دوفصلنامه محاسبات و سامانه‌های توزیع شده
سال هفتم، شماره ۲، شماره پیاپی ۱۴، صفحه ۴۰ تا ۵۵، سال ۱۴۰۳

ارائه مدلی برای بهبود امنیت در رایانش ابری جهت جلوگیری از حملات انکار سرویس توزیع شده با استفاده از ماشین یادگیری افراطی و هوش مصنوعی

امیر حسین نظری افشار[۱] و حمیدرضا دوست[۲]

۱- فارغ‌التحصیل کارشناسی ارشد دانشگاه آزاد تهران واحد یادگار امام خمینی(ره) شهرری

۲- دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات گرایش تجارت الکترونیک از دانشگاه آزاد واحد علوم و تحقیقات

چکیده

رایانش ابری با ارائه خدمات به صورت آنلاین به کاربران/سازمان ها در کاهش هزینه‌های زیرساخت کمک می‌کند. در دسترس بودن این خدمات از اهمیت بالایی برخوردار است، در غیر این صورت، کاربران یا سازمان‌ها باید زیان مالی یا اعتبار زیادی را متحمل شوند. در همین راستا نیز مهاجمان می‌توانند از حملات انکار سرویس توزیع شده استفاده کنند تا این سرویس های ابری برای کاربران قانونی در دسترس نباشد. در این حمله، مهاجمان بار بسیار زیادی را بر روی خدمات ارائه شده توسط سرور قربانی در شبکه عمومی وارد می‌کنند. چندین راه حل مبتنی بر یادگیری ماشین برای شناسایی حملات انکار سرویس توزیع شدهدر رایانش ابری پیشنهاد شده است که این پژوهش مدلی برای بهبود امنیت در رایانش ابری جهت جلوگیری از حملات انکار سرویس توزیع شده با استفاده از ماشین یادگیری افراطی و هوش مصنوعی ارائه می‌کند.. در این روش، یک مدل بهبود یافته SaE-ELM توسعه یافته است که می‌تواند استراتژی جهش، نرخ متقاطع و عملگر متقاطع را تطبیق دهد و قادر است به طور خودکار تعداد مناسب نورون های لایه پنهان را تعیین کند. برای ارزیابی روش پیشنهادی که برای تشخیص حمله در وب استفاده می‌شود از الگوریتم OSELM استفاده شده است و با چند روش دیگر هم‌رده مبتنی بر معیارهای مختلف برای ارزیابی در نظر گرفته شد. برای شبکه پیشنهادی ۱۵ نرون در لایه پنهان تعداد ۲۵۰۰ تکرار در آموزش و تابع هسته زیگمودی پیشنهاد شد و با استفاده از مجموعه داده NSL-KDD ارزیابی شد. روش پیشنهادی به دقت تشخیص ۸۶،۸۰، درصد با NSL-XKD دست یافت و آزمایش‌ها نشان داد که عملکرد سیستم تشخیص حمله پیشنهادی بهتر از سیستم مبتنی بر SaE-ELM اصلی و تکنیک‌های پیشرفته است. با این حال، زمان آموزش طولانی‌تری نسبت به سیستم مبتنی بر SaE-ELM نتیجه شد.

واژه‌های کلیدی: امنیت، رایانش ابری، حملات انکار سرویس توزیع شده، ماشین یادگیری افراطی و هوش مصنوعی.

تاریخچه مقاله:

تاریخ ارسال: ۱۴۰۳/۰۷/۲۵

تاریخ اصلاحات: ۱۴۰۳/۱۲/۰۱

تاریخ پذیرش: ۱۴۰۳/۱۲/۲۳

تاریخ انتشار: ۱۴۰۳/۱۲/۲۵

ایمیل نویسنده مسئول:
Root.afshar@gmail.com

۱ - مقدمه و بیان مسئله

رایانش ابری در واقع یک الگوی اصلی است که دسترسی به استخر مشترکی از منابع محاسباتی را برای کاربران ابری به صورت "بر-حسب-تقاضا" یا "پرداخت-بر اساس-مصرف" فراهم می‌کند [۱]. رایانش ابری به طور فزاینده‌ای درحال تبدیل شدن به یک مدل سازمانی محبوب است که در آن منابع محاسباتی به هنگام نیاز، براساس تقاضای کاربر در دسترس است. پیشنهاد با ارزش منحصر به فرد رایانش ابری فرصت‌های جدید را برای برآورده کردن اهداف فناوری اطلاعات و کسب‌وکار ایجاد می‌کند. در واقع رایانش ابری از فن‌آوری اینترنت برای تحویل قابلیت‌های مبتنی برIT به عنوان یک خدمات که هر کاربر نیازمند (دارای نیاز به آن) است، استفاده می‌کند. یعنی از طریق رایانش ابری می‌توان به هر چیزی از هر نقطه به هر کامپیوتری بدون هیچ گونه نگرانی در مورد هر چیزی مانند فضای ذخیره‌سازی آن، هزینه، مدیریت و غیره دسترسی داشت. محاسبات ابری را به عنوان نتیجه ای از روند تکامل فن آوری های محاسباتی مختلف نشان می دهد. رایانش ابری یک زیرساخت محیط استقرار جدید است که با وعده حمایت از خدمات مورد تقاضا مانند محاسبات، نرم افزار و دسترسی به داده‌ها به شیوه‌ای انعطاف‌پذیر با پهنای باندی معین، و منابع ذخیره‌سازی و محاسبه در گردش بدون نیاز به اطلاع کاربر نهایی از محل فیزیکی و پیکربندی سیستم تحویل دهنده‌ی خدمات، ارائه می‌شود و مدلی برای فعالسازی مناسب تقاضای شبکه برای

دسترسی به یک منبع مشترک از منابع محاسباتی قابل تنظیم که می‌تواند به سرعت با حداقل تلاش مدیریتی و یا خدمات تعاملی ارائه دهنده، مقرر و منتشر شود [۲].

رایانش ابری مزایای متعددی را از لحاظ هزینه‌ی سرمایه‌گذاری و صرفه‌جویی در هزینه‌های عملیاتی برای کاربران و سازمان‌ها ارائه می‌دهد. با وجود چنین مزایایی، موانعی نیز وجود دارند که استفاده از رایانش ابری را محدود می‌کنند. امنیت یک موضوع اصلی است که همیشه در نظر گرفته می‌شود. فقدان این ویژگی حیاتی منجر به تاثیر منفی این الگوی محاسباتی شده و در نتیجه ضررهای شخصی، حقوقی، و مالی را در پی دارد [۲].

حمله انکار سرویس توزیع شده[1] یک حمله‌ی جدی در فضای ابر محسوب می‌شود و به عنوان یکی از تهدیدات امنیتی محاسبات ابری است که برروی دسترس‌پذیری خدمات ابری تأثیر می‌گذارد. بنابراین، دفاع کردن بر علیه این حملات ضروری می‌باشد. در پژوهش [۳](مقاله پایه)، یک سیستم تشخیص حمله انکار سرویس توزیع شده معرفی شده‌است که مبتنی بر یک ماشین یادگیری افراطی تکاملی قابل تطبیق[2] است. مدل SAE-ELM با استفاده از دو ویژگی بهبود یافته است، که اولین آن، می‌تواند با مناسب‌ترین عملگر ترکیب، خود را سازگار کند. دوم، به طور اتوماتیک می‌تواند مناسب‌ترین تعداد نورون‌های لایه پنهان را تشخیص دهد. این ویژگی‌ها با بهبود توانایی یادگیری و کلاس‌بندی مدل را انجام میشود. سیستم پیشنهادی با استفاده از ۴ دیتابیس[3] ارزیابی شده‌است. تشخیص دقت به ترتیب برابر با مقادیر ۸۶,۸۰٪، ۹۸,۹۰٪، ۸۹,۱۷٪ و ۹۹,۹۹٪ در پایگاه‌داده‌های مذکور است. آزمایشات نشان می‌دهند که عملکرد سیستم تشخیص حمله پیشنهادی بهتر از سیستمی است که بر اساس SAE-ELM اصلی و حالت تکنیک‌های پیشرفته است. هرچند که نشان‌دهنده زمان آموزش طولانی‌تری نسبت به سیستم مبتنی بر SaE-ELM می‌باشد [۳]. تشخیص دادن ناهنجاری‌های سایبری و حملات به عنوان یکی از نگرانی‌هایی است که امروزه در حیطه امنیت سایبری در حال افزایش است. دانش هوش مصنوعی، مخصوصاً تکنیک‌های یادگیری ماشین می‌تواند برای دنبال کردن این مباحث استفاده شوند. هرچند، تأثیرگذاری مدل امنیتی مبتنی بر یادگیری ممکن است با توجه به ویژگی‌های امنیتی و مشخصه‌های داده‌ها متفاوت است. در پژوهش [۴]، سارکر[4] و همکاران(۲۰۲۱)، "یادگیری سایبری" را معرفی می‌کنند، یک مدل‌سازی امنیت سایبری بر اساس یادگیری ماشین با انتخاب ویژگی مربوطه، و یک تجزیه و تحلیل تجربی جامع بر روی چندین مدل امنیتی یادگیری ماشین تأثیر می‌گذارد. در مدل‌سازی کردن یادگیری سایبری، آنها یک مدل کلاس‌بندی باینری را در تشخیص دادن آنومالی و یک مدل کلاس‌بندی چند کلاسه برای چند نوع از حملات سایبری در نظر گرفته می‌شوند. برای ساختن مدل امنیتی، اول ده تکنیک کلاس‌بندی یادگیری ماشین محبوب استفاده می‌شوند، مانند بیز ساده، رگرسیون منطقی، نزول گرادیان منطقی، k نزدیک‌ترین همسایه، ماشین بردار پشتیبان، درخت تصمیم‌گیری، جنگل تصادفی، تقویت تطبیقی، افزایش گرادیان فوق‌العاده، و همچنین تجزیه و تحلیل تفکیک خطی اعمال می‌شوند. سپس مدل امنیتی مبتنی بر شبکه عصبی مصنوعی با در نظر گرفتن چندین لایه پنهان معرفی می‌شوند. تأثیرگذاری این مدل‌های امنیتی مبتنی بر یادگیری با هدایت کردن دامنه‌ای از آزمایشات، با استفاده از دو تا از محبوبترین پایگاه‌داده‌های امنیتی[5]، بوده است. در این پژوهش نیز هدف است تا مدلی ترکیبی مبنی بر پژوهش های [۳, ۴] جهت امنیت ابر ارائه شود تا پاسخگویی سوال مهم پژوهش "آیا امکان ارائه مدلی برای بهبود امنیت در رایانش ابری جهت جلوگیری از حملات انکار سرویس توزیع شده با استفاده از ماشین یادگیری افراطی و هوش مصنوعی امکانپذیر است؟" باشد.

