دوره چهاردهم، شماره دوم، پاییز و زمستان ۱۴۰۰

مجله فناوری اطلاعات در طراحی مهندسی

Information Technology in Engineering Design

http://ited.sinaweb.net

مروری بر سیستم‌های تشخیص نفوذ از دیدگاه ساختار و روش‌های بهبود کارایی در آن‌ها

شهرزاد رحیمی[۱] مسعود نیازی ترشیز[۲*] سید عابد حسینی[۳]

[۱]گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران.

[۲]گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران*.

[۳]گروه مهندسی برق، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران.

(تاریخ دریافت: ۱۴۰۱/۰۵/۱۳ تاریخ پذیرش: ۱۴۰۱/۰۶/۲۳)

چکیده

سیستم‌های تشخیص نفوذ به منظور کاهش ضعف امنیتی نرم‌افزارها، لزوم حفظ امنیت اطلاعات و افزایش کارایی در شبکه‌های کامپیوتری توسعه یافته‌اند. در حوزه شبکه امنیت، کنترل دسترسی و تشخیص به موقع حملات شبکه از مباحث مهم پژوهشی هستند. عملاً هیچ سیستمی امنیت کامل ندارد به همین دلیل پژوهشگران مختلف به دنبال روش‌های کشف و طراحی انواع سیستم‌های خبره تشخیص نفوذ بر اساس روش‌های آماری، داده‌کاوی و شبکه‌های عصبی می‌باشند. یکی از مهم‌ترین اجزای ساختار امنیتی شبکه‌های رایانه‌ای، سیستم کشف نفوذ می‌باشد که در مباحث امنیت شبکه‌های رایانه‌ای جایگاه ویژه‌ای دارد. ایده اصلی یک سیستم تشخیص نفوذ، تشخیص ترافیک بد یعنی ترافیکی که باعث آسیب و از بین رفتن امنیت در رایانه و یا شبکه‌های رایانه‌ای می‌باشد، است. هدف این مقاله نیز بررسی و مرور کلی سیستم‌های تشخیص نفوذ است.

کلمات کلیدی: سیستم‌های تشخیص نفوذ، حملات، الگوریتم‌های هوشمند، تست نفوذ.

*عهده دار مکاتبات :

مسعود نیازی ترشیز

نشانی: گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران

پست الکترونیک : nizai@mshdiau.ac.ir

شماره تماس : ۰۹۱۵۳۱۵۶۷۳۴

۱-مقدمه

با افزایش استفاده از اینترنت، حجم زیادی از اطلاعات بین دستگاه های ارتباطی مختلف رد و بدل می‌شود. داده‌ها باید به طور ایمن بین دستگاه‌های ارتباطی منتقل شوند و بنابراین، امنیت شبکه یکی از حوزه‌های تحقیقاتی غالب برای سناریوی شبکه فعلی است. بنابراین سیستم‌های تشخیص نفوذ به طور گسترده همراه با مکانیسم‌های امنیتی دیگر مانند فایروال و کنترل دسترسی استفاده می‌شوند. از سویی دیگر تکامل در سناریوهای حمله به گونه‌ای بوده است که یافتن سیستم‌های تشخیص نفوذ کارآمد و بهینه با به روز رسانی‌های مکرر به یک چالش بزرگ تبدیل شده است. باوجود استفاده از سیستم‌های تشخیص نفوذ (IDS [1]) به‌منظور شناسایی حملات مختلف، تعداد و پیچیدگی حملات سایبری ناشناخته افزایش یافته است. این منجر شده است که توزیع و ناهمگنی برنامه‌ها خدمات شبکه را پیچیده و چالش‌برانگیز می‌کند [۲]. حملات سایبری با پیشرفت‌های سخت‌افزاری، نرم‌افزاری و توپولوژی‌های شبکه با توجه به تحولات اخیر در شبکه‌ها به‌طور مداوم با الگوریتم‌های بسیار پیچیده در حال تکامل هستند. حملات سایبری مخرب مسائل جدی امنیتی را ایجاد می‌کند که نیاز به یک سیستم جدید شناسایی، نفوذپذیر و قابل‌اعتماد برای شناسایی IDS را می‌طلبد. روش IDS ابزاری فعال برای تشخیص نفوذ است که برای شناسایی و طبقه‌بندی به موقع حملات یا نقض سیاست‌های امنیتی به‌طور خودکار در زیرساخت‌های سطح شبکه و سطح میزبان استفاده می‌شود. بر اساس رفتارهای نفوذی، سیستم تشخیص نفوذ را می‌توان به دو دسته سیستم تشخیص نفوذ مبتنی بر شبکه (NIDS[2]) و سیستم تشخیص نفوذ مبتنی بر میزبان (HIDS[3]) طبقه‌بندی نمود و معمولاً برای دست‌یابی به حداکثر کارایی و امنیت این سیستم‌هایی تشخیص نفوذ به صورت ترکیبی نیز مورد استفاده قرار می‌گیرند که با نام سیستم‌های تشخیص نفوذ توزیع‌شده (DIDS[4]) شناخته می‌شوند یک سیستم IDS که از رفتار شبکه استفاده می‌کند، NIDS نامیده می‌شود. رفتارهای شبکه با استفاده از تجهیزات شبکه از طریق بازتاب توسط دستگاه‌های شبکه مانند سوئیچ‌ها، مسیریاب‌ها جمع‌آوری می‌شوند و به‌منظور شناسایی حملات و تهدیدهای احتمالی پنهان در ترافیک شبکه، تجزیه و تحلیل می‌شوند [۱و۳].

با توجه به اهمیت امنیت در شبکه، محققان سیستم‌های تشخیص نفوذ مختلفی ارائه نموده‌اند. سهم این مقاله به این صورت است که ابتدا انواع حملات بیان می‌شود. سپس سیستم‌های تشخیص نفوذ معرفی شده و مزایا و معایب هر کدام بیان می‌شوند. یکی دیگر از اهداف مقاله بهبودهای گوناگونی که توسط محققان مختلف در تحقیقات ارائه شده است، بحث شده است.

ساختار پژوهش به شرح زیر است در این پژوهش ابتدا در بخش ۲ به مفاهیم اولیه پژوهش و مرور کارهای گذشته پرداخته می‌شود و سپس در بخش ۳ بحث و نتیجه‌گیری پژوهش آورده شده است.

۲-مفاهیم پژوهش و مرور کارهای گذشته

۲-۱-انواع حملات

[1] Intrusion Detection System
[2] Network-based Intrusion Detection System
[3] Host-based Intrusion Detection System
[4] Distributed-based Intrusion Detection System

در محیط‌های شبکه ای چهار مؤلفه‌ی کلیدی وجود دارد که عبارت‌اند از: افراد، اشیاء هوشمند، محیط‌های زمینه‌ای و فرآیندها. یک سیستم شبکه‌ی اینترنت به‌طور طبیعی نیاز به فرآیندهای امنیتی از قبیل شناسایی، احراز هویت، حفظ محرمانگی، انکارناپذیری و قابلیت اطمینان دارد و به همین دلیل باید در مقابل حملات مختلف مقاوم باشد. شبکه‌ها با حملات مختلفی مواجه هستند که در ادامه به‌صورت فهرست‌وار به برخی از آن‌ها اشاره می‌کنیم [۴].

- حملات منع سرویس (DOS[1]): در حملات منع سرویس، سرویس‌های عادی شبکه از دسترس خارج می‌شوند و دسترسی اشیاء و کاربران به سرور و سایر منابع غیرممکن می‌شود.
- حملات دیداس[2]: به‌طورکلی هدف در این نوع حملات، تلاش برای قطع موقت یا دائمی و یا تعلیق خدمات یک میزبان متصل به اینترنت است. اهداف حمله DOS معمولاً سایت‌ها یا خدمات میزبانی وب سرور با ویژگی‌های مناسب مانند بانک‌ها، کارت‌های اعتباری و حتی سرورهای ریشه را هدف قرار می‌دهند. حمله DOS کامپیوتر هدف را وادار به ریست شدن یا مصرف منابعش می‌کند، بنابراین نمی‌تواند به سرویس‌های موردنظرش سرویس بدهد و همچنین سیاست‌های مورد قبول فراهم‌کنندگان سرویس‌های اینترنتی را نقض می‌کنند. به صورت کلی زمانی یک حمله DDOS به سایت اتفاق می‌افتد که دسترسی به یک کامپیوتر یا منبع شبکه عمداً در نتیجه کار مخرب به کاربر دیگری مسدود یا کاهش داده شود. این حملات لزوماً داده‌ها را مستقیماً یا همیشگی تخریب نمی‌کنند، اما عمداً دسترس پذیری منابع را به خطر می‌اندازند و این در حالی است که در حمله Dos بسته‌های اطلاعاتی به طور مستقیم از سیستم هکر یا مهاجم ارسال می‌شود و به طور کلی یک سیستم اطلاعاتی در این حمله نقش دارد و بالطبع یک IP مسئول انجام حمله است.
- جعل: از جمله مهم‌ترین حملات، جعل است. اهمیت این حمله از آن جهت است که خود این حمله می‌تواند زمینه‌ساز حملات دیگری نظیر حمله مسیریابی، حمله جایگزینی، حمله تکرار، حمله منع سرویس و ... شود. در این دسته از حملات مهاجم با ایجاد یک پیغام نادرست (جعلی) ممکن است به ایجاد یک حلقه[3] مسیریابی بپردازد. یک جعل کننده ابتدا به کانال گوش می‌دهد و یک سری اطلاعات را از کانال ناامن دریافت می‌کند و سپس به ارسال اطلاعات جعلی می‌پردازد. معمولاً نقاط ورود اطلاعات بیشتر مورد توجه یک جعل کننده قرار می‌گیرد. یک اسپوفر[4] ممکن است برای رسیدن به اهداف خود کاربران را گمراه کند تا آن‌ها اطلاعات خود را در یک صفحه جعلی وارد کنند و از این طریق به اطلاعات مورد نیاز خود دست یابد.
- سیبل[5]: در حمله سیبل یک گره (شئ) برای خود هویت‌های چندگانه‌ای را ایجاد می‌کند و این بدان معنا است که یک مهاجم می‌تواند در یک‌زمان دارای چندین هویت باشد. این حمله باعث کاهش یکپارچگی و امنیت داده‌ها می‌شود. در واقع مهاجم به‌وسیله‌ی حمله سیبل، یک لباس مبدل می‌پوشد و سعی می‌کند رفتار خود را عادی نشان دهد.

