هشتمین کنفرانس ملی مباحث نوین در کامپیوتر و فناوری اطلاعات
8th National Conference on Advanced Topics in Computer and Information Technology
۲۹ آذر ماه ۱۴۰۳

بررسی تهدیدات سایبری و شناسایی نفوذ بدافزارها در زیرساخت‌های شبکه‌ای با استفاده از هوش مصنوعی

محمد حسین نشاط آور
neshatavar@gmail.com

چکیده : در سال‌های اخیر یکی از مهمترین چالش‌های امنیت اطلاعات و شبکه‌های ارتباطی افزایش روزافزون بدافزارها و به دنبال آن یافتن راه‌های مناسب جهت حفاظت سیستم‌ها در مقابل آنهاست که از مهمترین دغدغه‌های برنامه‌نویسان و متخصصین امنیت اطلاعات شناخت به موقع و یافتن راه‌های مقابله با اثرات مخرب این‌گونه بدافزارها می‌باشد. در مقابله با این روند شرکت‌های ضدبدافزاری به طور جدی به دنبال راه‌های بهتری برای شناسایی تهدیدات سایبری و نفوذ بدافزارها هستند. استفاده از الگوریتم‌های هوش مصنوعی یکی از روش‌هایی است که محققان توانسته‌اند در سال‌های اخیر با استفاده از آن به شناسایی تهدیدات سایبری و نفوذ بدافزارها در زیرساخت‌های شبکه‌ای بپردازند. لذا در این تحقیق سعی کردیم تا با استفاده از هوش مصنوعی به شناسایی تهدیدات سایبری و نفوذ بدافزارها در زیرساخت‌های شبکه‌ای با دقت بالایی بپردازیم. نتایج بدست آمده حاکی از آن است که روش پیشنهادی با دقت ۹۶.۴۷ درصد برای داده‌های آموزشی و دقت ۹۳.۹۸ درصد برای داده‌های آزمایشی قادر به تشخیص انواع بدافزارها در سیستم‌های رایانه‌ای شناسایی تهدیدات سایبری و نفوذ بدافزارها در زیرساخت‌های شبکه‌ای می‌باشد.

کلمات کلیدی: تهدیدات سایبری– بدافزار-زیرساخت شبکه- هوش مصنوعی-شناسایی

۱ – مقدمه

با توجه به گسترش و پیشرفت وسایل دیجیتالی در عصر حاضر و امروزه پیشرفت فناوری از یک طرف سبب تسهیل در امور بشر و دسترسی به آرامش و آسایش بیشتر شده و از طرف دیگر آثار و تبعات مخربی نیز به همراه داشته است. به تبع به وجود آمدن فضای سایبری مواجه شدن دولت‌ها با حملات سایبری در عصر حاضر اجتناب‌ناپذیر است؛ تعداد و آثار این حملات به گونه‌ای است که حملات سایبری می‌توانند به عنوان تهدیدی جدی‌تر از آنچه امروزه با آن مواجهیم ارزیابی شوند[۲،۱]. با توجه به روند رو به جلو استفاده از محیط شبکه‌ها به خصوص اینترنت، وجود نقاط آسیب‌پذیری مختلف در نرم‌فزارها باعث پیدایش بدافزارها در این شبکه‌ها شده است که امن‌سازی این محیط‌ها نسبت به گذشته از اهمیت بالاتری برخوردار شده است[۳]. بدافزار مجموعه دستوراتی است که توانایی ضربه زدن به سیستمی که بر روی آن اجرا می شود را داراست که با هدف آسیب رساندن به کامپیوتر، شبکه، اطلاعات و غیره توسعه داده شده است. بدافزارها می‌توانند به شکل متن سند، اجرایی یا هرگونه نرم‌افزار دیگری باشند. بصورت وسیع، بدافزارها را می‌توان به عنوان کرم‌های کامپیوتری، ویروس‌ها، روت‌کیت، باج‌افزارها، تبلیغ‌افزارها، نرم‌افزارهای جاسوسی، تروجان، ترس‌افزارها، بات‌ها برنامه‌های بالقوه ناخواسته و مابقی برنامه‌های تخریب‌گر طبقه‌بندی نمود. بدافزارها قادر به انجام انواع کارهای مخرب، از سرقت اطلاعات حساس گرفته تا از بین بردن کل سامانه‌ها یا دستگاه‌ها هستند. بسیاری از هکرها با بهره‌گیری از بدافزارهای مختلف درصدد نفوذ به حساب‌های کاربری و دستگاه‌های الکترونیکی کاربران متصل به اینترنت هستند تا بتوانند با سوءاستفاده از اطلاعات آنها به اهداف شوم خود دسترسی پیدا کنند[۴،۵،۶]. استفاده از الگوریتم‌های هوش مصنوعی یکی از روش‌هایی است که محققان توانسته‌اند در سال‌های اخیر با استفاده از آن به تشخیص بدافزارها بپردازند و در این راه به پیشرفت‌هایی نیز دست یافته‌اند که در ادامه به ذکر برخی از آنها خواهیم پرداخت.

