به نام خدا

عنوان:شناسایی حملات سایبری با استفاده از الگوریتم های هوش مصنوعی

تاریخ:۲۵-آبان_۱۴۰۰

نوع مسئله:یادگیری بانظارت(طبقه بندی)

مجموعه داده:کا دی دی۹۹[1]

کار های گذشته:

(حدیث کریمی پور و همکاران،۲۰۲۰)مجموعه ای مبتنی بر یادگیری عمیق برای تشخیص حمله سایبری در سیستم های کنترل صنعتی

ادغام شبکه های ارتباطی و اینترنت اشیا در سیستم های کنترل صنعتی آسیب پذیری آنها را در برابر حملات سایبری افزایش می دهد و نتایج مخربی را به دنبال دارد. سیستم های تشخیص نفوذ سنتی ، که عمدتا برای پشتیبانی از سیستم های فناوری اطلاعات توسعه یافته اند ، بر مدل های از پیش تعیین شده بسیار حساب می کنند و بیشتر در مورد حملات سایبری خاص آموزش می بینند. علاوه بر این ، بیشترسیستم های تشخیص سنتی ماهیت نامتعادل مجموعه داده های سیستم های های کنترل صنعتی را در نظر نمی گیرند ، بنابراین هنگام استفاده از آنها مدل های ایجاد شده از دقت کم و نرخ مثبت کاذب بالا رنج می برند. درمقاله نام برده شده ، محققان یک مدل یادگیری عمیق برای ایجاد نمایش های متوازن جدید از مجموعه داده های نامتعادل ارائه می دهند. نمایندگی های جدید در یک مدل تشخیص حمله یادگیری عمیق به طور خاص برای محیط کنترل صنعتی طراحی شده است. مدل تشخیص حمله پیشنهادی از طبقه بندی کننده های شبکه عصبی عمیق و درخت تصمیم برای تشخیص حملات سایبری از نمایندگی های جدید استفاده می کند. عملکرد مدل پیشنهادی

[1] KDD99

بر اساس اعتبار سنجی ۱۰ برابر بر روی دو مجموعه داده سستم های کنترل صنعتی واقعی ارزیابی شده است. نتایج این محققان نشان می دهد که روش پیشنهادی از طبقه بندی کننده های معمولی ، از جمله جنگل تصادفی ،شبکه عصبی عمیق،ادابوست ، و همچنین مدلهای اخیر موجود در ادبیات ، بهتر عمل می کند. رویکرد پیشنهادی توسط نویسندگان این مقاله یک تکنیک تعمیم یافته است که می تواند با حداقل تلاش در زیرساخت های سیستم های کنترل صنعتی موجود پیاده سازی شود.

(قاسم ابو الحاجی،۲۰۲۰)،یک سیستم تشخیص و طبقه بندی کارآمد مبتنی بر یادگیری عمیق برای حملات سایبری در شبکه های ارتباطی اینترنت اشیا

با گسترش سریع دستگاههای با منابع محدود و فناوریهای ارتباطی با سرعت بالا ، اینترنت اشیاء به عنوان استاندارد اولیه برای شبکه های کم توان شناخته شده است. با این وجود ، زیرساخت های اینترنت اشیاء به دلیل محدودیت در محاسبه ، ذخیره سازی و ظرفیت ارتباطی دستگاه های نقطه پایانی ، در برابر حملات سایبری آسیب پذیر هستند. از یک سو ، اکثریت حملات سایبری تازه توسعه یافته با کمی تغییر در حملات سایبری که قبلاً ایجاد شده اند ایجاد می شود تا یک حمله جدید ایجاد کند که معمولاً از طریق شبکه اینترنت اشیا به عنوان یک ترافیک معمولی تلقی می شود. از سوی دیگر ، تأثیر روشهای یادگیری عمیق با حوزه امنیت سایبری به دلیل عملکرد چشمگیر آنها به تمایل اخیر بسیاری از برنامه های امنیتی تبدیل شده است. در مقاله نام برده شده،محققان توسعه جامع یک سیستم تشخیص و طبقه بندی هوشمند و مستقل جدید مبتنی بر یادگیری عمیق را برای حملات سایبری در شبکه های ارتباطی اینترنت اشیا ارائه می دهند که از قدرت شبکه های عصبی کانولوشن ، سیستم تشخیص و طبقه بندی نفوذ با استفاده از شبکه عصبی کانولوشن[۲]از محاسبات با کارایی بالا استفاده می کند که از پردازنده های گرافیکی انودیا واحدهای پردازش

[۲] IoT-IDCS-CNN

گرافیکی مبتنی بر کوداو[۳] پردازش موازی که از سی پی یو های اینتل با سرعت بالا I9 استفاده می کند. به طور خاص ، سیستم پیشنهادی از سه زیر سیستم تشکیل شده است: یک زیر سیستم مهندسی ویژگی ، یک زیر سیستم یادگیری ویژگی ها و یک زیر سیستم طبقه بندی ترافیک. تمام زیر سیستم ها در این تحقیق توسعه ، تأیید ، یکپارچه و معتبر شده اند. برای ارزیابی سیستم توسعه یافته محققان این مقاله از مجموعه داده های شبکه امنیت آزمایشگاهی-کشف دانش[٤] استفاده کرداند که شامل تمام حملات کلیدی در محاسبات اینترنت اشیا می شود. نتایج شبیه سازی بیش از ۹۹,۳ و ۹۸,۲ دقت طبقه بندی حملات سایبری را برای طبقه بندی کننده کلاس دوتایی (عادی در مقابل ناهنجاری) و طبقه بندی کننده چند طبقه (پنج دسته) به ترتیب نشان داد. سیستم پیشنهادی با استفاده از روش اعتبارسنجی متقابل کا فولد تأیید شد و با استفاده از پارامترهای ماتریس در همریختگی یعنی منفی واقعی ، واقعی مثبت ، منفی کاذب ، مثبت کاذب ، ارزیابی شد. همراه با سایر معیارهای عملکرد طبقه بندی ، از جمله دقت ، فراخوانی ، نمره اف وان و نرخ هشدار کاذب. نتایج آزمایش و ارزیابی سیستم پیشهادی توسط نویسندگان این مقاله از بسیاری از سیستم های مبتنی بر یادگیری ماشین بهتر عمل می کند.