۲- کارهای مرتبط

مقاله‌ای برای کاهش حملات انکار سرویس توزیع شده در رایانش ابری ارائه شد که نویسندگان مقاله معتقدند که رایانش ابری به کاربران خود راه راحت تری جهت استفاده از منابع و مدلی ارائه می کند که در آن کاربران بر اساس میزان استفاده از منابع خود هزینه دریافت می کنند. این مدل به عنوان "پرداخت به ازای هر استفاده" شناخته می

[1] Distributed denial of service(DDOS)
[2] Self-Adaptive Evolutionary Extreme Learning Machine (SAE-ELM).
[3] NSL-KDD ،ISCX IDS 2012 ،UNSW-NB15 و CICIDS 2017
[4] Sarker et.al.
[5] UNSW-NB15 و NSL-KDD

شود. کاربران می توانند در هر زمان از هر کجا به خدمات ابری دسترسی داشته باشند. آنها فقط به یک اتصال اینترنتی فعال نیاز دارند. با وجود همه این مزایای ابر، این تکنولوژی با معایبی نیز همراه است. موضوع مربوط به امنیت ابر امروزه بزرگترین نگرانی است. چون همه چیز در ابر به شکل مجازی است، مهاجمان و هکرها شبکه را با بسته‌های حمله پر می‌کنند و شناسایی این بسته‌ها دشوار است. حمله انکار سرویس توزیع شده یک حمله اختصاصی ابری است که در آن منبع حمله همیشه بیش از یک است و چندین ماشین با ارسال بسته‌هایی با سربار داده های بزرگ به کاربر حمله می کند. چنین حملاتی با غلبه بر شبکه با ترافیک ناخواسته، منابع را در دسترس کاربر قرار نمی دهد. در این مقاله تحقیقاتی هدف اصلی فیلتر کردن بسته‌های داده با سربار داده‌های بزرگ برای جلوگیری از حمله انکار سرویس توزیع شده است و میانگین زمان شکست امنیتی محاسبه می‌شود تا بتوان یک طرح پویا جایگزین را اتخاذ کرد [۵].

مقاله‌ای برای تشخیص مؤثر حملات انکار سرویس توزیع شده اخیر: رویکرد یادگیری عمیق ارائه شد و نویسندگان مقاله معتقدند که انکار سرویس توزیع شده) انکار سرویس توزیع شده (یک تهدید غالب برای در دسترس بودن خدمات آنلاین به دلیل اندازه و فراوانی آنهاست. با این حال، توسعه یک مکانیسم امنیتی موثر برای محافظت از شبکه در برابر این تهدید یک چالش بزرگ است زیرا انکار سرویس توزیع شده از رویکردهای حمله مختلف همراه با چندین ترکیب ممکن استفاده می‌کند. علاوه بر این، بسیاری از مدل‌های مبتنی بر یادگیری عمیق دارای هزینه پردازش بالایی هستند یا ممکن است برای شناسایی حملات انکار سرویس توزیع شده گزارش‌شده اخیر عملکرد خوبی نداشته باشند زیرا این مدل‌ها از مجموعه داده‌های قدیمی برای آموزش و ارزیابی استفاده می‌کنند. برای پرداختن به مسائلی که قبلا ذکر شد، این مقاله مدلی را پیشنهاد می‌کند، یک چارچوب سیستم تشخیص نفوذ یکپارچه، که مجموعه‌ای از الگوریتم‌های مهندسی ویژگی را با شبکه عصبی عمیق ترکیب می‌کند. انتخاب ویژگی مجموعه بر اساس پنج طبقه‌بندی کننده یادگیری ماشین است که برای شناسایی و استخراج مرتبط‌ترین ویژگی‌های مورد استفاده توسط مدل پیش‌بینی‌کننده استفاده می‌شود. این رویکرد عملکرد مدل را با پردازش تنها زیرمجموعه‌ای از ویژگی‌های مرتبط بهبود می‌بخشد و در عین حال نیاز محاسباتی را کاهش می‌دهد. این مقاله عملکرد مدل را بر اساس، یک مجموعه داده مدرن و واقعی[6] متشکل از ترافیک عادی و حمله انکار سرویس توزیع شده ارزیابی می کند. این ارزیابی معیارهای اعتبارسنجی مختلف مانند دقت، دقت، امتیاز F1 و بازخوانی را برای استدلال در مورد اثربخشی چارچوب پیشنهادی در برابر سیستم تشخیص نفوذ های پیشرفته در نظر می گیرد [۶].

مقاله‌ای برای تجزیه و تحلیل حملات انکار سرویس توزیع شده در رایانش ابری به صنعت فناوری اطلاعات پاکستان ارائه شد که نویسندگان مقاله معتقدند که فناوری محاسبات ابری در حال توسعه مداوم و با چالش‌های متعدد در زمینه امنیت است. در این زمینه، یکی از نگرانی‌های اصلی برای رایانش ابری، قابل اعتماد بودن خدمات ابری در صنعت فناوری اطلاعات پاکستان است. این مشکل نیاز به حل سریع دارد زیرا سازمان‌های فناوری اطلاعات در پاکستان که خدمات ابری را اتخاذ می‌کنند، در معرض افزایش هزینه‌ها در حالی که در معرض خطر بیشتری هستند، قرار خواهند گرفت. نظرسنجی انجام شده سیستم تشخیص نفوذ در اوت ۲۰۰۸ تایید می کند که امنیت مانع اصلی برای کاربران ابری در پاکستان است. در این مقاله یک مدل مبتنی بر ریاضی را برای برآورد نیازهای کاربر در مورد سرمایه‌گذاری منابع خود بر اساس تئوری صف پیشنهاد می‌شود تا بر این مسائل امنیتی در فناوری ابر غلبه شود. آنها در حال اتخاذ یک سیستم و تجزیه و تحلیل دنیای واقعی با استفاده از آزمایش‌های مجموعه داده هستند. در این مقاله، راه حلی برای غلبه بر حملات انکار سرویس توزیع شده در یک محیط رایانش ابری در خدمات فناوری اطلاعات پاکستان پیشنهاد شده است. راه‌حل پیشنهادی بر اساس قانون ترکیبی Dempsters تجزیه و تحلیل اثبات مخلوط انواع مختلف حملات ابری در صنایع فناوری اطلاعات در پاکستان است [۷].

مقاله‌ای برای جلوگیری از حملات انکار سرویس توزیع شده در رایانش ابری با استفاده از الگوریتم خوشه‌ای ارائه شد. نویسندگان مقاله معتقدند که امنیت یکی از موضوعات و بحثهای مهم در هر سیستمی به حساب می‌آید به خصوص سیستمهایی که به صورت مجازی کار می‌کنند. در

[6] CICDDoS2019

صورتی که امنیت سیستم به خطر بیفتد آسیبهای جبران ناپذیری را وارد میکند. مبحث رایانش ابری سطح وسیعی از سیستمها را در دنیای مجازی دربرمیگیرد بنابراین داشتن ایمنی مناسب موضوعی قابل توجه دراین زمینه میباشد. به این منظور دراین مقاله سعی بر آن شده تا راهکاری برای امنیت رایانش ابری ارائه داده شود. طی بررسیهای به عمل آمده الگوریتم آستانه تطبیق پذیر بهینهای برای آن پیشنهاد داده شده است. ابتدا مفاهیم پایهای در رایانش ابری و معماری کلی آن شرح داده شده، در بخش بعد انواع حملات انکار سرویس توزیع شده تشریح شده است در ادامه به تشریح حملاتی که در رایانش ابری صورت میگیرد پرداخته شده است و همچنین تاثیر شبکه‌های مبتنی بر نرم افزار در جلوگیری از حملات بیان شده و مدل تلفیقی گرافیکی شبکه-های مبتنی بر نرم افزار و قسمتهای مختلف آن به طور کامل شرح داده شده است. در بخش بعد به بررسی مزایا و معایب دو نوع الگوریتم خوشهای پرداخته شده است، و در آخر الگوریتم آستانه تطبیق پذیر بهینهای برای تشخیص نفوذ و جلوگیری از حمله پیشنهاد داده شده است [۸].

مقاله‌ای برای بررسی روش‌های مقابله با حملات انکار سرویس توزیع شده در محیط محاسبات ابری ارائه شد. نویسندگان مقاله معتقدند که محاسبات ابری به عنوان یک تکنولوژی برتر می باشد، که سرویس‌هایی را بر اساس تقاضای کاربران تامین می‌کند. حال این تقاضاها مسایلی از قبیل امنیت داده ها، در دسترس بودن و غیره را بوجود می آورد. حال در این بین حملاتی از قبلی حملات انکار سرویس و انکار سرویس توزیع شده، در دسترس بودن این شبکه را تحت تاثیر قرار می دهند. حملات انکار سرویس توزیع شده، حملات واضحی می باشند که برای جلوگیری از استفاده مشروع از یک سرویس می باشند. و همچنین این نوع از حملات به عنوان یکی از تهدیدات بزرگ نه تنها برای محاسبات ابری بلکه برای اینترنت هم محسوب می شوند. حاملیان حملات انکار سرویس توزیع شده، به فکر تخریب سرورهای مختلف می باشند تا ناراحتی برای کاربران ایجاد کرده یا در برخی موارد ضررهای مالی فراوانی را به شرکت هایی که به صورت بر خط به کسب و کار می پردازند، به همراه داشته باشند، در این مقاله، آنها انواع روش های مقابله با حملات انکار سرویس توزیع شده را مورد بررسی قرار داده و مزایا و معایب هر یک را مورد تجزیه و تحلیل قرار دادند [۹].

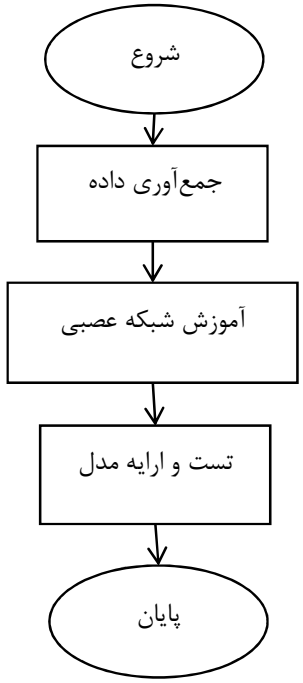
۲- تحلیل روش پیشنهادی

روش پیشنهادی بسیاری از ویژگی‌های جدید را برای یافتن مقادیر بهینه پارامترهای وزن‌های پیوند مخفی ورودی و بایاس‌های پنهان[7] به صورت کارآمدتر ترکیب کرده است. می-تواند به طور خودکار بهترین استراتژی جهش مناسب را برای یک فرد از جمعیت در طول هر نسل انتخاب کند. عامل پوسته پوسته شدن مورد استفاده در جهش به طور تصادفی از یک محدوده از پیش تعیین شده برای هر فرد ایجاد می شود. نرخ متقاطع به طور خودکار در طول کل فرآیند تکامل به روز می شود. اما در این مدل تنها از یک اپراتور متقاطع (یونیفرم) استفاده شده است. فرآیند جستجو برای یافتن مقادیر بهینه پارامترهای این مدل را می توان با ترکیب چند عملگر متقاطع بیشتر کرد. زیرا انتخاب بهینه عملگرهای متقاطع در مراحل مختلف فرآیند بهینه‌سازی در مقابل یک عملگر واحد برای فرآیند کامل متفاوت است. این به دلیل قابلیت های اکتشافی متمایز اپراتورها است. چندین کار استفاده از چند عملگر را به جای یک عملگر واحد برای بهبود عملکرد در انواع مختلف برنامه ها پیشنهاد کرده اند. این به ما انگیزه می دهد تا از چندین اپراتور متقاطع برای بهبود بیشتر عملکرد روش پیشنهادی استفاده کنیم. ما مدل اصلی SaE-ELM را اصلاح کرده‌ایم تا بهترین اپراتور متقاطع مناسب برای یک فرد را از بین استخر موجود در یک نسل، به‌طور خودکار انتخاب کنیم. این منجر به بهینه سازی بهتر پارامترهای مدل وزن‌های پیوند مخفی ورودی و بایاس‌های پنهان می شود. که در نهایت باعث بهبود دقت آموزش و تست مدل می شود. علاوه بر این، تعیین خودکار تعداد مناسب نورون‌های لایه پنهان نیز با استفاده از تکنیک پیشنهادی گنجانده شده است، که نیاز به تنظیم دستی را حذف می‌کند. سپس مدل اصلاح شده برای شناسایی حملات انکار سرویس توزیع شده در رایانش ابری استفاده می-شود.