- Banumathi و همکاران در سال ۲۰۲۴ جهت شناسایی بدافزارها استفاده از حافظه کوتاه مدت را پیشنهاد نمودند و از الگوریتم ترکیبی ملخ و جستجوی فاخته برای انتخاب ویژگی‌های موثر استفاده کردند. نتایج تجربی نشان می‌دهد که روش پیشنهادی با دقت ۹۸.۹۵ درصد از عملکرد خوبی جهت شناسایی بدافزارها برخوردار است[۷].
- Santosh و همکاران در سال ۲۰۲۴ جهت تشخیص بدافزار اندروید از الگوریتم‌های بهینه‌سازی شعله پروانه، بهینه‌سازی چندوجهی و بهینه‌سازی نهنگ برای انتخاب ویژگی‌های موثر و از الگوریتم‌های درخت تصمیم، جنگل تصادفی، نزدیکترین همسایه، ساده‌ترین بیز و نزدیکترین مرکز برای طبقه‌بندی استفاده کردند. نتایج بدست آمده نشان داده است که ترکیب الگوریتم‌های بهینه‌سازی نهنگ و نزدیکترین همسایه نسبت به سایر الگوریتم‌های مورد مقایسه با دقت ۹۸.۵۳ درصد از عملکرد بهتری جهت تشخیص بدافزار اندروید برخوردار است[۸].
- Kattamuri و همکاران در سال ۲۰۲۳ جهت تشخیص بدافزار و تهدید سایبری از درخت تصمیم و الگوریتم‌های بهینه‌سازی کلونی مورچه‌ها، بهینه‌سازی جستجوی فاخته و بهینه‌سازی گرگ خاکستری استفاده کردند. نتایج بدست آمده نشان داد که الگوریتم بهینه‌سازی کلونی مورچه‌ها با انتخاب ۱۲ ویژگی با دقت ۹۹.۳۷ درصد قادر به تشخیص بدافزار است[۹].
- Bayat و همکاران در سال ۲۰۲۱ جهت تشخیص و بررسی حملات بدافزاری از الگوریتم‌های داده کاوی و فراابتکاری استفاده کردند. بنابراین آنها با استفاده از الگوریتم شاهین هریس به بهبود شبکه عصبی پرسپترون پرداختند. نتایج بدست آمده نشان داده است که مدل پیشنهادی با دقت ۹۷.۱۸ درصد قادر به تشخیص بدافزارها بوده و از عملکرد خوب و قابل قبولی در تشخیص انواع حملات بدافزاری برخوردار می‌باشد[۱۰].
- Anggraini و همکارانش در سال ۲۰۲۰ جهت تشخیص حملات بدافزار استفاده از الگوریتم طبقه‌بندی ناویز و تکنیک گسسته‌سازی در فواصل 3-Interval و 5-interval را ارائه دادند. نتایج تجربی نشان می‌دهد که استفاده از الگوریتم ناویز جهت تشخیص بدافزار زمانی که داده‌ها از مرحله تشخیص و گسسته‌سازی عبور نکرده‌اند دارای دقتی برابر با ۶۹.۷۲ درصد بوده است، زمانی که داده‌ها با فاصله 3-Interval از مرحله تشخیص عبور کنند دقت برابر با ۷۸.۱۶ درصد خواهد بود و در زمانی که میزان فاصله برابر با 5-interval باشد به دقتی برابر با ۹۷.۷۹درصد دست یافته‌اند [۱۱].

۲ – فضای سایبری

فضای سایبری یک شبکه گسترده جهانی است که شبکه‌های مختلف رایانه‌ای در اندازه‌های متعدد و حتی رایانه‌های شخصی را با استفاده از سخت‌افزارها و نرم‌افزارهای گوناگون و با قراردادهای ارتباطی به یکدیگر وصل می‌کند. فناوری‌های ارتباط راه دور اساس فضای سایبری را تشکیل می‌دهند. هر چند برخی از این فناوری‌های مانند تلگراف و تلفن، در اوایل قرن نوزده اختراع شده بودند اما همه‌گیر و ارزان شدن این فناوری‌ها و بالا رفتن توان فنی آنها که شرط اصلی ظهور فضای سایبری است که در چند سال اخیر اتفاق افتاده است. بنابراین فضای سایبری رایانه‌ای به مکانی الکترونیک که در آن گروهی از افراد با یکدیگر دیدار و مباحثه می‌کنند، اطلاق می‌گردد. از نظر فنی نیز فضای سایبری به معنای فضای اطلاعاتی که بوسیله سیستم‌های رایانه‌ای شبکه‌های دیجیتالی که در نهایت با مادر همه شبکه‌ها یعنی اینترنت ارتباط پیدا می‌کند، می‌باشد؛ به عبارتی در هر زمینه غیرفیزیکی که بوسیله سیستم‌های رایانه‌ای آنلاین به وجود می‌آید، می‌تواند به عنوان فضای سایبری تلقی شود. در این راستا فضای سایبری دارای تأثیرهای گوناگونی بر جوامع در فضای واقعی است که در قالب مزایا و معایبی در جامعه جلوه‌گر خواهد بود. بنابراین می‌توان اقرار کرد که این فناوری‌ها ابزارهایی صرف نیستند بلکه بر شیوه‌های ارتباطی بشر و نیز فرآیندهای اندیشه و خلاقیت او نیز تأثیر دارند و آنها را تحت‌الشعاع قرار می‌دهند[۱۲،۱۳]. در فضای سایبری کاربران می‌توانند بدون در نظر گرفتن اینکه این اطلاعات و خدمات در کدام نقطه دنیا واقع شده اند، به هرگونه خدمات اطلاعاتی الکترونیکی دست یابند. محیط سایبری زمینه فعالیت‌های اقتصادی مهم و ابزار ضروری برای انجام کلیه معاملات تجاری و در سطح بین‌المللی بدون دخالت مستقیم بشر، فراهم آورده است. تفاوت محیط سایبر در مقایسه با سایر محیط‌ها در چند ویژگی مهم نهفته است که در ادامه به بیان آنها خواهیم پرداخت [۱۴] :