(ناواال چیلکارتی و همکاران،۲۰۱۷)، طرح تشخیص حمله توزیع شده با استفاده از روش یادگیری عمیق برای اینترنت اشیاء

امنیت سایبری همچنان یک مسئله جدی برای هر بخشی در فضای مجازی است زیرا تعداد موارد نقض امنیت در حال افزایش است. مشخص است که هزاران حمله روز صفر[٥]به دلیل افزودن حملات مداوم در حال ظهور هستند پروتکل های مختلف عمدتا از اینترنت اشیاء .بیشتر این حملات انواع کوچکی از حملات سایبری هستند که قبلاً شناخته شده بودند. این نشان می دهد که

[۳] Compute Unified Device Architectures (CUDA)
[٤] NSL-KDD
[٥] Zero day attack

حتی مکانیسم های پیشرفته مانند سیستم های یادگیری ماشین سنتی با مشکل تشخیص این جهش های کوچک حملات در طول زمان روبرو هستند. از سوی دیگر ، موفقیت یادگیری عمیق در زمینه های مختلف داده های بزرگ ، علایق متعددی را در زمینه های امنیت سایبری به خود جلب کرده است. یادگیری عمیق به دلیل بهبود جنبه های الگوریتم سی پی یو و شبکه عصبی کاربردی بوده است. استفاده از یادگیری عمیق برای تشخیص حمله در فضای مجازی می تواند یک مکانیسم مقاوم در برابر جهش های کوچک یا حملات جدید باشد زیرا قابلیت استخراج ویژگی های سطح بالا را دارد. قابلیتهای خودآموز و فشرده سازی معماریهای یادگیری عمیق مکانیزم های کلیدی برای کشف الگوی پنهان از داده های آموزشی هستند تا حملات از ترافیک خوش خیم متمایز شوند. در مقاله نام برده شده محققان تحقیقات خود را با هدف اتخاذ رویکرد جدید ، یادگیری عمیق ، در زمینه امنیت سایبری انجام داده اند تا امکان شناسایی حملات در اینترنت اجتماعی فراهم شود .از سوی دیگر عملکرد مدل یادگیری عمیق با رویکرد یادگیری ماشین سنتی مقایسه شده است و تشخیص حمله توزیع شده در برابر سیستم تشخیص متمرکز ارزیابی می شود. آزمایشات این محققان نشان داده است که سیستم تشخیص حمله توزیع شده توسط نویسندگان این مقاله با استفاده از مدل یادگیری عمیق بر سیستم های تشخیص متمرکز برتر است. همچنین نشان داده شده است که مدل عمیق در تشخیص حمله موثرتر از نمونه های کم عمق آن است.

(پروانه سلیمانس برایجانی و همکاران،۱۳۹٦)،ارائه یک الگوریتم مناسب برای پیشبینی حملات سایبری مبتنی بر یادگیری ماشینی

امروزه حملات سایبری، به طور گسترده با استفاده از آسیب پذیری های موجود در شبکه ها با قابلیت ها و شیوه های مختلفی، با اهداف متنوع به ویژه حمله به دارایی های اقتصادی، سیاسی و امنیتی افراد، سازمان ها و کشورها در حال افزایش هستند. طی سال های اخیر تحقیقات گسترده ای در حوزه سایبری صورت گرفته که اکثر این تحقیقات تمرکز خود را بر شناسایی و تشخیص نفوذ

قرار داده اند. این سیستم ها، تشخیص خود را پس از وقوع حمله یا در حین اجرای آن صورت می دهند. حال آنکه برای افزایش توانایی و قابلیت سیستم های دفاع سایبری، نیاز به بکارگیری مدل های پیشرفته تری وجود دارد که بتوانند علاوه بر تشخیص به هنگام، راهکارهای پیش بینی و دفاع پیش دستانه را نیز فراهم و حملات را قبل از وقوع و قبل از انجام فعالیت های خرابکارانه در شبکه متوقف سازند.نویسندگان در مقاله نام برده شده پس از بررسی مهم ترین روش های پیش بینی نفوذ موجود، به معرفی و ارائه یک سیستم کارآمد برای کمک به عملکرد و پاسخگویی به موقع و دقیق تر سیستم های سایبری مبتنی بر پیش بینی با برخورداری از الگوهای یادگیرنده می پردازند. سیستم ارائه شده قبل از آنکه شبکه در معرض خطر قرار گیرد آن را پایش کرده و از اطلاعات گذشته در راستای پیش بینی آینده استفاده می نماید. این سیستم پیش بینی نفوذ، می تواند کلاس یا گام بعدی حمله در حال اجرا را با بکارگیری تکنیک های یادگیری عمیق با دقت و سرعت مناسبی تعیین نماید و در مقابل حملات سایبری چند مرحله ای سطح امنیت شبکه را ارتقاء بخشد. نتایج حاصل از تحقیقات نویسنگان مقاله نام برده نشان می دهد که به کمک این سیستم پیش بینی، می توان یک مکانیسم دفاعی فعال در مقابل حملات پیشرو را فراهم آورد و امنیت هرچه بیشتر شبکه را تضمین نمود.

