هفتمین کنفرانس ملی مباحث نوین در کامپیوتر و فناوری اطلاعات
7th National Conference on Advanced Topics in Computer and Information Technology
۲ آذر ماه ۱۴۰۲

استفاده از الگوریتم بهینه‌سازی خفاش جهت مقابله با حملات سایبری

مهران اسماعیلی

چکیده : در سال‌های اخیر با گسترش شبکه جهانی وب دسترس‌پذیری اینترنت به شکل معناداری سبک زندگی امروزی را تحت تأثیر قرار داده است به نحوی که کاربردهای گسترده اینترنت در زمینه ارتباطات، دادوستد، بانکداری الکترونیک وغیره علاوه بر افزایش راحتی کاربران حفظ محرمانگی اطلاعات در برابر مخاطرات اینترنتی را به یک مساله مهم تبدیل کرده است. امروزه خطر حملات سایبری یکی از مهمترین چالش‌های موجود در اینترنت به شمار می‌رود؛ از این رو پژوهشگران طی سال‌های اخیر تلاش‌های زیادی جهت شناسایی و مقابله با اینگونه حملات با استفاده از الگوریتم‌های داده‌کاوی و فراابتکاری داشته‌اند. براین اساس و در این تحقیق سعی گردید تا با استفاده از الگوریتم بهینه‌سازی خفاش و بهبود شبکه عصبی مصنوعی به شناسایی این حملات با دقت بالایی بپردازیم. نتایج بدست آمده از پیاده‌سازی روش پیشنهادی بر روی مجموعه داده دریافتی از سایت UCI نشان داد که میزان شاخص‌های دقت، حساسیت، تشخیص و صحت به ترتیب ۳.۰۱ درصد، ۲.۹۱ درصد، ۳.۱۸ درصد و ۱.۹۲ درصد بهبود یافته‌اند.

کلمات کلیدی: حملات سایبری –فیشینگ-شبکه عصبی مصنوعی-الگوریتم بهینه‌سازی خفاش

۱ - مقدمه

امروزه اینترنت به یک جزء ضروری از فعالیت‌های اجتماعی و مالی روزمره زندگی تبدیل شده است به نحوی که دستیابی به مشتریان در سراسر جهان را بدون هیچگونه محدودیتی نسبت به محل کسب‌وکارشان تسهیل کرده و از تجارت الکترونیک استفاده مؤثر می‌نماید[۱]. تعداد مشتریانی که برای انجام خرید و سایر فعالیت‌ها بر اینترنت تکیه دارند بطور چشمگیری در حال افزایش می‌باشد که این امر روزانه صدها میلیون دلار را از طریق اینترنت منتقل می‌کند که این مقدار پول سبب وسوسه کلاهبرداران جهت انجام عملیات متقلبانه خواهد بود[۲]. بنابراین کاربران اینترنت ممکن است در معرض انواع مختلف تهدیدات وب قرار بگیرند که این امر سبب خسارت مالی، سرقت هویت، از دست دادن اطلاعات خصوصی، آسیب شهرت نام تجاری و از دست دادن اعتماد مشتریان در تجارت الکترونیک و بانکداری آنلاین می‌شود[۳]. بنابراین می‌توان گفت یکی از مهمترین چالش‌های اینترنت خطر حملات فیشینگ[1] و کلاهبرداری‌های اینترنتی است که سبب ایجاد خسارت‌های فراوانی به مشتریان و سازمان‌ها می‌شود. حملات سایبری در چند سال اخیر رشد قابل توجه‌ای داشته است و سالانه تعداد زیادی وبسایت جعلی در اینترنت ایجاد می‌شود که هدف آنها سرقت اطلاعات کاربران است[۵،۴]. حجم زیان ناشی از حملات سایبری در سال بیش از میلیاردها دلار است و این نوع از حملات به علت آنکه روی جعل وبسایت‌های بانکی و مالی متمرکز است لذا دارای زیان قابل توجه‌ای است[۶]. از این رو پژوهشگران طی سال‌های اخیر تلاش‌های زیادی جهت شناسایی و مقابله با اینگونه حملات با استفاده از الگوریتم‌های رایج طبقه‌بندی و فراابتکاری داشته‌اند.

