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

حفظ محرمانگی اطلاعات شخصی کاربران در سیستم‌های رایانه‌ای و تلفن‌های همراه با استفاده از الگوریتم گرگ خاکستری

الهه جان مشهدی [۱]
گروه مهندسی کامپیوتر، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران
delijan1354@gmail.com

علیرضا صفائی [۲]
گروه مهندسی کامپیوتر، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران
alisafasafaei@yahoo.com

چکیده : امنیت و حفظ محرمانگی اطلاعات شخصی کاربران یکی از ضروری‌ترین نیازهای جامعه می‌باشد که انواع مختلفی مانند امنیت فردی، امنیت دارایی، امنیت اطلاعات، امنیت اسناد و غیره را پوشش می‌دهد. تاکنون پیشنهاداتی جهت حفظ حریم خصوصی و امنیت سیستم‌های نرم‌افزاری توسط محققان صورت گرفته است. با این وجود هنوز هم به تحقیقات بیشتری نیازمند هستند تا دقت آنها افزایش بیشتری پیدا نماید. لذا در این تحقیق بر آن شدیم تا با استفاده از شبکه عصبی مصنوعی و الگوریتم گرگ خاکستری روشی ارائه دهیم که با دقت بالایی به شناسایی و تشخیص انواع بدافزار جهت حفظ محرمانگی اطلاعات شخصی کاربران در سیستم‌های رایانه‌ای و تلفن همراه بپردازد. نتایج بدست آمده از پیاده‌سازی روش پیشنهادی حاکی از آن است که مقادیر معیارهای دقت، ویژگی، حساسیت، صحت و F-Measur به ترتیب برابر با ۹۹.۵ درصد، ۹۹.۴۲ درصد، ۹۹.۵۹ درصد، ۹۹.۴۳ درصد و ۹۹.۵ درصد می‌باشد. همچنین مقایسه دقت روش پیشنهادی در این تحقیق با دقت الگوریتم‌های اسب، فیل و کفتار حاکی از آن است که روش پیشنهادی در این تحقیق نسبت به الگوریتم‌های مورد مقایسه از دقت و در نتیجه عملکرد بهتری جهت شناسایی و تشخیص انواع بدافزار جهت حفظ محرمانگی اطلاعات شخصی کاربران در سیستم‌های رایانه‌ای و تلفن همراه برخوردار است.

کلمات کلیدی: امنیت– تشخیص -سیستم رایانه‌ای-الگوریتم گرگ خاکستری- محرمانگی اطلاعات

۱ - مقدمه

امنیت یکی از ضروری‌ترین نیازهای جامعه می‌باشد که انواع مختلفی مانند امنیت فردی، امنیت دارایی، امنیت اطلاعات، امنیت اسناد و غیره را پوشش می‌دهد. گستردگی دسترسی به اینترنت در سطوح مختلف جامعه و پیدایش روزافزون برنامه‌های کاربردی جهت تبادل اطلاعات، مخاطرات دنیای سایبری را به یک مسئله مهم تبدیل کرده است به گونه‌ای که در سال‌های اخیر و با گسترش روزافزون استفاده از فضای مجازی و اینترنت، مسئله امنیت کاربران و سامانه‌ها و شرکت‌ها اهمیت بالاتری پیدا کرده است[۱]. درز اطلاعات حیاتی و یا شخصی کاربران می‌تواند حریم خصوصی آنها را نقض کرده و در مواردی به باج خواهی و یا ضررهای جبران ناپذیر منجر شود. این امر نیاز روزافزونی را ایجاد کرده تا محققان امنیت به دنبال روش‌های جلوگیری از آن باشند. اما هر چه تکنولوژی پیشرفت می‌کند این حملات نیز هدفمندتر و زیرکانه‌تر می‌شوند[۲،۳]. همچنین با پیشرفت فراوان در فناوری ارتباطات و گسترش استفاده از تلفن همراه و دستگاه‌های هوشمند، سیستم عامل اندروید به عنوان یکی از پرکاربردترین سیستم‌های عامل موبایل در جهان مطرح شده است. با افزایش استفاده از اپلیکیشن‌ها و برنامه‌های موبایلی، بدافزارها نیز به صورت گسترده‌تر و پیچیده‌تری در این سیستم‌ها نفوذ کرده‌اند. بدافزارها می‌توانند به دسترسی غیرمجاز به اطلاعات کاربر، نفوذ به حریم خصوصی، تخریب سیستم، سرقت