براساس شکل۱ اطلاعات مربوط به حمله انکار سرویس توزیع شده جمع‌آوری می‌شود و این داده‌ها به عنوان ورودی به شبکه عصبی داده می‌شود. کلیه موارد سبب تنظیم

[7] Extreme Learning Machine

پارامترهای شبکه عصبی برای تولید یک مدل قابل اطمینان و ایده‌آل انجام می‌شود. بعد از تست مجموعه داده و اطمینان از صحت روش پیشنهادی مدل آن به عنوان یک موتور تشخیص قابل استفاده است.



شکل۱: بلوک دیاگرام روش پیشنهادی

مدل‌های مختلف یادگیری ماشین با در نظر گرفتن مسائل ذکر شده در بالا، ممکن است با توجه به قابلیت‌های یادگیری از داده‌های امنیتی، عملکرد متفاوتی داشته باشند. دلیل آن این است که اثربخشی یک مدل امنیتی مبتنی بر یادگیری ممکن است بسته به اهمیت ویژگی‌های امنیتی مرتبط و ویژگی‌های داده متفاوت باشد. در سناریوی دنیای واقعی، مسائل امنیت سایبری ممکن است با تعداد زیادی ویژگی امنیتی، چندین کلاس حمله شناخته شده یا ناشناخته یا ناهنجاری ها درگیر باشد. بنابراین، یک تکنیک انتخاب ویژگی موثر و یک مدل طبقه‌بندی قوی معمولاً شامل ساخت یک سیستم تشخیص نفوذ هوشمند است. انواع مختلفی از تکنیک‌های یادگیری ماشین و کاربرد آن‌ها در حوزه امنیت سایبری، به طور خلاصه در سارکر و همکاران مورد بحث قرار گرفته‌اند [۴]. با این حال یک تحلیل تجربی دقیق با در نظر گرفتن موارد ذکر شده در بالا برای تصمیم گیری هوشمندانه در منطقه مورد نیاز است. بنابراین، هدف ما ارائه یک تحلیل تجربی جامع در مورد اثربخشی مدل‌های امنیتی مختلف مبتنی بر یادگیری ماشین با در نظر گرفتن مسائل است تا تصمیمی هوشمندانه در چنین سناریوهای متنوع دنیای واقعی در منطقه اتخاذ کنیم. در SaE-ELM، بهترین استراتژی جهش برای یک بردار هدف به طور خودکار بر اساس میزان موفقیت آن استراتژی در نسل‌های گذشته انتخاب می‌شود. با این حال، تنها یک اپراتور متقاطع (یکنواخت) در طول فرآیند تکامل کامل استفاده می‌شود. در بسیاری از مطالعات، مشخص شده است که استفاده از عملگرهای متقاطع مختلف در طول مراحل مختلف فرآیند تکامل، می‌تواند فرآیند جستجوی راه‌حل بهینه را بهبود بخشد. بنابراین، برای بهبود بیشتر عملکرد SaE-ELM، در روش پیشنهادی، از مجموعه ای از اپراتورهای متقاطع به جای یک واحد استفاده می کنیم. بهترین عملگر متقاطع مناسب برای تولید یک بردار آزمایشی خاص به طور خودکار بر اساس میزان موفقیت آن عملگر در نسل‌های گذشته انتخاب می‌شود. تعیین خودکار تعداد مناسب نورون های پنهان نیز در مدل اصلاح شده گنجانده شده است. مدل پیشنهادی ماشین یادگیری افراطی تکاملی خود تطبیقی با سازگاری متقاطع نامیده می شود.

سازگاری اپراتور متقاطع: برای این منظور از بردار به نام انتخابگر متقاطع و احتمالات عملگرهای متقاطع مختلف به همراه بردار نرخ متقاطع استفاده می شود. طول انتخابگر متقاطع برابر با اندازه جمعیت (ρ) است و عناصر آن با مقادیر تصادفی در محدوده [۰،۱] مقداردهی اولیه می شوند. ما از چهار عملگر متقاطع استفاده کرده‌ایم، یعنی حساب کل، یکنواخت، حلقه و اکتشافی. احتمالات آنها در طول نسل n به صورت qs,v برای $s = 1$ تا ۴ نشان داده می شود. در ابتدا، همه عملگرها احتمال مساوی برای انتخاب شدن دارند بنابراین احتمالات آنها ۰,۲۵ تنظیم می شود.

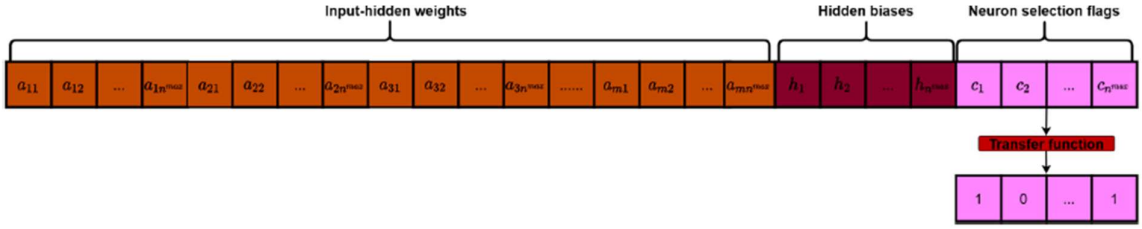
برای هر بردار آزمایشی، یک عدد تصادفی در محدوده [۰،۱] تولید می‌شود. اگر مقدار آن بزرگتر یا مساوی با مقدار نرخ متقاطع باشد، آنگاه متقاطع انجام نمی شود و بردار آزمایشی همان بردار هدف است. اگر مقدار تصادفی کمتر از نرخ متقاطع باشد، متقاطع انجام می شود. انتخاب یک عملگر متقاطع به مقادیر انتخابگر متقاطع و احتمالات اپراتورها بستگی دارد. اگر مقدار انتخابگر متقاطع کمتر از احتمال کل حساب $(q\ 1,v)$ باشد، از آن استفاده می شود. اگر مقدار انتخابگر متقاطع بیشتر از احتمال کل محاسبات باشد اما کمتر

از مجموع احتمالات کل حساب و یکنواخت باشد (q 2,v)، از یکنواخت استفاده می شود. اگر مقدار انتخابگر متقاطع بیشتر از مجموع احتمالات کل و یکنواخت باشد اما کمتر از مجموع احتمالات کل، یکنواخت و حلقه (q 3,v) باشد، از متقاطع حلقه استفاده می شود. اگر مقدار انتخابگر متقاطع به هیچ یک از این محدوده ها تعلق نداشته باشد، از متقاطع اکتشافی استفاده می شود. پس از تعداد ثابتی از نسل ها به نام دوره یادگیری متقاطع (lp c)، احتمال عملگرهای متقاطع به صورت زیر به روز می شود.

$$q_{s,v} = \frac{u_{s,v}}{\sum_{s=1}^{4} u_{s,v}}, Where\ , u_{s,v} = \frac{\sum_{l=p-l}^{p-1} np_{s,v}^{c}}{\sum_{l=p-l}^{p-1} np_{s,v}^{c} + \sum_{l=p-l}^{p-1} nf_{s,v}^{c}} + \psi \quad (1)$$

در اینجا، $np_{s,v}^{c}$، v و $nf_{s,v}^{c}$ تعداد بردارهای آزمایشی را نشان می‌دهند که با عملگر s در نسل v تولید می‌شوند و پس از مرحله انتخاب در نسل بعدی v+ 1 وارد می‌شوند و به ترتیب در نسل بعدی وارد نمی‌شوند. برای جلوگیری از نرخ موفقیت تهی احتمالی از یک ثابت مثبت کوچک ψ استفاده می شود.

تعیین خودکار نورون های پنهان: تعداد نورون های لایه پنهان مورد نیاز در SaE-ELM کمتر از پارامترهای وزن‌های پیوند مخفی ورودی و بایاس‌های پنهان است. اما نیاز به تنظیم دستی تعداد نورون ها وجود دارد. برای غلبه بر این مشکل، ما تعیین خودکار تعداد مناسب نورون‌های لایه پنهان را در مدل پیشنهادی خود وارد کردیم. این مدل قادر است به طور خودکار تعداد مناسب نورون های پنهان را از یک محدوده، برای هر بردار راه حل در یک نسل انتخاب کند. ما یک کران بالایی بر روی تعداد نورون‌های پنهان می‌گیریم (n max)، و تعداد نورون‌ها (n) برای یک بردار محلول خاص به‌طور خودکار از n max انتخاب می‌شود. شکل ۲ رمزگذاری یک بردار راه حل پیشنهاد شده در مدل پیشنهادی ما را نشان می دهد. قسمت اول وزن پیوندهای پنهان ورودی را نشان می دهد و قسمت دوم سوگیری های پنهان را نشان می دهد. بخش سوم پرچم هایی را برای انتخاب نورون نشان می دهد. همه عناصر بردار حل در محدوده [۱،۱] پیوسته هستند، بنابراین، نمی توان از آنها به عنوان پرچم، مستقیما استفاده کرد. از تابع انتقال برای نگاشت این مقادیر به ۰ یا ۱ استفاده کرده ایم. مقدار صفر نشان می دهد که نورون مربوطه غیرفعال شده است در حالی که یک مقدار نشان دهنده یک نورون فعال است.