۲– فضای سایبری

واژه فضای سایبری را نخستین بار ویلیام گیبسون[2] نویسنده داستان

[1] Phishing attacks
[2] William Gibson

علمی تخیلی در کتاب نورومنسر[3] در سال ۱۹۸۴ به کار برده است. سایبر پیشوندی برای توصیف یک شخص، یک شی، یک ایده و یا یک فضاست که مربوط به دنیای رایانه و اطلاعات بوده که همگی در نتیجه انتشار روزافزون رایانه پدید آمده‌اند. فضای سایبری یک محیط الکترونی و غیرفیزیکی است که از طریق آن اطلاعات ایجاد، ارسال، دریافت، ذخیره، پردازش و حذف می‌شوند، ترکیب دو کلمه فضا و سایبر حاکی از آن است که این عبارت دارای دو بعد است؛ این واژه تشریح سرزمین غیرفیزیکی تشکیل شده توسط نظام‌های رایانه‌ای می‌باشد. در واقع به دنیای کامپیوترها و جامعه‌ای که از آنها استفاده می‌نماید کلیه منابع اطلاعاتی موجود در شبکه‌های کامپیوتری و دارای فرهنگ خاصی مبتنی بر شبکه‌های ارتباطی الکترونیکی هستند فضای سایبر یا دنیای مجازی گفته می‌شود، در سطح معنایی فضای سایبر فضایی خیالی بین شبکه‌های رایانه‌ای است؛ فضای مجازی افراد و کاربران در شبکه‌های اجتماعی محیط‌های گفتگو، فروشگاه و ...با یکدیگر ارتباط برقرار نموده، به گشت و گذار، خرید و فروش، بحث و تبادل نظر می‌پردازند بدون اینکه هیچگونه حرکتی داشته باشند. فضای سایبر برای توصیف هر مفهومی که در ارتباط با شبکه‌های رایانه‌ای، فناوری اطلاعات، اینترنت و جامعه اطلاعاتی، بکار برده شده است و افراد و کاربران در این فضا به تجربه اجتماعی از تعامل تبادل و اشتراک‌گذاری اطلاعات، کسب و کار، بازی و تفریح، بحث‌های گروهی که بصورت غیرفیزیکی است،دست پیدا می‌کنند[۷].

۳- حملات سایبری

حمله سایبر یا حمله شبکه رایانه‌ای عبارت است از مجموعه اعمالی که برای ایجاد اختلال، قطعی، کاهش کیفیت یا نابودی اطلاعات مقیم در رایانه‌های موجود در فضای سایبری انجام می‌شود، فرآیند حمله سایبری معمولاً بر روی یک سامانه یا مجموعه‌ای از سامانه‌های هدف متمرکز می‌شود. در حمله سایبری ابتدا یک هدف مشخص تعیین شده و سپس مهاجم‌ها شروع به جمع‌آوری اطلاعات از طریق شبکه اینترنت، مقالات ATM، شبکه مطالعات و وب‌سایت‌های هدف و انجام آزمایش‌های تست نفوذ بر روی وب و شناسایی مؤلفه‌های تکنیکی هدف مانند سیستم عامل و جمع‌آوری اطلاعات از طریق مهندسی اجتماعی می‌کنند و در آخر حمله سایبر اتفاق می‌افتد که در شکل (۱) مراحل کار نشان داده شده است.



شکل (۲) فرآیند حمله سایبری

در این فرآیند معمولاً عملیات شناسایی و پویش زیادی به منظور استخراج اطلاعات لازم از سامانه هدف انجام می‌شود در این مرحله می‌توان عملیات شناسایی را با عمق بیشتری انجام داد زیرا معمولاً در این مرحله شاید نیاز به محرمانگی و مخفی کاری نسبت به مرحله اصلی حمله به مراتب کمتر باشد سپس سعی می‌شود که به سامانه هدف دسترسی پیدا کرد برای این کار یا می‌توان از یک حمله جدید استفاده کرد یا از اطلاعاتی که طی مرحله کشف یا از روش‌های مهندسی اجتماعی به دست آمده استفاده نمود. هنگامی یک حساب کاربری در سامانه هدف وجود داشته باشد شاید نیازمند ارتقاء حقوق دسترسی خود در سامانه هدف به منظور دست یافتن به اهداف باشد، هدف در این مرحله معمولاً به دست آوردن حقوق دسترسی مناسب در حقوق دسترسی حساب کاربری مدیر سامانه یا ریشه است. هنگامی که حقوق دسترسی مناسب در سامانه را به دست آمده باشد می‌توان هر صدمه‌ای را به آن زده یا هر اطلاعات لازمی را استخراج کرد؛ در طول فرآیند حمله باید آثار حمله از بین برده شود آنگاه موقع یورش به سامانه فرا می‌رسد در نهایت هم باید به تثبیت مواضع در سامانه پرداخته شود[۸].

۴- انواع حملات سایبری

امروزه تغییر ماهیت و شدت حملات به سمتی پیش رفته است که امکان قتل انسان‌ها از طریق حملات سایبری وجود دارد در نتیجه کشورها برای راه‌اندازی جنگ علیه دشمنان و کشتن مخالفان خود ممکن است نیازی به گزینه‌های نظامی نداشته باشند، گرچه در بسیاری از اوقات آنان بعد از یک تنش سیاسی با کشوری دیگر یا در زمان جنگ نظامی با آن اقدام به حملات سایبری نموده و تهاجمات امنیتی به نوعی مکمل جنگ‌های نظامی است. در ادامه به برخی از انواع حملات سایبری توسط هکرها اشاره خواهیم نمود[۹].