[1] Denial of Service
[2] Distributed Denial-Of-Service (DDOS)
[3] Loop
[4] Spoofer
[5] Sybil

- ویژگی دستگاه‌ها: این دسته از حملات بر اساس خصوصیات خاصی که تجهیزات مورد استفاده در شبکه دارند به وجود می‌آید و دارای ساختارهای متفاوت و متعددی می‌باشند. در این حملات سعی می‌شود که توان محاسباتی، پردازشی و انرژی تجهیزات را به تحلیل ببرند و یا اطلاعات ناقص و یا غلط در اختیار آن‌ها بگذارند.
- سطح دسترسی: در حمله به سطح دسترسی ممکن است هر شئ حق دسترسی به یک سری اطلاعات را نداشته باشد اما به شیوه‌ای غیرمتعارف به استراق سمع بپردازد و اطلاعات حساس را به دست آورد. این حمله می‌تواند شامل دو نوع حمله فعالانه و غیرفعال باشد.
- حمله تخاصمی: یک مهاجم می‌تواند در هرجایی که یک سیستم شبکه راه‌اندازی می‌شود وجود داشته باشد (مهاجم داخلی یا مهاجم خارجی) و بر این اساس به شناسایی موقعیت اشیاء مختلف بپردازد و از اطلاعات ارسالی آن‌ها سوءاستفاده کند. مهاجم در چنین مواردی می‌تواند به‌سادگی و با سعی و خطا و جمع‌آوری مستمر اطلاعات به موفقیت برسد و اطلاعات حساس و حیاتی را استخراج کند.
- استراتژی حملات: یک مهاجم در این دسته از حملات سعی می‌کند تا استراتژی یک سیستم شبکه را با چالش مواجه کند. معمولاً در این شیوه حملات هم از روش‌های فیزیکی استفاده می‌شود و هم از روش‌های منطقی بهره برده می‌شود.
- حمله سطح اطلاعات: تمامی تجهیزات شبکه شامل سنسورهایی هستند که به‌صورت مستمر به جمع‌آوری، تولید و بازنشر اطلاعات می‌پردازند. این سنسورها تحت نظارت پارامترهای مختلفی هستند و با توجه به باز بودن محیط شبکه، این اطلاعات می‌تواند توسط مهاجمان به‌راحتی تغییر کند.
- وقفه: هدف حملات وقفه این است که سیستم را از دسترس‌پذیری خارج کند. چنین اختلالی در سیستم شبکه ممکن است عوارض غیرقابل تصوری را داشته باشد.
- استراق سمع: مهاجم با استراق سمع کانال‌های ارتباطی، محرمانگی اطلاعات را از بین می‌برد.
- دگرگونی: دستگاه‌های اینترنت اشیا و شبکه‌های کامپیوتری برای داشتن عملکرد مناسب باید دارای اطلاعات یکپارچه باشند. یک مهاجم می‌تواند با ایجاد تغییرات مدنظر عملکرد کلی سیستم را با اخلال مواجه کند.
- جعل[1]: با ایجاد تهدیدات احراز هویتی می‌توان ساختار کلی شبکه را به خطر انداخت و زمینه حملات گسترده را فراهم کرد.
- تکرار پیام[2]: یک مهاجم می‌تواند با تکرار یک پیام و یا اصلاح و تغییر در ساختار یک پیام به ایجاد یک تهدید امنیتی بپردازد و نهایتاً حمله‌ای را به سیستم وارد کند. بسیاری از مهاجمان اطلاعات فعلی را برای سوءاستفاده احتمالی در آینده نگهداری می‌کنند.
- حمله مرد میانی: یک فرد (شئ) می‌تواند به‌راحتی در بین دو موجودیت (شئ) دیگر قرار بگیرد و اطلاعات دریافتی از طرفین را به‌گونه‌ای تغییر دهد که به اهداف مدنظر خود برسد.
- حملات مبتنی بر میزبان[3]: ما در سیستم‌های شبکه دارای میزبان‌های مختلفی هستیم. در حقیقت ما با نرم‌افزارها و سخت‌افزارهای مختلفی مواجه هستیم که خود این موضوع می‌تواند حملات مختلفی را در پی داشته باشد.

[1] Fabrication
[2] Message Replay
[3] Host-based attacks

- سازش کاربران/نرم‌افزارها/سخت‌افزارها[1]: سازش کاربران /نرم‌افزارها/ سخت‌افزارها در یک سیستم شبکه می‌تواند رخ دهد. در این حمله دو کاربر می‌توانند با یکدیگر سازش کنند و اطلاعاتی را به یکدیگر منتقل کنند. این موضوع حتی ممکن است بین نرم‌افزارها و سخت‌افزار به وقوع بپیوندند.
- حمله مبتنی بر پروتکل: انحراف در یک پروتکل نیز یکی از مسائلی است که می‌تواند منجر به یک حمله شود. یک مهاجم می‌تواند با ایجاد انحراف و اختلال در یک پروتکل امنیتی برخی از ویژگی‌های امنیتی را نقض کند [۵].

۲-۲-سیستم‌های تشخیص نفوذ

نفوذ مجموعه اقدامات غیرقانونی است که صحت، محرمانگی و یا دسترسی به یک منبع را به خطر می‌اندازد. نفوذها به دسته‌های زیر تقسیم می‌شوند:

- ورودی غیرقانونی: ورود غیرقانونی هنگامی روی می‌دهد که یک بیگانه به شناسه کاربر و کلمه رمز معتبر دسترسی پیدا می‌کند.
- حملات ایفای نقش: حملات ایفای نقش هنگامی روی می‌دهند که نفوذی سیستم را متقاعد کند که وی یک کاربر مجاز با امتیاز بالا است.
- کنترل امنیت: نفوذ گر تلاش می‌کند تا جنبه‌های امنیتی سیستم از قبیل کلمات رمز را اصلاح کند.
- نشت: اطلاعات به خارج از سیستم انتقال داده می‌شوند.
- جلوگیری از سرویس: منابع برای سایر کاربران غیرقابل‌دسترس می‌شوند.
- استفاده خرابکارانه: این دسته از نفوذها شامل حملات متفاوتی از قبیل حذف فایل‌ها، سوءاستفاده از منابع و غیره هستند.

ارزیابی نرم‌افزار بدافزار[2] یک چالش بحرانی برای طراحی سیستم‌های تشخیص نفوذ مطرح می‌کند. حمله‌های بدافزاری پیچیده‌تر شده و چالش‌های زیادی برای شناسایی بدافزار نامعلوم و مبهم ایجاد کرده است به‌طوری‌که طراحان بدافزار از روش‌های گریز مختلفی برای گرفتن اطلاعات به‌منظور جلوگیری از تشخیص توسط یک IDS استفاده می‌کنند [۶]. به‌علاوه، یک افزایش در تهدیدات امنیتی مانند حمله‌ی روز صفر طراحی‌شده برای کاربران اینترنت هدف وجود دارد؛ بنابراین، امنیت کامپیوتر برای استفاده از فنّاوری اطلاعات ضروری شده که بخشی از زندگی روزانه ما شده است. به عنوان یک نتیجه، کشورهای مختلفی مانند استرالیا و آمریکا به‌طور قابل‌توجهی به‌وسیله‌ی حمله‌ی روز صفر[3] تحت فشار قرارگرفته‌اند. بر طبق گزارش تهدید امنیت اینترنت سیمانتک[4] ۲۰۱۷، بیش از سه میلیون حمله‌ی روز صفر در ۲۰۱۶ گزارش‌شده و حجم و شدت حملات روز صفر بزرگ‌تر از قبل بوده است [۷]. همان‌طور که در آمار نقض تعمد در ۲۰۱۷ اشاره شده است، به‌طور تقریبی نه میلیون داده توسط هکران از ۲۰۱۳ به بعد دزدیده یا گم‌شده است. یک گزارش توسط سیمانتک یافته شده است که تعداد وقایع نقض تعهد امنیت بیشتر شده است. درگذشته، مجرمان سایبری به‌طور اولیه بر روی مشتریان بانکی، دزدی حساب‌های بانکی یا دزدی کارت‌های اعتباری تمرکز نموده‌اند [۷]؛ اما تولید بدافزار جدید بلند پروازانه تر شده و بر روی خود بانک‌ها هدف قرار داده‌اند. گاهی اوقات در تلاش برای گرفتن میلیون‌ها دلار در یک حمله بوده اند. برای این علت، تشخیص حملات روز صفر خیلی اهمیت دارد.

[1] User/software/hardware-compromise
[2] Malware
[3] Zero-day attack
[4] Symantec

حوادث برجسته جرائم سایبری سهولت گسترش تهدیدات سایبری در سطح بین‌المللی را نشان داده است، زیرا یک سازش ساده می‌تواند خدمات یا امکانات اساسی یک تجارت را مختل کند. یک تعداد زیاد از مجرمان سایبری در جهان برای دزدیدن اطلاعات، دریافت درآمد غیرقانونی و یافتن اهداف جدید برانگیخته شده‌اند. بدافزارها عمداً برای سازش با سیستم‌های کامپیوتری و گرفتن مزایای استفاده از هرگونه ضعف در سیستم‌های تشخیص نفوذ ایجادشده است. در ۲۰۱۷، مرکز امنیت سایبری استرالیا (ACSC[1]) به‌طور بحرانی سطوح مختلف از پیچیدگی به کار گرفته‌شده توسط مهاجمان را بررسی نمودند [۸]؛ بنابراین یک نیاز برای توسعه‌ی یک IDS مؤثر برای تشخیص بدافزار جدید وجود دارد. هدف یک IDS شناسایی انواع مختلف بدافزارها تا حد امکان است که نمی‌توانند به‌وسیله‌ی یک دیوار آتش معمولی به دست آیند. با افزایش حجم بدافزار کامپیوتری، توسعه‌ی IDS بهبودیافته به‌طور قابل‌توجهی اهمیت دارد.

یک IDS عملاً سه وظیفه‌ی پایش، تشخیص و واکنش را انجام می‌دهد و در واقع یک نوع بسته- اسنیفر[2] (Sniffer) محسوب می‌شود که ترافیک شبکه را تجزیه و تحلیل کرده و اگر بخواهد تلاشی برای نفوذ به شبکه انجام گیرد آن را شناسایی کرده و اگر پس از تشخیص، حملات را از بین ببرد، سیستم مربوطه به عنوان یک سیستم IPS[3] مطرح می‌گردد. سیستم‌هایی نظیر IDS ها در یک شبکه به کارآمدی کلیه تجهیزات، فرآیندها و کارکنانی وابسته می‌باشند که در مواقع لزوم به رخدادها پاسخ می‌دهند. با توجه به این نکته که حسگرهای IDS در هر زمان تعداد زیادی اخطار تولید می‌کنند و در شبکه امکان پاسخگویی به همه آن‌ها وجود ندارد، لازم است حساسیت IDS ها را به‌گونه‌ای تنظیم نمود که فقط تهدیدات اساسی را اعلام نمایند؛ اما این کار باعث می‌شود تعدادی از حمله‌ها تشخیص داده نشود. برای جلوگیری از بروز اشکال، می‌توان هر یک از IDS ها را برای یک کاربرد[4] خاص تخصیص داد.