اطلاعات حساس و در بدترین حالت، آسیب به سلامت و امنیت کاربران منجر شوند[۴]. با توجه به این حقایق امنیت و حفظ محرمانگی اطلاعات شخصی کاربران به حوزه اصلی پژوهش‌ها تبدیل شده است زیرا نیاز به توسعه مکانیزمی وجود دارد که بتواند به طور فعال حملات را شناسایی کند. امروزه بدافزارها ناهنجاری‌های بسیاری را در حوزه فناوری اطلاعات ایجاد کرده‌اند و باعث مشکلات بسیاری در عملکرد سیستم‌ها شده‌اند به شکلی که وجود بدافزارها تبدیل به یک معضل اساسی شده است و تا به امروز کشورها خسارات بسیاری بابت آسیب‌های بدافزارها دیده‌اند. تاکنون جوامع هزینه‌های بالایی را صرف مجهز نمودن شبکه‌ها و سیستم‌های اطلاعاتی کرده‌اند تا بتوانند راهی به منظور مقابله با این بدافزارها پیدا نمایند[۵]. در این راستا کاربردهای هوش مصنوعی و یادگیری ماشین در امنیت و حفظ محرمانگی اطلاعات شخصی کاربران تنها به فرآیند نظارت و کنترل مسائل مختلف محدود نمی‌شود بلکه حضور هوش مصنوعی توانسته امنیت سایبری را نیز به یک امنیت هوشمند تبدیل نماید. یادگیری ماشین به عنوان یکی از شاخه‌های وسیع و پرکاربرد هوش مصنوعی به تنظیم و اکتشاف شیوه‌ها و الگوریتم‌هایی می‌پردازد که براساس آنها سیستم‌ها توانایی یادگیری پیدا می‌کنند و قادر خواهند انواع بدافزار را جهت حفظ محرمانگی اطلاعات شخصی کاربران در سیستم‌های رایانه‌ای و تلفن همراه شناسایی و تشخیص دهند[۶].

۲ – کارهای پیشین

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 ناوبیز و تکنیک گسسته‌سازی در فواصل 3-Interval و 5-interval را ارائه دادند. نتایج تجربی نشان می‌دهد که استفاده از الگوریتم ناوبیز 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].

۳ – بدافزار

بدافزار یا نرم‌افزار بدخواه یکی از ابزارهای اقدامات ضد امنیتی می‌باشد که بدون اجازه صاحب سیستم قصد انجام کارهای ناخواسته یا خرابکارانه را در سیستم دارد. اصطلاح بدافزار از دو واژه بدخواهانه[1] و نرم‌افزار[2] تشکیل شده 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. 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

[1] Malicious

[2] Software

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[۱۲].