- نامحدود بودن فضای سایبر
- ناملموس بودن محیط سایبر
- توسعه و تغییر پذیری
- پیچیدگی و تخصصی بودن
- دسترسی آسان و سریع
- استفاده گسترده از فضای سایبر

۳ – انواع تهدید در فضای سایبری

بازیگران دولتی و غیردولتی از قدرت سایبری استفاده می‌کنند تا به اهداف اجتماعی، ایدئولوژیکی سیاسی، نظامی و مالی خود در فضای سایبری و دنیای واقعی دست یابند این اهداف در فضای مجازی از شیوه‌های متفاوتی حاصل می‌شوند که مهمترین تهدیدات سایبری عبارتند از [۱۵]:

- جنگ سایبری
- جرائم سایبری
- جاسوسی سایبری
- آشفتگی سایبری
- تروریسم سایبری

۴ – ویژگی تهدیدهای سایبری

تهدیدهای سایبری ویژگی‌های منحصر به فردی دارند که مهمترین ویژگی‌های تهدیدهای سایبری عبارتند از [۱۶]:

- هزینه کم ورود، صرف زمان کم و سرعت بالای اقدام
- تعداد بازیگران در فضای سایبری
- تأثیرگذاری شگرف
- ناشناس ماندن بازیگران و عدم قابلیت ردیابی
- کمرنگ شدن نقش جغرافیا
- پایین بودن احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری
- ساختار فضای اینترنت

۵ – ابزارهای جاسوسی در فضای سایبری

برخی از مهمترین ابزارهای جاسوسی و نفوذ بدافزارها در فضای سایبری عبارتند از [۱۶]:

- هک
- ارائه دهندگان خدمات اینترنتی
- نرم‌افزارهای جاسوسی
- ویروس‌ها
- کرم‌ها
- روت کیت

۶ – بدافزارها و نحوه انتشار آنها

بدافزار برنامه‌ای می‌باشد که به طور عمده برای انجام فعالیت‌های مخربی از جمله سرقت اطلاعات کاربر، جاسوسی اینترنتی و غیره طراحی گردیده است. . از دیدگاه تخصصی بدافزار در حالت کلی برنامه‌ای کامپیوتری بوده که با هدف آسیب‌رسانی به سیستم‌های کامپیوتری طراحی شده است. بدافزارها علاوه بر اینکه با عملیات خرابکارانه به منابع و اطلاعات سیستم‌ها دسترسی پیدا می‌کنند به سرویس‌دهی و فعالیت‌های سیستم‌ها آسیب وارد کرده و با سرقت غیرمجاز اطلاعات شخصی افراد؛ سبب وارد کردن هزینه‌های گزاف به قربانیان می‌شوند. از انواع بدافزارها می‌توان به ویروس کامپیوتری[1]، کرم[2]، تروجان[3]، جاسوس‌افزار[4]، باج‌افزار[5]، وایپر[6]، بات نت[7]، روت کیت[8]، بدافزار ویندوز، بدافزار مک، بدافزار اندروید و .... اشاره کرد. این بدافزارها وقتی که راهی برای ورود به سیستم پیدا کنند سیستم را آلوده کرده و به سرعت به منظور یافتن قربانیان جدید شروع به اسکن مجدد کرده و خود را درون شبکه تکثیر می‌کنند. یکی از بزرگترین چالش‌ها در این زمینه مقابله با سرعت زیاد انتشار بدافزارها است زیرا یک سیستم آلوده به بدافزار قادر خواهد بود صدها سیستم دیگر را آلوده کند و هرکدام از این صدها سیستم دیگر نیز می‌توانند سیستم‌های دیگری را آلوده نمایند[۱۸].

