APJ 6 (3):76-88, Autumn 2025

Arman Process Journal (APJ)

Quarterly Journal of ICT APJ

License Number: 87090

Arman Process Journal (APJ)

Homepage: https://www.armanprocessjournal.ir

Approaches to Address the Challenge of Intrusion in Cloud Computing Services

Hosein Mansouri [1]

[1] ***Department of Computer Engineering, Khodabandeh Branch, Islamic Azad University, Khodabandeh, Iran***

ABSTRACT

Nowadays, cloud computing is the preferred choice of any organization based on information and communication technology due to its flexible services and outstanding pay-as-you-go features. Some cloud-based networks face various security challenges due to the lack of fixed infrastructure and centralized management. However, the security and privacy of cloud computing systems is a fundamental problem of cloud computing due to their distributed architecture and vulnerability to unwanted inputs. The role of unwanted attack detection systems in cloud security is very important because it acts as a preventive security layer and, in addition to identifying known attacks, can detect many unknown attacks. In this article, we intend to review these systems and describe approaches to deal with the challenge of intrusion into cloud computing services.

RESEARCH PAPER

Received: 2025-8-17
Accepted: 2025-12-24

KEYWORDS:
Cloud Computing,
Security,
Disturbance Penetration,
Attack,

* Corresponding author:
h.mansouri@iau.ac.ir

نشریه تخصصی آرمان پردازش، دوره ۶، شماره ۳، سال ۱۴۰۴

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

رویکردهای مقابله با چالش نفوذ در خدمات رایانش ابری

حسین منصوری

گروه مهندسی کامپیوتر ، واحد خدابنده ، دانشگاه آزاد اسلامی، خدابنده، ایران

چکیده

مقاله پژوهشی

امروزه رایانش ابری به دلیل خدمات انعطاف پذیر و ویژگی برجسته مبتنی بر پرداخت خدمات به میزان استفاده، انتخاب و برگزیده هر سازمان مبتنی بر فناوری اطلاعات و ارتباطات است. برخی شبکه‌های مبتنی بر رایانش ابری به علت فقدان زیرساخت ثابت و مدیریت متمرکز با چالشهای امنیتی مختلفی روبرو هستند. با این وجود، امنیت و حریم شخصی سیستمهای رایانش ابری به دلیل معماری توزیع شده‌ی آنها و آسیب پذیری در برابر ورودی‌های ناخواسته مشکل اساسی رایانش ابری است. نقش سیستمهای شناسایی حمله‌های ناخواسته در امنیت ابر بسیار مهم است زیرا مانند یک لایه‌ی پیشگیرانه ی امنیتی عمل می‌کند و علاوه بر شناسایی حمله‌های شناخته شده می‌تواند بسیاری از حمله‌های ناشناخته را کشف کند. در این مقاله قصد داریم این سیستم های را بررسی نموده و رویکردهای مقابله با چالش نفوذ در خدمات رایانش ابری را توصیف نمائیم.