۴ – رابطه امنیت اطلاعات و حریم خصوصی

با توجه ویژگی‌های عصر امروزی که عصر اطلاعات نیز نامیده شده است مهمترین سرمایه برای هر فرد و یا سازمان اطلاعات است به همین جهت در این عصر، امنیت اطلاعات جزء یکی از مهمترین مسائل امروزی گشته است. امنیت اطلاعات در واقع محافظت از اطلاعات در برابر طیف وسیعی از تهدیدات شامل دسترسی، کاربرد، افشاء، قطع، تغییر یا انهدام غیرمجاز اطلاعات است که با هدف تضمین استمرار فعالیت‌های کاری، به حداقل رساندن ریسک‌های کاری و به حداکثر رساندن میزان بازده سرمایه‌گذاری‌ها و فرصت‌ها صورت می‌پذیرد. طبق این دیدگاه، امنیت اطلاعات، تأثیر مثبت و دراماتیکی بر سازمان دارد. همچنین امنیت اطلاعات، کنترلی برای تضمین تداوم حفاظت از دارایی‌های سازمان از آسیب یا از دست دادن معنا شده است. به عبارت دیگر امنیت اطلاعات به حفاظت از اطلاعات و به حداقل رساندن خطر افشای اطلاعات در بخش‌های غیرمجاز اشاره دارد. امنیت اطلاعات مجموعه‌ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری و علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیر مجاز است [۱۳]. از منظر امنیت باید گفت که حفظ صحت (مالیت و مالکیت) اطلاعات و حفظ محرمانگی آنها تأمین کننده امنیت اطلاعات است یعنی اینکه اولاً اطلاعات شخصی یک فرد دچار تغییر و اصلاح غیرمجاز نشده و اطلاعات نادرست تولید نشود و ثانیاً اطلاعات شخصی افراد بدون مجوز قانونی تصاحب نشوند. ثالثاً بدون مجوز قانونی کسی مبادرت به افشا یا وقوف بر آنها نکند. از منظر حریم خصوصی اطلاعاتی آنچه بیش از همه مدنظر است، صیانت از اطلاعات واقعی و صحیح منتسب به اشخاص است، نه لزوماً تأمین و تضمین صحت اطلاعات و اصولاً قوانین حمایت کننده از اشخاص در قبال اطلاعات نادرست پیش از رواج فناوری اطلاعات و ارتباطات نیز وجود داشته‌اند (مثل جرم‌انگاری افترا). از آنجا که نقض هر یک از دو مؤلفه صحت و محرمانگی در خصوص اطلاعات ممکن است توأم با نقض حریم خصوصی اطلاعاتی به مفهوم پیش گفته باشد، یا نباشد، لذا در باب نسبت امنیت اطلاعات به مفهوم اخص کلمه با حریم خصوصی اطلاعاتی نمی‌توان قائل به انطباق کامل میان این دو شد و نسبت آنها را تساوی تلقی نمود بلکه به نظر می‌رسد با توجه به گسترده‌تر بودن بحث امنیت اطلاعات از حریم خصوصی اطلاعاتی از میان نسب اربعه می‌توان قائل به عموم و خصوص مطلق شد [۱۴].

۵ – سیستم عامل اندروید

سیستم عامل اندروید نخست به منظور تلفن‌های هوشمند و تبلت‌ها طراحی شد، سپس شرکت گوگل از این سیستم عامل برای تلوزیون‌ها و حتی اتومبیل‌ها استفاده کرد. از زمان ارائه نخستین نسخه، این سیستم عامل در حال بالغ شدن است و در طول این بازه ۱۶ نسخه از این سیستم عامل ارائه شده است. با گذشت زمان این سیستم عامل به علت مزایای بسیاری که دارد بسیار مورد توجه مردم در سرتاسر دنیا قرار گرفت، و این محبوبیت از چشم مهاجمان دور نماند و بدافزارهای مختلفی به منظور این سیستم عامل طراحی شد، به علت آن که امروزه اکثر مردم بیشتر کارهای روزانه خود و کارهایی که با اینترنت انجام می‌دهند از طریق موبایل‌ها و تبلت‌ها انجام می‌گیرد، اطلاعات مهمی در دستگاه‌هایشان ذخیره می‌شود و بدافزارها در این سیستم‌ها توانسته ضررهای جبران ناپذیری برای کاربران داشته باشد. همچنین موجب شد که تشخیص بدافزارها به منظور ایمن نمودن این سیستم عامل مورد توجه پژوهشگران قرار بگیرد و همواره در تلاش باشند تا با روش‌های مختلف بتوانند به بالاترین دقت در تشخیص بدافزارها در این سیستم عامل برسند. در حال حاضر ایمن نمودن این سیستم عامل از بدافزارها بزرگترین دغدغه پژوشگران و کاربران می‌باشد. در سیستم عامل اندروید برنامه‌ها این توانایی را دارند که اطلاعات و توانایی‌های خودشان را اشتراک‌گذاری کنند و این کار را از راه اشتراک‌گذاری انجام می‌دهند. این حالت دسترسی باید به درستی مدیریت گردد[۱۵].