رشد سریع بدافزار سبب بوجود آمدن تهدیدهای بسیار زیادی در حوزه امنیت اطلاعات شده است. بنابراین مراکز دفاع سایبری که همانند مرزهای یک کشور هستند از اهمیت زیادی برخوردار بوده و در کنار فضای مجازی می‌توانند مورد تهدید و هجوم قرار بگیرند. نرم‌افزارهای مخرب در طول زمان از یک مزاحمت غیرجدی تبدیل به یک تهدید امنیتی جدی شده‌اند که این امر سبب شده است توجه محققان امنیتی در سراسر جهان به این موضوع جلب شود. بنابراین به منظور تعیین رفتار، حالت وخیم بودن و عملیات انواع نرم‌افزارهای مخرب؛ باید مورد تجزیه و

[1] Computer Virus
[2] Worm
[3] Trojan
[4] Spyware
[5] Ransomware
[6] Wiper
[7] Botnet
[8] Rootkit

تحلیل قرار بگیرند[۱۹]. با توجه به افزایش تهدیدها از سوی بدافزارها، آشنایی با انواع آنها می‌تواند در شناخت و مقابله با آنها بسیار مؤثر باشد که برخی از مهمترین انواع بدافزارها عبارتند از:

- از طریق سیستم عامل
- از طریق شبکه‌های بیسیم
- از طریق اشتراک فایل
- از طریق شبکه‌های اجتماعی
- از طریق سامانه‌های مجازی
- از طریق سایت‌های اینترنتی و ایمیل

۷ –هوش مصنوعی

سیستم‌های هوش مصنوعی (AI) سیستم‌های نرم‌افزارها و حتی گاه سخت‌افزارها هستند که توسط انسان طراحی شده‌اند تا در صورتی که یک تکلیف پیچیده به عهده آنان قرار گیرد آنان بصورت فیزیکی یا در ابعاد دیجیتالی با درک محیط اطراف خود از طریق به دست آوردن داده‌ها و تحلیل و تفسیر داده‌های به دست آورده ساختاریافته یا ساختارنیافته[۹]، استدلال کردن براساس یافته‌ها یا با تجزیه و تحلیل اطلاعاتی که از این داده‌ها به دست آورده‌اند عمل کنند و برای انجام دادن بهترین عمل با هدف انجام دادن تکلیف اولیه تصمیم بگیرند. سیستم‌های هوش مصنوعی می‌توانند قواعد نمادین[۱۰] یا مدل‌های اعدادی[۱۱] را یاد بگیرند. آنها همچنین می‌توانند رفتار خود را براساس تحلیل تأثیر اعمال قبلی خود بر محیط وفق دهند. در سال‌های اخیر در پی پیشرفت‌هایی که در زمینه رایانه و هوش مصنوعی و همچنین کشف روابط آشوبی در سری‌های زمانی غیرخطی پدید آمد، فعالیت‌هایی در جهت پیش‌بینی قیمت در بورس اوراق بهادار در کشورهای مختلف انجام شد. تکنیک‌های هوش مصنوعی که شامل شبکه‌های عصبی، داده کاوی، الگوریتم ژنتیک و منطق فازی است نتایج موفقیت‌آمیزی در زمینه حل مسایل پیچیده به دست آورده‌اند[۲۰]. هوش مصنوعی به شکل ساده آن بیش از ده‌ها سال است که وجود داشته است. بطور عادی یادگیری ماشین در قالب الگوریتم‌های ساده که دستورهایی هستند که برنامه‌نویس آنها را طراحی کرده مورد استفاده قرار می‌گرفت. در ابتدا کارکرد هوش مصنوعی به کارهای محدودی با داده‌های محدود خلاصه می‌شد. امروزه انسان‌ها با استفاده از اینترنت و دستگاه‌هایی که به نحوی به اینترنت متصل‌اند[۱۲] در حال تولید داده‌ها در حجمی گسترده‌اند. در نتیجه انسان‌ها در آغاز قادر به تحلیل حجم سنگینی از داده‌ها در زمان بهینه نبودند. بنابراین محققان دست به طراحی برنامه‌هایی زدند که به جای آنکه برنامه‌نویس به تحلیل داده‌ها و نتیجه‌گیری بپردازد نرم‌افزار طراحی شده چنین تحلیلی را انجام دهد. امروزه بیش از پانزده رویکرد برای استفاده و طراحی یادگیری ماشین وجود دارد که هر یک از یک نوع الگوریتم استفاده می‌کنند. هدف اصلی یک الگوریتم دسته‌بندی به حداکثر رساندن دقت پیش‌بینی است و برای این منظور الگوریتم‌های گوناگونی ایجاد شده است که برخی از مهم‌ترین آنها به شرح زیر است[۲۱].