واژگان کلیدی:
رایانش ابری،
امنیت،
نفوذ اختلال،
حمله امنیتی،

نویسنده مسئول:
h.mansouri@iau.ac.ir

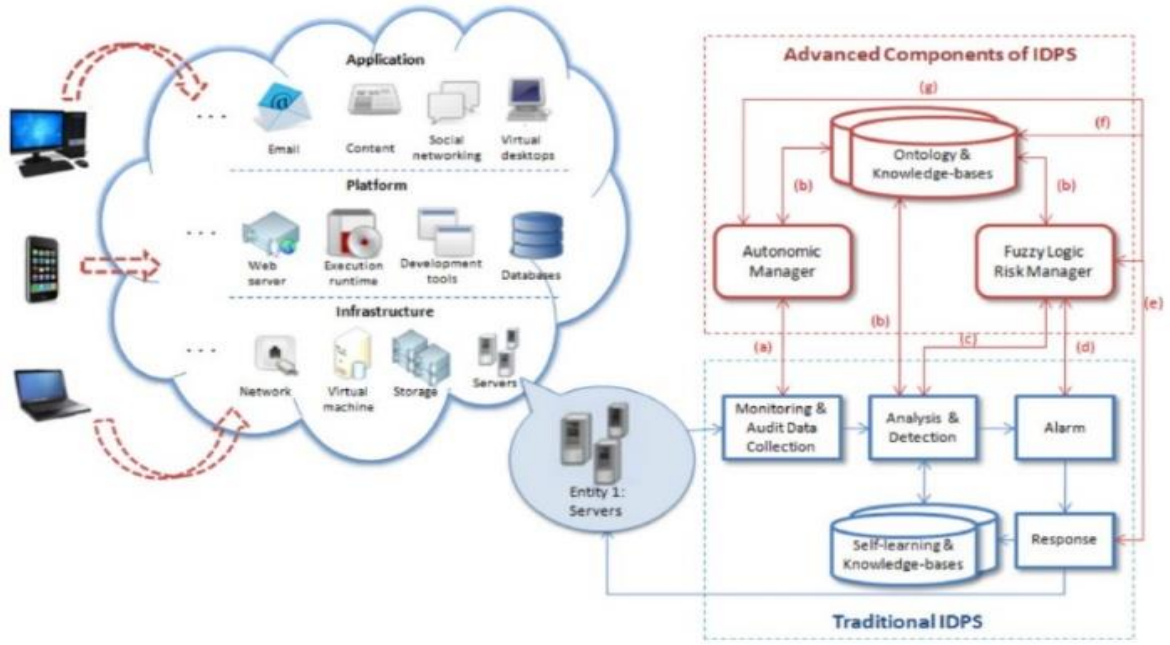
۱- مقدمه

رایانش ابری مدلی است برای فراهم کردن دسترسی آسان بر اساس تقاضای کاربر از طریق شبکه به مجموعه‌ای از منابع رایانشی قابل تغییر و پیکربندی مانند شبکه‌ها، سرورها، فضای ذخیره سازی، برنامه‌های کاربردی و سرویس‌ها که این دسترسی بتواند با کمترین نیاز به مدیریت منابع و یا نیاز به دخالت مستقیم فراهم کننده سرویس به سرعت فراهم شده یا آزاد گردد. معماری ابر، یک معماری توزیع شده و باز است که به عنوان هدف مناسب برای ورودهای ناخواسته در نظر گرفته می‌شود. بنابراین امنیت محیط ابری هنگامی که حمله‌های شبکه‌ای و حمله‌های خاص ابر، کاربران ابر را تهدید می‌کنند در خطر است. سیستمهای امنیتی شبکه‌ای سنتی مانند دیوار آتش بهترین روشهای متوقف کردن حملات بیرونی هستند اما حمله‌های درونی و حمله‌های پیچیده‌ی بیرونی نمی‌توانند به راحتی با این مکانیزم‌ها برطرف شوند و نیاز به سیستمهای شناسایی قدرتمندتری است. هدف سیستم‌های تشخیص نفوذ جلوگیری از نفوذ نیست بلکه تشخیص آن است و البته ضعف‌های کلی را نیز به مدیر سیستم اطلاع می‌دهد. در واقع سیستم های تشخیص نفوذ نخستین خط دفاعی در مقابل نفوذهای احتمالی می‌باشند. به عنوان نمونه‌ای از حملات مورد استفاده در سیستمهای تشخیص نفوذ در رایانش ابری می‌توان به حملات پهنای باند، حملاتی که اپلیکیشن‌های ویژه‌ای را مورد هدف قرار می‌دهند و حملات مربوط به لایه اتصال اشاره کرد [1].

۲- طبقه بندی سیستم های تشخیص و پیشگیری از نفوذ

حملاتی که منشا خارجی دارند حملات خارجی نامیده می شوند. حملات داخلی شامل تلاش کاربران داخلی غیر مجاز برای به دست آوردن و سوء استفاده از ورود غیر مجاز است. تشخیص نفوذ فرآیند نظارت بر کامپیوترها یا شبکه‌ها برای ورود غیر مجاز یا تغییر فایل است [2]. بیشتر حملات در گروهی متمایز به نام حوادث رخ می دهند. اگر چه بسیاری از رویدادها ماهیت مخرب دارند برخی نیز مخرب نیستند به عنوان مثال ممکن است شخصی آدرس رایانه را اشتباه تایپ کند و به طور تصادفی سعی کند بدون مجوز به سیستم دیگری متصل شود. یک IDS[1] نرم افزاری است که فرایند تشخیص نفوذ را خودکار می‌کند و نفوذ احتمالی را تشخیص می دهد. IDPS یک سامانه نرم‌افزاری یا سخت‌افزاری است که تمامی قابلیت‌های یک سیستم تشخیص نفوذ را دارد و همچنین می‌تواند برای جلوگیری از حوادث احتمالی تلاش کند. IPS[2] با یک مشخصه از IDS متمایز می‌شود. IPS می‌تواند به یک تهدید شناسایی شده با تلاش برای جلوگیری از موفقیت آن پاسخ دهد [3] و محتوای حمله یا محیط امنیتی را تغییر می‌دهد. می‌تواند پیکربندی سایر کنترل‌های امنیتی را تغییر دهد تا یک حمله را مختل کند، مانند پیکربندی مجدد یک دستگاه شبکه برای مسدود کردن دسترسی مهاجم یا قربانی، یا تغییر فایروال مبتنی بر میزبان روی یک هدف برای جلوگیری از حملات دریافتی. برخی از IPSها می‌توانند بخش‌های مخرب یک حمله را حذف یا جایگزین کنند تا آن را خوش‌خیم کنند. به دلیل نرخ بالای هشدار نادرست تشخیص ناهنجاری، IPS به اشتباه یک فعالیت عادی غیرمزاحم قانونی را به عنوان مخرب شناسایی می‌کند و به آن فعالیت شناسایی شده به طور نادرست پاسخ می‌دهد.

کادر آبی در شکل ۱، یک IDPS سنتی را نشان می‌دهد که با جمع‌آوری داده‌های حسابرسی، تجزیه و تحلیل داده‌ها و تشخیص نفوذ، ایجاد زنگ هشدار و انجام پاسخ مناسب در یک ابر کار می-کند. این فرآیند فقط برای یکی از موجودیت‌ها نشان داده می‌شود، در حالی که برای محافظت از منابع ابری در برابر فعالیت‌های مخرب، باید برای همه موجودیت‌ها به طور مداوم انجام شود.



شکل (۱): یک نمونه از IDPS برای یکی از موجودیت‌های درون محاسبات ابری

I.Functional layer

شکل ۲ نشان می‌دهد که IDPS چهار عملکرد اساسی امنیتی را انجام می‌دهد: آنها نظارت، شناسایی، تجزیه و تحلیل و پاسخ به فعالیتهای غیرمجاز را درFunctional layer (لایه عملکردی) نشان می‌دهند. IDPS با تجزیه و تحلیل داده های جمع آوری شده نفوذ را تشخیص می‌دهد. محیط نظارت شده می‌تواند مبتنی بر شبکه، میزبان یا مبتنی بر برنامه باشد.