۶ – چالش‌های امنیتی در اندروید

به علت محبوبیت بسیار بالا و استفاده‌های بسیار از سیستم عامل اندروید، موضوع امنیت و حفظ حریم خصوصی کاربرها در این سیستم عامل اهمیت ویژه‌ای پیدا کرده است. از بین تمامی کالاهای دیجیتالی که از اندروید استفاده می‌نمایند، گوشی‌های هوشمند دارای ویژگی‌های منحصر به فردی هستند که آنان را به یک هدف مناسب به منظور حمله کنندگان تبدیل نموده است. اتصال دائمی به اینترنت، منابع محدود که مانع از اجرای روش‌های شایع امنیتی می‌گردد، در کنار اطلاعات حساسی که بر روی گوشی است همانند مکان کنونی و قبلی کاربر، تاریخچه تماس‌های دریافت شده و ارسال شده، دفترچه اطلاعات مخاطبان، ایمیل‌های ذخیره شده، عکس‌ها و فیلم‌های بر روی گوشی و امکان

سواستفاده‌های مالی که قربانی می‌بایست آن را روی قبض تلفن همراه خودش پرداخت نماید از جمله این ویژگی‌ها می‌باشند. پس حفظ امنیت گوشی‌های اندروید به لیست چالش‌های امنیتی اضافه شده است. به منظور محافظت از داده‌های حساسی که بر روی گوشی است می‌بایست روش‌های کنترل دسترسی اعمال گردد به شکلی که با منابع محدود گوشی همانند قدرت پردازشی پایین و محدودیت انرژی سازگاری داشته باشد، کارایی گوشی را پایین نیاورد، متناسب با دانش غیرتخصصی کاربرها باشد و عمل کردن با آن به منظور کاربران آسان باشد[۱۶،۱۷].



شکل ۱: چالش‌های امنیتی اندروید

۷ –شبکه عصبی مصنوعی

در سال ۱۹۴۳ شبکه‌های عصبی مصنوعی برای اولین بار توسط مک کولاک و پیتس معرفی شدند [۱۸]. شبکه عصبی مصنوعی که از سیستم عصبی زیستی الهام گرفته شده است ایده‌ای برای پردازش اطلاعات است که همانند مغز انسان به پردازش اطلاعات می‌پردازد. امروزه به علت پشرفت تکنولوژی و پیچیده‌تر شدن مسائل در جهان استفاده از روش‌های نوین و جدید جایگزین اکثر روش‌های سنتی شده است که دیگر قادر نخواهند بود وضعیت موجود را بدرستی تخمین بزنند. از طرفی پیچیده شدن فرآیندهای موجود منجر به ایجاد مشکلاتی شده است که روش‌های سنتی قادر نخواهند بود در مورد آنها تصمیم‌گیری کنند. لذا روش‌ها و الگوریتم‌های جدیدی از قبیل شبکه عصبی مصنوعی جهت تحلیل این فرآیندها پدید آمده است. شبکه‌های عصبی مصنوعی که جهت مسائل طبقه‌بندی و شناسایی الگو طراحی شده‌اند، زیر شاخه‌ای از هوش مصنوعی هستند که قادر به درک ارتباطات و کشف نظم بین مجموعه‌ای از متغیرها می‌باشند. این شبکه از مجموعه نورون‌های عصبی با وزن‌های متفاوت با یکدیگر تشکیل شده است که پیام‌های ارسالی از هر نورون با یکدیگر جمع شده و بصورت یک پیام به مغز ارسال می‌گردد. شبکه عصبی مصنوعی از اجزای سازنده‌ای همچون لایه‌ها و وزن‌ها تشکیل شده است به نحوی که رفتار این شبکه‌ها به ارتباط بین این اجزا وابسته می‌باشد. شبکه‌های عصبی دارای سه نوع لایه ورودی، میانی و خروجی هستند که وظیفه دریافت داده‌ها، پردازش و تولید کمیت خروجی را برعهده دارند[۱۹].