(دانیل اس برمن و همکاران،۲۰۱۹)،بررسی روشهای یادگیری عمیق برای امنیت سایبری

مقاله نام برده شرده شرح مختصری از نحوه اموزش روش یادگیری عمیق ، از جمله رمزگذارهای خودکار عمیق ، ماشین های بولتزمن ، شبکه های عصبی بازگشتی ، شبکه های عصبی مولد و چندین شبکه دیگر می باشد، سپس محققان مقاله نام برده شده نحوه استفاده و کاردبر هر یک از روشهای یادگیری عمیق در حوزه امنیت سایبری را مورد بحث قرار می دهند .نویسندگان مقاله نام برده شده طیف وسیعی از انواع حملات شامل بدافزار ، هرزنامه ، تهدیدهای داخلی ، نفوذ به شبکه ، تزریق داده های اشتباه و دامنه مخرب مورد استفاده بات نت ها مورد بررسی قرار داده اند.

(میروسلاو کومار و همکاران،۲۰۱۸)، فشرده سازی پارامترهای ترافیک شبکه برای تشخیص حملات سایبری بر اساس یادگیری عمیق

در مقاله نام برده شده روش فشرده سازی پارامترهای ترافیک شبکه در سیستم های تشخیص حملات سایبری به شبکه های مخابراتی با استفاده از شبکه عصبی ارائه شده همچنین تجزیه و تحلیل اجزای اصلی آن به صورت غیر خطی پیشنهاد شده است .نوینسدگان این مقاله توصیه می کنند شبکه عصبی عمیق شامل یک پرسپترون با لایه های زیاد باشد تا با استفاده از معماری عمیق بر محدودیت های پرسپترون کلاسیک چند لایه غلبه کند .مطالعات تجربی محققان تایید کرده است که روش پیشنهادی محققان این مقاله در طول تجزیه و تحلیل پارامترهای ترافیک شبکه ابعاد داده ها را کاهش می دهند همچنین دقت و صحت نتایج را بهبود می بخشد.

(ریکاردو تائورمینا و همکاران،۲۰۱۸)، روش یادگیری عمیق در تشخیص و بومی سازی حملات سایبری-فیزیکی به سیستم های توزیع آب

اخیرا افزایش فراوانی و شدت حملات سایبری-فیزیکی به تصفیه خانه ها و سیستم های توزیع ، مستلزم توسعه طرح های تشخیص نفوذ است که به حفاظت از این زیرساخت های حیاتی کمک می کند.**در مقاله نام برده شده محققان** یک الگوریتم است که به طور خاص برای تشخیص و بومی سازی حملات سایبری علیه سیستم های توزیع آب می باشند طراحی کرده اند. الگوریتم بر اساس ایده یادگیری یک مدل داده محور است که بازتولید الگوهای تمام فرآیندهای هیدرولیک مشاهده در یک سیستم توزیع می باشد. مدل با استفاده از داده های مربوط به شرایط عادی سیستم های توزیع آموزش داده شده است، به منظور بازتولید الگوهای ناهنجار ضعیف ، مانند الگوهای ناشی از حملات سایبری. فرایند مدل سازی با استفاده از رمزگذارهای خودکار[۱]انجام می شود، معماری شبکه عصبی عمیق قادر به ایجاد یک نمایش فشرده و معنی دار از الگوی داده ورودی با ابعاد بالا می باشد.این الگوریتم پس از توسعه یافتن توسط محققان مقاله نام برده شده بر روی سه مجموعه داده که برای شناسایی حملات سایبری ایجاده شده اند تست شده است، نتایج نشان می دهد که

[۱] Autoencoders

الگوریتم طراحی شده توسط نویسندگان این مقاله می تواند تمام حملات موجود در مجموعه داده ها را شناسایی کند، از جمله آنهایی که یکپارچگی داده ها را به خطر می اندازند. الگوریتم طراحی شده توسط نویسندگان این مقاله دارای دو ویژگی مهم دیگر است:اجزای مورد حمله را بومی می کند و فقط با استفاده از داده های مربوط به شرایط عادی کارکرد سیستم توزیع ، که عموماً به طور گسترده برای سیستم های آب و برق دردسترس است توسعه می یابد.

(علی ماروسی و همکاران ،۱۳۹۸)تشخیص نفوذ در شبکه با استفاده از ترکیب شبکه‌های عصبی مصنوعی به‌صورت سلسله مراتبی

با رشد فناوری اطلاعات، امنیت شبکه به‌عنوان یکی از مباحث مهم و چالش بسیار بزرگ مطرح است. سامانه‌های تشخیص نفوذ، مؤلفه اصلی یک شبکه امن است که حملاتی را که توسط فایروال‌ها شناسایی نمی‌شود، تشخیص می‌دهد. این سامانه‌ها با داده‌های حجیم برای تحلیل مواجه هستند. بررسی مجموعه داده‌های سامانه‌های تشخیص نفوذ نشان می‌دهد که بسیاری از ویژگی‌ها، غیرمفید و یا بی‌تأثیر هستند؛ بنابراین، حذف برخی ویژگی‌ها از مجموعه به‌عنوان یک راه‌کار برای کاهش حجم سربار و درنتیجه بالا بردن سرعت سیستم تشخیص، معرفی می‌شود. برای بهبود عملکرد سیستم تشخیص نفوذ، شناخت مجموعه ویژگی بهینه برای انواع حملات ضروری است. در مقاله نام برده شده محققان مدلی که بر اساس ترکیب شبکه‌های عصبی مصنوعی به‌منظور تشخیص نفوذ است ارئه می کنند، همچنین روشی را برای استخراج ویژگی‌های بهینه، بر روی مجموعه داده کا دی دی سی یو پی ۹۹[۷] که مجموعه داده استاندارد جهت آزمایش روش‌های تشخیص نفوذ به شبکه‌های کامپیوتری می‌باشد، ارائه می‌کنند.