به‌صورت کلی سه روش برای شناسایی و تشخیص نفوذ به شبکه وجود دارد که به شرح زیر هستند:

شناسایی امضاء: در این روش، به محض اینکه سامانه، ترافیکی را تشخیص دهد آن را با اطلاعات پایگاه داده خود مقایسه کرده و در صورت بروز تطابق اعلام هشدار می‌کند.

تشخیص رفتار غیرعادی[5]: در این روش، سامانه با رصد ترافیک شبکه و مقایسه بین رفتار عادی شبکه و رفتار غیرعادی که بر اثر عملی صورت گرفته پی به تشخیص نفوذ می‌برد.

تشخیص رفتار غیرعادی پروتکل‌ها: تحلیل ترافیک و اطمینان از عدم وجود بسته‌های غیرقانونی با مقایسه بخش پروتکل.

برای محافظت بهتر از شبکه، سامانه‌ی IDS با هدف شناسایی فعالیت بدخواهانه یا تخلف سیاستی خودکار با ارتقای به موقع در مواجه با چالش‌های جدید لازم است. سازوکارهای تشخیصی این سامانه به دو قسمت اصلی تقسیم می‌شود: تشخیص سوءاستفاده (MIDS[6]) و تشخیص بر اساس رفتارهای غیرمتعارف (AIDS[7]).

تشخیص MIDS کلیه‌ی مشخصه‌های حملات شناخته‌شده را در یک پایگاه داده ذخیره می‌کند و ترافیک شبکه را در صورت تطابق مشخصه‌هایش با آن‌ها در پایگاه داده به عنوان حمله دسته‌بندی می‌کند. این طبقه‌بندی IDS می‌تواند حملات شناخته‌شده را به‌طور

[1] Australian cyber security center
[2] Packet-Sniffer
[3] Intrusion Prevention System
[4] Application
[5] Anomaly
[6] Misuse IDS
[7] Anomaly IDS

مؤثر و دقیق شناسایی کند. با این وجود، این دسته‌بندی در تشخیص حمله ناشناخته به مشکل می‌خورد که موضوع بحرانی در شبکه‌های مدرن است که همانند حملات روز صفر به‌دفعات رخ می‌دهند. روش‌های AIDS توانایی تشخیص این‌گونه حملات را دارد که بنابراین به AIDS در سالیان اخیر توجه زیادی شده است. روش‌های AIDS تشخیص رفتار غیرمتعارف است که روش‌های یادگیری ماشینی را برای تشخیص نفوذ به شبکه اعمال می‌کند و بر اساس این روش‌ها ابتدا در مجموعه داده‌های از قبل جمع‌آوری‌شده آموزش داده می‌بیند و سپس، حمله به شبکه را از طریق مدل آموزش‌یافته تشخیص می‌دهد.

۲-۲-۱- انواع سیستم‌های تشخیص نفوذ

در حالت کلی IDSها را می‌توان به دو دسته‌ی کلی تقسیم‌بندی نمود.

- سیستم‌های تشخیص نفوذ تحت شبکه: در بسیاری از موارد عملاً یک Sniffer هستند که با بررسی بسته‌ها و پروتکل‌ها، به جستجوی تلاش‌هایی که برای حمله صورت می‌گیرد می‌پردازند و ترافیک به صورت بلادرنگ بر روی خطوط ارتباطی، مورد نظارت قرار می‌گیرد. به‌عبارت دیگر معیار NIDS ها، تنها بسته‌هایی است که بر روی شبکه‌ها رد و بدل می‌گردد. با این وجود این سیستم‌ها در مواجه با بسته‌های رمز شده و یا شبکه‌هایی با سرعت و ترافیک بالا کارایی خود را از دست می‌دهند؛ مانند نرم‌افزار اسنورت[1] (Snort) در سیستم عامل لینوکس.
- نرم افزار Snort: نرم افزاری متن باز برای تشخیص نفوذ[2] و جلوگیری از نفوذ [3] است؛ که به زبان برنامه نویسی C نوشته شده است. در سال ۱۹۹۸ توسط مارتین روچ[4] ساخته شد و در حال حاضر توسط توسعه دهندگان سورس فایر[5] (Sourc fire) که زیرمجموعه شرکت سیسکو هستند، توسعه می یابد. این نرم افزار در سال ۲۰۰۹ بهترین نرم افزار متن باز شناخته شد. Snort محصولی رایگان و دارای پایگاه داده کاربردی است که بر روی سیستم عامل هایی مانند ویندوز، لینوکس، یونیکس و مک قابل نصب و استفاده است. آپدیت قوانین (Rules) به صورت رایگان در دسترس است. نرم افزار Snort بر روی شبکه و سیستم در صورت وجود ترافیک، همان لحظه آن را مورد بررسی قرار می‌دهد.
- این نرم افزار را در ۳ حالت می‌توان استفاده کرد:
  - حالت اسنیفر[6]: در این حالت، اسنورت ترافیک شبکه را به اصطلاح شنود [7]می‌کند.
  - حالت ثبت بسته ها[8]: در این حالت، گزارشی از ترافیک های شناسایی شده در حالت شنود تهیه می‌شود
  - حالت تشخیص نفوذ[9] : در این حالت، نفوذ و حمله به شبکه تشخیص داده می‌شود و ترافیک ورودی بر اساس قوانین ایجاد شده توسط کاربر بررسی می‌شوند.

[1] SNORT
[2] Intrusion Detection System
[3] Intrusion Prevention System(IPS)
[4] Martin Roesch
[5] Source fire
[6] Sniffer Mode
[7] Sniff
[8] . Packet Logger Mode
[9] Network Intrusion Detection

- سیستم‌های تشخیص نفوذ میزبان: معیار تشخیص حملات در این سیستم‌ها، اطلاعات جمع‌آوری‌شده بر روی کلاینت‌های شبکه است. در این سیستم‌ها نرم‌افزار به‌صورت تک‌به‌تک بر روی تمامی سیستم‌ها نصب می‌شود و به صورت مجزا فعالیت می‌کنند. این سرویس کوچک[1] در ماشین مقصد (میزبان) می‌توانند کلیه تحرکات آن را مورد نظارت قرار دهند و با تحلیل عملیات انجام‌شده، سعی در تشخیص تلاش‌هایی که برای نفوذ به کلاینت[2] (Client) مذکور انجام می‌شود دارند. در این سیستم حفاظتی، به هنگامی‌که رخدادی خارج از روال عادی روی دهد، بلافاصله از طریق SNMP هشدارهایی به‌طور خودکار برای مسئولین شبکه ارسال می‌گردد. برای رسیدن به یک سیستم تشخیص نفوذ کامل، بهترین راه استفاده‌ی هم‌زمان از هر دو نوع این ابزارهاست.

۲-۲-۱-۱-تفاوت میان IPS و IDS

تشخیص IDS شبکه را پایش کرده و در صورت تشخیص حمله اخطار می‌دهند و درواقع بیش از یک دستگاه گردآوری کننده اطلاعات و آگاه‌کننده اختلالات شبکه نیستند که تنها قادرند هر بسته‌ای را که قصد عبور دارد ارزیابی و تحلیل کنند. روش IPS از ورودی بدون مجوز به شبکه یا سرویس‌دهنده جلوگیری به عمل می‌آورد. روش IPS نسل جدیدی از فن‌آوری IDS است که دارای مکانیسم پیشگیری هستند و نه فقط واکنش که توانایی مسدود کردن حملات را داشته باشد و می‌تواند به بیرون راندن تراکم موجود در شبکه، قطع و وصل ارتباط شبکه داخلی با شبکه خارجی و کنترل رفت و آمدها به داخل و خارج شبکه اشاره کرد. ذاتاً تمام IPS ها IDS نیستند [۹و۱۰].

حمله‌های سایبری پیچیده‌تر شده و چالش‌های بیشتری در تشخیص نفوذ دقیق ایجاد شده است. شکست برای جلوگیری از نفوذ می‌تواند منجر به کاهش اعتبار سرویس‌های امنیتی مانند رازداری داده، درستی و قابل دسترسی بودن می‌شود. روش‌های تشخیص نفوذ زیادی در تحقیقات برای مقابله با تهدیدات امنیت رایانه پیشنهاد شده‌اند که به‌طور گسترده‌ای به سیستم‌های تشخیص نفوذ مبتنی بر امضا (SIDS) و سیستم‌های تشخیص نفوذ مبتنی بر خلاف قاعده (AIDS) تقسیم می‌شوند. در [۶] یک طبقه‌بندی از IDS هم‌دوره و یک مرور گسترده از کارهای اخیر و یک مرور از پایگاه‌های داده‌ای که معمولاً برای ارزیابی اهداف استفاده می‌شوند، آورده شده است. همچنین روش‌های گریز استفاده‌شده توسط مهاجمان برای اجتناب از تشخیص ارائه‌شده است.

مقاله [۶] مروری درباره‌ی کارهای تحقیقاتی انجام‌شده بر روی IDS ها تا سال ۲۰۱۹ انجام داده است. یک طبقه‌بندی از سیستم‌های پیشنهادی بر طبق علم رده‌بندی انجام داده است. این مقاله یک مرور جامع و ساختاری از IDS های موجود فراهم کرده است به‌طوری که یک محقق می‌تواند به‌طور سریع با جنبه‌های کلیدی تشخیص غیرمتعارف آشنا شود. این مقاله همچنین یک مرور از روش‌های داده‌کاوی اعمال‌شده برای طراحی سیستم‌های تشخیص نفوذ فراهم کرده است. روش‌های مبتنی بر نامتعارف بودن و مبتنی بر امضا توصیف شده‌اند. همچنین چندین فن در هر روش بیان شده است. پیچیدگی روش‌های AIDS مختلف و تکنیک‌های ارزیابی آن‌ها بحث شده است. این روش‌ها به وسیله‌ی یک مجموعه از پیشنهادها شناسایی بهترین روش‌ها دنبال شده اند که وابسته به طبیعت نفوذ هستند. چالش‌ها برای IDS های فعلی همچنین بحث شده است. این مقاله یک بحث در مورد مسائل پایگاه داده IDS ارائه نموده است که هدف اصلی برای جامعه‌ی تحقیقاتی در ناحیه‌ی سیستم‌های تشخیص نفوذ است. در مقاله [۶] یک

[1] Agent
[2] Client

مطالعه‌ی هم زمان و ساختاری بر روی سیستم تشخیص نفوذ در مقوله‌های تکنیک‌ها و پایگاه‌های داده انجام شده و همچنین چالش‌های تکنیک‌ها و سپس توصیه‌ها بیان شده است.