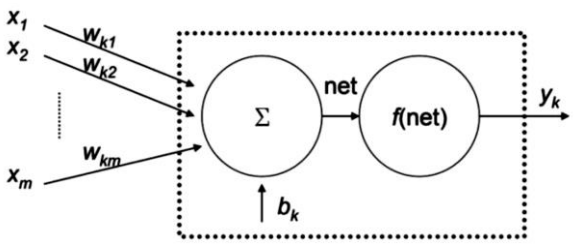
- سرقت اطلاعات پزشکی
- حمله به بخش‌های شیمیایی و دارویی

[3] Neuromancer

- کنترل هواپیما
- تغییر مسیر قطارها
- استفاده از کدهای بمب منطقی
- حمله به شبکه‌های برق
- حمله به سامانه‌های آب

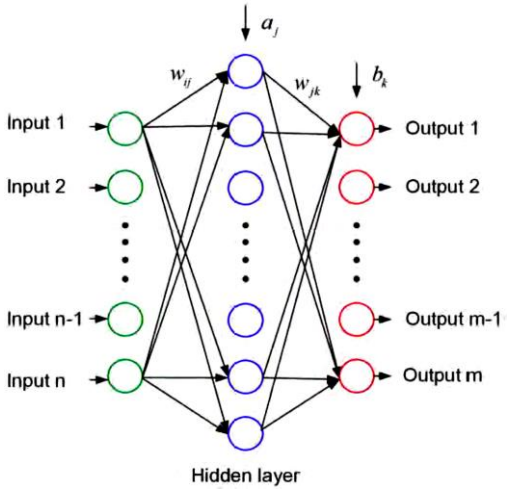
۵- شبکه‌های عصبی مصنوعی

شبکه عصبی مصنوعی[۴] یکی از تکنیک‌های مهم و کاربردی داده‌کاوی در تشخیص الگو و طبقه‌بندی است. شبکه عصبی مصنوعی در واقع یک مدل ریاضی و شبیه‌سازی شده از عملکرد مغز انسان و ارتباطات بین نورون‌های عصبی است. در این تکنیک داده‌کاوی مجموعه‌ای از سلول‌های عصبی به صورت نورون[۵] مصنوعی مدل‌سازی شده که بر روی ورودی خود تاثیر می‌گذارند. در شکل (۲) یک نورون مصنوعی و عملکرد آن نمایش داده شده است[۱۰] :



شکل (۲) ساختار یک نورون مصنوعی و اجزای آن[۱۰]

طبق شکل (۲) یک نورون مصنوعی مجموعه‌ای از عملگرهای ریاضی است که بر روی ورودی اعمال می‌شوند، نورون مصنوعی ورودی‌های را در اعدادی تحت نام اوزان۶ ضرب نموده و حاصل ضرب را در نهایت با یک مقدار ثابت به نام بایوس جمع نموده و تحویل یک تابع به نام تابع فعالیت می‌نماید که نقش کنترل کننده مقدار خروجی یک نورون را دارد. یک شبکه عصبی مصنوعی را می‌توان مجموعه‌ای از نورون‌های مصنوعی در نظر گرفت که مطابق شکل (۳) در لایه‌های مختلف توزیع شده‌اند[۱۱] :



شکل (۳) ساختار یک شبکه عصبی مصنوعی و لایه‌های آن[۱۱]

همانگونه که در شکل (۳) مشاهده می‌شود شبکه عصبی از سه لایه ورودی[۷]، مخفی[۸] و خروجی[۹] تشکیل شده است که وظیفه دریافت داده‌ها، پردازش و تولید کمیت خروجی را به عهده دارند و عبارتند از :

- لایه ورودی[۱۰] : تعداد نرون‌های لایه ورودی برابر با متغیرهایی است که برای شبیه‌سازی یک مدل مورد نیاز است.
- لایه‌های مخفی[۱۱] : لایه‌ها و تعداد نرون‌های لایه مخفی بوسیله آزمون و خطا مشخص می‌گردد. با استفاده از ورودی‌ها و مقادیر وزن بین این لایه‌ها نحوه عملکرد لایه‌های مخفی تعیین می‌شود.
- لایه خروجی[۱۲] خروجی نهایی شبکه در این لایه نشان داده می‌شود.

۶- الگوریتم خفاش

الگوریتم خفاش یکی از الگوریتم‌های فراابتکاری الهام گرفته از طبیعت است که در سال ۲۰۱۰ یانگ آن را معرفی کرد [۱۲]. خفاش‌ها تنها پستاندارانی می‌باشند که می‌تواند پرواز نماید و بر خلاف سایر پستانداران دارای بینایی بسیار ضعیفی می‌باشند اما در مقابل به کمک سیستم صوتی و بازخورد آن می‌توانند محیط اطراف را درک و تجزیه تحلیل

[4] Artificial Neural Network - ANN
[5] Neuron
[6] Weight
[7] Input layer
[8] Hidden layer
[9] Output layer
[10] Input Layer
[11] Hidden Layer
[12] Output Layer