(دیپانکار داسگپتا و همکاران ،۲۰۰۶)هوش محاسباتی در امنیت سایبری

[۷] KDD CUP 99

ثابت شده است که تکنیک های هوش محاسباتی در تصمیم گیری در محیط های پویا انعطاف پذیر هستند .آنها معمولاً شامل منطق فازی ، محاسبه تکاملی ، سیستم عامل های هوشمند ، شبکه های عصبی ، خودکارهای سلولی[۸]، سیستم های ایمنی مصنوعی و سایر مدل های محاسباتی مشابه هستند .استفاده از این تکنیک ها امکان ایجاد ماژول های پشتیبانی کارآمد و قوی را فراهم می کند و راه حل های ارتباط متقابل را برای برنامه های مختلف امنیت سایبری ارائه می دهد.

(ویتالی فورد و همکاران ،۲۰۱٤)،کاربرد های یادگیری ماشین در امنیت سایبری

تکنیک های یادگیری ماشین به دلیل ویژگی های منحصر به فرد خود مانند سازگاری ، مقیاس پذیری و پتانسیل سازگاری سریع با چالش های جدید و ناشناخته در بسیاری از زمینه های علمی مورد استفاده قرار گرفته اند .امنیت سایبری یک حوزه رو به رشد است که به دلیل پیشرفت چشمگیر در شبکه های اجتماعی ، فناوری های ابری و وب ، بانکداری آنلاین ، محیط تلفن همراه ، شبکه هوشمند و غیره توجه زیادی را به خود جلب کرد است و روش های متنوع یادگیری ماشین با موفقیت در این زمینه به کار گرفته شده اند.مشکلات مختلف در امنیت کامپیوتر وجود دارد در مقاله نام برده شده محققان کاربردهای مختلف یادگیری ماشین در امنیت سایبری را مورد بحث و بررسی قرار می دهند .مطالعات محققان این مقاله شامل تشخیص فیشینگ ، تشخیص نفوذ در شبکه ، آزمایش خصوصیات امنیتی پروتکل ها ، احراز هویت با پویایی فشار کلید ، رمزنگاری[۹]، اثبات تعامل انسان ، تشخیص اسپم در شبکه های اجتماعی ، پروفایل مصرف انرژی مترهای هوشمند و مسائل مربوط به امنیت خود تکنیک های یادگیری ماشین است .

(وای جی گو و همکاران،۲۰۱۸)، استفاده ازشبکه های عصبی بازگشتی و جی ٤۸ برای تجزیه و تحلیل تهدید در فضای امنیت سایبری اندروید

[۸] Cellular Automata

[۹] cryptography

شبکه های عصبی بازگشتی[1] کلاس خاصی از الگوریتم های یادگیری عمیق هستند که در سال های اخیر در زمینه علم داده بسیار مورد توجه قرار گرفته اند .در شبکه های عصبی بازگشتی ، گره های ورودی نه تنها ورودی های فعلی ، بلکه خروجی های قبلی را نیز در نظر می گیرند از این رو به آنها بازگشتی میگویند .در شرایط امروز ، تلفن های هوشمند تقریباً بخشی از زندگی روزمره هر فرد شده اند. تقاضا ، استفاده از دستگاه های اندروید بسیار زیاد شده است .با تسلط دستگاه های اندرویدی بر سهم کنونی بازار ، مسأله امنیت دستگاه های اندرویدی به طور طبیعی مطرح می شود .از سوی دیگر، میزان داده های بدافزار موجود برای تحقیقات نیز زیاد است .در مقاله نام برده شده نویسندگان قدرت و کارایی شبکه های عصبی بازگشتی اعمال شده بر روی داده های بدافزار اندرویدی را نشان می دهند .نویسندگان مقاله نامبرده شده یک مجموعه داده با بیش از سطر برچسب زده شده به عنوان مخرب یا سالم را مورد بررسی قرار می دهند. از آزمایش و تجزیه و تحلیل داده های محققان مقاله نام برده شده ، دقت پیش بینی ۰,۹٦٤ را با استفاده از شبکه های عصبی بازگشتی بدست آورده اند.

(میچل چارز و همکاران ،۲۰۱٤)، تکنیک های یادگیری ماشین برای تشخیص حملات سایبری

افزایش استفاده از خدمات ابری،تعداد روزافزون کاربران، تغییرات در زیرساخت شبکه‌ای که دستگاه‌های دارای سیستم‌عامل تلفن همراه را به هم متصل می‌کند، و فناوری شبکه در حال تکامل دائمی، چالش‌های جدیدی را برای امنیت سایبری ایجاد می‌کند که قبلاً هرگز پیش‌بینی نشده بود.در نتیجه، برای مقابله با تهدیدات ناشی، مکانیسم‌های امنیتی شبکه، حسگرها و طرح‌های حفاظتی نیز باید به منظور رسیدگی به نیازها و مشکلات کاربران امروزی تکامل یابند.