در طول دهه‌های گذشته مقالاتی بر روی تشخیص نفوذ به چاپ رسیده است. جدول ۱ روش‌های IDS و پایگاه‌های داده پوشش داده توسط این مرور و مقالات پیشین گذشته نشان داده است. مرور بر روی سیستم تشخیص نفوذ و طبقه‌بندی در [۱۱] انجام شد که در آن سیستم‌های تشخیص نفوذ بر اساس روش‌های تشخیص طبقه‌بندی انجام شد. محققان در ۲۰۰۰ بر روی روش‌های تشخیص نفوذ بر اساس رفتار و پروفایل‌های دانش حملات انجام دادند. در [۶] یک طبقه‌بندی از سیستم‌های تشخیص نفوذ انجام شد. نویسندگان در [۶] یک دسته‌بندی با پنج زیر دسته با یک جنبه عمیق بر روی ویژگی‌های آن‌ها انجام دادند: مبتنی بر آمار، مبتنی بر الگو، مبتنی بر قاعده، مبتنی بر حالت و مبتنی بر اکتشاف. در دست دیگر، کار ما بر روی ویژگی تشخیص امضاء، تشخیص نامتعارف، طبقه‌بندی و پایگاه‌های داده تمرکز نموده است.

در [۶] بر روی موارد زیر تمرکز شده است:

- دسته‌بندی انواع مختلف IDS با انواع عمده‌ای از حملات بر اساس روش‌های نفوذ
- ارائه یک دسته‌بندی از معیارهای ارزیابی IDS نامتعارف شبکه و بحث بر روی اهمیت انتخاب ویژگی
- ارزیابی پایگاه داده IDS موجود با بحث چالش‌های تکنیک‌های گریز

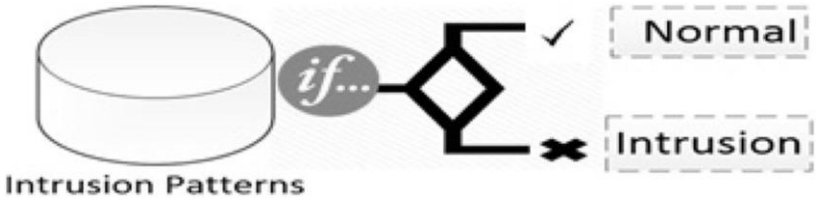
نفوذ را می‌توان هر نوع فعالیت غیرمجاز که باعث آسیب به یک سیستم اطلاعاتی می‌شود، تعریف کرد. این به معنای آن است که هر حمله که می‌تواند یک تهدید ممکن برای اطلاعات محرمانه، درستی یا قابل‌دسترس باشد، به عنوان یک نفوذ در نظر گرفته شود. برای مثال، فعالیت‌هایی که خدمات کامپیوتر را برای کاربران قانونی غیر پاسخگو می‌سازند به عنوان یک نفوذ در نظر می‌گیرند. یک IDS یک نرم‌افزار یا سیستم سخت‌افزاری است که عملیات بدافزاری را در سیستم‌های رایانه‌ای شناسایی نموده به‌طوری‌که برای امنیت سیستم برای به دست‌گیری اجازه داده شود. هدف یک IDS شناسایی انواع مختلف ترافیک شبکه‌ای بدافزاری و کاربرد کامپیوتر است که نمی‌تواند به وسیله‌ی دیوار آتش سنتی شناسایی کرد. این امر برای دستیابی به حفاظت بالا در برابر اقداماتی که در دسترس بودن، یکپارچگی یا محرمانه بودن سیستم‌های رایانه‌ای را به خطر می‌اندازد، حیاتی است. سیستم‌های IDS را می‌توان به‌طور گسترده در دو گروه طبقه‌بندی کرد: سیستم تشخیص نفوذ مبتنی بر امضا (SIDS) و سیستم تشخیص نفوذ مبتنی بر نامتعارف (AIDS).

۲-۲-۱-۲-سیستم‌های تشخیص نفوذ مبتنی بر امضا

سیستم‌های تشخیص نفوذ امضا بر اساس تکنیک‌های یادگیری ماشین برای یافتن یک حمله‌ی معلوم می‌باشند. این‌ها همچنین به عنوان تشخیص مبتنی بر دانش یا تشخیص سوءاستفاده شناخته می‌شوند. در SIDS، روش‌های تطبیقی برای یافتن یک نفوذ پیشین استفاده شده‌اند. به‌عبارت‌دیگر، هنگامی‌که یک امضای نفوذ با امضای نفوذ پیشین تطابق یابد که در پایگاه داده امضا وجود دارد، یک سیگنال آلارم رها می‌شود. برای SIDS، گزارش‌های مربوط به میزبان بررسی می‌شوند تا توالی فرمان‌ها یا عملیاتی که پیش از این به عنوان بدافزار شناسایی شده‌اند یافته شوند [۱۲].

شکل ۱ کار مفهومی روش‌های SIDS را نشان می‌دهد. ایده‌ی اصلی برای ایجاد یک پایگاه داده‌ی امضاهای نفوذ و مقایسه‌ی مجموعه‌ی فعلی از عملیات در برابر امضاهای موجود و برخاستن یک هشدار است، اگر یک تطبیق یافته شود، است. برای مثال،

یک قانون به شکل اگر: مقدم- آنگاه: تالی ممکن است منجر به Aاگر (آدرس منبع IP = آدرس IP مقصد) آنگاه برچسب به عنوان یک حمله در نظر گرفته شود.



شکل ۱ کار مفهومی روش‌های SIDS [۶]

تشخیص SIDS معمولاً یک دقت تشخیص عالی برای نفوذ معلوم پیشین می‌دهد؛ اما SIDS در تشخیص حملات روز صفر مشکل دارد. زیرا امضای تطبیق یافته در پایگاه داده تا زمانی که امضای حمله‌ی جدید استخراج و ذخیره شود، موجود نمی‌باشد [۱۳]. SIDS در ابزارهای زیادی نظیر اسنورت[1] (Snort) [۱۴] و نت استات[2] (NetSTAT) [۱۵].به کار برده شده است.

روش‌های سنتی بسته‌های شبکه SIDS را بررسی نموده و در برابر یک پایگاه داده امضاها تلاش می‌کنند؛ اما این روش‌ها قادر به شناسایی حملاتی که چندین بسته را پوشش می‌دهند نمی‌باشند. از آنجایی‌که بدافزار مدرن پیچیده‌تر است، استخراج اطلاعات امضا بر روی چندین بسته لازم است. این نیاز دارد که IDS محتوی بسته‌های زودتر را فراخوانی کند. با ملاحظه به ایجاد یک امضا برای SIDS، به‌طورکلی یک تعداد از روش‌هایی وجود دارند که امضاها به صورت ماشین‌های حالت ایجاد می‌شوند [۶].

نرخ افزایشی حمله‌های روز صفر دارای تکنیک‌های SIDS است که کمتر مؤثرند زیرا امضای پیشینی برای هر حمله‌ای وجود ندارد. انواع چند دگردیسی بدافزار و افزایش مقدار حمله‌های هدف می‌تواند شایستگی این نمونه‌ی سنتی را تحلیل کند. یک راه‌حل بالقوه برای این مشکل استفاده از تکنیک‌های تشخیص نفوذ است، که با توصیف رفتارهای قابل قبول و نه موارد غیرعادی عمل می‌کند، همان‌طور که در بخش بعدی توضیح داده شده است.

۲-۲-۱-۳-سیستم‌های تشخیص نفوذ مبتنی بر غیرمتعارف بودن

سیستم‌های تشخیص نفوذ مبتنی بر غیرمتعارف بودن علاقه‌ی محققان زیادی را بر طبق ظرفیت آن برای غلبه بر محدودیت‌های SIDS به خود جلب نموده است. در AIDs یک مدل معمولی رفتار یک سیستم کامپیوتری را با استفاده از یادگیری ماشین ایجاد می‌کند که به صورت آماری یا مبتنی بر دانش هستند. هرگونه انحراف قابل توجه بین رفتار مشاهده شده و مدل به عنوان یک ناهنجاری در نظر گرفته می‌شود که می‌تواند به عنوان یک نفوذ تعبیر شود. فرض این گروه از تکنیک‌ها این است که رفتارهای مخرب با رفتارهای معمولی کاربران متفاوت است. رفتارهای غیرمعمولی کاربران که به رفتارهای استاندارد شبیه نیست به عنوان نفوذ دسته‌بندی می‌شود. توسعه‌ی AIDS متشکل از دو فاز است: فاز آموزش و فاز آزمایش. در فاز آموزش، پروفایل ترافیک معمولی برای یادگیری یک مدل رفتار معمولی استفاده‌شده و سپس در فاز آزمایش، یک مجموعه داده جدید برای برقرار سازی ظرفیت سیستم به منظور تعمیم دهی نفوذهای مشاهده نشده پیشین استفاده می‌شود. تشخیص با روش AIDS می‌تواند به یک تعداد از دسته‌ها بر اساس روش استفاده شده برای آموزش، برای نمونه، مبتنی بر آمار، مبتنی بر دانش و مبتنی بر یادگیری ماشین دسته‌بندی شود [۶].

[1] Snort
[2] NetSTAT

مزیت اصلی AIDS توانایی شناسایی حملات روز صفر بر طبق این حقیقت است که فعالیت کاربر غیرمعمولی به یک پایگاه داده‌ی امضا وابسته نمی‌باشد. روش AIDS یک سیگنال خطر را تحریک می‌کند در وقتی‌که رفتار بررسی شده مختلف با رفتار معمول باشد. علاوه بر این، AIDS مزایای مختلفی دارد. ابتدا، آن‌ها توانایی کشف فعالیت‌های بدافزاری داخلی را دارند. اگر یک مزاحم شروع به تراکنش در یک حساب دزدی باشد که در یک فعالیت عادی کاربر شناسایی نشده است، شروع به دادن یک هشدار می‌کند. ثانیاً برای یک مجرم سایبری بسیار دشوار است که تشخیص دهد رفتارهای معمولی کاربران بدون ایجاد هشدار به عنوان سیستم از پروفایل‌های سفارشی ساخته شده است [۶].

جدول تفاوت‌ها میان تشخیص مبتنی بر امضا و تشخیص مبتنی بر غیرمتعارف بودن نشان داده شده است. روش SIDS می‌تواند فقط مزاحم‌های معروف را شناسایی کند درحالی‌که AIDS می‌تواند حملات روز صفر را شناسایی کند؛ اما AIDS می‌تواند منجر به یک نرخ مثبت اشتباه بالا شود زیرا نامتعارف بودن ممکن است فقط فعالیت‌های معمولی جدید در مقایسه با مزاحم‌های جدید باشد.