نمایند. رفتار خفاش‌ها در یافتن غذا و سرپناه به کمک سیستم صوتی و بازخورد آن جالب و حیرت انگیز است به گونه‌ای که خفاش‌ها در زمانی که طعمه از آنها دور است با نرخ ارسال پالس صوتی اندک محیط اطراف را مورد پیمایش قرار می‌دهند و طول موج آنها در این وضعیت بلند و در حین حال فرکانس ارسال صوت آنها اندک است. بر عکس این وضعیت نیز در زمان نزدیک شدن به طعمه اتفاق می‌افتد به گونه‌ای که خفاش با نزدیک شدن به طعمه نرخ ارسال صوت خود را افزایش داده و این حالت باعث می‌شود طول موج امواج صوتی کاهش و در مقابل فرکانس ارسال اصوات افزایش یابد تا خفاش واکنش سریع‌تری به یافتن طعمه‌ها از خود نشان دهد.

الگوریتم خفاش[۱۳] یک الگوریتم دسته جمعی و مبتنی بر جمعیت است که از رفتار ارسال و دریافت اصوات صوتی توسط خفاش‌ها الگوبرداری و بوسیله زینگ شی یانگ[۱۴] مدلسازی شده است. از الگوریتم خفاش می‌توان برای حل مسائل بهینه‌سازی مختلف استفاده نمود و هر راه‌حل مسئله را در قالب یک خفاش که دارای بردار سرعت و موقعیت می‌باشد نمایش داد. زینگ برای مدلسازی رفتار خفاش‌ها و استفاده از مفاهیم آن در حل مسئله مجموعه‌ای از فرضیات نسبتا ساده در مورد خفاش‌ها را بکار برد تا بتواند الگوریتم خفاش را به سادگی مدلسازی نماید. بعنوان نمونه در مدلسازی زینگ خفاش‌ها می‌توانند فاصله‌ها را بصورت خودکار تشخیص داده و در حین جستجو برای یافتن جواب بهینه فرکانس خود را تغییر دهند و با مقدار بلندی صدای آنها بر حسب نزدیکی به جواب تغییر نماید. بطور کلی برای مدلسازی الگوریتم خفاش فرضیات ذیل توسط زینگ ارایه و معرفی شد[۱۳]:

- یک خفاش به عنوان یک راه‌حل مسئله بهینه‌سازی فرض می‌شود و هر خفاش می‌تواند به کمک بازخورد اصوات۱۵ فاصله خود را از طعمه یا سایر خفاش‌ها محاسبه نماید.
- هر خفاش دارای یک بردار موقعیت و سرعت است که به ترتیب با متغییر v_i و x_i نمایش داده می‌شود به گونه‌ای که بردار موقعیت بر اساس بردار سرعت تغییر و بروزرسانی می‌شود.
- هر خفاش برای پرواز و ارسال اصوات دارای یک فرکانس در محدوده مشخص است که طول موج آن یا λ بر اساس آن تغییر پیدا می‌نماید.
- خفاش‌ها پالس‌های صوتی خود را با نرخ مشخص در بازه $r \in [۱,۰]$ تولید نمایند تا از بازخورد آنها فضای جستجوی مسئله را مورد جستجو قرار دهند. فرکانس ارسال شده توسط هر خفاش با نزدیک شدن به طعمه مرتبا افزایش می‌یابد.
- بلندی صدای که هر خفاش می‌تواند تولید نماید بین یک مقدار کمینه و بیشینه است که با نزدیک شدن به طعمه این مقدار کاهش می یابد.

الگوریتم خفاش از مکانیزم جستجوی سراسری۱۶ و محلی۱۷ همزمان جهت یافتن جواب‌های بهینه استفاده می‌نماید. در الگوریتم خفاش هر راه‌حل مسئله بهینه‌سازی به صورت یک خفاش کدگذاری۱۸ می‌شود که مجموعه‌ای از راه‌حل‌های اولیه می‌توان فضای جستجوی مسئله را مورد پیمایش قرار داده تا راه‌حل بهینه استخراج شود و در واقع اعضای جمعیت خفاش با تکرار متوالی الگوریتم خفاش به سمت جواب‌های بهینه همگرا شوند. الگوریتم خفاش دارای اجزای ذیل است که هر کدام از آنها نقش مهمی در عملکرد صحیح الگوریتم برای یافتن جواب بهینه دارند :

- هر خفاش دارای یک بردار موقعیت است که در واقع راه‌حل مسئله در فضای جستجوی مسئله در نظر گرفته می‌شود.
- هر خفاش دارای بردار سرعتی است که خفاش از آن برای تغییر بردار موقعیت استفاده می‌نماید.
- فرکانسی که هر خفاش برای ارسال اصوات بکار می‌برد در تعیین سرعت خفاش نقش مهمی دارد.
- از مفهوم بلندی صدا در جستجوی محلی الگوریتم خفاش استفاده می‌شود.