I-۱- مبتنی بر شبکه

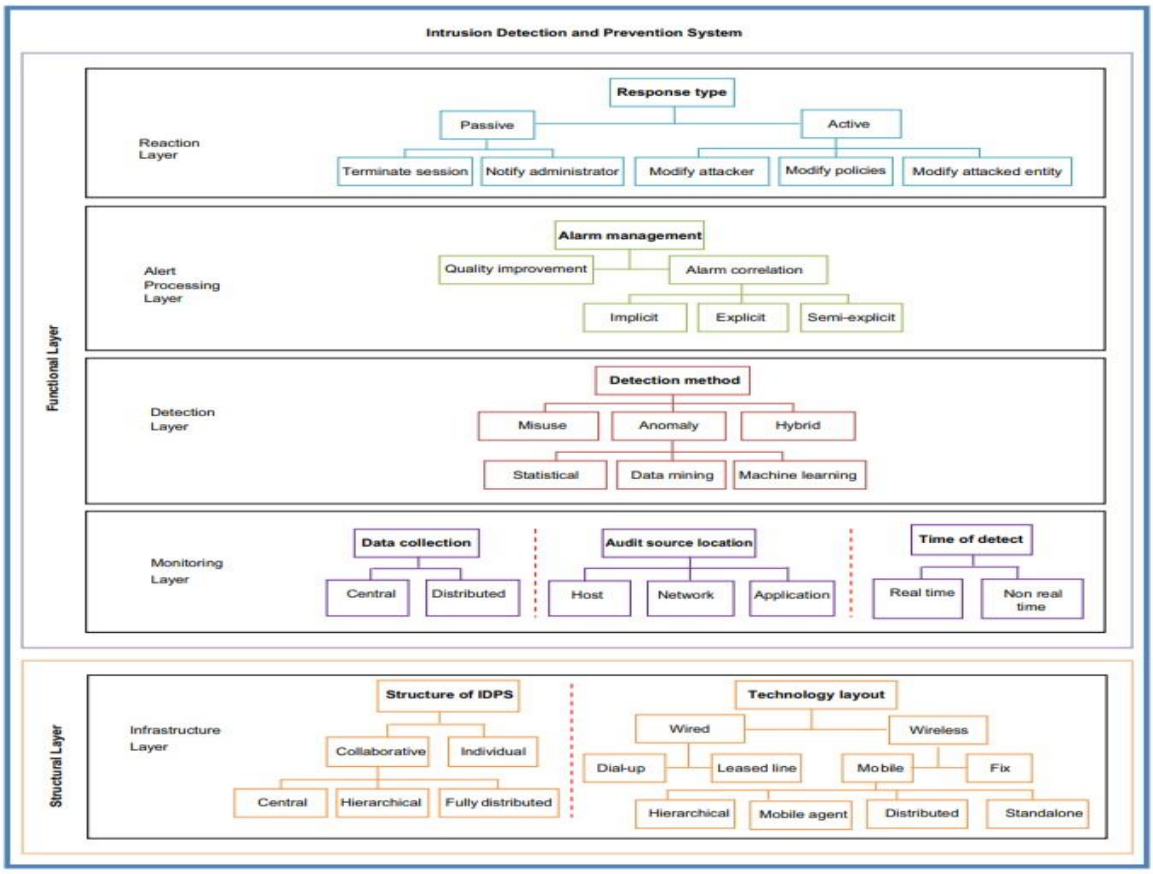
سامانه NIDS[۳] ترافیک شبکه را برای بخشهای خاص شبکه یا دستگاه‌ها نظارت می‌کند و شبکه و فعالیت پروتکل اپلیکیشن را برای شناسایی فعالیت های مشکوک تجزیه و تحلیل می‌کند.

I-۲- مبتنی بر میزبان

تمام یا بخش هایی از رفتار پویا و وضعیت یک سیستم کامپیوتری را نظارت می‌کند. یک NIDPS به صورت پویا بسته های شبکه را بازرسی می‌کند، اما یک HIDPS[۴] ممکن است تشخیص دهد که کدام برنامه به چه منابعی دسترسی دارد. همچنین یک رویکرد مکمل وجود دارد که هر دو مؤلفه مبتنی بر شبکه و مبتنی بر میزبان را ترکیب می‌کند که انعطاف پذیری بیشتری را در استقرار فراهم می‌کند.

I-۳- مبتنی بر برنامه کاربردی

بر روی رویدادهایی تمرکز می‌کند که در برخی از برنامه های کاربردی خاص از طریق تجزیه و تحلیل Log fileهای برنامه یا اندازه‌گیری عملکرد آنها رخ می‌دهد. ورودی آن منابع، داده برنامه-های در حال اجرا است. در تشخیص بلادرنگ، حملات زمانی شناسایی می‌شوند که سیستم یا شبکه برای نفوذ نظارت می‌شود و می‌تواند هر گونه انحراف را فوراً علامت‌گذاری کرده و پیشگیری مناسب را انجام دهد. IDPS بلادرنگ همچنین می‌تواند برای تجزیه و تحلیل offline از میان داده‌های رخداده از شناسایی نفوذهای گذشته اجرا شود. در مقابل، یک IDPS غیر بلادرنگ داده های حسابرسی را با تاخیر پردازش می‌کند. داده‌های حسابرسی را می توان به صورت مدل توزیع شده از چندین مکان مختلف یا منابع جمع‌آوری کرد، یا می‌توان آنها را در یک رویکرد متمرکز از یک منبع جمع‌آوری کرد. روش های شناسایی شده در سه کلاس استفاده نادرست، ناهنجاری و مدل ترکیبی با ترکیب دو کلاس اول طبقه بندی می‌شوند.