[1] Rnn

(میچل چارز و همکاران،۲۰۱۵) ،تکنیک‌های یادگیری ماشینی که برای شناسایی حملات سایبری به برنامه‌های کاربردی وب استفاده می‌شوند

افزایش استفاده از سرویس های ابری، تعداد فزاینده کاربران برنامه های کاربردی وب، تغییرات در زیرساخت شبکه که دستگاه های دارای سیستم عامل های تلفن همراه را به هم متصل می کند و فناوری شبکه دائماً در حال تحول، چالش های جدیدی را برای امنیت سایبری ایجاد می کند. در نتیجه، برای مقابله با تهدیدات ناشی، مکانیسم‌های امنیتی شبکه، حسگرها و طرح‌های حفاظتی نیز باید تکامل یابند تا نیازها و مشکلات کاربران را برطرف کنند. در مقاله نامبرده شده، محققین بر روی مقابله با حملات سایبری به لایه های مختلف برنامه در حال ظهور تمرکز می کنیم، زیرا این حملات به عنوان تهدیدات برتر و چالش اصلی برای امنیت شبکه و سایبری ذکر شده است. در مقاله نام برده شده محققین یک رویکرد یادگیری ماشینی برای مدل‌سازی رفتار نرمال برنامه و شناسایی حملات سایبری پیشنهاد کرده اند . مدل پیشنهادی محققین این مقاله از الگوهایی تشکیل شده است که با استفاده از تکنیک تقسیم بندی مبتنی بر نمودار و برنامه نویسی پویا به دست می آیند. مدل بر اساس اطلاعات به دست آمده از درخواست های اچ تی تی پی تولید شده توسط مشتری به یک وب سرور است. محققین این مقاله برای ارزیابی روش خود از محموعه داده های سی اس ای سی ۲۰۱۰ اچ تی تی پی استفاده کرده اند که نتایج حاصله رضایت بخش بوده است.

(دیف یو وانگ و همکاران،۲۰۱۹)، شناسایی اختلالات شبکه برق و حملات سایبری بر اساس یادگیری ماشینی

شبکه برق هوشمند مدرن در حالی که با تهدیدات امنیتی متعددی مواجه است همزمان می تواند روشی کارآمد برای مدیریت عرضه و مصرف انرژی فراهم کند. هر دو رویداد طبیعی و انسان می توانند باعث ایجاد اختلال در سیستم برق شوند. بنابراین، شناسایی علل و انواع اختلالات در سیستم برق برای اپراتورها جهت تصمیم گیری و واکنش مناسب بسیار مهم است. در مقاله نام برده

شده جهت حل این مشکل یک مدل تشخیص حمله برای سیستم برق مبتنی بر یادگیری ماشین پیشنهاد شده است که می‌تواند با استفاده از اطلاعات و گزارش‌های جمع‌آوری‌شده توسط واحدهای اندازه‌گیری فازور آموزش داده شود. محققین این مقاله مهندسی ویژگی را انجام داده اند و سپس داده ها را در اختیار مدل های مختلف یادگیری ماشین قرار داده اند، که در آن جنگل تصادفی به عنوان طبقه بندی اصلی آدابوست انتخاب شده است. مدل با استفاده از داده های سیستم قدرت شبیه سازی شده که از ۳۷ سناریو رویداد سیستم قدرت تشکیل شده است، ارزیابی می شود. سپس با استفاده از معیارهای ارزیابی مختلف دقت آن مورد ارزیابی قرار گرفته شده است و مدل پیشنهادی را با سایر مدل‌ها مقایسه کرده اند. همانطور که نتایج تجربی محققین این مقاله نشان می دهد که مدل پیشنهادی توسط محققین این مقاله می تواند به دقت ۹۳,۹۱٪ و نرخ تشخیص ۹۳,٦٪ بالاتر از هشت تکنیک اخیراً توسعه یافته دست یابد.

(مانجال ساروش و همکاران،۲۰۱۱)، ارزیابی الگوریتم های یادگیری ماشین برای تشخیص حملات دی داس[۱۱]

اخیراً، با افزایش آسیب جدی ناشی از حملات دی داس، تشخیص سریع حمله و مکانیسم‌های پاسخ مناسب ضروری است. سیستم های تشخیص دی داس مبتنی بر امضا نمی توانند حملات جدید را شناسایی کنند. سیستم‌های تشخیص ناهنجاری کنونی نیز قادر به شناسایی انواع حملات جدید نیستند، زیرا برای برنامه‌های کاربردی محدود در محیط‌های محدود طراحی شده‌اند. با این حال، مکانیسم‌های امنیتی موجود، دفاع مؤثری در برابر این حملات ارائه نمی‌دهند، یا قابلیت دفاعی برخی مکانیسم‌ها تنها به حملات دی داس خاص محدود می‌شود. تجزیه و تحلیل ویژگی های اساسی حملات دی داس ضروری است زیرا این حملات می توانند به راحتی پروتکل مورد استفاده یا روش عملیات را تغییر دهند. همچنین کارهای تحقیقاتی زیادی در شناسایی حملات با

---

۱۱ Ddo

استفاده از تکنیک های یادگیری ماشین انجام شده است. هنوز چه ویژگی‌های مربوطه وجود دارد و کدام تکنیک برای تشخیص حمله مناسب‌تر خواهد بود، یک سوال بدون جواب است. در مقاله نامبرده شده از مکانیزم‌های انتخاب ویژگی کای دو و اینفورمیشن گین[۱۲]برای انتخاب ویژگی‌های مهم استفاده می‌کنیم. با ویژگی های انتخاب شده، مدل های مختلف یادگیری ماشین، مانند نایو بیز، سی ٤,٥، ماشین بردارپشتیبان، کا نزدیک ترین همسایه، خوشه بند کی مینز وخوشه بندی فازی سی_ مینز برای تشخیص کارآمد حملات دی داس توسعه داده شده اند. نتایج تجربی محققان این مقاله نشان می‌دهد که خوشه‌بندی فازی سی_مینز دقت بهتری در شناسایی حملات می‌دهد.