۷ – کارهای پیشین

Faghihnia و همکاران در سال ۲۰۲۱ از مدل ماشین بردار پشتیبان که هسته‌های آن وزن‌دار شده به همراه پارامترهای هسته‌های ماشین بردار پشتیبان برای سیستم تشخیص حملات سایبری استفاده کردند. نتایج بدست آمده بر روی مجموعه داده DARPA نشان می‌دهد که روش پیشنهادی قادر است با دقت ۹۹.۹۸ درصد به تشخیص حملات سایبری بپردازد[۱۴].

[13] Bat algorithms
[14] Xin-She Yang
[15] Echolocation
[16] Global search
[17] Local search
[18] Coding

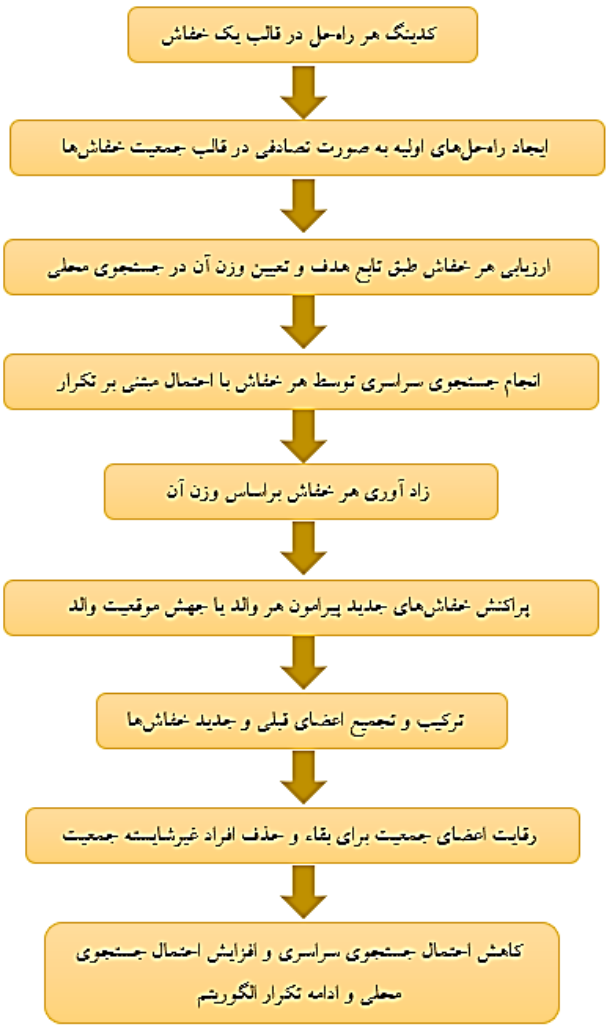
در پژوهشی Siahmarzkooh در سال ۲۰۲۱ از الگوریتم درخت تصمیم جهت تشخیص حملات سایبری و از الگوریتم خوشه‌بندی kmeans و شبکه بیزین جهت انتخاب ویژگی‌های مهم استفاده کرد. نتایج پیاده‌سازی روش پیشنهادی بر روی مجموعه داده دریافتی از سایت UCI که دارای ۱۱۰۵۵ نمونه بود نشان می‌دهند که روش پیشنهادی قادر است با دقت ۹۴.۶۵ درصد به تشخیص انواع حملات سایبری بپردازد[۱۵].

Safara و همکاران در سال ۲۰۲۰ جهت تشخیص وب‌سایت‌های جعلی استفاده از الگوریتم فراابتکاری کفتار به منظور انتخاب ویژگی‌های مناسب جهت طبقه‌بندی وب‌سایت‌های جعلی را پیشنهاد کردند. نتایج پیاده‌سازی روش پیشنهادی بر روی مجموعه داده دریافتی از سایت UCI که دارای ۱۱۰۵۵ نمونه بود نشان می‌دهند که روش پیشنهادی قادر است با دقت ۹۷.۶۴ درصد به تشخیص وب‌سایت‌های جعلی بپردازد[۱۶].

Benavides و همکاران در سال ۲۰۲۰ روش‌های طبقه‌بندی برای تشخیص حمله فیشینگ با استفاده از تکنیک‌های یادگیری عمیق را مورد بررسی جامع قرار دادند. نتایج حاصل از مطالعات آنها نشان می‌دهد حملات فیشینگ روشی است که توسط آن مهاجم تلاش می‌کند تا اطلاعات محرمانه‌ای را با این هدف که از آن به منظور کلاهبرداری استفاده کند از کاربر بدست آورد. بنابراین براساس نتایج بدست آمده از این تحقیق می‌توان گفت رایج ترین روش تشخیص فیشینگ در چند سال اخیر شبکه عصبی عمیق و شبکه عصبی حلقوی است که نسب به دیگر روش‌ها از دقت بیشتری برخوردار هستند[۱۷].