۷-۱-ماشین بردار پشتیبان[13]

ماشین بردار پشتیبان یک روش بسیار موثر برای رگرسیون، دسته‌بندی و تشخیص الگوی کلی هستند اما به طور گسترده در اهداف دسته‌بندی استفاده می‌شوند. این روش با نام SVM نیز شناخته می‌شوند. ماشین بردار پشتیبان بر مبنای طبقه‌بندی خطی داده‌ها فعالیت می‌کند که برای تبدیل داده‌ها از تکنیکی به نام تابع کرنل[۱۴] استفاده کرده و سپس بر اساس این تبدیل، مرز بهینه بین خروجی‌های ممکن را پیدا می‌کند. به عبارت ساده با انجام تبدیلات بسیار پیچیده مشخص می‌کند چگونه داده‌ها بر اساس برچسب‌ها یا خروجی‌های تعریف شده، جدا شوند[۲۲].

۷-۲-شبکه عصبی مصنوعی

شبکه‌های عصبی مصنوعی[۱۵] یا به زبان ساده‌تر شبکه‌های عصبی سیستم‌ها، روش‌های محاسباتی نوینی هستند برای یادگیری ماشینی، نمایش دانش و در انتها اعمال دانش به دست آمده در جهت پیش‌بینی پاسخ‌های خروجی از سامانه‌های پیچیده ایده اصلی اینگونه شبکه‌ها (تا حدودی) الهام گرفته از شیوه کارکرد سیستم عصبی زیستی برای پردازش داده‌ها و اطلاعات به منظور یادگیری و ایجاد دانش قرار دارد. عنصر کلیدی این ایده ایجاد ساختارهایی جدید برای سامانه پردازش اطلاعات است. این سیستم از شمار زیادی عناصر پردازشی فوق العاده بهم پیوسته با نام نورون تشکیل شده که برای حل یک مسأله باهم هماهنگ عمل می‌کند. با استفاده از دانش برنامه نویسی رایانه می‌توان ساختار داده‌ای طراحی کرد که همانند یک نورون عمل نماید سپس با

[9] structured or unstructured data
[10] symbolic rules
[11] numeric model
[12] Internet of things
[13] Support Vector Machines (SVM)
[14] Kernel Trick
[15] Artificial Neural Networks

ایجاد شبکه‌ای از این نورون‌های مصنوعی بهم پیوسته ایجاد یک الگوریتم آموزشی برای شبکه کرده و با اعمال این الگوریتم به شبکه آن را آموزش داد[۲۳].

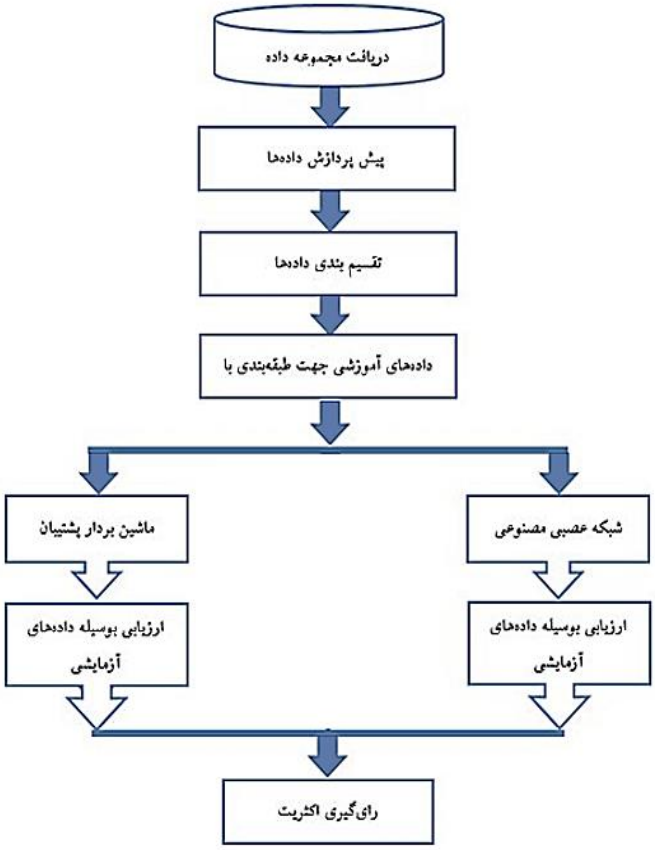
۸ –پیاده سازی روش پیشنهادی

در این مقاله تلاش نمودیم تا با ارائه راهکاری موثر و مفید با استفاده از الگوریتم‌های هوش مصنوعی به شناسایی تهدیدات سایبری و نفوذ بدافزارها در زیرساخت‌های شبکه‌ای بپردازیم. ایده اصلی در روش پیشنهادی استفاده از الگوریتم شبکه عصبی مصنوعی و الگوریتم ماشین بردار پشتیبان و مکانیسم رای‌گیری حداکثری می‌باشد. فلوچارت روش پیشنهادی در شکل (۱) نشان داده شده است. همانطور که مشاهده می‌شود در ابتدا به جمع‌آوری مجموعه داده مورد نظر پرداخته شد. بدین منظور داده‌های مورد نظر از سایت Kaggle[۱۶] گردآوری گردید. مجموعه داده دریافت شده شامل ۱۰۰۰۰۰ رکورد یا فایل می‌باشد که هر فایل دارای ۳۲ ویژگی است. در این مجموعه داده[۱۷]۳۱ ویژگی به عنوان ویژگی‌های اصلی بوده و یک ویژگی آن به عنوان برچسب[۱۸] و تعیین کننده نوع فایل از جهت سالم و یا آلوده بودن به بدافزار می‌باشد. سپس داده‌ها را مورد نرمالسازی قرار دادیم در واقع نرمال‌سازی روشی است که داده‌ها در زمانی که در یک دامنه قرار ندارند را در دامنه مشابه قرار می‌دهد. برای این منظور با استفاده از روش نرمالسازی Max-Min داده‌های موجود در مجموعه داده را در بازه بین صفر و یک نرمالسازی کردیم که در رابطه ۱ نشان داده شده است.