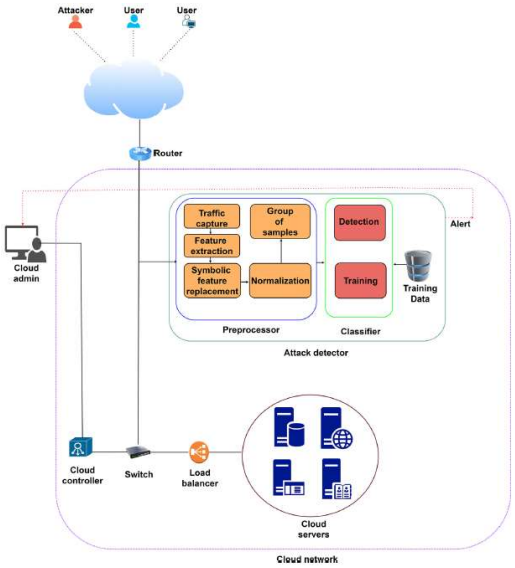
شکل ۲: رمزگذاری محلول در SaE-ELM-Ca

شکل ۳ سیستم تشخیص حمله انکار سرویس توزیع شده پیشنهادی را با مدل "ماشین یادگیری افراطی تکاملی خود تطبیقی با تطبیق متقاطع[۸]" نشان می دهد. آشکارساز حمله در نزدیکی روتر نصب شده است که شبکه ابری را به اینترنت متصل می کند. در کار حاضر، ما یک اتصال واحد به اینترنت را فرض می کنیم. مورد اتصالات متعدد را می توان با نصب یک آشکارساز جداگانه برای هر اتصال به طور مشابه انجام داد. آشکارساز حمله دارای دو جزء پیش پردازنده و یک طبقه بندی کننده است.

پیش پردازش: این ماژول ترافیک ورودی به ابر از اینترنت را ضبط می کند. سپس ترافیک گرفته شده را به گروه هایی از نمونه ها تبدیل می کند. این گروه ها برای تشخیص حمله به طبقه بندی کننده اعمال می شوند.

اولین قدم استخراج ویژگی های مفیدی است که برای طبقه بندی نمونه ها به عنوان حمله یا عادی استفاده می شود. در سیستم پیشنهادی، از ۹ ویژگی استفاده شده است، اطلاعات بیشتر در مورد ویژگی های مورد استفاده در جدول ۱ آورده شده است.

[8] SaE-ELM-Ca



شکل ۳: سیستم تشخیص حمله انکار سرویس توزیع شده پیشنهادی

جدول۱: ویژگی های مورد استفاده در سیستم پیشنهادی

S.N.	Feature name	Type
1	Flags	Symbolic
2	Flow duration	Continuous
3	Flow inter-arrival time	Continuous
4	Number of bytes from destination to source	Continuous
5	Number of bytes from source to destination	Continuous
6	Number of packets from destination to source	Continuous
7	Number of packets from source to destination	Continuous
8	Protocol name	Symbolic
9	Service name	Symbolic

گام بعدی پرداختن به ویژگی های نمادین داده ها است. رمزگذاری تک داغ برای تبدیل ویژگی های نمادین به ویژگی های گسسته استفاده می شود. در این، یک مقدار ویژگی به عنوان بردار مقادیر باینری نمایش داده می شود. فرض کنید یک ویژگی «protocol_name» وجود دارد که می‌تواند سه مقدار ««tcp، udp»» یا «icmp» داشته باشد. در این مورد، «tcp» به صورت (۱،۰،۰)، «udp» به صورت (۰،۱،۰) و «icmp» به صورت (۰،۰،۱) نمایش داده می‌شود. پس از آن، عادی سازی انجام می شود، که مقادیر ویژگی را در محدوده [۰،۱] مقیاس می کند. در نهایت، گروه‌هایی از نمونه‌ها برای ترافیک ضبط شده در طول هر دوره t ساخته می‌شوند. در اینجا هر نمونه از گروه به شکل $\Omega_i = [\Omega_{i1}, \Omega_{i2}, \Omega_{i3}, \dots, \Omega_{im}]$ می باشد.

آماده‌سازی داده‌ها شامل ناهنجاری‌ها و حملات، رمزگذاری ویژگی، و مقیاس‌بندی بر اساس ویژگی‌های مجموعه داده‌های داده شده است [۴].

مقیاس‌بندی ویژگی‌ها: مقیاس بندی ویژگی ها به عنوان نرمال سازی داده ها در وظیفه پیش پردازش داده ها نیز شناخته می شود. همه ویژگی‌های امنیتی در یک مجموعه داده ممکن است از نظر توزیع داده یکسان نباشند و از ویژگی به ویژگی متفاوت باشند. برای برخی از نقاط داده، مقدار بسیار کم است در حالی که برای برخی از نقاط داده، بسیار بیشتر است. بنابراین، ما از مقیاس‌سنج استاندارد[9] استفاده می‌کنیم، یک روش مقیاس‌بندی داده که برای نرمال‌سازی محدوده مقادیر ویژگی‌ها با مقدار میانگین = ۰ و انحراف استاندارد = ۱ استفاده می‌شود.

تقسیم داده‌ها: از آنجایی که هدف ما ایجاد مدل سازی امنیتی مبتنی بر یادگیری است، تقسیم داده ها می تواند به عنوان یک بخش مهم در نظر گرفته شود. دلیل آن این است که یک مدل امنیتی خوب ممکن است بر اساس تقسیم بد داده ها باشد. بنابراین، برای ساخت یک مدل و ارزیابی منصفانه، ابتدا داده‌های منابع داده را به عنوان داده ورودی در نظر می‌گیریم و با استفاده از تکنیک اعتبارسنجی متقاطع k برابر می‌کنیم. طبق تکنیک اعتبارسنجی متقابل k fold، ابتدا داده‌های ورودی ذکر شده در بالا را به‌طور تصادفی به k زیرمجموعه‌های متقابلاً منحصر به فرد یا folds, d1, d2, … , dk تقسیم می‌کنیم. هر فولد دارای اندازه تقریبا مساوی از نمونه های داده است. مدل برای تکمیل فرآیند کلی نیاز به k تکرار دارد. بنابراین، در هر تکرار i، ما از تمام نمونه‌های داده همه فولدها به جز di به عنوان مجموعه داده آموزشی استفاده می‌کنیم که می‌تواند برای ساختن مدل امنیتی حاصل استفاده شود. برای هدف ارزیابی از di به عنوان مجموعه داده آزمایشی در هر تکرار استفاده می شود. در نهایت، میانگین نتیجه به عنوان نتیجه مدل در نظر گرفته می شود.

رتبه بندی و انتخاب ویژگی: انتخاب ویژگی در حوزه امنیت سایبری می‌تواند درک بهتری از داده‌های امنیتی، راهی برای ساده‌سازی مدل امنیتی با کاهش هزینه محاسباتی یا پیچیدگی مدل، و همچنین ارائه نتایج قابل‌توجه در یک مدل مبتنی بر یادگیری ماشینی را فراهم کند. مجموعه داده‌های امنیتی ممکن است حاوی داده‌هایی با ابعاد بالا باشد و برخی از آنها ممکن است با ناهنجاری‌ها یا حملات مرتبط باشند، در حالی که برخی از آنها همبستگی کمتری دارند یا اصلاً

[9] Standard Scaler

همبستگی ندارند. بنابراین، به منظور ایجاد یک مدل امنیتی مبتنی بر طبقه‌بندی یادگیری ماشین، همه ویژگی‌های امنیتی در یک مجموعه داده ممکن است حاوی جزئیات مهمی نباشند. علاوه بر این، به دلیل مشکل بیش از حد برازش، پردازش بیشتر با تمام ویژگی‌های امنیتی می تواند نتایج ضعیفی را ارائه دهد. بنابراین، انتخاب ویژگی امنیتی نه تنها برای کاهش هزینه محاسباتی بلکه برای ایجاد یک مدل امنیتی کارآمدتر با نرخ دقت بالاتر مورد نیاز است. بنابراین، انتخاب ویژگی امنیتی به عنوان روشی در نظر گرفته می‌شود که می‌تواند برای فیلتر کردن آن دسته از ویژگی‌هایی که اهمیت کمتر، زائد یا بی‌تأثیر بر مدل‌سازی دارند، از مجموعه داده امنیتی داده شده مورد استفاده قرار گیرد.

برای دستیابی به این هدف، ابتدا همبستگی ویژگی‌های امنیتی را که به همبستگی پیرسون معروف است محاسبه کرده و بر اساس آن رتبه‌بندی می‌کنیم. انتخاب ویژگی مبتنی بر همبستگی بر این فرضیه استوار است: «زیر مجموعه‌های ویژگی خوب شامل ویژگی‌هایی هستند که به شدت با کلاس هدف همبستگی دارند، اما با یکدیگر همبستگی ندارند یا کمتر همبستگی دارند». اگر Xand Y دو متغیر زمینه‌ای تصادفی را نشان دهد، ضریب همبستگی بین Xand Y به صورت تعریف می‌شود [۴]:

$$r(X,Y)=\frac{\sum_{i=1}^{n}(X_i-\bar{X})(Y_i-\bar{Y})}{\sqrt{\sum_{i=1}^{n}(X_i-\bar{X})^2}\sqrt{\sum_{i=1}^{n}(Y_i-\bar{Y})^2}} \quad (۲)$$

در زمینه آمار، فرمول معادله (۲) اغلب برای تعیین اینکه این رابطه بین آن دو متغیر Xand Y چقدر قوی است استفاده می شود. در مدل‌سازی امنیتی ما، هرچه این مقدار بالاتر باشد، ویژگی امنیتی برای ساختن مدل امنیتی مبتنی بر یادگیری حاصل اهمیت بیشتری دارد. به عنوان مثال، مقدار ۱ (حداکثر) به این معنی است که نتیجه مدل امنیتی مبتنی بر یادگیری مستقیماً با آن ویژگی امنیتی مرتبط است و ۰ (min) به این معنی است که خروجی مدل اصلاً به آن ویژگی امنیتی بستگی ندارد. . بنابراین، در محدوده تحلیل ما، مقادیر ضریب همبستگی هر ویژگی امنیتی را در مدل‌سازی طبقه‌بندی باینری برای تشخیص ناهنجاری‌ها و مدل‌سازی طبقه‌بندی چند طبقه برای شناسایی انواع مختلف حملات محاسبه می‌کنیم.

طبقه بندی: طبقه بندی مورد استفاده در سیستم تشخیص حمله پیشنهادی مدل "ماشین یادگیری افراطی تکاملی خود تطبیقی با تطبیق متقاطع" پیشنهادی ما است. گروه‌هایی از نمونه‌های آماده‌شده توسط پیش‌پردازنده را به‌عنوان ورودی می‌گیرد و هر نمونه از گروه‌ها را به‌عنوان عادی یا حمله طبقه‌بندی می‌کند. این یک مدل تحت نظارت است و قبل از استفاده برای تشخیص حمله نیاز به آموزش با نمونه های برچسب دار دارد.