۸– شرح روش پیشنهادی

در این تحقیق ابتدا براساس مفاهیم زاد و ولد به بهبود الگوریتم خفاش پرداخته و در ادامه از الگوریتم خفاش بهبود یافته جهت کاهش خطای تشخیص حملات سایبری بوسیله شبکه عصبی استفاده خواهیم کرد. در روش پیشنهادی هر شبکه عصبی مصنوعی به صورت یک خفاش کدگذاری شده و طبق مکانیزم جستجوی سراسری و محلی تلاش می‌شود یک شبکه عصبی مصنوعی با حداقل خطای ممکن طبقه‌بندی[۱۹] جهت تشخیص وب‌سایت‌های عادی از مورد حمله قرار گرفته ارایه و استخراج شود. در واقع به کمک روش پیشنهادی اوزان[۲۰] و آستانه[۲۱] یک شبکه عصبی مصنوعی به عنوان عامل مهم در کاهش خطای تشخیص حملات سایبری توسط الگوریتم خفاش بهبود یافته انتخاب شده تا حملات سایبری با دقت بیشتری شناسایی شوند. چارچوب پیشنهادی برای بهبود الگوریتم خفاش با استفاده از مفاهیم تولید جواب پیرامون اعضای شایسته در شکل (۴) نمایش داده شده است.



شکل (۴) چارچوب روش پیشنهادی برای بهبود الگوریتم خفاش

طبق شکل (۴) در ابتدا هر راه‌حل مسئله به صورت بردار موقعیت خفاش با سرعت اولیه مشخص کدگذاری می‌شود سپس مجموعه‌ای از راه‌حل‌ها در فضای جستجوی مسئله به صورت تصادفی ایجاد و پراکنده می‌شوند و توسط تابع هدف مورد ارزیابی قرار گرفته و میزان شایستگی آنها تعیین

[19] Classification
[20] Weights
[21] Bais

می‌شود. هر خفاش با انتخاب یک فرکانس می‌تواند سرعت خود را در جستجوی سراسری تعیین نماید و براساس این سرعت و موقعیت آن می‌تواند موقعیت خود را بروزرسانی نماید. در ادامه بهترین و بدترین عضو جمعیت انتخاب شده و براساس شایستگی یک خفاش وزن آن در جمعیت برای جستجوی محلی تعیین می‌شود. هر چقدر میزان وزن یک عضو جمعیت بیشتر باشد تعداد جستجوی محلی با زادآوری پیرامون یک عضو جمعیت نیز بیشتر می‌شود. در پایان جستجوی سراسری و محلی الگوریتم خفاش اندازه جمعیت الگوریتم به علت زادآوری زیاد شده و به علت رقابت بین اعضاء فقط اعضای شایسته باقی مانده تا در نهایت اندازه جمعیت در پایان هر تکرار ثابت بماند و در نهایت در تکرار پایانی بهترین عضو جمعیت بعنوان جواب نهایی انتخاب می‌شود. در شکل (۵) فلوچارت الگوریتم خفاش نشان داده شده است.



شکل (۵) فلوچارت الگوریتم خفاش

همان گونه که توضیح داده شده وظیفه الگوریتم پیشنهادی استخراج یک شبکه عصبی مصنوعی با اوزان و آستانه‌های بهینه است تا از این طریق شبکه عصبی مصنوعی مورد نظر دارای حداقل خطای تشخیص جهت شناسایی حملات سایبری شود و با دقت مناسبی این حملات را تشخیص دهد. بنابراین برای ارزیابی روش پیشنهادی از شاخص‌های ارزیابی همچون دقت[۲۲]، حساسیت[۲۳]، تشخیص[۲۴] و صحت[۲۵] استفاده می‌شود.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \quad (۱)$$

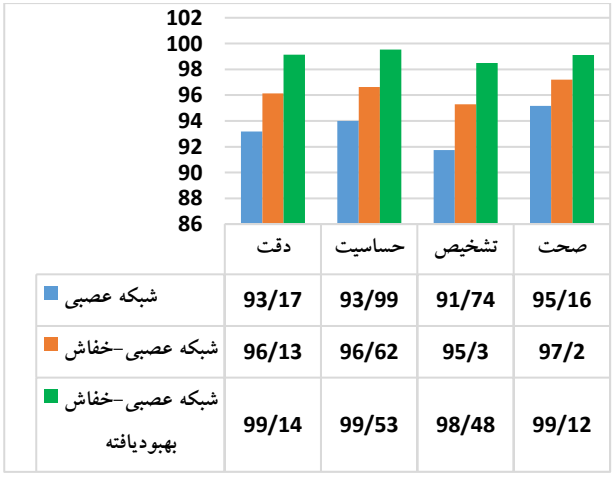
$$Sensitivity = \frac{TP}{TP+FN} \times 100 \quad (۲)$$

$$Specificity = \frac{TN}{TN+FP} \times 100 \quad (۳)$$

$$Precision = \frac{TP}{TP+FP} \times 100 \quad (۴)$$

۹- ارزیابی روش پیشنهادی

در سه حالت مختلف به ارزیابی روش پیشنهادی پرداختیم بدین گونه که در حالت اول تنها از شبکه عصبی ساده استفاده نمودیم و در حالت دوم شبکه عصبی را با الگوریتم خفاش بهبود دادیم و در حالت سوم شبکه عصبی را با الگوریتم بهبود یافته خفاش مورد ارزیابی قرار دادیم. نتایج بدست آمده از پیاده‌سازی روش پیشنهادی در شکل (۶) نمایش داده شده است.