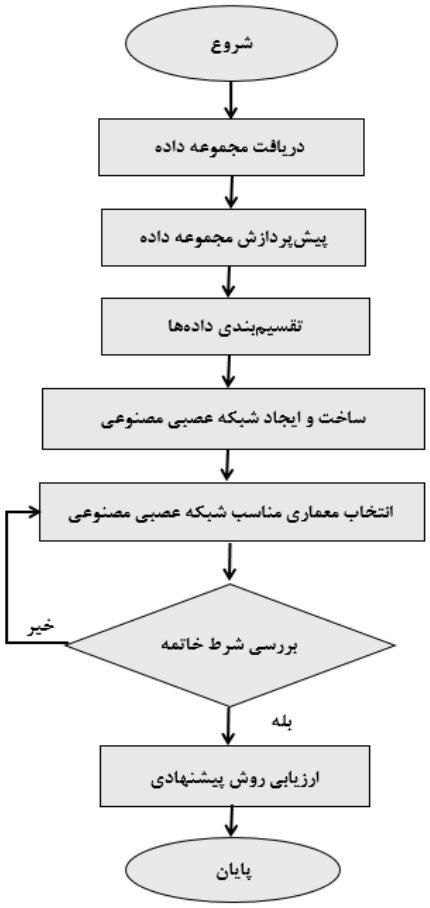
۸– الگوریتم گرگ خاکستری

الگوریتم گرگ خاکستری توسط میرجلیلی و همکاران ایشان در سال ۲۰۱۴ بر مبنای شکار دسته جمعی آنها ارائه شده است[۲۰]. گرگ خاکستری از خانواده گرگ‌های کشور کانادا است. گرگ‌های خاکستری در بالای زنجیره غذایی قرار دارند و ترجیح می‌دهند به صورت گروهی زندگی کنند. بطور میانگین، گروه‌های آنها ۵-۱۲ نفر است. جالب توجه است که آنها حکومت حاکم اجتماعی خیلی سختگیرانه‌تری دارند. به این صورت که گرگ آلفا، گرگ حاکم نیز در گروه نامیده می‌شود، چرا که دستورات او باید توسط گروه پیروی شود. آلفاها اساساً مسئول تصمیم‌گیری درباره شکار، جای خواب، زمان حرکت، و مانند آن هستند. دومین سطح درجه‌بندی گرگ‌های خاکستری بتا است، بتاها گرگ‌های تحت امر آلفا هستند که به آلفا در تصمیم‌گیری و دیگر فعالیت‌های گروه کمک می‌کنند. گرگ بتا، احتمالا بهترین کاندیدا برای آلفا شدن است و نقش یک معاون را برای آلفا و ناظم را برای گروه بازی می‌کند. پایین‌ترین طبقه گرگ خاکستری امگا است. گرگ‌های امگا نقش قربانی را برای سایر اعضای گروه دارند. آنها آخرین گرگ‌هایی هستند که اجازه خوردن غذا را دارند. اگر گرگی آلفا، بتا یا امگا نباشد او فرمانبردار(یا دلتا) نامیده می‌شود. گرگ‌های دلتا از آلفاها و بتاها تبعیت می‌کنند و به امگاها حکمرانی می‌کنند. پیشاهنگ‌ها و دیده‌بان‌ها، به این گروه تعلق دارند.

