت امنیت سیستم را بعمل آورد.

پیشنهاد ما برای چنین سیستم‌هایی، حذف ترافیک اضافه در زمان بررسی ناظر زیر سیستم و ارائه‌ی گزارش مفید به مدیریت ناظر سراسری جهت اقدام نهایی و رسیدگی به ترتیب اولویت حیاتی بودن حمله می‌باشد.

منابع

Balasubramaniyan, J. S., Garcia-Fernandez, J. O., Isacoff, D., Spafford, E., & Zamboni, D. (1998). *An architecture for intrusion detection using autonomous agents.* Paper presented at the Computer Security Applications Conference, 1998. Proceedings. 14th Annual.

Genge, B., Haller, P., & Kiss, I. (2016). A framework for designing resilient distributed intrusion detection systems for critical infrastructures. *International Journal of Critical Infrastructure Protection*.

Li, H., & Wu, Q. (2012). *A distributed intrusion detection model based on cloud theory.* Paper presented at the 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems.

Patel, A., Taghavi, M., Bakhtiyari, K., & JúNior, J. C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of network and computer applications*, *36*(1), 25-41.

Rajendran, P. K., Muthukumar, B., & Nagarajan, G. (2015). Hybrid intrusion detection system for private cloud: a systematic approach. *Procedia Computer Science*, *48*, 325-329.

Roschke, S., Cheng, F., & Meinel, C. (2009). *Intrusion detection in the cloud.* Paper presented at the Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on.

Sathya, G., & Vasanthraj, K. (2013). *Network activity classification schema in IDS and log audit for cloud computing.* Paper presented at the Information Communication and Embedded Systems (ICICES), 2013 International Conference on.

Seresht, N. A., & Azmi, R. (2014). MAIS-IDS: A distributed intrusion detection system using multi-agent AIS approach. *Engineering Applications of Artificial Intelligence*, *35*, 286-298.

Shelke, M. P. K., Sontakke, M. S., & Gawande, A. (2012). Intrusion detection system for cloud computing. *International Journal of Scientific & Technology Research*, *1*(4), 67-71.

Xin, W., Ting-lei, H., & Xiao-yu, L. (2010). *Research on the Intrusion detection mechanism based on cloud computing.* Paper presented at the 2010 International Conference on Intelligent Computing and Integrated Systems.