شکل (۲): یک لایه طبقه بندی از IDPS

II.تشخیص سوء استفاده

این روش از الگوهای شناخته شده رفتار غیرمجاز استفاده می‌کند. امضاها را برای پیش‌بینی و شناسایی تلاشهای مشابه بعدی فراخوانی می‌کند.

۳- تشخیص ناهنجاری

- برای آشکارکردن الگوهای رفتاری غیر عادی طراحی شده است. IDPS یک خط پایه از الگوهای استفاده عادی ایجاد می‌کند و هر چیزی که از این امر منحرف شود به عنوان نفوذهای احتمالی علامت گذاری می‌شود [4]. آنچه به عنوان یک ناهنجاری در نظر گرفته می‌شود می‌تواند متفاوت باشد. دسته بندی‌های مختلفی از ناهنجاری وجود دارد که سه مورد پرکاربرد آن به شرح زیر است [5] [6] :

- آماری: در این رویکرد، سیستم فعالیت کاربران مانند استفاده از CPU یا شماره اتصالات TCP را از نظر توزیع آماری و ایجاد پروفایل‌هایی که بیانگر رفتارهای آنها باشد مشاهده می‌کند. بنابراین، آنها دو پروفایل می‌سازند، یکی در مرحله تمرین ساخته می‌شود و دیگری پروفایل جاری در حین تشخیص است. اگر بین این دو پروفایل تفاوت وجود داشته باشد، ناهنجاری تشخیص داده می شود.
- یادگیری مبتنی بر ماشین: این تکنیک توانایی یادگیری و بهبود عملکرد خود را در طول زمان دارد. تمرکز بر ساختن سیستمی است که بتواند کارایی آن را در یک چرخه حلقه بهینه کند و بتواند استراتژی اجرای خود را با توجه به اطلاعات بازخورد تغییر دهد. سیستم فراخوانی مبتنی بر تجزیه و تحلیل توالی، شبکه بیزی و مدل مارکوف متداول ترین تکنیک‌های استفاده شده است.
- مبتنی بر داده کاوی: تکنیک های داده کاوی می‌توانند به بهبود فرآیند تشخیص نفوذ به وسیله آشکارسازی

الگوها، مشارکت‌ها، ناهنجاری ها، تغییرات و رویدادها و ساختارهای مهم در داده ها کمک کنند. طبقه بندی، خوشه بندی و تشخیص داده های پرت و کشف قوانین ارتباطی تکنیک های داده کاوی هستند که درIDPS استفاده می شوند.

III.رویکرد ترکیبی

این رویکرد برای افزایش قابلیت‌های IDPS فعلی با ترکیب دو روش سوء استفاده و ناهنجاری پیشنهاد شده است. ایده اصلی این است که سوء استفاده حملات شناخته شده را شناسایی می‌کند در حالی که ناهنجاری حملات ناشناخته را شناسایی می‌کند.

IV.لایه ساختاری

فناوری IDPS در لایه زیرساخت قرار دارد. طرح فناوری به ندرت توسط محققان مورد بحث قرار می‌گیرد، اما با توجه به اهمیت آن برای استقرار در یک محیط ابری، آن را مورد بررسی قرار می‌دهیم. دو نوع اتصال سیمی وجود دارد: شماره گیری از طریق شبکه تلفن عمومی سوئیچ شده و اتصال مستقیم از طریق خط اختصاصی یا اجاره‌ای که با شبکه نقطه به نقطه آنالوگ سازگار است. در شبکه های سیمی، ویژگی هایی مانند رفتار ترافیکی و توپولوژی شبکه را می‌توان در تشخیص نفوذ به کار برد [7]. شبکه سیار ad-hoc مجموعه ای از گره های سیار است که به طور خودکار بدون کمک مدیریت مرکزی زیرساخت پیکربندی می‌شوند. شبکه بی‌سیم IDPS انواع مختلفی دارد از جمله:

- Stand-alone : IDPS نفوذ را با اجرای مستقل بر روی هر نود شناسایی می‌کند.
- توزیع شده: هر نود در تشخیص نفوذ مشارکت می‌کند و از طریق یک عامل IDPS مرکزی پاسخ می‌دهد.
- به صورت سلسله مراتبی: آنها در شبکه‌های چند لایه مستقر می‌شوند و به خوشه‌هایی که یک سرخوشه مسئول است برای این نودهای محلی تقسیم شده اند.
- عوامل سیار: آنها قادر به حرکت از طریق یک شبکه بزرگ هستند اما با یک وظیفه خاص. عوامل مختلف عملکرد متفاوت دارند.

ساختار یک IDPS برپایه دو مدل است: فردی یا مشارکتی. یک چیدمان فردی IDPS با ادغام فیزیکی آن در یک فایروال به دست می‌آید. یک IDPS مشترک شامل چندین IDPS در یک شبکه بزرگ است که با یکدیگر ارتباط برقرار می‌کنند. هر IDPS دارای دو جزء است: عنصر تشخیص و کنترل کننده همبستگی. عناصر تشخیص شامل چندین مؤلفه شناسایی هستند که شبکه فرعی یا میزبان خود را به صورت جداگانه نظارت می‌کند و هشدارهای سطح پایین تولید می‌کند. سپس کنترل کننده همبستگی هشدارهای سطح پایین را به گزارش سطح بالایی از یک حمله تبدیل می‌کند. همانطور که شکل ۳ نشان می‌دهد IDPS مشترک را می‌توان به سه دسته به شرح زیر تقسیم کرد: [8]