$$\acute{V} = \frac{V - min(V)}{max(V) - min(V)} \qquad (۱)$$

که در این رابطه V مقدار اصلی ویژگی مربوط به رکورد یا فایلی که قرار است نرمال شود می‌باشد، $\acute{V}$ مقدار نرمال‌سازی شده ویژگی مربوط به رکورد مورد نظر است، max(V) حد بالای ویژگی و min(V) حد پایین مقدار ویژگی در بین کل رکوردهای مجموعه داده می‌باشد.

در ادامه با استفاده از روش هولداوت داده‌ها به دو مجموعه داده آموزشی و آزمایشی با نسبت ۷۰ به ۳۰ درصد تقسیم شدند. پس از تقسیم‌بندی داده‌ها به ایجاد و ساخت الگوریتم‌های مورد استفاده پرداختیم و در ادامه به آموزش و ارزیابی هر یک از طبقه‌بندهای مورد نظر به تعداد ۱۰۰۱ مرتبه پرداخته و پس از رای‌گیری حداکثری از برچسب‌های هرکدام از طبقه‌بندهای ذکر شده به ارزیابی دقت آنها با توجه به رابطه (۲) پرداخته و در نهایت از نتایج هرکدام میانگین‌گیری نموده و پاسخ بدست آمده بعنوان پاسخ نهایی در نظر گرفته شد.



شکل ۱: فلوچارت روش پیشنهادی

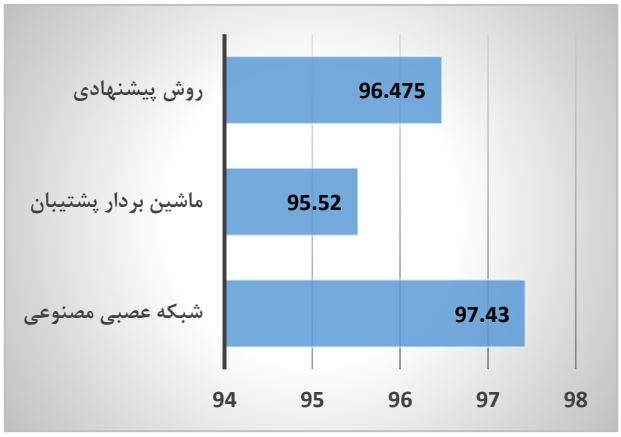
$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \qquad (۲)$$

۹- نتایج بدست آمده

همانطور که بیان شد در این مقاله تلاش نمودیم تا با ارائه راهکاری موثر و مفید با استفاده از الگوریتم‌های شبکه عصبی مصنوعی، ماشین بردار پشتیبان و مکانیسم رای‌گیری حداکثری به شناسایی تهدیدات سایبری و نفوذ بدافزارها در زیرساخت‌های شبکه‌ای بپردازیم. در ادامه به مقایسه نتایج بدست آمده برای داده‌های آموزشی و آزمایشی جهت شناسایی تهدیدات سایبری و نفوذ بدافزارها در زیرساخت‌های شبکه‌ای بصورت

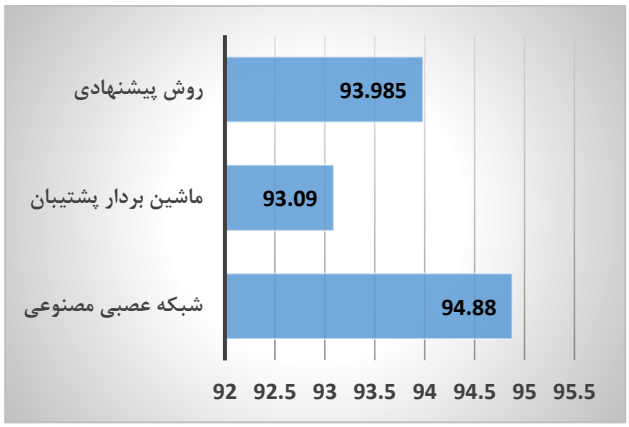
[16] www.kaggle.com/nsaravana/malware-detection
[17] Dataset
[18] Label

انفرادی و رای‌گیری حداکثری در شکل‌های (۲) و (۳) نشان داده شده است.