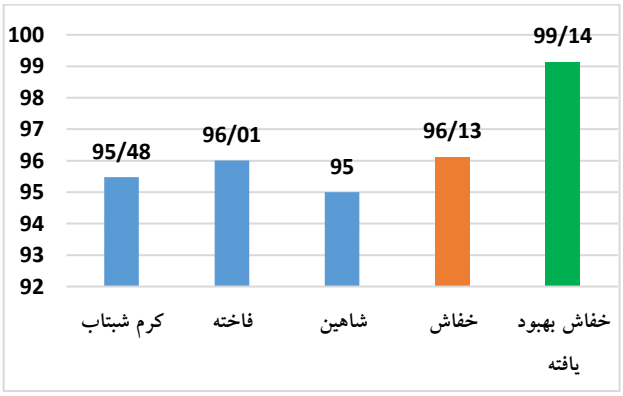


	دقت	حساسیت	تشخیص	صحت
شبکه عصبی	93/17	93/99	91/74	95/16
شبکه عصبی-خفاش	96/13	96/62	95/3	97/2
شبکه عصبی-خفاش بهبودیافته	99/14	99/53	98/48	99/12

شکل (۶) نتایج ارزیابی روش پیشنهادی

[22] Accuracy
[23] Sensitivity
[24] Specificity
[25] Precision

باتوجه به نتایج بدست در شکل (۶) مشاهده می‌کنیم که میزان شاخص‌های دقت، حساسیت، تشخیص و صحت در حالت دوم نسبت به حالت اول به ترتیب به میزان ۲.۹۶ درصد، ۲.۶۳ درصد، ۳.۵۶ درصد و ۲.۰۴ درصد افزایش داشته است. همچنین میزان شاخص‌های ذکر شده در حالت سوم نسبت به حالت دوم به ترتیب ۳.۰۱ درصد، ۲.۹۱ درصد، ۳.۱۸ درصد و ۱.۹۲ درصد افزایش پیدا کرده است. در ادامه به مقایسه دقت بدست آمده از پیاده‌سازی روش پیشنهادی با الگوریتم‌های شاهین، فاخته و کرم شبتاب پرداختیم که در شکل (۷) نشان داده شده است.



شکل (۷) نتایج ارزیابی دقت روش پیشنهادی با الگوریتم‌های شاهین، فاخته و کرم شبتاب

همانگونه که مشاهده می‌شود الگوریتم خفاش بهبود یافته نسبت به الگوریتم خفاش دقت تشخیص حملات سایبری را به میزان ۳.۰۱ درصد بهبود داده است. همچنین دقت الگوریتم خفاش بهبود یافته نسبت به الگوریتم‌های شاهین، فاخته و کرم شبتاب جهت تشخیص حملات سایبری به میزان ۴.۱۴ درصد، ۳.۱۳ درصد و ۳.۶۶ درصد بیشتر می‌باشد. بنابراین می‌توان گفت الگوریتم خفاش بهبود یافته نسبت به الگوریتم‌های مورد مقایسه دارای همگرایی بهتری است و کمتر در بهینه‌های محلی گرفتار می‌شود.

۱۰- نتیجه گیری

از آنجا که مهمترین چالش‌های موجود در اینترنت، خطر حملات سایبری و کلاهبرداری‌های اینترنتی می‌باشد که سبب وارد شدن خسارت‌های فراوانی به مشتریان و سازمان‌ها شده است؛ در این راستا ابزارهای زیادی توسط متخصصین و پژوهشگران جهت تشخیص و مقابله با این حملات ساخته شده است ولی از آنجایی که هکرها همواره روش کار خود را با هزینه اندک تغییر می‌دهند لذا همواره نیاز به بروز شدن روش‌ها و ابزارهای شناسایی و مقابله با انواع حملات سایبری می‌باشد. بنابراین در این تحقیق تلاش کردیم تا با استفاده از شبکه عصبی مصنوعی بهبودیافته توسط الگوریتم بهینه‌سازی خفاش این حملات را با دقت بالایی تشخیص دهیم. در این تحقیق ما در سه حالت مختلف به ارزیابی روش پیشنهادی پرداختیم بدین گونه که در حالت اول تنها از شبکه عصبی ساده استفاده نمودیم و در حالت دوم شبکه عصبی را با الگوریتم خفاش بهبود دادیم و در حالت سوم شبکه عصبی را با الگوریتم بهبود یافته خفاش مورد ارزیابی قرار دادیم. نتایج بدست آمده از پیاده‌سازی روش پیشنهادی نشان داد که میزان شاخص‌های دقت، حساسیت، تشخیص و صحت در حالت دوم نسبت به حالت اول به ترتیب به میزان ۲.۹۶ درصد، ۲.۶۳ درصد، ۳.۵۶ درصد و ۲.۰۴ درصد افزایش داشته است. همچنین میزان شاخص‌های ذکر شده در حالت سوم نسبت به حالت دوم به ترتیب ۳.۰۱ درصد، ۲.۹۱ درصد، ۳.۱۸ درصد و ۱.۹۲ درصد افزایش پیدا کرده است. در ادامه به مقایسه دقت بدست آمده از پیاده‌سازی روش پیشنهادی با الگوریتم‌های شاهین، فاخته و کرم شبتاب پرداختیم. نتایج بدست آمده نشان داد که دقت الگوریتم خفاش بهبود یافته نسبت به الگوریتم‌های شاهین، فاخته و کرم شبتاب جهت تشخیص حملات سایبری به میزان ۴.۱۴ درصد، ۳.۱۳ درصد و ۳.۶۶ درصد بیشتر می‌باشد.