- مرکزی

هر IDPS به عنوان یک عنصر تشخیص عمل می‌کند که در آن هشدارها را به صورت محلی تولید می‌کند. هشدارهای تولید شده به سرور مرکزی ارسال می‌شود که نقش یک کنترل کننده همبستگی را برای تجزیه و تحلیل آنها ایفا می‌کند. از طریق یک کنترل مدیریت متمرکز می توان یک تصمیم تشخیص دقیق بر اساس تمام اطلاعات هشدارهای موجود اتخاذ کرد. اشکال اصلی این رویکرد این است که واحد مرکزی به شدت آسیب پذیر است، هرگونه خرابی در سرور مرکزی منجر به غیرفعال کردن کل فعالیتهای همبستگی می‌شود. علاوه بر این، واحد مرکزی باید حجم بالای داده‌ای را که از عناصر تشخیص محلی دریافت و در مدت زمان معینی مدیریت کند.

- سلسله مراتبی

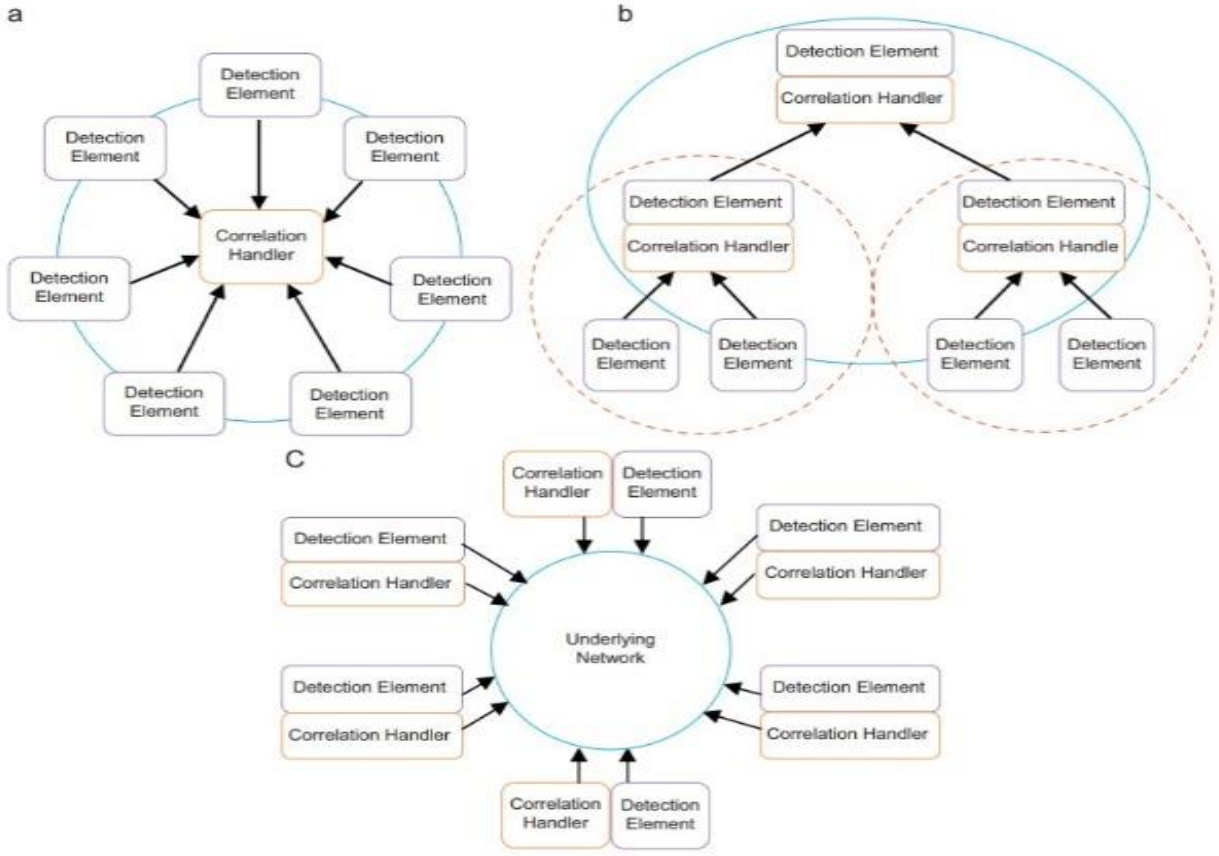
کل سیستم بر اساس ویژگی‌های مشابه تقسیم می‌شود به چندین گروه کوچک یا خصیصه‌های مشابه مانند جغرافیا، کنترل مدیریت و پلتفرم های نرم افزاری مشابه. IDPS در پایین‌ترین سطح به عنوان عناصر تشخیص کار می‌کند، در حالی که IDPS در سطح بالاتر با هر دو عنصر تشخیص و کنترلر همبستگی فراهم می‌شود و هشدارها را هم از سطح خود و هم از سطح پایین‌تر به هم مرتبط می‌کند. هشدارهای مرتبط برای تجزیه و تحلیل بیشتر به سطح بالاتری منتقل می‌شوند. این رویکرد نسبت به رویکرد متمرکز مقیاس پذیرتر است، اما همچنان از آسیب پذیری یک واحد مرکزی دستخوش تغییر می‌شود. علاوه بر این، نودهای سطح

بالاتر سطح بالاتری از ورودی دارند که پوشش تشخیص آنها را محدود می‌کند.