از آن‌جا که برای طبقه‌بندی سیستم‌های تشخیص نفوذ مبتنی بر ناهنجاری، طبقه‌بندی وجود ندارد، پنج زیر دسته بر اساس ویژگی‌های آن‌ها شناسایی شده است: مبتنی بر آمار، مبتنی بر الگو، مبتنی بر قانون، مبتنی بر حالت و مبتنی بر اکتشافی که در جدول ۱ نشان داده شده است.

جدول ۱: مقایسه روش‌های تشخیص نفوذ [۶]

روش تشخیص	مزایا	معایب
SIDS	• در شناسایی نفوذ با کمترین هشدار اشتباه خیلی مؤثر است • بی‌درنگ نفوذ را شناسایی می‌کند • برتری برای تشخیص حملات شناخته‌شده • طراحی ساده	• برای به‌روزرسانی اغلب به یک امضای جدید نیاز دارد • SIDS برای تشخیص حملات برای امضاهای معلوم نیاز دارد. هنگامی‌که نفوذ پیشین به یک نوع جدید کمی تغییر کند، آن‌گاه سیستم قادر به شناسایی این تغییر از حمله‌ی مشابه نیست • قادر به تشخیص حمله‌ی روز صفر نیست • برای تشخیص حملات چندگانه مناسب نیست • درک پایین از باطن حملات
AIDS	• قادر به تشخیص حملات جدید است • قادر به استفاده از امضای نفوذ است	• AIDS قادر به گرفتن بسته‌های رمزنگاری‌شده نمی‌باشد، بنابراین حمله ممکن است هنوز تشخیص داده نشده و به عنوان یک تهدید حضور داشته باشد. • اشتباه بالا در هشدارهای مثبت • ایجاد یک پروفایل معمولی برای هر سیستم کامپیوتری دینامیک سخت است • هشدارهای غیر دسته‌بندی‌شده • به آموزش اولیه نیاز دارد

۲-۳-بهبود سیستم‌های تشخیص نفوذ

رونق اخیر در یادگیری عمیق نشان داده است که استفاده از شبکه‌های عصبی عمیق یک راه ارزشمند برای رسیدگی به مشکلات تشخیص نفوذ شبکه است. مرجع [۱۶] یک روش یادگیری عمیق جدید را ارائه می‌کند که از شبکه‌های عصبی کانولوشنال (CNN [۱]) برای تجهیز یک شبکه کامپیوتری با ابزاری مؤثر برای تجزیه و تحلیل ترافیک در شبکه برای نشانه‌های فعالیت مخرب استفاده می‌کند. ایده اصلی این است که جریان‌های شبکه را به صورت تصاویر دوبعدی نشان می‌دهد و از این نمایش تصویری جریان‌ها برای آموزش معماری دوبعدی CNN استفاده می‌نماید. مزیت این است که روش نگاشت داده امکان ساخت داده‌های تصویری را می‌دهد که الگوهای داده بالقوه ناشی از جریان‌های همسایه را بیان می‌کند و منجر به‌دقت پیش‌بینی بهتری در مقایسه با دیگر معماری‌های تشخیص نفوذ می‌شود [۱۶] .

از سوی دیگر، موفقیت یادگیری عمیق (DL[۲]) در زمینه‌های مختلف کلان داده، علاقه‌های زیادی را در زمینه‌های امنیت سایبری به خود جلب کرده است. کاربرد DL به دلیل بهبود در جنبه‌های CPU و الگوریتم‌های شبکه عصبی (NN [۳]) عملی بوده است. استفاده از DL برای تشخیص حملات در فضای سایبری می‌تواند مکانیسمی مقاوم در برابر جهش‌های کوچک یا حملات جدید باشد زیرا قابلیت استخراج ویژگی در سطح بالایی دارد. قابلیت‌های خودآموز و فشرده‌سازی معماری‌های یادگیری عمیق، مکانیسم‌های کلیدی برای کشف الگوی پنهان از داده‌های آموزشی هستند، به‌طوری‌که حملات از ترافیک بی‌خطر متمایز می‌شوند. هدف این تحقیق اتخاذ رویکردی جدید، یادگیری عمیق، به امنیت سایبری است تا امکان شناسایی حملات در اینترنت اجتماعی اشیاء را فراهم کند. عملکرد مدل عمیق با رویکرد یادگیری ماشین سنتی مقایسه می‌شود و تشخیص حمله توزیع‌شده در برابر سیستم تشخیص متمرکز ارزیابی می‌شود. آزمایش‌ها نشان داده‌اند که سیستم تشخیص حمله توزیع‌شده ما نسبت به سیستم‌های تشخیص متمرکز با استفاده از مدل یادگیری عمیق برتری دارد. همچنین نشان داده شده است که مدل عمیق در تشخیص حمله نسبت به قطعات کم‌عمق خود مؤثرتر است [۱۷].

در [۱۸] یک سیستم تشخیص نفوذ مبتنی بر داده مفید با استفاده از هوش مصنوعی، به‌ویژه روش‌های یادگیری ماشین (ML[۴]) توسعه یافته است. در این مطالعه، دو روش طبقه‌بندی مختلف برای تشخیص نفوذ (ID) که هر کدام موارد استفاده منحصر به فرد خود را دارند، مقایسه شدند. الگوریتم بهینه‌سازی ازدحام ذرات (PSO[۵]) برای کاهش ابعاد قبل از استفاده از دو طبقه‌بندی کننده برای روش طبقه‌بندی استفاده شد. این مطالعه روش‌های طبقه‌بندی را برای دسته‌بندی ناهنجاری‌های شبکه در نظر گرفت. دو طبقه‌بندی کننده استفاده شده الگوریتم ازدحام ذرات و درخت تصمیم و الگوریتم ازدحام ذرات و k نزدیک‌ترین همسایه است. در این پژوهش نیز آزمایش‌ها روی مجموعه داده‌های KDD-CUP 99 انجام شد. نتایج نشان داد که PSO+KNN از الگوریتم طبقه‌بندی کننده PSO+DT ازنظر شناسایی ناهنجاری‌های شبکه بهتر عمل می‌کند [۱۸].

[1] Convolutional Neural Network
[2] Deep Learning
[3] Neural Network
[4] Machine learning
[5] Particle Swarm Optimization

مقاله [۲۳] یکی از کارهای اولیه در مورد استفاده از طبقه‌بندی بود در این کار، نویسندگان از فاصله همینگ استفاده کردند تا نشان دهند تماس‌های سیستم مخرب چگونه می‌توانند با «توالی عادی موجود» متفاوت باشند. شبکه‌های عصبی یک روش رایج برای خوشه‌بندی در IDS ها هستند. NN ها مجموعه‌ای از واحدهای پردازشی هستند که توسط اتصالات وزنی به هم متصل می‌شوند. دانش سیستم توسط ساختار شبکه‌ای که مجموعه‌ای از نورون‌ها و ارتباطات وزنی است ذخیره می‌شود. فرآیند یادگیری با تغییر وزن ارتباطات و همچنین افزودن و حذف آن‌ها انجام می‌شود [۱۹]. روش دیگری در خوشه‌بندی برای IDS از الگوریتم ژنتیک (GA [1]) استفاده می‌کند. از منظر الگوریتم ژنتیک، فرآیند تشخیص نفوذ شامل تعریف یک بردار برای اطلاعات رویداد است که نشان‌دهنده نفوذ است. در ابتدا یک بردار فرضی بر اساس نتایج در نظر گرفته، تائید و به‌روز می‌شود. این کار به‌طور مکرر انجام می‌شود تا زمانی که راه‌حلی پیدا شود. نقش الگوریتم ژنتیک ایجاد مفروضات جدید بر اساس نتایج قبلی است. GA شامل دو مرحله است: مرحله اول شامل رمزگذاری راه‌حل به عنوان رشته‌ای از بیت‌ها است و مرحله دوم تابعی را برای بررسی رشته بیت [۲۲] و [۲۴] پیدا می‌کند. درختان تصمیم راهی برای نمایش مجموعه‌ای از قوانین هستند که به یک دسته یا ارزش منتهی می‌شوند. درختانی که برای پیش‌بینی متغیرهای باینری استفاده می‌شوند درخت تصمیم نامیده می‌شوند زیرا نمونه‌ها را در دسته‌ها قرار می‌دهند. درختان تصمیم‌گیری که برای پیش‌بینی متغیرهای پیوسته استفاده می‌شوند، درختان رگرسیون نامیده می‌شوند [۲۰]. اکثر الگوریتم‌های یادگیری از درخت تصمیم بر اساس جستجوی حریصانه و از بالا به پایین در فضای درختی موجود عمل می‌کنند. در ID3، درخت تصمیم از یک مقدار آماری به نام بهره اطلاعات برای تعیین اثر یک ویژگی استفاده می‌کند. درختان تصمیم به‌طور گسترده‌ای در خوشه‌بندی IDSها استفاده شده‌اند [۲۱]. خوشه‌بندی یا تجمیع یا تقسیم‌پذیر است. اولی برای بهبود استحکام خوشه‌بندی استفاده می‌شود و دومی برای ابداع مجموعه‌های مختلفی از خوشه‌ها از یکدیگر استفاده می‌شود. رویکرد خوشه‌بندی همچنین می‌تواند رویکردی از پایین به بالا داشته باشد [۲۵]. این رویکرد با تشکیل گروه‌های متمایز شروع می‌شود که هرکدام شامل حداقل یک شیء هستند. سپس، اشیاء یا گروه‌های نزدیک به هم درنهایت یک گره کلی در بالاترین سطح تشکیل می‌دهند. در روش تقسیم، همه اشیا در یک خوشه در نظر گرفته می‌شوند و هر خوشه به دو خوشه کوچک‌تر تقسیم می‌شود. دو نمونه از رویکرد پایین به بالا عبارت‌اند از AGNESS و DIANA، که AGNESS در مقایسه با DIANA پیچیدگی برتری را نشان می‌دهد و به این نتیجه می‌رسد که یک راه‌حل مقرون به‌صرفه است [۲۶]. یک رویکرد جایگزین برای روش از پایین به بالا، خوشه‌بندی مبتنی بر چگالی است. فایده این روش مبتنی بر رشد خوشه‌ها بر اساس تراکم همسایگی آن‌ها است. این بدان معنی است که برای هر نقطه از داده در یک خوشه معین، همسایگان در شعاع مشخص‌شده خود قرار دارند [۲۷]. برخی از کاربردهای اخیر تشخیص رویکرد نیمه نظارت‌شده بر اساس الگوریتم فازی که بر روی ابر انجام می‌شود و زیرساخت مه [۲۸]، [۲۹]. اگرچه این الگوریتم‌ها دقت بالایی را ارائه می‌دهند، اما نیاز به دانش پیشینی از تعداد خوشه‌ها دارند. نویسندگان در [۳۰] یک ماشین بردار پشتیبان (SVM [2]) و درخت تصمیم را پیشنهاد می‌کنند و بر اساس ادعای خود موفق‌ترین روش ازنظر دقت در نظر گرفته می‌شود و می‌توان گفت که با توجه به دقتی که معمولاً از پشتیبان گیری پشتیبانی می‌کند. الگوریتم‌های ماشینی بااین‌حال، این روش تعداد ایستا از خوشه‌ها را فرض می‌کند که هنوز باید تعیین شوند. در [۳۱]، نویسندگان یک الگوریتم مبتنی بر یک الگوریتم ژنتیک چند هدفه برای شکل دادن به IDS پیشنهاد کردند.