مراجع

[1] Dai, S., Zha, L., Liu, J., Xie, X., & Tian, E. (2022). Fault detection filter design for networked systems with cyber attacks. *Applied Mathematics and Computation*, *412*, 126593.

[2] Nedeljkovic, D., & Jakovljevic, Z. (2022). CNN based method for the development of cyber-attacks detection algorithms in industrial control systems. *Computers & Security*, *114*, 102585.

[3] Dehghani, M., Ghiasi, M., Niknam, T., Kavousi-Fard, A., Tajik, E., Padmanaban, S., & Aliev, H. (2021). Cyber attack detection based on wavelet singular entropy in AC smart islands: False data injection attack. *IEEE Access*, *9*, 16488-16507.

[4] Jahromi, A. N., Karimipour, H., Dehghantanha, A., & Choo, K. K. R. (2021). Toward Detection and

Attribution of Cyber-Attacks in IoT-Enabled Cyber–Physical Systems. *IEEE Internet of Things Journal*, *8*(17), 13712-13722.

[5] Al-Haija, Q. A., McCurry, C. D., & Zein-Sabatto, S. (2020, September). Intelligent self-reliant cyber-attacks detection and classification system for IoT communication using deep convolutional neural network. In *International Networking Conference* (pp. 100-116). Springer, Cham.

[6] Handa, A., & Semwal, P. (2022). Evaluating performance of scalable fair clustering machine learning techniques in detecting cyber attacks in industrial control systems. In *Handbook of Big Data Analytics and Forensics* (pp. 105-116). Springer, Cham.

[7] Alqahtani, H., Sarker, I. H., Kalim, A., Hossain, M., Md, S., Ikhlaq, S., & Hossain, S. (2020, March). Cyber intrusion detection using machine learning classification techniques. In *International conference on computing science, communication and security* (pp. 121-131). Springer, Singapore.

[8] Almansob, S. M., & Lomte, S. S. (2017, April). Addressing challenges for intrusion detection system using naive Bayes and PCA algorithm. In *2017 2nd International Conference for Convergence in Technology (I2CT)* (pp. 565-568). IEEE.

[9] Elnour, M., Meskin, N., Khan, K., & Jain, R. (2020). A dual-isolation-forests-based attack detection framework for industrial control systems. *IEEE Access*, *8*, 36639-36651.

[10] Weng, C. H., Huang, T. C. K., & Han, R. P. (2016). Disease prediction with different types of neural network classifiers. Telematics and Informatics, 33(2),277-292.

[11] Peng, T., Zhou, J., Zhang, C., & Fu, W. (2017). Streamflow Forecasting Using Empirical Wavelet Transform and Artificial Neural Networks. Water, 9(6), 406.

[12] Yang, X. S. (2010). A new metaheuristic bat-inspired algorithm. In *Nature inspired cooperative strategies for optimization (NICSO 2010)* (pp. 65-74). Springer, Berlin, Heidelberg.

[13] Gandomi, A. H., Yang, X. S., Alavi, A. H., & Talatahari, S. (2013). Bat algorithm for constrained optimization tasks. *Neural Computing and Applications*, *22*(6), 1239-1255.

[14] Faghihnia, E., Farizani, S. R. K. T., & Kheirabadi, M. (2021). Improved intrusion detection system based on distributed self-adaptive genetic algorithm to solve support vector machine in form of multi kernel learning with auto encoder. *Journal of Intelligent Procedures in Electrical Technology*, *12*(45), 77-93.

[15] Tajari Siahmarzkooh, A. (2021). Intrusion Detection in Computer Networks using Decision Tree and Feature Reduction. *Electronic and Cyber Defense*, *9*(3), 99-108.

[16] Safara.M, Sabahnour. F, (2020). Increase the accuracy of detecting fake web pages using hyena optimization algorithm and artificial neural network. Journal of Command and Control, 3(4), 72-91.

[17] Benavides, E., Fuertes, W., Sanchez, S., & Sanchez, M. (2020). Classification of Phishing Attack Solutions by Employing Deep Learning Algorithms: A Systematic Literature Review. In Developments and Advances in Defense and Security (pp. 51-64). Springer, Singapore.