- کاملاً توزیع شده

هیچ هماهنگ کننده متمرکزی برای پردازش اطلاعات وجود ندارد، این سیستم‌های کاملاً مستقل را با کنترل مدیریت توزیع شده به خطر می‌اندازد. همه IDPS های شرکت کننده دو جزء عملکرد اصلی خود را دارند که با یکدیگر ارتباط برقرار می‌کنند [9]. مزایای IDPS کاملاً توزیع شده عبارتند از: موجودیت‌های شبکه نباید اطلاعات کاملی از توپولوژی شبکه داشته باشند. میتوان طراحی مقیاس پذیرتری داشت. هیچ عنصر مرکزی مسئول انجام همه کارهای همبستگی نیست و آلارم محلی همبستگی در این ساختار ساده تر است. در عین حال، رویکرد کاملاً توزیع شده مشکلات خاص خود را دارد [10] ازجمله:

اطلاعات همه هشدارها در طول تصمیم گیری تشخیص در دسترس نیست، بنابراین دقت ممکن است کاهش دهد. اطلاعات هشدار معمولا دارای یک ویژگی واحد مانند آدرس IP است که برای شناسایی حملات در مقیاس بزرگ مشکل ساز است.



شکل (۳): ساختارهای مختلف مدیریتIDPS مشترک – (a) مرکزی، (b) سلسله مراتبی و (c) کاملا توزیع شده

جدول ۱ فهرستی جامع از تکنیک های IDPSهای پیشنهادی را بر اساس طبقه بندی لایه‌های تعریف شده در بخش قبل ارائه می-دهد. آنچه از شکل مشهود است این است که تحقیقات اخیر بیشتر بر روی سیستم های مشارکتی متمرکز شده است تا راه حل هایی برای محیط بلادرنگ توزیع شده با استفاده از تکنیکهای تشخیص ترکیبی و فناوری های بی سیم ارائه دهد. با این حال، بسیاری از محققین راه حلی برای یک مشکل خاص ارائه کرده اند و سعی نکرده اند کل سیستم را از نظر مولفه های طبقه بندی پیشنهادی بهینه کنند. به عنوان مثال، تکنیک تشخیص با دقت بالا یکی از مهمترین مطلوب‌ترین حوزه‌های تحقیقاتی است بدون توجه به سایر چالشهای بعدی مانند نرخ هشدارکاذب و زمان یا نوع پاسخ. علاوه بر نادیده گرفتن کل سیستم مورد نیاز، IDPS پیشنهادی از

چندین مشکل رنج می‌برد. چالش های در حال تکاملی که توسعه IDPS را محدود می‌کند (به ویژه برای سیستم های مبتنی بر ناهنجاری) به شرح زیر است:

- IDPS سنتی به اندازه کافی برای پارادایم های کاری شبکه جدید مانند شبکه های تلفن همراه و بی سیم اعمال نشده است. آنها همچنین نتوانستند برای برآوردن الزامات شبکه های پرسرعت مقیاس شوند [11].
- پروفایل های ترافیک به طور منظم تغییر می‌کنند به دلیل برخی عوامل منفی (مانند نویز) در داده های ممیزی که ساختن پروفایل ترافیک عادی در حجم زیادی از ترافیک شبکه را دشوار می‌کنند.
- یکی از جدی ترین عوامل محدودیتی که استفاده گسترده از IDPS را مسدود می‌کند، نرخ هشدار نادرست تولید شده به شدت بالاست [12].
- با وجود پیشنهادات متعدد، تکنیک ها، مدل ها و سیستم های پیاده سازی شده (حتی تجاری) ، هیچ استاندارد یا معیار یکسانی در سطح جهانی برای ارزیابی IDPS وجود ندارد. اگرچه مشخصه عملکرد گیرنده (ROC) به طور گسترده‌ای برای ارزیابی دقت مورد استفاده قرار گرفته است، اما به دلیل نتایج ارزیابی اغلب ناقص و گمراه کننده آنها از ابزارهای ارزیابی مطلوب دور هستند [13].
- تشخیص حملات داخلی بسیار دشوار است، در عین حال تهدیدات داخلی در حال افزایش است. پیکربندی صحیح سیستم و ارائه سیاستها و مجموعه قوانین مناسب برای مزاحمان داخلی از وظایف بسیار چالش برانگیز است [14]. با این حال، در میان راه‌حل‌ها و تکنیک های مختلف، کاربردی ترین و قابل توجه ترین آنها مورد بحث قرا گرفته است.
- در میان تمام ویژگی ها، تکنیک های تشخیص در مرکز جذابیت قرار دارند. از طریق بررسی‌های موجود فهرستی از معیارها برای مقایسه تکنیک‌های تشخیص که بر اساس امضا، ناهنجاری یا ترکیبی از این‌ها است جمع‌آوری شد [15] [16].

۴- چالش‌های توسعه IDPS در محیط ابر

شناسایی چالشهایی که از پدیده‌های رایانش ابری نشات می-گیرند قبل از توسعه IDPS بسیار مهم است. چالشهای خاصی که توسعه‌دهندگان در طول توسعه IDPS برای محیطهای رایانش ابری با آن مواجه می‌شوند عبارتند از:

a. در IDPS سنتی به دلیل ماهیت ایستا سیستم نظارت شده، سیاستها تمایل به ایستایی دارند زیرا گروه‌های گره نیازمندیهای پایداری دارند که
در طول زمان شناسایی شده‌اند. برخلاف حالت سنتی، ماشینهای مجازی نظارت شده به صورت پویا اضافه و حذف می‌شوند، علاوه بر این، الزامات امنیتی هر ماشین مجازی متفاوت است.