[1] Genetic Algorithm
[2] Support Vector Machine

این الگوریتم خوشه‌بندی را به عنوان یک تابع بهینه‌سازی تعریف می‌کند که هدف آن یافتن حداقل فاصله خوشه و حداکثر فاصله بین اهداف خوشه است. سپس یک الگوریتم ژنتیک چند هدفه را حل می‌کند. در مقاله [۳۲] توابع بهینه‌ساز برای تعیین بهترین خوشه‌ها تعریف می‌شود و سپس با کمک الگوریتم‌های بهینه‌سازی، تعداد خوشه‌های بهینه مورد نیاز پیدا می‌گردد.

۲-۳-استخراج ویژگی در سیستم‌های تشخیص نفوذ

در سیستم‌های تشخیص نفوذ، با داده‌های حجیم برای تحلیل مواجه هستند. بررسی مجموعه داده سیستم‌های تشخیص نفوذ نشان می‌دهد که بسیاری از ویژگی‌های، ویژگی‌های غیرمفید، بی‌تأثیر در سناریوهای حمله و یا ویژگی‌های نامربوط هستند. بنابراین حذف ویژگی‌های نامناسب از مجموعه ویژگی، به عنوان یک راهکار مناسب برای کاهش مجموعه داده سیستم‌های تشخیص نفوذ معرفی می‌شود. نیازمندی دیگری که در سیستم‌های تشخیص نفوذ مطرح می‌باشد، دانستن مجموعه ویژگی بهینه برای هر نوع حمله است. چرا که در این صورت، سیستم تشخیص نفوذ قادر خواهد بود برای تشخیص هر نوع حمله، تنها از مجموعه ویژگی متناسب با آن حمله استفاده کند [۳۳].

برای بهبود بیشتر، مجموعه‌ای از روش‌های مهندسی ویژگی، مانند انتخاب ویژگی، برای افزایش کیفیت داده‌ها ساخته‌شده است. در این روش‌ها یک فرآیند داده برای آموزش و ساخت طبقه‌بندی کننده مؤثر مورد استفاده قرار می‌گیرد [۳۵ -۳۹]. محققان در [۴۰] یک سیستم تشخیص نفوذ مبتنی بر ناهنجاری را با استفاده از روش SOM[1] فازی پیشنهاد کرد. در [۴۱]یک مدل تشخیص نفوذ پیشنهاد شد که روش نیوبیز[2] و DL را با هم استفاده کرد و از الگوریتم ژنتیک نیز برای انتخاب ویژگی خوب بهره برد. در [۴۲] نیز یک مدل تشخیص برای ارتباطات نفوذی پیشنهاد شده است. این کار تحقیقاتی پنج روش طبقه‌بندی را آزمایش می‌کند همچنین در [۴۳] یک رویکرد طبقه‌بندی‌کننده ترکیبی با استفاده از الگوریتم درختی برای تشخیص نفوذ شبکه ارائه گردید و مدل بر روی مجموعه داده kdd با صحت ٪۸۹/۲۴ ارزیابی شده است. مقاله [۴۴] مدلی بر اساس الگوریتم جنگل تصادفی برای انتخاب یک ویژگی مهم ارائه کرد که این مدل با استفاده از NSL-KDD مورد ارزیابی قرار گرفت. نتایج این مقاله نیز صحت ٪۹۹,۳۳ 99.33٪، TP٪DR 0.993 ، و FP٪FAR 0.001 است.

محققان در [۳۵] مدلی از یک مجموعه تشخیص نفوذ مبتنی بر SVM با تبدیل LMDRT به عنوان یک روش مؤثر برای افزایش کیفیت داده پیشنهاد کردند. همچنین در [۴۵] یک مدل یادگیری عمیق برای تشخیص نفوذ شبکه با استفاده از فرا ابتکاری دوگانه PSO توسعه داده شد مدل فوق بر روی مجموعه داده CICIDS2017 ارزیابی شد و ACC 92.92٪، DR 92.38٪ و FAR 3.24٪ می‌باشد. نویسندگان در [۳۹] نیز یک سیستم تشخیص نفوذ جدید پیشنهاد کرده‌اند که بر روی زیرمجموعه ویژگی‌ها با استخراج ویژگی‌های مهم با استفاده از روش احتمالی کار می‌کند. روش BRS برای دسته‌بندی نمونه‌ها به دسته‌های عادی، متوسط و غیرعادی بر اساس مجموعه ناهموار اجرا می‌شود. این مدل بر روی مجموعه داده CICIDS2017 آموزش‌دیده و آزمایش شده

[1] Self-organizing map

[2] Naive Bayes classifier

است و ACC 97.6 ٪، DR 96.38٪ و FAR 3.00 ٪ را نشان می‌دهد. نویسندگان مقاله [۴۶] یک مدل IDS ترکیبی پیشنهاد کردند که مدل طبقه‌بندی کننده درخت تصمیم، درختREP ، الگوریتم JRIP و جنگل PA ترکیب می‌کند. عملکرد مدل جدید با استفاده از مجموعه داده CICIDS2017 ارزیابی‌شده و ACC 96.66 ٪، DR 94.475٪ و FAR 4.47 ٪ ارائه شده است. از بررسی ادبیات پیشرفته، ثابت شده است که روش‌های یادگیری و کیفیت داده‌ها دو هستند. وظایف مفیدی که استحکام IDS را تعیین می‌کند [۴۷، ۳۵، ۴۱-۴۴، ۴۵، ۳۹،۴۰]. این تحقیقات بسیاری از روش‌ها را برای کیفیت بالای داده‌ها با نه تنها کاهش و انتخاب ویژگی‌ها، بلکه ساخت طبقه‌بندی‌کننده‌های بهبودیافته برای دسته‌بندی بهتر فعالیت‌های داده، اجرا می‌کنند.

۲-۴-مشکلات مرتبط با NIDS

- نرخ تشخیص کاذب: NIDS مبتنی بر ناهنجاری به اشتباه فعالیت‌های سیستم عادی اما قبلاً دیده نشده را به عنوان یک ناهنجاری طبقه‌بندی می‌کند. این باعث افزایش نرخ FP می‌شود. از سوی دیگر، دلیل افزایش نرخ منفی کاذب، فراوانی بالای حملات جدید در فضای مجازی است. NIDS مبتنی بر امضا، امضاهای حمله شناخته‌شده را ذخیره می‌کند و نمی‌تواند حملات جدید را شناسایی کند [۴۹،۴۸]. علاوه بر این، برخی از NIDS مبتنی بر امضا ممکن است آن‌قدر خاص باشند که یک تغییر خفیف در حمله بتواند از شناسایی آن جلوگیری کند. در چنین شرایطی، کارشناسان امنیتی هیچ اطلاعی از وقوع حمله ندارند. منفی‌های کاذب را نمی‌توان به‌راحتی قضاوت کرد. ازنظر تئوری، ترکیبی از روش‌های تشخیص مبتنی بر امضا و تشخیص مبتنی بر ناهنجاری قرار است بهبودی نسبت به هر دو رویکرد واحد باشد؛ اما در مورد رویکرد ترکیبی که در آن یک آشکارساز ناهنجاری فهرستی از مشاهدات غیرعادی ایجاد می‌کند که توسط آشکارساز مبتنی بر امضا به حملات شناخته‌شده طبقه‌بندی می‌شوند. در چنین حالتی، اگر آشکارساز ناهنجاری نتواند یک حمله را به دلیل شباهت آن با الگوهای رفتاری عادی تشخیص دهد، در مرحله بعد توسط آشکارساز مبتنی بر امضا قابل شناسایی نیست [۴۹].
- ارزیابی IDS با ترافیک شبکه بلادرنگ بزرگ: افزایش چشمگیر داده‌های اینترنت و کاربران، نظارت بر ترافیک شبکه به صورت بلادرنگ را به یک کار گیج‌کننده تبدیل کرده است. برای بهبود IDSها، تجزیه و تحلیل کامل رفتار ترافیکی عادی و غیرعادی ضروری است. یادگیری و تشخیص دقیق الگوهای حمله از چنین داده‌های عظیمی به حجم عظیمی از داده‌های آموزشی برای ایجاد نتایج بهتر نیاز دارد. مدل‌سازی و ارزیابی IDSها با ترافیک شبکه واقعی بزرگ یکی از چالش‌های کلیدی فعلی است.
- مجموعه داده‌های نفوذ ناکارآمد: اخیراً الگوهای ناشناخته عظیمی از نفوذهای شبکه شناسایی شده‌اند که هنوز هم به‌طور مداوم با سرعتی سریع در حال افزایش هستند؛ بنابراین به‌روزرسانی دوره‌ای مجموعه داده‌های نفوذ یک ضرورت است. این به ارائه معماری مناسب برای آزمایش ناهنجاری‌های شبکه قدیمی و همچنین اخیراً مشاهده شده کمک می‌کند. یک نگرانی بزرگ در یک محیط چند ابری، در دسترس نبودن مجموعه داده‌ها برای تجزیه و تحلیل حملات امنیتی اخیر، به دلیل مسائل مربوط به حریم خصوصی است. در دسترس نبودن مجموعه داده‌های نفوذ کارآمد که شامل مقدار مناسبی از انواع نفوذ مرتبط هستند، یک مسئله بزرگ است.

- عدم تعادل داده‌ها: توزیع نابرابر رکورد در مجموعه داده‌های نامتعادل منجر به جهت‌گیری طبقه‌بندی سوابق می‌شود. نرخ تشخیص یک دسته با رکوردهای کمتر در مقایسه با نرخ تشخیص یک دسته با اکثر رکوردها بیشتر کمتر است. انواع روش‌های متعادل‌سازی داده‌ها برای انتقال این موضوع در دسترس هستند، اما به قیمت افزایش پیچیدگی محاسباتی و پیچیدگی زمان اجرا.
- کُند بودن یادگیرنده IDS: آهستگی یادگیرنده IDS ها مسئله دیگری است که معمولاً نادیده گرفته می‌شود؛ اما باید به آن توجه شود تا به نیازهای فعلی وضعیت کلان داده بپردازد. تشخیص به‌موقع نفوذ می‌تواند سیستم‌ها/سازمان‌های هدف را از آسیب‌های عظیم نجات دهد.
- خسته‌کننده بودن برچسب زدن دسته در IDS یادگیری نظارت‌شده: رویکردها وقتی یک مجموعه داده به چند گیگابایت یا حتی بیشتر از اندازه می‌رسد، برچسب‌گذاری دسته برای کارشناسان حوزه بسیار خسته‌کننده است.