در جدول زیر روش های مورد استفاده در برخی از مقالات نام برده شده را باهم مقایسه کرده ایم:

نام مقاله	الگوریتم های مورد استفاده	دقت	روش
مجموعه ای مبتنی بر یادگیری عمیق برای تشخیص حمله سایبری در سیستم های کنترل صنعتی	شبکه های عصبی مصنوعی	۹٦,۰۰	یک مدل شبکه عصبی برای محیط های کنترل صنعتی آموزش داده و با دو مجموعه داده مورد ارزیابی قرار داده اند و با کار های محققین پیشین مقایسه کرده اند.
روش یادگیری عمیق در تشخیص و بومی سازی حملات سایبری-فیزیکی به سیستم های توزیع آب	شبکه های عصبی خود رمز نگار، الگوریتم ایکس جی بی تی	۸۳,۵ ۹٤,۱	دو مدل ایکس جی بی تی و شبکه های عصبی خود رمزنگار را بر روی سه مجموعه داده آموزش داده و دقت آنها را مورد

[۱۲] Information gain

			ارزیابی و مقایسه قرار داده است
طرح تشخیص حمله توزیع شده با استفاده از روش یادگیری عمیق برای اینترنت اشیاء	شبکه های عصبی	۹۹.۲۰	از شبکه های عصبی استفاده شده
یک سیستم تشخیص و طبقه بندی کارآمد مبتنی بر یادگیری عمیق برای حملات سایبری در شبکه های ارتباطی اینترنت اشیا	شبکه های عصبی کانولوشنی	۹۹,۲۵	سه سیستم به شرح زیر توسعه داده اند:سیستمی برای مهندسی ویژگی سیستمی جهت یادگیری و یک سیستم جهت طبقه بندی
کاربرد های یادگیری ماشین در امنیت سایبری	درخت تصمیم،نایو بیز،ماشین بردار پشتیبان،شبکه های عصبی،لجستیک رگرسیون	۹٤.۱۸ ۹۱.۷۱ ۹۵.۱۱	مدل های مختلف را آموزش داده و نتایج آنها را با هم مقایسه کرده است

بیان مسئله:

با پیشرفت های اخیر تکنولوژی به سرعت در حال تغییر جهان است .بیست سال پیش ،سرعت اینترنت در مقایسه با امروز چیزی نبود.از سوی دیگر تجزیه و تحلیل و بهبود وضعیت امنیت سایبری دیگر یک مشکل در مقیاس انسانی نیست، با پیشرفت فناوری امنیتی ، مهاجمان سایبری در حال توسعه تکنیک های جدیدی برای نقض شدید امنیت سازمان ها و حمله به سیستم های با کدها و برنامه های مخرب خود هستند .تهدیدهایی مانند باج افزارها ، نرم افزارهای جاسوسی ،

حملات مهندسی اجتماعی ، تروجان ها و غیره به طور مداوم در حال رشد هستند و اینترنت را به مکانی ترسناک برای کاربران عمومی تبدیل کرده اند.باید ابزارهای دقیق تر و سریع تر ایجاد شود تا به تیم های امنیت اطلاعات کمک کنندکه خطر نفوذ به سیستم ها را کاهش داده و وضعیت امنیتی کاربران خود را به طور چشم گیری بهبود ببخشند. هوش مصنوعی و یادگیری ماشینی کاربردهای زیادی در زمینه های مختلف مانند صنعت پزشکی ، امور مالی ، بازی ، امنیت داده ها ، شبکه های اجتماعی و موارد دیگر دارند .یکی از زمینه هایی که می توان از هوش مصنوعی به صورت تدریجی در آن استفاده کرد ، امنیت سایبری است.هوش مصنوعی و یادگیری ماشینی به فناوری های حیاتی در امنیت اطلاعات تبدیل شده اند ، زیرا قادرند میلیون ها رویداد را به سرعت تجزیه و تحلیل کنند و انواع مختلفی از تهدیدها را شناسایی کنند. استفاده از فناوری های هوش مصنوعی و یادگیری ماشین برای امنیت سایبری مزایای زیادی دارد ، اما پیاده سازی آنها چالش برانگیز است زیرا به زیرساخت ها و پیش نیازهای خوبی نیاز دارند ،یادگیری ماشین و هوش مصنوعی نیازمند حجم عظیمی از داده های گذشته است برای نشان دادن نتیجه دقیق . هرچه بیشتر بهتر،یادگیری ماشین این داده ها را تجزیه و تحلیل می کند و یک راه حل کارآمد برای مشکلات فعلی و آینده ایجاد می کند .جمع آوری چنین داده هایی یک چالش بزرگ است .یادگیری ماشین می تواند در مرحله اولیه زمان بر باشد .مسئله مهم دیگر این است که هوش مصنوعی و یادگیری ماشین هنوز در مراحل اولیه خود در زمینه امنیت سایبری هستند .بنابراین ، در حال حاضر ، شما نمی توانید فقط به آنها وابسته باشید.