آموزش: برای آموزش طبقه بندی کننده، از مجموعه داده آموزشی استفاده می شود و در پایان، بهترین بردار راه حل در جامعه، مقادیر بهینه وزن پیوندهای پنهان ورودی و بایاس های لایه پنهان را نشان می دهد. در این مرحله، طبقه‌بندی‌کننده آموزش داده می‌شود.

۵- نتایج و شبیه سازی

حمله انکار سرویس توزیع شده یک تهدید امنیتی جدی برای محاسبات ابری است که بر در دسترس بودن خدمات ابری تأثیر می گذارد. بنابراین دفاع در برابر این حملات امری ضروری می شود. در روش پیشنهادی، ما یک سیستم تشخیص حمله انکار سرویس توزیع شده را بر اساس یک ماشین یادگیری افراطی تکاملی خود تطبیق‌پذیر ارائه می‌کنیم. مدل "ماشین یادگیری افراطی تکاملی خود تطبیق‌پذیر[10]" با ترکیب دو ویژگی دیگر بهبود یافته است. اولا، می تواند بهترین اپراتور متقاطع مناسب را تطبیق دهد. ثانیا، می تواند به طور خودکار تعداد مناسب نورون های لایه پنهان را تعیین کند. این ویژگی ها قابلیت های یادگیری و طبقه بندی مدل را بهبود می بخشد. در این بخش روش پیشنهادی گفته شده را مورد آزمایش قرار می‌دهیم و نتایج مراحل مختلف ارزیابی را نمایش خواهیم داد و این ارزیابی در نرم افزار مطلب و وکا انجام شده است.

مجموعه داده: مجموعه داده KDD شامل مجموعه‌ای از داده‌ها است که براساس ۴۱ ویژگی مشتق شده برای هر اتصال و همچنین یک برچسب برای آن اتصال است که وضعیت اتصال را براساس دو نوع عادی و حمله خاصی مشخص می‌کند این ویژگی‌ها به صورت پیوسته، گسسته و یا نمادین هستند که در محدوده‌های متفاوتی قرار دارند و در چهار دسته طبقه‌بندی می‌شوند [۳]:

[10] SaE-ELM

- ویژگی‌های ذاتی یک اتصال شامل ویژگی‌های اساسی یک اتصال پروتکل هدایت انتقال است. به عنوان مثال، مدت زمان اتصال، نوع پروتکل، خدمات شبکه (شبکه راه دور و ...) و ... .
- ویژگی محتوایی در اتصال به منظور ارزیابی بسته‌های پروتکل هدایت انتقال اصلی استفاده می‌شود، به‌عنوان مثال، تعداد ورودهایی که ناموفق بوده‌اند.
- ویژگی‌های میزبانی یکسان مربوط به بررسی اتصالات در دو ثانیه گذشته است که در اتصال فعلی مقصد یکسانی دارند و محاسبه آمار مربوط به رفتار پروتکل، خدمات و ... .
- ویژگی‌های مشابه براساس خدمات مشابه مربوط به بررسی اتصالات در دو ثانیه گذشته است که در اتصال فعلی خدو خدمات یکسانی استفاده می‌کنند.

مجموعه داده‌ها شامل انواع حمله‌های مختلفی است، که در یکی از چهار دسته زیر گروه‌بندی می‌شوند [۱۰]:

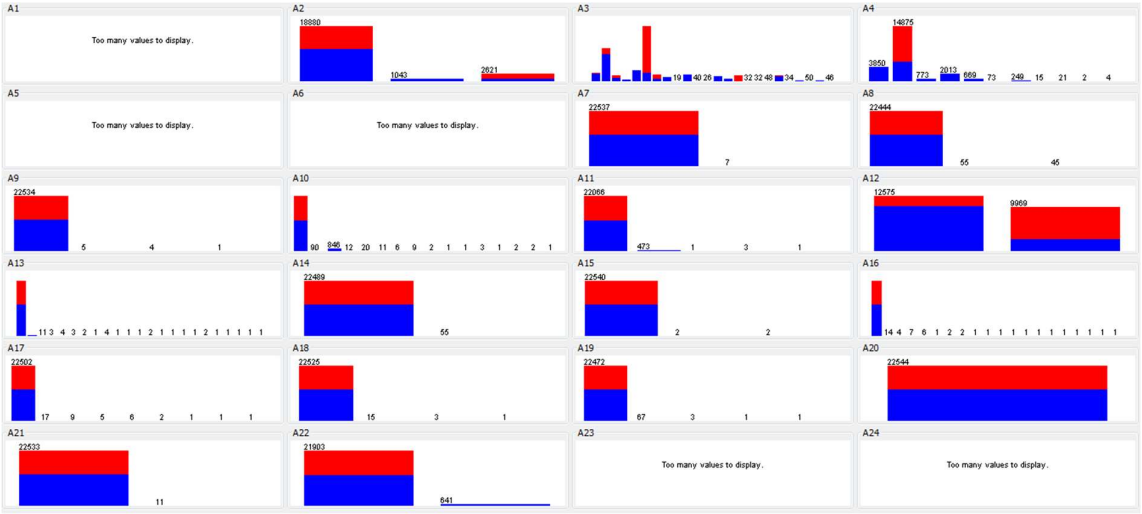
- **نرم‌افزار پروب**[11]: اسکن سیستم میزبان و اسکن پورت که به عنوان پیش‌زمینه‌هایی برای حملات دیگر هستند. مهاجم شبکه را برای جمع‌آوری اطلاعات و یا پیدا کردن آسیب‌پذیری‌های شناخته‌شده اسکن می‌کند
- **حمله انکار سرویس:** ایجاد بیش از حد درخواست‌هایی جهت استفاده از منابع محاسباتی یا حافظه‌ای، به‌طوری که کاربران قانونی از دسترسی به این منابع منع شوند و سرویس از دسترس خارج شود
- **حملات کاربر از راه دو**[12]ر: دسترسی‌های غیرمجاز دستگاه راه دور با توجه به بهره‌برداری از آسیب‌پذیری ماشین‌های داخلی.
- حمله کاربر به ریشه[13]: دسترسی غیرمجاز به کاربران فوق‌العاده (ریشه) و استفاده از امتیازات محلی با استفاده از حساسیت سیستم. به عنوان مثال، سرریز بافر.

سیستم‌های سایبری و گروه فناوری آزمایشگاه لینکلن ام‌آی‌تی[14]، مجموعه داده ترافیک شبکه را جمع‌آوری کردند. این آزمایشگاه لن[15] در نیروی هوایی ایالات متحده با حملات متعدد شبیه‌سازی شد و نه هفته از داده تی‌سی‌پی دامپ[16] را جمع‌آوری کرد. این مجموعه داده توسط شبیه‌سازی حملات مختلف بر روی سیستم عامل‌های مختلف مانند ویندوز، یونیکس و غیره جمع‌آوری شده است. چهار گیگابایت از داده فشرده شده تی‌سی‌پی دامپ خام با پنج میلیون سوابق اتصال پردازش شدند. یک اتصال بعنوان دنباله‌ای از بسته‌های پروتکل هدایت انتقال انتقالی بین برخی از مهرهای زمانی تعریف شده است. در یک اتصال خاص، داده از آدرس آی پی منبع به آدرس آی پی هدف جریان می‌یابند. حالا این مجموعه داده، مجموعه داده بنچمارک[17] برای پژوهش در سیستم تشخیص نفوذ ارایه شده است [۱۱].

تجزیه‌وتحلیل بیشتر این مجموعه داده نشان می‌دهد که مسائلی وجود دارند که بر ارزیابی عملکرد سیستم تشخیص نفوذ تاثیر می گذارند. یک مجموعه داده جدید[18] توسط [۱۱] برای غلبه بر ۱۷۰ مسئله عنوان شده پیشنهاد می‌شود. رکوردهای زائد و تکراری به منظور کاهش بزرگی طبقه‌بندکننده‌ها حذف شده است. این مجموعه داده متشکل از ۱۴۸،۵۱۷ رکورد اتصال در هر دو مجموعه آموزش و اتصال است. در کل رکوردها، ۱۲۱۵۶۹، ۱۷۶۱۴، ۹۳۳۴ به ترتیب از پروتکلهای کنترل انتقال، دیاگرام کاربر و پیام کنترل اینترنت است. این مجموعه شامل ۷۷۰۵۴ اتصال نرمال و ۷۱۴۶۳ آنرمال هستند. این مجموعه، ۴۱ ویژگی و یک برچسب کلاس، دارد. برخی از ویژگی‌ها پیوسته هستند اما بقیه ویژگی‌ها قطعی هستند. مقادیر ویژگی پیوسته متعلق به مجموعه نامحدود هستند در حالی که مقادیر قطعی از یک مجموعه قطعی تخصیص داده شدند. ویژگی‌های مشخصی[19] قطعی هستند و همه دیگر موارد پیوسته هستند. عدد ویژگی F۴۲، برچسب کلاسی است که نشان می‌دهد که آیا اتصال خاص در مورد مجموعه داده باینری نرمال یا غیرنرمال است. تعداد داده‌های آموزش در مجموعه داده استفاده شده

[11] Probe
[12] R2L
[13] U2R
[14] MIT
[15] LAN

[16] TCP dump
[17] KDDCup
[18] NSL-KDD
[19] F2 ،F3 ،F4 ،F7 ،F12 ،F14 ،F15 ،F21 و F22، F42



شکل ۴: نمایی از مجموعه داده

۱۲۵۹۷۴ و تعداد داده‌های استفاده شده در آزمایش ۲۲۵۴۵ عدد است [۱۱].

معیارهای ارزیابی: پارامترهای استاندارد ارزیابی عملکرد برای بررسی نتایج سیستم تشخیص نفوذ ارایه شده مبتنی بر مدل مشخص[20] استفاده می‌شوند. ماتریس اغتشاش[21] برای محاسبه پارامترهای عملکردی روش پیشنهادی استفاده می‌شود. جدول ۴-۱، ماتریس اغتشاش را برای دسته‌بند کننده دودویی نشان می‌دهد. ماتریس اغتشاش نتایج کلاس واقعی را در مقابل کلاس پیش بینی نشان می‌دهد. در این آزمایشات، اتصالات نرمال، رویدادهای مثبت را نشان می‌دهد در حالی که اتصالات غیرنرمال رویدادهای منفی را نشان می‌دهد. در جدول ۴-۱، مثبت واقعی تعداد رویدادهای اتصال نرمال واقعی است که به درستی بصورت نرمال طبقه بندی شده‌اند. مثبت کاذب، تعداد رویدادهای اتصالات غیر نرمال است که به اشتباه بعنوان اتصالات نرمال طبقه‌بندی شدند. منفی کاذب، تعداد رویدادهای اتصالات نرمال است که به اشتباه بعنوان اتصالات غیرنرمال طبقه‌بندی شده‌اند. منفی واقعی تعداد رویدادهای اتصالات غیر نرمال است که به درستی بصورت غیرنرمال طبقه‌بندی شدند.