۲-۵-مجموعه داده‌های تشخیص نفوذ

مدل‌های تشخیص نفوذ معمولاً با استفاده از مجموعه داده‌های نفوذی که شامل الگوهای ترافیک شبکه عادی و غیرعادی هستند، ارزیابی می‌شوند. مجموعه داده‌های نفوذی قدیمی در حال حاضر به دلیل تاکتیک‌های حمله تکامل‌یافته منسوخ‌شده‌اند. این مجموعه داده‌ها باید شامل حملات مدرن و همچنین ترافیک‌های واقعی شبکه باشد تا دقت تشخیص NIDS را افزایش دهد.

این مقاله شرح مختصری از مجموعه داده‌های نفوذ برچسب‌گذاری شده در دسترس عموم و روش‌های ML را ارائه می‌کند. سپس توضیح مختصری در مورد آثار ادبی ارائه می‌شود که در آن روش‌های یادگیری ماشین برای پیاده‌سازی NIDS در سناریوهای شبکه‌های مختلف مانند شبکه‌های سنتی، شبکه‌های ابری، Ad-Hoc، WSN و شبکه‌های IoT [1] استفاده می‌شوند

مجموعه داده‌های نفوذ در چندین اثر ادبی موجود با اهداف مختلف مورد بررسی و تجزیه و تحلیل قرار می‌گیرند [۵۰-۵۲]. این بخش مجموعه داده‌های نفوذی در دسترس عموم را توصیف می‌کند، مانند KDD Cup ‘99 و Network Security Laboratory-KDD (NSL-KDD) , و Aegean Wi-Fi Intrusion Dataset (AWID) و Yahoo Webscope S5 anomaly benchmark و Numenta Anomaly Benchmark (NAB) و Kyoto 2006+و UNSW-NB 15 و BoT_IoT و Drebin و Contagio و Genome.

یکی از پر کاربردترین داده‌ها در تحقیقات داده NSL-KDD است که ویژگی‌های مجموعه داده NSL-KDD به ۳ نوع طبقه‌بندی می‌شوند.

- ویژگی‌های اساسی: این نشان‌دهنده ویژگی‌های مربوط به یک اتصال TCP/IP است.
- ویژگی‌های ترافیک: این گروه شامل ویژگی‌های مربوط به یک بازه است و بیشتر به ویژگی‌های میزبان مشابه و ویژگی‌های خدمات مشابه تقسیم می‌شود. این زیرگروه‌ها به‌طور مشخص فقط اتصالات مربوط به میزبان و خدمات را با توجه به اتصال فعلی بررسی می‌کنند.
- ویژگی‌های محتوا: حملاتی مانند R2L و U2R الگوهای متوالی مکرر قابل توجهی ندارند. ماهیت این نوع حملات در محتوای داده‌های خود حمله تعبیه‌شده است؛ بنابراین، بخش داده باید برای فعالیت مشکوک بررسی شود، به عنوان مثال: تعداد دفعاتی که تلاش برای ورود ناموفق بود.

[1] Internet of Things

۲-۶-انواع معیارهای ارزیابی

در این بخش معیارهای ارزیابی برای دسته‌بندی بررسی می‌شود. برای ارزیابی باید برچسبی که دسته‌بند به حمله نسبت داده با برچسب مرجع مقایسه شود. برای این کار از ماتریس سردرگمی استفاده می‌شود [۵۳و۵۴].

معیارهای عملکرد IDS ماتریس سردرگمی برای به تصویر کشیدن دسته‌های واقعی و پیش‌بینی‌شده در حملات امنیت سایبری استفاده می‌شود. ماتریس سردرگمی با عبارات زیر نشان داده می‌شود.

مثبت واقعی :(TP) یک نمونه حمله به درستی به عنوان یک حمله پیش‌بینی می‌شود.

منفی واقعی :(TN) یک نمونه عادی به درستی به عنوان یک نمونه غیر حمله یا عادی پیش‌بینی‌شده است.

مثبت کاذب :(FP) یک نمونه عادی به اشتباه به عنوان حمله پیش‌بینی می‌شود.

منفی کاذب :(FN) یک حمله واقعی به اشتباه به عنوان غیر حمله یا نمونه عادی پیش‌بینی می‌شود.

موارد مثبت کاذب در مواردی که یک فعالیت عادی شبکه به‌عنوان حمله طبقه‌بندی می‌شود، می‌تواند زمان ارزشمند مدیران امنیتی را تلف کند. منفی‌های کاذب بدترین تأثیر را بر سازمان‌ها دارند زیرا حمله به هیچ وجه شناسایی نمی‌شود.

با توجه به پارامترهای مطرح‌شده معیارهای ارزیابی مختلفی ارائه‌شده است که ازجمله مهم‌ترین آن‌ها می‌توان به معیارهای خاصیت[1]، حساسیت[2] و صحت[3] اشاره کرد.

معیار صحت: مهم‌ترین معیار برای تعیین کارایی یک الگوریتم دسته‌بندی است و صحت کل یک دسته‌بند را محاسبه می‌کند. این معیار نشان‌دهنده این موضوع است که چند درصد از کل مجموعه داده به‌درستی دسته‌بندی‌شده است.

$$\text{Accuracy} = \frac{T_p + T_N}{T_p + F_p + T_N + F_N} * 100 \qquad (۱)$$

معیار حساسیت: تعیین می‌کند که نمونه‌های حمله تا چه میزان در دسته مثبت قرار داده‌شده‌اند، یا به‌عبارت دیگر چه تعدادی از حملات به‌درستی تشخیص داده‌شده‌اند.

$$\text{Sensitivity} = \frac{T_p}{T_p + F_N} * 100 \qquad (۲)$$

معیار خاصیت: تعیین می‌کند که چه تعدادی از نمونه‌های نرمال به‌درستی تشخیص داده‌شده‌اند.

$$\text{Specificity} = \frac{T_p}{F_p + T_N} * 100 \qquad (۳)$$

معیار دقت: یک متریک عمومی جهت اندازه‌گیری مفید بودن الگوریتم پیشنهادی است که به صورت رابطه (۴) محاسبه می‌شود.

[1] Specificity
[2] Sensitivity
[3] Accuracy

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (۴)$$

معیار فراخوانی: یکی دیگر از متریک‌های ارزیابی در سیستم‌های تشخیص نفوذ است که به صورت رابطه (۵) قابل محاسبه است.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (۵)$$

معیار F: از ترکیب دو پارامتر دقت و فراخوانی محاسبه می‌شود.

$$\text{F} - \text{score} = \frac{2*\text{Precision}*\text{Recall}}{\text{Precision} + \text{Recall}} \quad (۶)$$

۲-۷- تحلیل تحقیقات پیشین

با توجه به تحقیقات پیشین، روش‌های طبقه‌بندی مختلفی برای دسته‌بندی داده‌های مربوط به تشخیص نفوذ ارائه نمودند. یکی از ابزارهایی که در مقایسه با سایر روش‌ها می‌تواند موثر باشد، استفاده از ابزارهای بهینه‌سازی هوشمند و فرا اکتشافی است. این الگوریتم‌ها می‌توانند در بهبود نتایج بدست آمده از تشخیص نفوذ موثر باشند. تنها مشکل آن‌ها سرعت اجرای آن‌ها است. ابزار دیگر که می‌توانند در بهبود تشخیص نفوذ موثر باشند استفاده از منطق فازی است، اما منطق فازی نیاز به دانش فرد خبره دارد. در مقایسه با ابزار روش‌های بهینه‌سازی توصیه نمی‌شود. موضوع مهم دیگری که پیشنهاد می‌شود بیشتر مورد توجه قرار داد، موضوع انتخاب ویژگی‌های سودمند است که برای انتخاب ویژگی بهینه از ابزارهای بهینه‌سازی هوشمند استفاده نمود. این رویکرد منجر به بهبود حجم محاسبات، بهبود دقت و کارایی روش طبقه بندی می‌شود. یک رویکرد دیگر که در آینده می‌توان پیشنهاد داد استفاده از خوشه‌بندی و سپس روش طبقه‌بندی برای دسته بندی کل داده‌های مربوط به تشخیص نفوذ است. خوشه‌بندی را می‌توان برای دسته‌بندی داده‌ی حمله و نفوذ یافته به کار برد. سپس از دسته‌بندی کننده مناسب برای دسته بندی حملات استفاده نمود. این موضوع را در تحقیقات آینده می‌توان مورد توجه قرار داد.

۳-بحث و نتیجه‌گیری

در دنیای امنیت سایبری، سیستم‌های تشخیص نفوذ (همان‌طور که از نامش پیداست) به عنوان ابزاری برای شناسایی فعالیت‌های مخربی که ممکن است در داخل یک شبکه رخ دهد یا وارد شبکه شود، استفاده می‌شود. همان‌طور که اشاره شد کوید ۱۹ و بحث همه‌گیری و قرنطینه در سراسر جهان، از سویی دیگر تشویق به فعالیت بیشتر رایانه‌ای از سوی افراد و سازمان‌ها منجر به افزایش میزان جرائم سایبری و ترافیک مخرب شد و هم اکنون به سیستم‌های امنیت سایبری مؤثرتری جهت افزایش سطح فعالیت‌های مخرب سایبری، نیاز داریم. از نظر امنیت سایبری، نفوذ را می‌توان نوعی فعالیت مخرب انجام‌شده در یک سیستم اطلاعاتی توصیف کرد. این می‌تواند نوعی حمله بدافزار مانند تروجان، حمله DDoS، رویداد نشت داده و غیره باشد. افراد یا سازمان‌ها یا گروه‌های مخرب می‌توانند این حملات را برای منافع شخصی، دلایل پولی، انتقام‌گیری یا دلایل مخرب دیگری انجام دهند، با این وجود، این حملات مخرب تلقی می‌شوند، زیرا برای آسیب رساندن به سازمان و یا افراد آن انجام می‌شوند. ما یک IDS را به عنوان یک نرم‌افزار یا سیستم سخت‌افزاری (یا ترکیبی از این دو) در نظر می‌گیریم که به دنبال حفظ امنیت سیستم از طریق نظارت، شناسایی و شناسایی حملات مخربی است که ممکن است وارد یا روی یک شبکه باشند.