b. سیاستهای امنیتی معمولا توسط یک مدیر سیستم که مسئولیت امنیت کل سیستم را بر عهده دارد ایجاد و مدیریت می‌شود.

c. ابر دارای چندین مدیر امنیتی سیستم است که تاثیرات منفی بر زمان پاسخ به نفوذ دارد.

d. درگیر شدن با فعالیتهای مخرب یک خودی به راحتی با پیوستن یک مهاجم به یک ارائه دهنده خدمات ابری قابل دسترسی است.

e. بیشتر پیشنهادات موجود برای حل این مشکل عمدتا در مورد نظارت بر فعالیتهای کارکنان و تدوین خط مشی ارائه دهنده ابر است.

f. زیرساخت مشترک و فناوری مجازی سازی آسیب پذیری بیشتری را در محاسبات ابری ایجاد می‌کند. هرگونه نقص در فوق‌ناظر که اجازه ایجاد ماشینهای مجازی و اجرای چندین سیستم عامل را می‌دهد، دسترسی و کنترل نامناسب را به پلتفرم نشان می‌دهد.

g. یک مسئله بسیار مهم در رایانش ابری هزینه انتقال داده است. بنابراین تحقیقات جدید باید تلاش کنند تا با کاهش پهنای باند شبکه، داده‌ها را مقرون به صرفه برای IDPS در محیط ابری ارائه دهند.

h. از آنجاییکه سوئیچ نیز مجازی شده است، مسائل اضافی مربوط به دید به ترافیک بین ماشین مجازی در یک پلتفرم میزبان مجازی است. بنابراین راه حلهای سنتی برای نظارت فیزیکی قادر به بازرسی این ترافیک شبکه نیستند.

i. علاوه بر این، خود پلتفرم‌های مجازی سازی جدید دارای آسیب پذیری‌هایی هستند که ممکن است منجر به سازش بزرگ شود، بنابراین باید از نظر وصله های خطای پیکربندی و غیره نظارت و ارزیابی شوند.

j. معمولا هر شرکتی رویه های امنیتی را برای ارائه نمایه ریسک حفظ می‌کند، اما ارائه دهندگان خدمات ابری مایل به ارائه گزارش امنیتی نیستند.

k. عدم شفافیت در شیوه‌های مدیریت امنیت مانند: حسابرسی سیاستهای امنیتی، ثبت آسیب پذیری و پاسخ به حادثه منجر به ناکارآمدی تکنیکهای سنتی مدیریت ریسک در غیاب آگاهی مشتری می‌شود.

l. علاوه بر این، ردیابی داده ها در پلتفرمهای مختلف دید و سیاستهای دسترسی ارائه دهندگان خدمات مختلف و همچنین لایه‌های انتزاعی نرم افزاری و سخت افزاری مختلف در یک ارائه دهنده یک کار چالش برانگیز است.

۵- نتیجه‌گیری

برخی شبکه‌های مبتنی بر رایانش ابری به علت فقدان زیرساخت ثابت و مدیریت متمرکز با چالشهای امنیتی مختلفی روبرو هستند. دامنه سیستمهای IDS که میتواند شامل یک تا چندین سیستم باشد، معمولا به دو دسته تشخیص مبتنی بر شبکه (NIDS) و تشخیص مبتنی بر میزبان (HIDS) تقسیم می‌شود. در مورد اول، سیستم ترافیک ورودی شبکه را تحلیل میکند و موارد شناسایی شده را با دیتابیسی از تهدیدات شناخته شده مقایسه کرده و در صورت تایید به مدیر اصلی هشدار و گزارش میدهد اما در مورد دوم، سیستم، فایلهای مهم سیستم عامل را بر روی دستگاهها و میزبان‌های شخصی اجرا کرده و حین رصد بسته‌ها و شناسایی موارد مشکوک به کاربر یا مدیر هشدار می دهد. زمانی که سیستمهای تشخیص نفوذ از طریق شبکه برخی از اعمال مخرب را اسکن می کنند، برای خواندن نتایج اسکن و رفع تهدیدات، نیازمند نیروهای انسانی نیز هستیم اما سیستمهای پیشگیری از نفوذ به طور خودکار با اسکن ترافیک شبکه از

تمامی تهدیدات شناخته شده قبل از اینکه خسارتی ایجاد کنند، جلوگیری می کنند. در صورت استفاده از این دو سیستم، علاوه بر افزایش امنیت اطلاعات سازمان، متخصصان امنیت نیز مجبور به نظارت ۲۴ ساعته بر روی ترافیک شبکه نیستند. بنابراین توصیه میشود که این دو سیستم را همواره برای انواع حملات به روز نگه دارید.

مراجع

[1] J. Joaquim, k. bakhtiyari and m. J. o. N. a. C. A. a. taghavi, "Journal of Network and Computer Application authors Mona Taghavi, Kaveh Bakhtiyari ,Joaquim Junior".

[2] M. H. J., “"Principles of information و .W. M. E security," ed: Course Technology Ptr, 2011, p. ”315.