شکل ۲: مقایسه میانگین نتایج بدست آمده برای داده‌های آموزشی

باتوجه به آنچه که در شکل (۲) نشان داده شده است مشاهده می‌کنیم که دقت داده‌های آموزشی بدست آمده برای شبکه عصبی مصنوعی برابر ۹۷.۴۳ درصد، دقت برای ماشین بردار پشتیبان برابر ۹۵.۵۲ درصد و دقت برای روش پیشنهادی که از رای‌گیری حداکثری استفاده نموده است برابر ۹۶.۴۷ درصد می‌باشد که در واقع حد واسط بین دقت هر کدام از طبقه‌بندهای مورد نظر بوده و به عنوان یک نتیجه قابل قبول می‌توان از روش پیشنهادی جهت شناسایی تهدیدات سایبری و نفوذ بدافزارها در زیرساخت‌های شبکه‌ای استفاده نمود. در ادامه و در شکل (۳) نتایج بدست آمده برای داده‌های آزمایشی نشان داده شده است.



شکل ۳: مقایسه میانگین نتایج بدست آمده برای داده‌های آزمایشی

باتوجه به آنچه که در شکل (۳) نشان داده شده است مشاهده می‌کنیم که دقت داده‌های آزمایشی بدست آمده برای شبکه عصبی مصنوعی برابر ۹۴.۸۸ درصد، دقت برای ماشین بردار پشتیبان برابر ۹۳.۰۹ درصد و دقت برای روش پیشنهادی که از رای‌گیری حداکثری استفاده نموده است برابر ۹۳.۹۸ درصد می‌باشد که در واقع حد واسط بین دقت هر کدام از طبقه‌بندهای مورد نظر بوده و به عنوان یک نتیجه قابل قبول می‌توان از روش پیشنهادی جهت شناسایی تهدیدات سایبری و نفوذ بدافزارها در زیرساخت‌های شبکه‌ای استفاده نمود.

۱۰- نتیجه گیری

با توجه به گسترش و پیشرفت وسایل دیجیتالی در عصر حاضر و امروزه پیشرفت فناوری از یک طرف سبب تسهیل در امور بشر و دسترسی به آرامش و آسایش بیشتر شده و از طرف دیگر آثار و تبعات مخربی نیز به همراه داشته است. به تبع به وجود آمدن فضای سایبری مواجه شدن دولت‌ها با حملات سایبری در عصر حاضر اجتناب‌ناپذیر است؛ تعداد و آثار این حملات به گونه‌ای است که حملات سایبری می‌توانند به عنوان تهدیدی جدی‌تر از آنچه امروزه با آن مواجهیم ارزیابی شوند. با توجه به روند رو به جلو استفاده از محیط شبکه‌ها به خصوص اینترنت، وجود نقاط آسیب‌پذیری مختلف در نرم‌فزارها باعث پیدایش بدافزارها در این شبکه‌ها شده است که امن‌سازی این محیط‌ها نسبت به گذشته از اهمیت بالاتری برخوردار شده است. در سال‌های اخیر یکی از مهمترین چالش‌های امنیت اطلاعات و شبکه‌های ارتباطی افزایش روزافزون بدافزارها و به دنبال آن یافتن راه‌های مناسب جهت حفاظت سیستم‌ها در مقابل آنهاست که از مهمترین دغدغه‌های برنامه‌نویسان و متخصصین امنیت اطلاعات شناخت به موقع و یافتن راه‌های مقابله با اثرات مخرب این‌گونه بدافزارها می‌باشد. در مقابله با این روند شرکت‌های ضدبدافزاری به طور جدی به دنبال راه‌های بهتری برای شناسایی تهدیدات سایبری و نفوذ بدافزارها هستند. استفاده از الگوریتم‌های هوش مصنوعی یکی از روش‌هایی است که محققان توانسته‌اند در سال‌های اخیر با استفاده از آن به شناسایی تهدیدات سایبری و نفوذ بدافزارها در زیرساخت‌های شبکه‌ای بپردازند. در این تحقیق سعی کردیم با استفاده از هوش‌مصنوعی به شناسایی تهدیدات سایبری و نفوذ بدافزارها در زیرساخت‌های شبکه‌ای با دقت بالا بپردازیم. نتایج بدست آمده حاکی از آن است که روش پیشنهادی با دقت ۹۶.۴۷ درصد برای داده‌های آموزشی و دقت ۹۳.۹۸ درصد برای داده‌های آزمایشی قادر به تشخیص انواع بدافزارها در سیستم‌های رایانه‌ای شناسایی تهدیدات سایبری و نفوذ بدافزارها در زیرساخت‌های شبکه‌ای می‌باشد. باتوجه به نتایج بدست آمده درمی‌یابیم

که نتایج بدست آمده از روش پیشنهادی در واقع حد واسط بین دقت هر کدام از طبقه‌بندهای مورد نظر بوده و به عنوان یک نتیجه قابل قبول می‌توان از روش پیشنهادی جهت شناسایی تهدیدات سایبری و نفوذ بدافزارها در زیرساخت‌های شبکه‌ای استفاده نمود.