۹ –پیاده سازی روش پیشنهادی

پیاده‌سازی روش پیشنهادی در این تحقیق جهت شناسایی و تشخیص انواع بدافزار به منظور حفظ محرمانگی اطلاعات شخصی کاربران در سیستم‌های رایانه‌ای و تلفن‌های همراه بر روی سیستمی با پردازنده Corei7و میزان حافظ اصلی ۴ گیگابایت و سیستم عامل ویندوز ۱۰ اجرا شد. همچنین جهت پیاده‌سازی روش پیشنهادی از نرم‌افزار MATLAB R2017a استفاده نمودیم. برای این منظور در این تحقیق مجموعه داده موردنظر پس از دریافت در بازه بین صفر و یک مورد نرمال‌سازی قرار گرفت و در ادامه داده‌های موجود با استفاده از روش

هولداوت با نسبت ۷۰ به ۳۰ درصد به دو مجموعه داده آموزشی و مجموعه داده آزمایشی تقسیم‌بندی شدند. پس از مراحلی که ذکر شد به ایجاد شبکه عصبی پیشنهادی پرداختیم و در ادامه شبکه عصبی پیشنهادی ایجاد و با داده‌های آموزشی به وسیله الگوریتم گرگ خاکستری مورد آموزش قرار گرفت و در ادامه با استفاده از داده‌های آزمایشی ارزیابی و عملکرد آن مورد بررسی قرار گرفت. فلوچارت روش پیشنهادی در شکل (۳) نشان داده شده است.



شکل ۲: فلوچارت روش پیشنهادی

مراحل روش پیشنهادی به‌طور خلاصه و طبق آنچه که در شکل (۲) نشان داده شده است بدین صورت است که پس از دریافت مجموعه داده مربوطه از سایت Kaggle[3] داده‌های آن مورد پیش‌پردازش قرار گرفته و سپس داده‌ها بصورت تصادفی و با نسبت ۷۰ به ۳۰ به دو دسته داده‌های آموزشی و آزمایشی تقسیم‌بندی می‌شوند و در ادامه شبکه عصبی مصنوعی ایجاد و تعداد لایه‌ها و نورون‌های میانی آن توسط الگوریتم گرگ خاکستری تعیین و با استفاده از داده‌های آموزشی مورد آموزش قرار داده می‌شود. در پایان به ارزیابی روش پیشنهادی با استفاده از داده‌های آزمایشی پرداختیم.

۱۰ – معیارهای ارزیابی روش پیشنهادی

در این تحقیق برای سنجش و ارزیابی عملکرد روش پیشنهادی براساس ماتریس درهم‌ریختگی از معیارهای دقت، حساسیت، ویژگی، صحت، F-Measure استفاده می‌شود که عبارتند از :

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

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

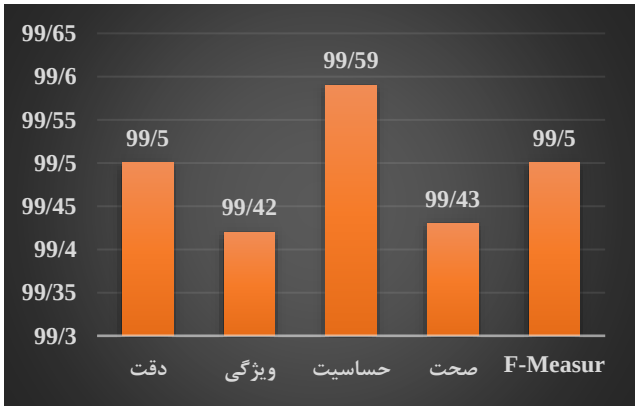
$$Specificity = \frac{TN}{FP+TN} \times 100 \quad (۳)$$

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

$$F-Measur = 2 \times \left(\frac{sensitivity \times precision}{sensitivity+precision} \right) \quad (۵)$$