[3] P. Mell, “K. Scarfone and P. Mell, و K. Scarfone "Guide to intrusion detection and prevention systems (idps)," NIST Special Publication, vol. ”.800, p. 94, 2007

[4] J. Heidemann, “G. Thatte, و G. Thatte, U. Mitra U. Mitra, and J. Heidemann, "Parametric methods for anomaly detection in aggregate traffic,"IEEE/ACM Transactions on Networking (TON), vol. 19, pp. 512-525, ”.2011

[5] P. Bertok,, “"A program- و X. D. Hoang, J. Hu based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference," Journal of Network and Computer Applications, ”.–vol. 32, pp. 1219

[6] I. M. Osman, “"Alert و H. T. Elshoush correlation in collaborative intelligent intrusion detection systems A survey," Applied Soft ”.Computing, vol. 11, pp. 4349-4365, 2011

[7] E. و J. M. Estevez-Tapiador, P. Garcia-Teodoro Diaz-Verdejo, “"Anomaly detection methods in wired networks: a survey and taxonomy," Computer Communications, vol. 27, pp. 1569- ”1584, 2004

[8] I. M. Osman, “"Alert و H. T. Elshoush correlation in collaborative intelligent intrusion detection systems A survey," Applied Soft ”.Computing, vol. 11, pp. 4349-4365, 2011

[9] C. Fahy, و M. Zach ,P. Leitner ,M. Leitner “"Fault management based on peer-to-peer paradigms; a case study report from the celtic project madeira," in 10th IFIP/IEEE ”International Symposium

[10] S. Karunasekera, “"A و C. Leckie ,C. V. Zhou survey of coordinated attacks and collaborative amp; & intrusion detection," Computers ”.Security, vol. 29, pp. 124-140, 2010

[11] J.-M. Park, “"An overview of و A. Patcha anomaly detection techniques: Existing solutions and latest technological trends," Computer Networks, vol. 51, pp. 3448-3470, ”2007

[12] F. Roli, “"Alarm و R. Perdisci, G. Giacinto clustering for intrusion detection systems in computer networks," Engineering Applications of Artificial Intelligence, vol. 19, pp. 429-438, ”2006

[13] J. W. Ulvila, “"Evaluation of و J. E. Gaffney Jr intrusion detectors: A decision theory approach," in IEEE Symposium on Security and P 2001, Oakland, CA , USA. &Privacy, 2001. S ”.pp.50-61, 2001, pp. 50-61

[14] R. F. Trzeciak, و A. P. Moore, D. M. Cappelli “"The “Big Picture” of Insider IT Sabotage Across U.S Critical Infrastructures," in Insider Attack and Cyber Security. vol. 39, S. J. Stolfo, ”.S. M. Bellovin, A. D

[15] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-E. Vázquez, “"Anomaly-based و Fernández network intrusion detection: Techniques, amp; & systems and challenges," Computers ”,Security, vol. 28, pp. 18-28

[16] S. Parvin, “"Anomaly و M. Xie, B. Tian detection in wireless sensor networks: A survey," Journal of Network and Computer ”.Applications, vol. 34, pp. 1302-1325, 2011

[17] A. Alwabel, "Mobile و S. Khanum, M. Usman Agent Based Hierarchical Intrusion Detection System in Wireless Sensor Networks," International Journal of Computer Science Issues, IJCSI, vol. 9, 2012.

[18] O. Chung-Ming, "O. Chung-Ming, "Host-based intrusion detection systems adapted from agent-based artificial immune systems," Neurocomputing, 2012.

[19] S. Jain, "Database Intrusion و A. Jaiswal Prevention Cum Detection System with Appropriate Response," International Journal of Information Technology, vol. 2, pp. 651-656, ۲۰۱۰.

[20] C. Westphall, و A. Schulter ,K. Vieira "Intrusion Detection for Grid and Cloud Computing," IT Professional, vol. 12, pp. 38-43, 2010.

[21] J. Xu, "A New Distributed و Y. Li, C. Jing Intrusion Detection Method Based on Immune Mobile Agent Life System Modeling and Intelligent Computing." vol. 6328, K. Li, M. Fei, L. Jia, and G. Irwin, Eds., ed: Springer Berlin / Heidelberg, 2010, pp. 233-243.

[22] V. J. و O. Awodele, S. Idowu, O. Anjorin Joshua, "A Multi-Layered Approach to the Design of Intelligent Intrusion Detection and Prevention System (IIDPS)," Issues in Informing Science and Information Technology, vol. 6, 2009.

[23] V. Sainani, "A Multiagent-based و M.-L. Shyu Intrusion Detection System with the Support of Multi-Class Supervised Classification," in Data Mining and Multi-agent Integration, L. Cao, Ed., ed: Springer US, 2009, pp. 127-142.

[24] M. Kahani, و A. Ghaemi Bafghi ,A. Rasoulifard "Incremental Hybrid Intrusion Detection Using Ensemble of Weak Classifiers," in Advances in Computer Science and Engineering. vol. 6, H. Sarbazi-Azad, B. Parhami, S.-G. Miremadi, and S. Hessabi, Eds., ed: Springer Berlin Heidelberg, 2009, pp. 577-584.

[25] C.-Y. Lin, "A real-time و G.-J. Yu ,M.-Y. Su network intrusion detection system for large-scale attacks based on an incremental mining amp; Security, vol. 28, & approach," Computers pp. 301-309, 2009.

[26] E. Corchado, "Mining Network و Á. Herrero Traffic Data for Attacks through MOVICAB-IDS Foundations of Computational Intelligence Volume 4." vol. 204, A. Abraham, A.-E. Hassanien, and A. de Carvalho, Eds., ed: Springer Berlin / Heidelberg, 2009, pp. 377-394.

[27] M. Carvalho, "Agent-Based و A. Byrski Immunological Intrusion Detection System for Mobile Ad-Hoc Networks Computational Science – ICCS 2008." vol. 5103, M. Bubak, G. van Albada, J. Dongarra, and P. Sloot, Eds., ed: Springer Berlin / Heidelberg, 2008, pp. 584-593.

[1] Intrusion Detection System
[2] Intrusion Prevention System
[3] Network IDS
[4] Host IDPS