اهمیت:

در سال ۲۰۲۰ ، هزینه متوسط نقض اطلاعات ۳,۸٦ میلیون دلار در سطح جهان و ۸,٦٤ میلیون دلار در ایالات متحده بود .این هزینه ها شامل هزینه های کشف و پاسخگویی به این نقض و درآمد از دست رفته و آسیب طولانی مدت که به اعتبار شرکت ها تجاری وارد شده است می باشد.حملات

سایبری معمولاً یکی از شدیدترین خطرات برای امنیت جهانی تلقی می شوند .حملات سایبری از نظر دسترس پذیری و کارآیی مانند پنج سال قبل نیستند .بهبود فناوری و تکنیک های تهاجمی کارآمدتر این فرصت را برای مجرمان سایبری فراهم می کند که حملاتی را در مقیاس وسیع و با تأثیر بیشتر آغاز کنند .متجاوزان از روش های جدید استفاده می کنند و استراتژی های جامع تری را برای به خطر انداختن سیستم ها استفاده می کنند .به همین ترتیب ، سازمان ها استفاده از سیستم های دفاعی قوی که از هوش مصنوعی برای مبارزه با حملات سایبری استفاده می کنند ، آغاز کرده اند.الگوریتم های هوش مصنوعی قادرند میلیون ها رویداد را به سرعت تجزیه و تحلیل کنند و انواع مختلفی از تهدیدها را شناسایی کنند از بدافزارهایی که از آسیب پذیری های روز صفر استفاده می کنند تا شناسایی رفتارهای خطرناک که ممکن است منجر به فیشینگ شود .این الگوریتم ها با گذشت زمان یاد می گیرند و از اطلاعات گذشته استفاده می کنند تا انواع جدیدی از حملات را در حال حاضر شناسایی کنند.هوش مصنوعی روش ها و خدمات دفاعی را برای شناسایی و پاسخگویی به تهدیدات سایبری امکان پذیر می کند .استفاده از هوش مصنوعی در امنیت بسیار مفید بوده است به ظوری که در یک تحقیق ٦٩درصد از شرکت ها معتقد بوده اند به دلیل افزایش تعداد حملات روش هاس سنتی برای جاوگیری از انها نمی توانند پاسخگو باشند و بعترین راه حل اشتفاده از هوش مصنوعی میباشد.به گفته بسیاری از متخصصان فناوری اطلاعات ، امنیت دلیل اصلی پذیرش هوش مصنوعی در شرکت ها است .هوش مصنوعی نه تنها امنیت کلی فضای شایبری را افزایش می دهد ، بلکه عملیات شناسایی و جلوگیری را نیز به صورت خودکار انجام می دهد که این مسئله به تنهایی باعث صرفه جویی در زمان وهزینه ها می شود.

اهداف:

۱-پیداکردن الگوریتم مناسب برای شناسایی حملات سایبری

۲-کشف الگو های ناهنجار که منجر به نقض اطلاعات می شوند

۳-کاهش هزینه آموزش مدل ها و افزایش کارایی آنها

تعارف:

هوش مصنوعی:[۱۳]

هوش مصنوعی که گاهی اوقات هوش ماشینی نیز نامیده می شود شبیه سازی فرایندهای هوش طبیعی[۱۴]توسط ماشین ها به ویژه سیستم های رایانه ای است. به عبارت دیگر، هوش مصنوعی به سامانه‌هایی گفته می‌شود که می‌توانند واکنش‌هایی مشابه رفتارهای هوشمند انسانی از جمله، درک شرایط پیچیده، شبیه‌سازی فرایندهای تفکری و شیوه‌های استدلالی انسانی و پاسخ موفق به آن‌ها، یادگیری و توانایی کسب دانش و استدلال برای حل مسائل را داشته باشند،بطور خلاصه هوش مصنوعی را دانش ساخت وطراحی عامل هوشمند تعریف کرده اند.این علم کاربرد های فراوانی در علوم رایانه، علوم مهندسی،تجارت،پزشکی و بسیاری از علوم دیگر دارد بعنوان مثال: در پزشکی تجزیه و تحلیل صدا قلب،ربات های پرستار،ارائه مشاوره و پیش‌بینی احتمال مرگ بیمار برای هر روش جراحی....،در امورمالی و تجارت تجزیه وتحلیل بازار های مالی،پیش بینی قیمت سهام ها،معاملات الگوریتمی،مدیریت دارای و...از کاربرد های هوش مصنوعی در این علوم هستند. هوش مصنوعی، موضوعی بسیار گسترده است که شاخه‌های متعددی دارد. شاخه های هوش مصنوعی عبارتند از:یادگیری ماشینی،[۱۵]شبکه های عصبی[۱۶]سیستم های خبره[۱۷]، پردازش زبان طبیعی ،[۱۸] تشخیص گفتار[۱۹]و بینایی ماشین[۲۰]و- رباتیک[۲۱] و منطق فازی[۲۲]است.

---

۱۳ Artificial Intelligence
۱۴ Natural Intelligence
۱۵ machine learning
۱۶ Neural network
۱۷ Expert Systems
۱۸ Natural language processing
۱۹ speech recognition
۲۰ Machine vision
۲۱ robotic
۲۲ Fuzzy logic

یادگیری ماشین:

یادگیری ماشینی بخشی از هوش مصنوعی می باشد،که به مطالعه الگورتیم های رایانه ای که میتوانند به طور خودکار از طریق تجربه وبا استفاده از داده ها بهبود یابند می پردازد. این شاخه ای از هوش مصنوعی است بر اساس این ایده که سیستم ها می توانند از داده ها بیاموزند ، الگوها را تشخیص داده و با حداقل دخالت انسان تصمیم گیری کنند طراحی شده است.در ادامه به شرح چند الگوریتم مورد استفاده در این پروژه می پردازیم که عبارت اند از:

درخت تصمیم:

الگوریتم درخت تصمیم به خانواده الگوریتم های یادگیری ماشین با نظارت[۲۳]تعلق دارد. می توان از این الگوریتم برای حل مسائل طبقه بندی و رگرسیون استفاده کرد. هدف این الگوریتم ایجاد مدلی است که مقدار یک متغیر هدف را پیش بینی می کند، که برای این منظور درخت تصمیم از نمایش درختی برای حل مسئله استفاده می کند. گره برگ مربوط به یک برچسب کلاس است و ویژگی ها در گره داخلی درخت نشان داده می شوند.