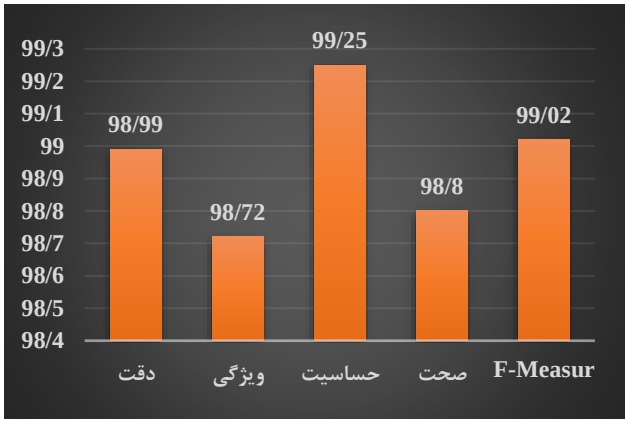
۱۱- نتایج بدست آمده

شبکه عصبی مصنوعی ایجاد شده را در این تحقیق توسط الگوریتم گرگ خاکستری بهبود داده و با یک لایه میانی و ۱۸ نورون میانی به تعداد ۱۰۰۰ مرتبه مورد آموزش و ارزیابی قرار گرفت. در ادامه نتایج بدست آمده برای داده‌های آموزشی و آزمایشی در شکل‌های (۳) و (۴) نشان داده شده است.



شکل ۳: نتایج بدست برای داده های آموزشی

[3] www.kaggle.com/nsaravana/malware-detection

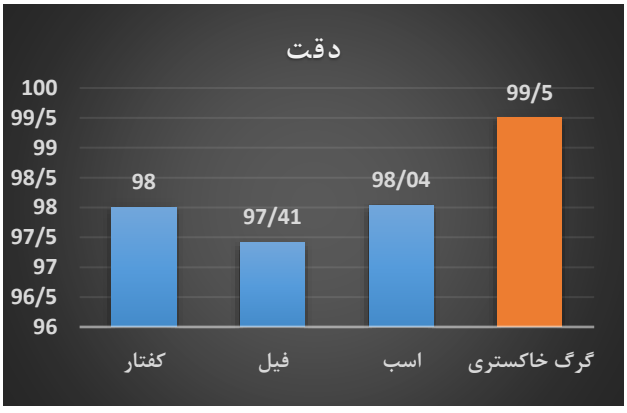


شکل ۴: نتایج بدست آمده برای داده‌های آزمایشی

باتوجه به نتایج بدست آمده از پیاده‌سازی روش پیشنهادی که در شکل (۳) و (۴) نشان داده شده است مشاهده می‌کنیم روش پیشنهادی از دقت و عملکرد خوبی جهت شناسایی و تشخیص انواع بدافزار جهت حفظ محرمانگی اطلاعات شخصی کاربران در سیستم‌های رایانه‌ای و تلفن همراه برخوردار است.

۱۲- مقایسه روش پیشنهادی با برخی از الگوریتم‌های فراابتکاری

در ادامه به مقایسه دقت بدست آمده از پیاده‌سازی روش پیشنهادی جهت شناسایی و تشخیص انواع بدافزار جهت حفظ محرمانگی اطلاعات شخصی کاربران در سیستم‌های رایانه‌ای و تلفن همراه با الگوریتم‌های اسب، فیل و کفتار پرداختیم که در شکل (۵) نشان داده شده است.



شکل ۵: مقایسه دقت روش پیشنهادی با برخی از الگوریتم‌های فراابتکاری

باتوجه به نتایج بدست آمده مشاهده می‌کنیم دقت روش پیشنهادی بوسیله الگوریتم گرگ خاکستری نسبت به الگوریتم‌های مورد مقایسه از عملکرد بالاتری جهت شناسایی و تشخیص انواع بدافزار جهت حفظ محرمانگی اطلاعات شخصی کاربران در سیستم‌های رایانه‌ای و تلفن همراه برخوردار است.