پارامترهای مورد بررسی عبارتند از: دقت، نرخ مثبت واقعی، نرخ منفی واقعی، نرخ مثبت کاذب، نرخ منفی کاذب و زمان آزمون. زمان آزمون، زمان واقعی واحد پردازش مرکزی[22] گرفته شده توسط سیستم تشخیص نفوذ برای طبقه‌بندی تمام اتصالات آزمون را نشان می‌دهد. مقادیر پارمترهای دیگر با تعریف معادلات ۳ تا ۷ محاسبه شده است.

صحت: نزدیکی توافق بین مقدار میانگین حاصل از تعداد زیادی از نتایج آزمون و مقدار مرجع پذیرفته شده. به صحت «درستی میانگین» نیز گفته می‌شود. به طور کلی تعداد صحیح‌ها تقسیم بر تعداد کل نمونه‌ها است و به صورت درصد عنوان می‌شود. این معیار دقت کل یک طبقه‌بند را محاسبه می‌کند. در واقع این معیار مشهورترین و عمومی‌ترین معیار محاسبه کارایی الگوریتم‌های طبقه‌بندی است که نشان می‌دهد، طبقه‌بند طراحی شده چند درصد از کل مجموعه رکوردهای آزمایشی را بدرستی طبقه‌بندی کرده است.

$$TP\ Rate = \frac{(TP)}{(TP+FN)} \quad (۳)$$

$$TN\ Rate = \frac{(TN)}{(FP+FN)} \quad (۴)$$

$$FP\ Rate = \frac{(FP)}{(FP+TN)} \quad ۵)$$

$$FN\ Rate = \frac{(FN)}{(FN+TP)} \quad (۶)$$

$$Accuracy = \frac{(TP+TN)}{(TP+FP+FN+TN)} \quad (۷)$$

جدول ۲: ماتریس اغتشاش برای IDS مبتنی بر OS-ELM

کلاس واقعی		کلاس پیش بینی
غیرنرمال	نرمال	
مثبت کاذب	مثبت واقعی	نرمال
منفی واقعی	منفی کاذب	غیرنرمال

[20] OS-ELM
[21] Confusion
[22] CPU

براساس جدول ۴-۱ برای اندازه‌گیری اثربخشی مدل یادگیری سایبری، نتایج حاصل را از نظر دقت، یادآوری، امتیاز F و همچنین دقت مدل بر حسب درصد محاسبه می‌کنیم. برای این کار، ابتدا نرخ مثبت واقعی، نرخ منفی واقعی، نرخ مثبت کاذب و نرخ منفی کاذب را محاسبه می کنیم که به صورت زیر تعریف می شوند:

مثبت واقعی: مدل امنیتی به درستی طبقه مثبت ناهنجاری یا حملات را شناسایی یا طبقه بندی می کند.

منفی واقعی: مدل امنیتی به درستی طبقه منفی ناهنجاری یا حملات را شناسایی یا طبقه بندی می کند.

مثبت کاذب: مدل امنیتی به اشتباه طبقه مثبت ناهنجاری یا حملات را شناسایی یا طبقه بندی می کند.

منفی کاذب: مدل امنیتی به اشتباه طبقه منفی ناهنجاری یا حملات را شناسایی یا طبقه بندی می‌کند.

ارزیابی و نتایج شبیه سازی

در روش پیشنهادی، ما آموزش سایبری را ارائه کرده‌ایم، که در آن یک مدل طبقه‌بندی باینری برای تشخیص ناهنجاری‌ها و یک مدل طبقه‌بندی چند کلاسه برای انواع مختلف حملات سایبری در نظر گرفته‌ایم. در مدل‌سازی خود، تأثیر ویژگی‌های امنیتی را نیز در نظر گرفته‌ایم و در نهایت یک مدل مؤثر مبتنی بر یادگیری ماشین با انتخاب ویژگی ایجاد کردیم. در حین ساخت مدل‌های امنیتی، از محبوب‌ترین تکنیک‌های طبقه‌بندی یادگیری ماشین و همچنین یادگیری شبکه‌های عصبی مصنوعی با در نظر گرفتن چندین لایه پنهان استفاده کرده‌ایم. در نهایت، اثربخشی این مدل‌های امنیتی مبتنی بر یادگیری را با انجام طیف وسیعی از آزمایش‌ها با استفاده از مجموعه داده امنیتی محبوب[۲۳] بررسی کرده‌ایم [۳, ۴]. ما معتقدیم که تجزیه و تحلیل تجربی و یافته‌های ما می‌تواند به عنوان یک راهنمای مرجع هم در دانشگاه و هم در صنعت در حوزه امنیت سایبری برای ساخت موثر مدل‌سازی و سیستم امنیتی مبتنی بر داده بر اساس تکنیک‌های یادگیری ماشین استفاده شود.

در کلیه ارزیابی‌ها روش ارایه شده با روش مشابه ارایه شده در [۱۲] مورد مقایسه قرار گرفته است. برای یکسان‌سازی و ارایه نتایج مطلوب هر دوروش در نرم‌افزار متلب پیاده‌سازی شده است. بعد از استخراج داده‌ها توسط پروفایل‌ساز آلفا این اطلاعات باید در اختیار طبقه‌بند OSELM ارایه شده قرار گیرد. در سیستم تشخیص نفوذ مبتنی بر OS-ELM، چهار تابع فعال سازی[۲۴] استفاده می‌شوند. این توابع فعال‌سازی توسط معادلات ۸ تا ۱۱ تعریف می‌شوند[۱۳]. در این معادلات، x و Ø به ترتیب ورودی و خروجی را نشان می‌دهد. a و b پارامترهای یادگیری گره‌های پنهان هستند.

$$for\ RBF: \emptyset = e^{-b\|x-a\|^2} \quad (۸)$$

$$for\ \sin: \emptyset = \sin(ax+b) \quad (۹)$$

$$for\ sigmoid: \emptyset = \frac{1}{1-e^{-(ax+b)}} \quad (۱۰)$$

$$for\ hardlim: \emptyset = \begin{cases} 1 & if\ (ax+b) \geq 0 \\ 0 & otherwise \end{cases} \quad (۱۱)$$

طبقه‌بندی داده‌ها به معنای مرتبط نمودن یک داده به یک طبقه از پیش تعریف شده است. به عبارت دیگر هدف از طبقه‌بندی داده‌ها، یافتن طبقه خروجی مناسبی است که با کمترین خطا خروجی مناسب را نشان می‌دهد. این کار می تواند با مربوط کردن یک داده جدید به یکی از طبقات از پیش تعریف شده صورت پذیرد و یا در طبقه‌بندی پویا منجر به تعریف طبقه موضوعی جدیدی برای داده در دست بررسی گردد. طبقه‌بندی جزء روش‌های یادگیری با نظارت به شمار می‌آید. به آن معنی که ابتدا مجموعه داده‌ای به سیستم داده می‌شود که طبقه آنها مشخص شده است. سپس انتظار می‌رود سیستم با دیدن این نمونه‌ها بتواند نمونه‌های جدید را طبقه‌بندی کند. .هدف طبقه‌بندی، تحلیل نمونه‌های آموزشی و ساخت مدل دقیقی برای هر طبقه با استفاده از ویژگی‌های موجود در داده‌ها و سپس استفاده از این مدل‌ها برای طبقه‌بندی داده‌های آتی است. عمده روش‌های طبقه‌بندی داده‌ها در یکی از دو دسته الگوریتم‌های آماری و مفهومی جای می‌گیرند. در این پژوهش نیز بعد از استخراج ویژگی‌های گفته شده در بخش قبل با استفاده از طبقه‌بندی داده‌ها مخرب یا عدم مخرب بودن درخواست مورد نظر تشخیص داده می‌شود.

[23] NSL-KDD

[24] sin ،rbf ،sigmoid and hardlim

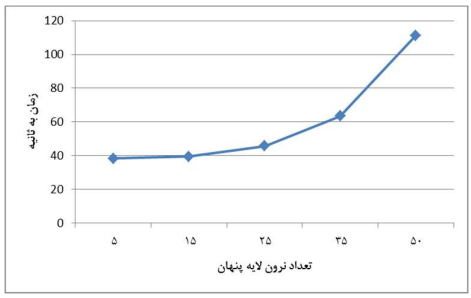
با توجه به ابعاد بزرگ مجموعه داده، مجموعه‌ای از روش‌های انتخاب ویژگی همانند پروفایل‌سازهای ارایه شده در روش پیشنهادی اعمال می شوند.

جدول ۳: فیلترهای اعمال شده برای انتخاب ویژگی و ویژگی های پیشنهاد شده توسط فیلتر

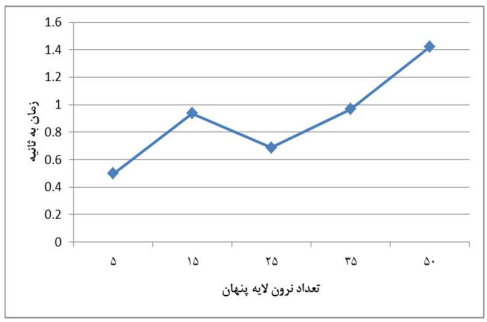
ردیف	تکنیک انتخاب ویژگی	ویژگی‌های پیشنهاد شده
۱	انتخاب ویژگی اول[25]	F۴, F۵, F۶, F۱۲, F۲۶, F۲۹, F۳۰, F۳۷
۲	انتخاب ویژگی دوم[26]	F۱, F۲, F۳, F۵, F۶, F۱۲, F۲۳, F۲۴, F۲۹, F۳۰, F۳۲, F۳۳, F۳۴, F۳۵, F۳۶, F۳۷, F۳۸, F۳۹, F۴۰
۳	انتخاب ویژگی سوم[27]	F۴, F۵, F۶, F۱۲, F۲۶, F۲۹, F۳۰, F۳۷
۴	انتخاب ویژگی چهارم[28]	F۱, F۲, F۳, F۴, F۵, F۶, F۱۲, F۲۳, F۲۴, F۲۶, F۲۹, F۳۰, F۳۲, F۳۳, F۳۴, F۳۵, F۳۶, F۳۷, F۳۸, F۳۹, F۴۰

جدول ۳ ویژگی‌های پیشنهاد شده توسط تکنیک پیشنهادی را نشان می‌دهد. تمام ویژگی‌های پیشنهاد شده توسط این سه روش انتخاب ویژگی به صورت مجموعه‌ای از ویژگی‌های مطلوب تجمیع می‌شوند. در این آزمایش، ۲۱ ویژگی از کل ۴۱ ویژگی پیشنهاد شده است. این، مجموعه ویژگی را تا ۴۸,۷۸٪ کاهش می‌دهد که بطور قابل ملاحظه نیازمندی حافظه را کاهش می‌دهد.