این مقاله نیز بر اساس مرور، مطالعه و بررسی مقالات عمده ذکرشده در دو دهه گذشته به این نتیجه می‌رسد که وضعیت فعلی فناوری IDS از کمبود داده‌های مرتبط رنج می‌برد. همچنین آینده فناوری IDS احتمالاً به سمت یادگیری ماشین و هوش مصنوعی می‌رود و پیشرفت‌های فعلی در حال تحقیق و توسعه هستند همچنین برای بهبود دقت فناوری IDS، کاهش خطاها، تشخیص موارد مثبت/منفی کاذب و غیره بسیار با اهمیت هستند. همچنین با توجه به پیچیدگی این سیستم‌ها، آن‌ها باید به‌درستی درک، توسعه و تجزیه و تحلیل شوند. مقالات تحقیقاتی می‌توانند به عنوان ابزاری برای بهبود سیستم‌های IDS مورد استفاده قرار گیرند. یک بررسی بر اساس طبقه‌بندی‌های قبلی پایه‌ای برای ایجاد این پژوهش هستند.

مراجع

[1] Jmila, H., & Khedher, M. I. (2022). Adversarial machine learning for network intrusion detection: A comparative study. *Computer Networks*, 109073.

[2] Gavel, S., Raghuvanshi, A. S., & Tiwari, S. (2021). Distributed intrusion detection scheme using dual-axis dimensionality reduction for Internet of things (IoT). *The Journal of Supercomputing*, *77*(9), 10488-10511.

[3] Mendonça, R. V., Silva, J. C., Rosa, R. L., Saadi, M., Rodriguez, D. Z., & Farouk, A. (2022). A lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithms. *Expert Systems*, *39*(5), e12917.

[4] Keerthika, M., & Shanmugapriya, D. (2021). Wireless Sensor Networks: Active and Passive attacks-Vulnerabilities and Countermeasures. *Global Transitions Proceedings*, *2*(2), 362-367.

[5] Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials*, *20*(4), 3453-3495.

[6] Gajjar, H., & Malek, Z. (2020, July). A survey of intrusion detection system (IDS) using OpenStack private cloud. In *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)* (pp. 162-168). IEEE.

[7] Singh, U. K., Joshi, C., & Singh, S. K. (2017). Zero day attacks defense technique for protecting system against unknown vulnerabilities. *International Journal of Scientific Research in Computer Science and Engineering*, *5*(1), 13-18.

[8] Aljoufi, R., & Lasebae, A. (2021). Multi-task Learning for Intrusion Detection and Analysis of Computer Network Traffic. In *E3S Web of Conferences* (Vol. 229, p. 01057). EDP Sciences.

[9] Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. *Eai Endorsed Transactions on Security and Safety*, *3*(9), e2.

[10] Naseer, S., & Saleem, Y. (2018). Enhanced network intrusion detection using deep convolutional neural networks. *KSII Transactions on Internet and Information Systems (TIIS)*, *12*(10), 5159-5178.

[11] Kim, A., Park, M., & Lee, D. H. (2020). AI-IDS: Application of deep learning to real-time Web intrusion detection. *IEEE Access*, *8*, 70245-70261.

[12] Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. *Eai Endorsed Transactions on Security and Safety*, *3*(9), e2.

[13] Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. (2019, January). Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0305-0310). IEEE.

[14] Zhang, L., Li, M., Wang, X., & Huang, Y. (2019, July). An improved network intrusion detection based on deep neural network. In *IOP Conference Series: Materials Science and Engineering* (Vol. 563, No. 5, p. 052019). IOP Publishing.

[15] Riyaz, B., & Ganapathy, S. (2020). A deep learning approach for effective intrusion detection in wireless networks using CNN. *Soft Computing*, *24*(22), 17265-17278.

[16] Andresini, G., Appice, A., & Malerba, D. (2021). Nearest cluster-based intrusion detection through convolutional neural networks. *Knowledge-Based Systems*, *216*, 106798.

[17] Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, *82*, 761-768.

[18] Ogundokun, R. O., Awotunde, J. B., Sadiku, P., Adeniyi, E. A., Abiodun, M., & Dauda, O. I. (2021). An enhanced intrusion detection system using particle swarm optimization feature extraction technique. *Procedia Computer Science*, *193*, 504-512.

[19] Debar, H., Becker, M., & Siboni, D. (1992, May). A neural network component for an intrusion detection system. In *Proceedings 1992 IEEE Computer Society Symposium on Research in Security and Privacy* (pp. 240-240). IEEE Computer Society.

[20] Jo, S., Sung, H., & Ahn, B. (2015). A comparative study on the performance of intrusion detection using decision tree and artificial neural network models. *Journal of Korea Society of Digital Industry and Information Management*, *11*(4), 33-45.

[21] Sahu, S., & Mehtre, B. M. (2015, August). Network intrusion detection system using J48 Decision Tree. In *2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 2023-2026). IEEE.

[22] Bhattacharjee, P. S., Fujail, A. K. M., & Begum, S. A. (2017). Intrusion detection system for NSL-KDD data set using vectorised fitness function in genetic algorithm. *Adv. Comput. Sci. Technol*, *10*(2), 235-246.

[23] Hofmeyr, S., Forrest, S., & Sornayaji, A. (1997). Lightweight intrusion detection for networked operating systems. *Journal of Computer Security*, *5*(2).

[24] Aloqaily, M., Otoum, S., Al Ridhawi, I., & Jararweh, Y. (2019). An intrusion detection system for connected vehicles in smart cities. *Ad Hoc Networks*, *90*, 101842.

[25] Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, *41*(4), 1690-1700.

[26] Puthran, S., & Shah, K. (2016, September). Intrusion detection using improved decision tree algorithm with binary and quad split. In *International symposium on security in computing and communication* (pp. 427-438). Springer, Singapore.

[27] Shah, B., & Trivedi, B. H. (2012). Artificial neural network based intrusion detection system: A survey. *International Journal of Computer Applications*, *39*(6), 13-18.

[28] Ashfaq, R. A. R., Wang, X. Z., Huang, J. Z., Abbas, H., & He, Y. L. (2017). Fuzziness based semi-supervised learning approach for intrusion detection system. *Information sciences*, *378*, 484-497.

[29] Yaseen, Q., AlBalas, F., Jararweh, Y., & Al-Ayyoub, M. (2016, September). A fog computing based system for selective forwarding detection in mobile wireless sensor networks. In *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W)* (pp. 256-262). IEEE.

[30] Puri, A., & Sharma, N. (2017). A novel technique for intrusion detection system for network security using hybrid svm-cart. *International Journal of Engineering Development and Research*, *5*(2), 155-161.

[31] Kabiri, P., & Ghorbani, A. A. (2005). Research on intrusion detection and response: A survey. *Int. J. Netw. Secur.*, *1*(2), 84-102.

[32] Shojafar, M., Taheri, R., Pooranian, Z., Javidan, R., Miri, A., & Jararweh, Y. (2019, November). Automatic clustering of attacks in intrusion detection systems. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)* (pp. 1-8). IEEE.

[33] Thakkar, A., & Lohiya, R. (2021). A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. *Artificial Intelligence Review*, 1-111.

[34] Alazzam, H., Sharieh, A., & Sabri, K. E. (2020). A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer. *Expert systems with applications*, *148*, 113249.

[35] Gu, J., Wang, L., Wang, H., & Wang, S. (2019). A novel approach to intrusion detection using SVM ensemble with feature augmentation. *Computers & Security*, *86*, 53-62.

[36] Jayakumar, K., Revathi, T., & Karpagam, S. (2015). Intrusion Detection using Artificial Neural Networks with Best Set of Features. *International Arab Journal of Information Technology (IAJIT)*, *12*.

[37] Ayo, F. E., Folorunso, S. O., Abayomi-Alli, A. A., Adekunle, A. O., & Awotunde, J. B. (2020). Network intrusion detection based on deep learning model optimized with rule-based hybrid feature selection. *Information Security Journal: A Global Perspective*, *29*(6), 267-283.

[38] Ambusaidi, M. A., He, X., Nanda, P., & Tan, Z. (2016). Building an intrusion detection system using a filter-based feature selection algorithm. *IEEE transactions on computers*, *65*(10), 2986-2998.

[39] Prasad, M., Tripathi, S., & Dahal, K. (2020). An efficient feature selection based Bayesian and Rough set approach for intrusion detection. *Applied Soft Computing*, *87*, 105980.

[40] Karami, A. (2018). An anomaly-based intrusion detection system in presence of benign outliers with visualization capabilities. *Expert Systems with Applications*, *108*, 36-60.

[41] Tabash, M., Abd Allah, M., & Tawfik, B. (2020). Intrusion detection model using naive bayes and deep learning technique. *Int. Arab J. Inf. Technol.*, *17*(2), 215-224.

[42] Ghazali, A., Nuaimy, W., Al-Atabi, A., & Jamaludin, I. (2015). Comparison of classification models for Nsl-Kdd dataset for network anomaly detection. *Academic Journal of Science*, *4*(1), 199-206.

[43] Kevric, J., Jukic, S., & Subasi, A. (2017). An effective combining classifier approach using tree algorithms for network intrusion detection. *Neural Computing and Applications*, *28*(1), 1051-1058.

[44] Hadi, A. A. A., & Al-Furat, A. A. (2018). Performance analysis of big data intrusion detection system over random Forest algorithm. *International Journal of Applied Engineering Research*, *13*(2), 1520-1527.

[45] Elmasry, W., Akbulut, A., & Zaim, A. H. (2020). Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic. *Computer Networks*, *168*, 107042.

[46] Ahmim, A., Maglaras, L., Ferrag, M. A., Derdour, M., & Janicke, H. (2019, May). A novel hierarchical intrusion detection system based on decision tree and rules-based models. In *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)* (pp. 228-233). IEEE.

[47] Guezzaz, A., Asimi, Y., Azrour, M., & Asimi, A. (2021). Mathematical validation of proposed machine learning classifier for heterogeneous traffic and anomaly detection. *Big Data Mining and Analytics*, *4*(1), 18-24.

[48] Patel, H., Singh Rajput, D., Thippa Reddy, G., Iwendi, C., Kashif Bashir, A., & Jo, O. (2020). A review on classification of imbalanced data for wireless sensor networks. *International Journal of Distributed Sensor Networks*, *16*(4), 1550147720916404.

[49] Singh, G., & Khare, N. (2022). A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques. *International Journal of Computers and Applications*, *44*(7), 659-669.

[50] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, *60*, 19-31.

[51] Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. *Computers & Security*, *86*, 147-167.

[52] Divekar, A., Parekh, M., Savla, V., Mishra, R., & Shirole, M. (2018, October). Benchmarking datasets for anomaly-based network intrusion detection: KDD CUP 99 alternatives. In *2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)* (pp. 1-8). IEEE.

[53] Kumar, G. (2014). Evaluation metrics for intrusion detection systems-a study. *Evaluation*, *2*(11), 11-7.

[54] Axelsson, S. (2000). Intrusion detection systems: A survey and taxonomy.

[55] Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials*, *20*(4), 3453-3495.