۱۳- نتیجه گیری

در سال‌های اخیر یکی از مهمترین چالش‌های امنیت اطلاعات و شبکه‌های ارتباطی، افزایش روز افزون انواع 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 این راستا استفاده از الگوریتم‌های هوش مصنوعی بعنوان یکی از روش‌های نوظهور و امیدوار کننده توانسته است کاربرد بسیاری جهت شناسایی و تشخیص انواع بدافزارها داشته باشد که لذا در این تحقیق بر آن شدیم تا با استفاده از هوش مصنوعی روشی ارائه دهیم که با دقت بالایی به شناسایی و تشخیص انواع بدافزار جهت حفظ محرمانگی اطلاعات شخصی کاربران در سیستم‌های رایانه‌ای و تلفن همراه بپردازد. نتایج بدست آمده از پیاده‌سازی روش پیشنهادی حاکی از آن است که مقادیر معیارهای دقت، ویژگی، حساسیت، صحت و F-Measur به ترتیب برابر با ۹۹.۵ درصد، ۹۹.۴۲ درصد، ۹۹.۵۹ درصد، ۹۹.۴۳ درصد و ۹۹.۵ درصد می‌باشد. همچنین مقایسه دقت روش پیشنهادی در این تحقیق با دقت الگوریتم‌های اسب، فیل و کفتار حاکی از آن است که روش پیشنهادی در این تحقیق نسبت به الگوریتم‌های مورد مقایسه از دقت و در نتیجه عملکرد بهتری جهت شناسایی و تشخیص انواع بدافزار جهت حفظ محرمانگی اطلاعات شخصی کاربران در سیستم‌های رایانه‌ای و تلفن همراه برخوردار است.

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,

Security, confidentiality, privacy and patient safety in the hospital information systems from the users' perspective: A cross-sectional study. International Journal of Medical Informatics, 175, 105066

[14] Li, Y., & Hu, X. (2022). Social network analysis of law information privacy protection of cybersecurity based on rough set theory. Library Hi Tech, 40(1), 133-151.

[15] Abdul Kadir, A. F., Habibi Lashkari, A., & Daghmehchi Firoozjaei, M. (2024). Android Operating System. In Understanding Cybersecurity on Smartphones: Challenges, Strategies, and Trends (pp. 25-42). Cham: Springer Nature Switzerland.

[16] Sharma, A., Singh, S. K., Kumar, S., Chhabra, A., & Gupta, S. (2021, September). Security of android banking mobile apps: Challenges and opportunities. In *International conference on cyber security, privacy and networking* (pp. 406-416). Cham: Springer International Publishing.

[17] Rawat, A., Kumar, A., Singh, A. K., & Arora, K. (2024). Exploring Android Security Landscape: Threats, Vulnerabilities, and Best Practices. *International Research Journal on Advanced Engineering and Management (IRJAEM)*, *2*(06), 1831-1839.

[18] 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

[19] Zadeh, L. A. (1996). Fuzzy sets. In *Fuzzy sets, fuzzy logic, and fuzzy systems: selected papers by LotfiA Zadeh* (pp. 394-432).

[20] Mirjalili, S., Mirjalili, S. M., & Lewis, A. (2014). Grey Wolf Optimizer Adv Eng Softw 69: 46–61.

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] Phattanaviroj, T., Moslehpour, M., & Walawalkar, A. M. (2024). Data Ethics and Privacy. In *Challenges in Large Language Model Development and AI Ethics* (pp. 321-353). IGI Global.

[5] Keshk, M., Turnbull, B., Sitnikova, E., Vatsalan, D., & Moustafa, N. (2021). Privacy-preserving schemes for safeguarding heterogeneous data sources in cyber-physical systems. *IEEE Access*, *9*, 55077-55097.

[6] Shashidhara, R., Ahuja, N., Lajuvanthi, M., Akhila, S., Das, A. K., & Rodrigues, J. J. (2021). SDN-chain: Privacy-preserving protocol for software defined networks using blockchain. *Security and Privacy*, *4*(6), e178.

[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] 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.

[13] Alipour, J., Mehdipour, Y., Karimi, A., Khorashadizadeh, M., & Akbarpour, M. (2023).