مراجع

[1] Alhammad, N., Alajlani, M., Abd-Alrazaq, A., Epiphaniou, G., & Arvanitis, T. (2024). Patients' Perspectives on the Data Confidentiality, Privacy, and Security of mHealth Apps: Systematic Review. *Journal of Medical Internet Research*, *26*, e50715.

[2] Almaiah, M. A., Al-Rahmi, A., Alturise, F., Hassan, L., Lutfi, A., Alrawad, M., ... & Aldhyani, T. H. (2022). Investigating the effect of perceived security, perceived trust, and information quality on mobile payment usage through near-field communication (NFC) in Saudi Arabia. *Electronics*, *11*(23), 3926.

[3] Ullah, I., Boreli, R., & Kanhere, S. S. (2023). Privacy in targeted advertising on mobile devices: a survey. *International Journal of Information Security*, *22*(3), 647-678.

[4] Singh, J., & Singh, J. (2021). A survey on machine learning-based malware detection in executable files. *Journal of Systems Architecture*, *112*, 101861.

[5] Pundir, S., Obaidat, M. S., Wazid, M., Das, A. K., Singh, D. P., & Rodrigues, J. J. (2023). MADP-IIME: malware attack detection protocol in IoT-enabled industrial multimedia environment using machine learning approach. *Multimedia Systems*, *29*(3), 1785-1797.

[6] Davies, S. R., Macfarlane, R., & Buchanan, W. J. (2021). Differential area analysis for ransomware attack detection within mixed file datasets. *Computers & Security*, *108*, 102377.

[7] Banumathi, C. S., & Rajendra, A. B. (2024). Hybridized grasshopper optimization and cuckoo search algorithm for the classification of malware. *Bulletin of Electrical Engineering and Informatics*, *13*(5), 3616-3627.

[8] Santosh Jhansi, K., Chakravarty, S., & Ravi Kiran Varma, P. (2022). A two-tier fuzzy meta-heuristic hybrid optimization for dynamic android malware detection. *SN Computer Science*, *4*(2), 117.

[9] Kattamuri, S. J., Penmatsa, R. K. V., Chakravarty, S., & Madabathula, V. S. P. (2023). Swarm optimization and machine learning applied to PE malware detection towards cyber threat intelligence. *Electronics*, *12*(2), 342.

[10] Bayat. H, Shabirinia. Misaa. (2021). Conference on Advanced Topics in Computer and Information Technology

[11] Anggraini, I., Kunang, Y. N., & Firdaus, F. (2020). Penerapan Naive Bayes Pada Detection Malware dengan Diskritisasi Variabel. Telematika, 13(1), pp.11-21

[12] Chen, X., Shen, J., & Susilo, W. (2022). *Cyberspace Safety and Security*. Springer.

[13] Van den Berg, B., & Kuipers, S. (2022). Vulnerabilities and cyberspace: A new kind of crises. *Oxford Research Encyclopedia of Politics*.

[14] Vukelić, M. (2024). Characteristics of cyberspace as a distinct domain of conflict: A case study of US strategic operations. *Medjunarodni problemi*, *76*(1), 55-86.

[15] Zatti, S. (2020). Space and cyber threats. *Handbook of Space Security: Policies, Applications and Programs*, 245-263.

[16] Trzonkowski, K., Khalina, O., Kolisnichenko, P., Rozumovych, N., & Zhyhulin, O. (2023). Information systems for financial and economic security in the face of cyberthreats: study of characteristics in the context of modern administrative and legal mechanism. *Amazonia Investiga*, *12*(69), 315-324.

[17] Kessell, B. (2023). Hacker, influencer, counter-culture spy: cyberspace actors' models of

misinformation and counter-operations.

[18] Sandeep, H. R. (2019, May). Static analysis of android malware detection using deep learning. In *2019 International Conference on Intelligent Computing and Control Systems (ICCS)* (pp. 841-845). IEEE.

[19] Dutta, N., Jadav, N., Tanwar, S., Sarma, H. K. D., Pricop, E., Dutta, N., ... & Pricop, E. (2022). Introduction to malware analysis. *Cyber Security: Issues and Current Trends*, 129-141.

[20] Minh, D., Wang, H. X., Li, Y. F., & Nguyen, T. N. (2022). Explainable artificial intelligence: a comprehensive review. *Artificial Intelligence Review*, 1-66.

[21] Sun, Z., Sandoval, L., Crystal-Ornelas, R., Mousavi, S. M., Wang, J., Lin, C., ... & John, A. (2022). A review of earth artificial intelligence. *Computers & Geosciences*, *159*, 105034.

[22] Shmilovici, A. (2009). Support vector machines. In Data mining and knowledge discovery handbook (pp. 231-247). Springer, Boston, MA.

[23] McCulloch, W. S., & Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. The bulletin of mathematical biophysics, 5(4), pp.115-133