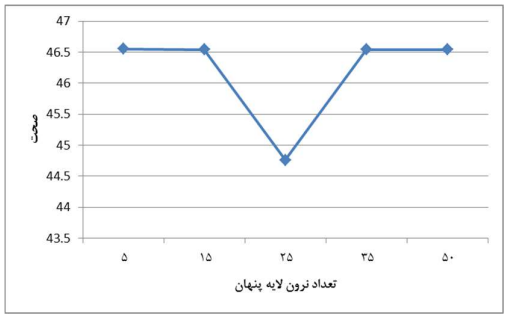
در اولین ارزیابی از طبقه‌بند پیشنهادی برای تعیین تعداد نرون لایه پنهان آزمایشات برروی روش‌های معرفی شده با تعداد ۵ تا ۵۰ نرون در لایه پنهان انجام شد. نتایج زمان آموزش و آزمایش به همراه صحت ارایه شده در آموزش و آزمایش در شکل ۵ نشان داده شده است. همانگونه که در شکل ۵ الف و ب نشان داده شده است با افزایش تعداد نرون‌های لایه پنهان به میزان زمان لازم برای آموزش و آزمایش افزوده می‌شود. بنابراین تعداد کمتر تعداد نرون در لایه پنهان به سرعت سیستم پیشنهادی می‌تواند بسیار کمک نماید. در نمودارهای صحت ارایه شده تعداد ۵، ۱۵، ۳۵ و ۵۰ عدد نرون در لایه پنهان دارای مقادیر بسیار نزدیک به‌هم هستند و در تعداد نرون ۲۵ عدد یک افت صحت به ثبت رسیده است.



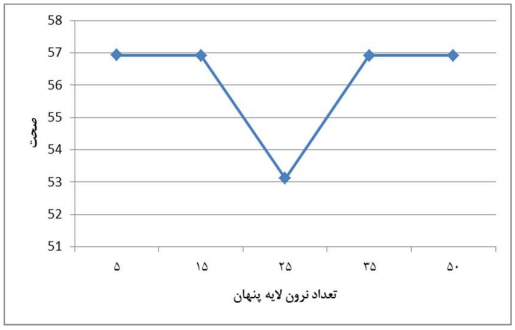
الف) زمان آموزش



(ب) زمان آزمایش



ج) صحت آموزش



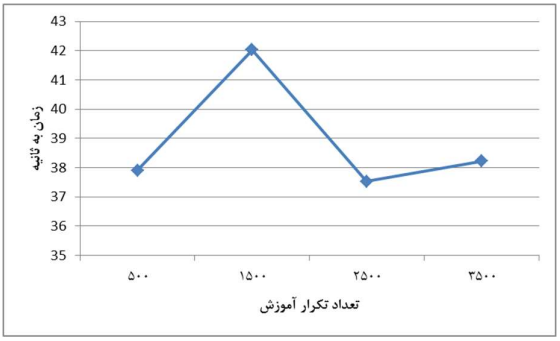
د) صحت آزمایش

شکل ۵: زمان و صحت روش پیشنهادی با تعداد نرون‌های مختلف لایه پنهان

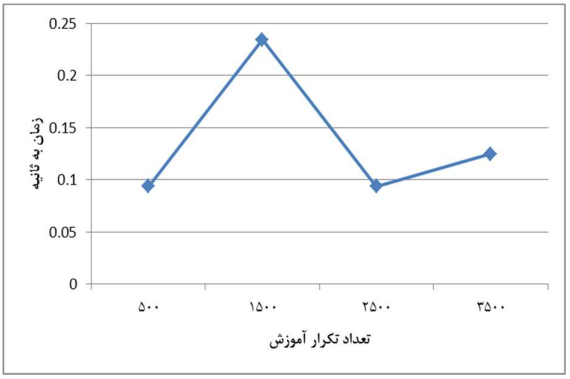
[25] Filtere subset eval
[26] Consistency subset eval
[27] CFS subset eval
[28] Optimal features

همانگونه که در شکل ۶ الف و ب نشان داده شده است با افزایش تعداد تکرار آموزش به میزان زمان لازم برای آموزش و آزمایش افزوده می‌شود. بنابراین تعداد کمتر تکرار در آموزش به سرعت سیستم پیشنهادی می‌تواند بسیار کمک نماید. در نمودارهای صحت ارایه شده تعداد ۲۵۰۰ تکرار در آموزش دارای بالاترین مقدار صحت بوده و بعد از آن به ترتیب ۳۵۰۰، ۱۵۰۰ و ۵۰۰ قرار دارد.

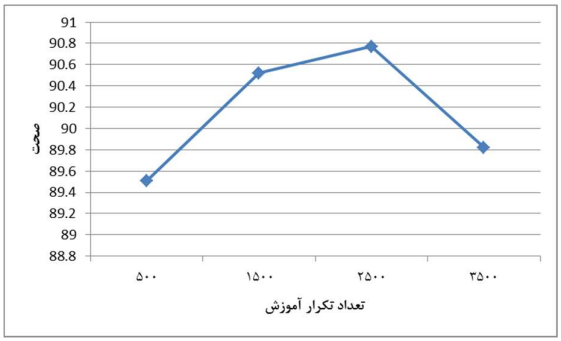
عملکرد سیستم تشخیص حمله انکار سرویس توزیع شده پیشنهادی با سیستم‌های مبتنی بر مدل‌های یادگیری ماشینی پرکاربرد مانند ماشین بردار پشتیبانی مقایسه می‌شود. شبکه عصبی مصنوعی مورد استفاده یک مدل سه لایه با ۱۰۰ نورون در لایه پنهان است. برای ماشین بردار پشتیبان، توابع «۱» و «۲»[29] متلب با پارامترهای پیش‌فرض استفاده می‌شوند. این مقایسه در ادامه نشان داده شده است. مشاهده می شود که سیستم پیشنهادی عملکرد بهتری نسبت به این سیستم‌ها نشان می‌دهد. برای مجموعه داده NSL-KDD سیستم پیشنهادی پیشرفت قابل توجهی را نشان می دهد. مقایسه عملکرد سیستم تشخیص حمله پیشنهادی با کارهای قبلی و تکنیک های پیشرفته در ادامه نشان داده شده است. سیستم پیشنهادی علاوه بر مجموعه داده‌های کامل، با همان مجموعه داده‌های جزئی نیز ارزیابی می‌شود. ارزیابی سیستم پیشنهادی با همان مجموعه داده‌های جزئی، بهبود عملکرد را نسبت به کارهای قبلی نشان می‌دهد. این ارزیابی نشان می دهد که عملکرد سیستم پیشنهادی بهتر یا قابل مقایسه با تکنیک های پیشرفته است.



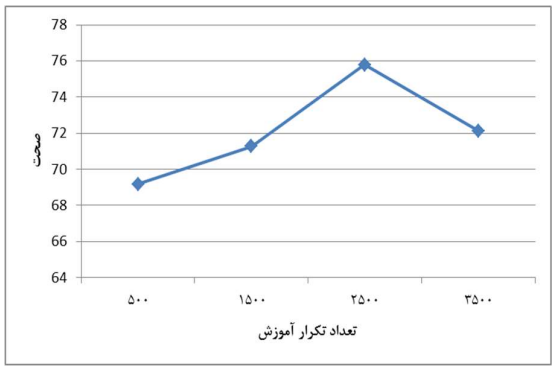
الف) زمان آموزش



(ب) زمان آزمایش



ج) صحت آموزش

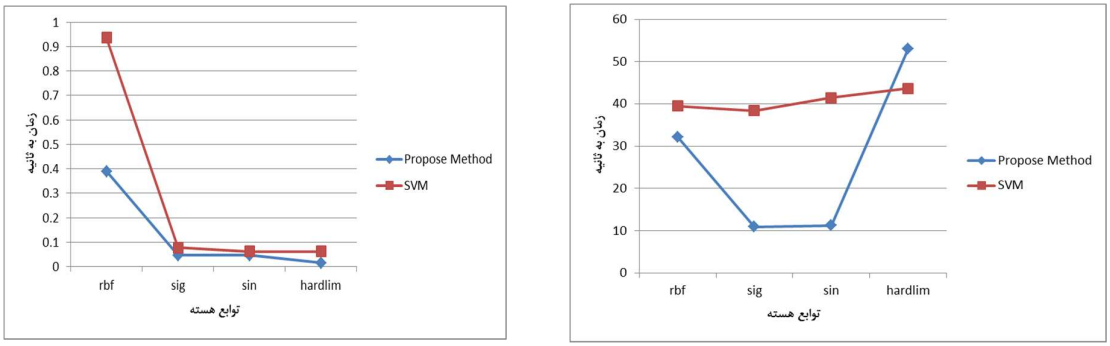


د) صحت آزمایش

شکل۶: زمان و صحت روش پیشنهادی با تعداد نرون‌های مختلف لایه پنهان(۲۵۰۰ تکرار)

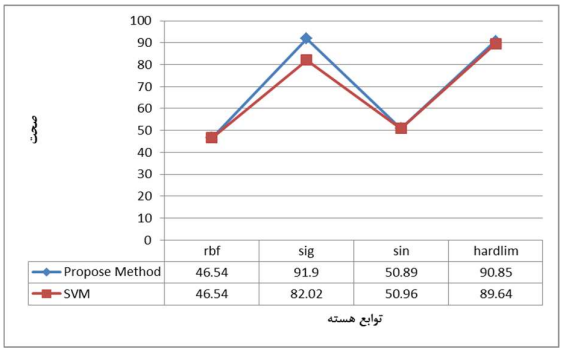
همانگونه که در شکل ۷ الف مشخص است زمان آموزش روش پیشنهادی در تمامی توابع به‌غیر از تابع hardlim دارای زمان کمتری بوده و همچنین در نمودار ۷ب که زمان‌های آموزش را نشان می‌دهد در تمامی توابع به نسبت روش مورد مقایسه دارای مقدار بهتری است. همچنین از نظر صحت در نمونه‌های آموزش و آزمایش توابع مختلف روش پیشنهادی مقادیر بهتر یا برابری با روش مورد مقایسه داشته که حتی میزان صحت با تابع sigmoid مقدار ۹۱,۹ درصد به

[29] Fitctree and fitcsvm

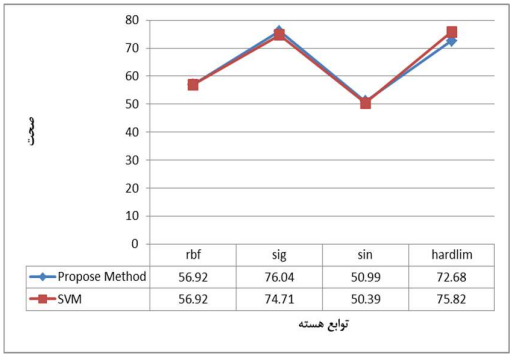


الف) زمان آموزش

ب) زمان آزمایش



ج) صحت آموزش



د) صحت آزمایش

شکل ۷: ارزیابی روش پیشنهادی با توابع هسته مختلف و مقایسه با روش مشابه

ثبت رسیده است و به نسبت روش مورد مقایسه بهبود ۹ درصدی از خود نشان داده است.

رایانش ابری انواع مختلفی از منابع را در قالب خدمات از طریق اینترنت فراهم می کند. در دسترس بودن خدمات ابری برای عملکرد روان این فناوری بسیار مهم است. مهاجمان می توانند از حملات انکار سرویس توزیع شده برای مختل کردن در دسترس بودن سرویس های ابری استفاده کنند. در کار حاضر، یک سیستم تشخیص حمله انکار سرویس توزیع شده مبتنی بر یادگیری ماشین برای محاسبات ابری پیشنهاد شده است. ابتدا، یک نسخه بهبودیافته از ماشین یادگیری افراطی تکاملی خود تطبیقی به نام ماشین یادگیری افراطی تکاملی خود تطبیقی با تطبیق متقاطع توسعه یافته است. مدل توسعه یافته قادر به تطبیق بهترین استراتژی جهش مناسب، نرخ متقاطع و عملگر متقاطع است. همچنین می تواند تعداد مناسب نورون های پنهان را به طور خودکار تعیین کند. این ویژگی ها قابلیت یادگیری مدل را بهبود می بخشد. سپس از این مدل برای ساخت سیستم تشخیص حمله انکار سرویس توزیع شده استفاده می شود. عملکرد سیستم پیشنهادی ما با استفاده از مجموعه داده پیشرفته NSL-KDD ارزیابی شده است. مقایسه عملکرد سیستم پیشنهادی ما با سیستم‌های مبتنی بر ماشین یادگیری افراطی تکاملی خود تطبیقی اصلی و سایر مدل‌های یادگیری ماشین مانند ماشین بردار پشتیبان نشان می‌دهد که عملکرد بهتری نسبت به این سیستم‌ها دارد. پس از تمام آزمایش‌ها، متوجه می‌شویم که سیستم پیشنهادی می‌تواند حملات با مقادیر بالای دقت، حساسیت، ویژگی، دقت و امتیاز F را شناسایی کند که هسته اصلی هر سیستم تشخیص حمله انکار سرویس توزیع شده پیشنهادی جدید است. همچنین مشاهده می شود که سیستم پیشنهادی بهتر از سیستم مبتنی بر ماشین یادگیری افراطی تکاملی خود تطبیقی اصلی از نظر معیارهای پیشرفته عمل می کند. این نشان می‌دهد که استفاده از عملگرهای متقاطع مختلف در طول مراحل مختلف فرآیند تکامل برای جستجوی راه‌حل بهینه در مقایسه با یک اپراتور واحد به خوبی عمل می‌کند. مقایسه سیستم پیشنهادی با برخی از سیستم‌های مبتنی بر مدل یادگیری ماشینی پرکاربرد و تکنیک‌های پیشرفته نیز سودمندی آن را نشان داده است. نقطه ضعف سیستم

پیشنهادی زمان آموزش طولانی تری نسبت به سیستم مبتنی بر ماشین یادگیری افراطی تکاملی خود تطبیقی است. این جنبه می تواند قابل تحمل باشد زیرا روند آموزش سیستم پیشنهادی بسیار مکرر نیست. بنابراین، می‌توان گفت که سیستم پیشنهادی ما در تشخیص انکار سرویس توزیع شده و انواع دیگر حملات در محیط‌های رایانش ابری بسیار مفید است.

۵- نتیجه‌گیری

در این پژوهش در این فصل ارزیابی روش‌پیشنهادی انجام شده است. برای ارزیابی روش پیشنهادی که برای تشخیص حمله در وب استفاده می‌شود و برای این عمل از الگوریتم OSELM استفاده شده است. برای ارزیابی، روش پیشنهادی را با چند روش دیگر هم‌رده ارزیابی نموده‌ایم و معیارهای مختلفی برای ارزیابی در نظر گرفته شده است. با توجه به بررسی معیارهای معرفی شده و تست شده روش پیشنهادی دارای صحت بالاتری بوده و از نظر سایر معیارها نیز برتری مناسبی نسبت به سایر الگوریتم‌ها بر روی داده‌های مجموعه تست از خود نشان داده است. در انتها برای شبکه پیشنهادی تعداد ۱۵ نرون در لایه پنهان تعداد ۲۵۰۰ تکرار در آموزش و تابع هسته زیگمودی پیشنهاد شده است. سیستم پیشنهادی با استفاده از مجموعه داده NSL-KDD ارزیابی شده است. این سیستم به دقت تشخیص ۸۶،۸۰ درصد با NSL-XKD دست می‌یابد. آزمایش‌ها نشان می‌دهد که عملکرد سیستم تشخیص حمله پیشنهادی بهتر از سیستم مبتنی بر ماشین یادگیری افراطی تکاملی خود تطبیقی اصلی و تکنیک‌های پیشرفته است. با این حال، زمان آموزش طولانی تری نسبت به سیستم مبتنی بر ماشین یادگیری افراطی تکاملی خود تطبیقی نشان می دهد.

از جمله پیشنهادات آتی برای ادامه مسیر پایان‌نامه پیش‌رو می‌توان به پیاده‌سازی و عملیاتی کردن کامل مدل پیشنهادی در دنیای واقعی و استخراج معایب و مزایای در هنگام کار در دنیای حقیقی و همچنین ارتقای امنیتی مدل پیشنهادی با استفاده از روش‌های اکتشافی چه در فاز تشخیص و چه در فاز انتخاب ویژگی و بررسی حملات پیشرفته‌تر برروی مدل اشاره نمود. جمع‌آوری داده‌های امنیتی جدیدتر با ابعاد بالاتر در محیط اینترنت اشیا و ساختن یک سیستم امن مبتنی بر داده با استفاده از تکنیک‌های یادگیری می‌تواند کار آینده باشد.

۶- منابع

1. *Subramanian, N. and A. Jeyaraj, Recent security challenges in cloud computing. Computers & Electrical Engineering, 2018. 71: p. 28-42.*
2. *Nandgaonkar, S.V. and A. Raut, A comprehensive study on cloud computing. International Journal of Computer Science and Mobile Computing, a Monthly Journal of Computer Science and Information Technology, 2014. 3: p. 733-738.*
3. *Kushwah, G.S. and V. Ranga, Optimized extreme learning machine for detecting DDoS attacks in cloud computing. Computers & Security, 2021. 105: p. 102260.*
4. *Sarker, I.H., Cyberlearning: effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. Internet of Things, 2021. 14: p. 100393.*
5. *Daffu, P. and A. Kaur. Mitigation of DDoS attacks in cloud computing. in 2016 5th International Conference on Wireless Networks and Embedded Systems (WECON). 2016. IEEE.*
6. *Ortet Lopes, I., et al., Towards effective detection of recent DDoS attacks: A deep learning approach. Security and Communication Networks, 2021. 2021.*
7. *Memon, K., et al., Analyzing distributed denial of service attacks in cloud computing towards the Pakistan information technol-ogy industry. Indian Journal of Science and Technology, 2020. 13(29): p. 2062-2072.*
8. *Alwandi Khordmand, H., prevention of DDOS attacks in cloud computing using cluster-algorithm, . international science and engineering conference, 2014.*
9. *Hossein Niya, F.a.M., Mohsen and Pedearan Moghadam, Farhang, , investigation of methods to deal with DDOS attacks in cloud computing environment,. the second national conference of new achievements in electricity and computer, Esfarain,, 2015.*
10. *Witten, I.H. and E. Frank, Data mining: practical machine learning tools and techniques with Java implementations. Acm Sigmod Record, 2002. 31(1): p. 76-77.*
11. *Tavallaee, M., Bagheri, E., Lu,W., & Ghorbani, A. A., A detailed analysis of the KDD CUP 99 data set. IEEE Symposium on*

Presenting a model for improving security in cloud computing to prevent DDOS attacks using extreme machine learning and artificial intelligence

A.H Nazari Afshar[1] and H Doost[2]

[1]Tehran Azad University, Yadegar Imam Khomeini Branch, Shahr-e Ray

[2]Tehran Azad University, Science and Research Branch

Abstract

Cloud computing helps users/organizations reduce infrastructure costs by providing services online. The availability of these services is of great importance, otherwise, users or organizations have to suffer a lot of financial or reputational losses. In this regard, attackers can use DDoS attacks to make these cloud services unavailable to legitimate users. In this attack, attackers impose a huge load on the services provided by the victim server on the public network. Several machine learning-based solutions have been proposed to detect DDoS attacks in cloud computing. This research presents a model to improve security in cloud computing to prevent DDOS attacks using extreme machine learning and artificial intelligence. In this method, an improved SaE-ELM model is developed that can adapt the mutation strategy, crossover rate, and crossover operator, and is able to automatically determine the appropriate number of hidden layer neurons. To evaluate the proposed method used for web attack detection, the OSELM algorithm was used and it was considered with several other peer methods based on different criteria for evaluation. For the proposed network, 15 neurons in the hidden layer, 2500 iterations in training and Zigmoid kernel function were proposed and evaluated using the NSL-KDD dataset. The proposed method achieved a detection accuracy of 86.80% with NSL-XKD and experiments showed that the performance of the proposed attack detection system is better than the original SaE-ELM-based system and advanced techniques. However, it resulted in a longer training time than the SaE-ELM-based system.

Computational Intelligence for Security and Defense Applications, CISDA 2009, (Cisda) (pp.1–6) http://doi.org/10.1109/CISDA.2009.5356528., 2009.

12. *Enache, A.-C. and V.V. Patriciu. Intrusions detection based on support vector machine optimized with swarm intelligence. in 2014 IEEE 9th IEEE international symposium on applied computational intelligence and informatics (SACI). 2014. IEEE.*
13. *Liang, N.-Y., et al., A fast and accurate online sequential learning algorithm for feedforward networks. IEEE Transactions on neural networks, 2006. 17(6): p. 1411-1423.*

امیر حسین نظری افشار فارغ‌التحصیل کارشناسی ارشد رشته مهندسی کامپیوتر گرایش نرم افزار از دانشگاه آزاد واحد یادگار امام (ره) و نشانه رایانامه ایشان عبارتند از :

root.afshar@gmail.com

حمیدرضا دوست دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات گرایش تجارت الکترونیک از دانشگاه آزاد واحد علوم و تحقیقات و نشانه رایانامه ایشان عبارتند از:

dhamidreza@rocketmail.com

روش ارجاع: ا.ح نظری افشار و ح. دوست. ارائه مدلی برای بهبود امنیت در رایانش ابری جهت جلوگیری از حملات DDOS با استفاده از ماشین یادگیری افراطی و هوش مصنوعی. دوفصلنامه محاسبات و سامانه‌های توزیع شده، سال هفتم، شماره۲، شماره پیاپی ۱۴، صفحه ۴۰ تا ۵۵ سال ۱۴۰۳.

How to cite: A.H. Nazari Afshar and H. Doost.: Presenting a model for improving security in cloud computing to prevent DDOS attacks using extreme machine learning and artificial intelligence. Journal of Distributed Computing and Systems (JDCS), Vol 7, Issue 2, Pages 40 – 55, 2025.