جنگل تصادفی[۲۴]

جنگل‌های تصادفی یک روش یادگیری جمعی[۲۵]برای طبقه‌بندی، رگرسیون و سایر وظایف است که با ساختن تعداد زیادی درخت تصمیم در زمان آموزش عمل می‌کند. برای کارهای طبقه بندی،

[۲۳] supervised machine learning
[۲۴] Random Forest
[۲۵] ênsemble learning

خروجی جنگل تصادفی کلاسی است که توسط اکثر درختان انتخاب شده است. برای وظایف رگرسیون، میانگین یا میانگین پیش‌بینی درختان منفرد برگردانده می‌شود.

نایو بیز:[۲۶]

الگوریتم ساده بیز یک الگوریتم یادگیری نظارت شده است که بر اساس قضیه بیز است و برای حل مسائل طبقه بندی استفاده می شود.طبقه‌بندی‌کننده ساده بیز یکی از ساده‌ترین و مؤثرترین الگوریتم‌های طبقه‌بندی است که به ساخت مدل‌های یادگیری ماشین سریع کمک می‌کند که بتوانند پیش‌بینی‌های سریع انجام دهند.

یادگیری عمیق:[۲۷]

یادگیری عمیق که در زبان فارسی به یادگیری ژرف نیز ترجمه شده است بخشی از خانواده یادگیری ماشینی می باشد که بر روش های تمرکز دارد که مبتنی بر الگوریتم های شبکه عصبی مصنوعی[۲۸] هستند. این الگوریتم ها د تلاش اند که مغز انسان را شبیه‌سازی کنند.به طور خلاصه در یادگیری عمیق شبکه های عصبی مصنوعی و الگوریتم های مشابه مغز بشر از مجموعه های عظیم داده مهارت های مورد نظر را فرا می گیرند.همانطور که ما از طریق تجربه چیزهای جدید یاد می گیریم الگوریتم یادگیری عمیق نیز با هر بار تکرار یک کار مهارت خود را نسبت به دفعات قبلی بهبود می بخشد. دلیل استفاده از عبارت یادگیری عمیق این است که شبکه های عصبی لایه های مختلف یا عمیقی دارند که یادگیری را ممکن می سازد.

داده کاوی:[۲۹]

---

[۲۶] Naïve Bayes Classifier
[۲۷] Deep learning
[۲۸] Artificial neural network
[۲۹] Data mining

داده کاوی فرایندی برای تبدیل داده های خام به اطلاعات مفید می باشد،داده کاوی فرآیند استخراج و کشف الگوها در مجموعه داده های بزرگ است که شامل روش هایی در محل تلاقی یادگیری ماشین ، آمار و سیستم های پایگاه داده است.به عبارت دیگر داده کاوی یک زیرشاخه بین رشته ای علوم کامپیوتر و آمار با هدف کلی استخراج اطلاعات (با روشهای هوشمند) از مجموعه داده و تبدیل اطلاعات به یک ساختار قابل درک برای استفاده بیشتر است.

امنیت سایبری:[۳۰]

امنیت سایبری که به عنوان امنیت فناوری اطلاعات[۳۱]نیز شناخته می شود،شامل عمل محافظت از سیستم های مهم و اطلاعات حساس در برابر حملات دیجیتالی است ، برای مقابله با تهدیدات علیه سیستم ها و برنامه های شبکه ای طراحی شده است ، خواه این تهدیدها از داخل یا خارج از سازمان ناشی شوند.به طورکلی امنیت سایبری شامل حفاظت از سیستم ها و شبکه های رایانه ای در برابر افشای اطلاعات ، سرقت یا آسیب به سخت افزار ، نرم افزار یا داده های الکترونیکی آنها می باشد.

حمله سایبری:[۳۲]

حمله سایبری در رایانه‌ها و شبکه‌های رایانه‌ای حمله به هرگونه تلاش برای افشای، تغییر، غیرفعال کردن، تخریب، سرقت یا دستیابی و دسترسی غیرمجاز یا استفاده غیرمجاز از یک دارایی است،حمله سایبری به هر نوع تهاجمی گفته می شود که سیستم های اطلاعات رایانه ای ، شبکه های کامپیوتری ، زیرساخت ها یا دستگاه های رایانه شخصی را هدف قرار دهد.که بد افزار،فیشینگ،دی دواس[۳۳] و .. از متداول ترین این حملات هستند.

---

[۲] Cybersecurity
[۳۱] information technology
[۳۲] cyber attack
[۳۳] DDoS

بد افزار[۳۴]:

بدافزار نوعی برنامه کاربردی است که می تواند انواع کارهای مخرب را انجام دهد .برخی از انواع بدافزارها برای ایجاد دسترسی مداوم به یک شبکه طراحی شده اند ، برخی برای جاسوسی از کاربر به منظور دستیابی به اعتبارنامه یا سایر داده های ارزشمند طراحی شده اند ، در حالی که برخی دیگر به سادگی برای ایجاد اختلال طراحی شده اند.

فیشینگ[۳۹]

رمزگیری یا فیشینگ به تلاش برای به دست آوردن اطلاعاتی مانند نام کاربری، گذرواژه، اطلاعات حساب بانکی به طور کلی اطلاعات مهم کاربر از طریق جعل یک وبگاه، آدرس ایمیل و مانند آن‌ها گفته می‌شود.یا به بیان ساده‌تر هنگامی که شخصی تلاش می‌کند دیگری را فریب دهد تا اطلاعات شخصی او را در اختیارش بگیرد، یک حمله فیشینگ رخ می‌دهد.

ضرورت استفاده از هوش مصنوعی در امنیت سایبری:

مهاجمان راه‌های پیچیده‌تر و هوشمندانه‌تری برای هک کردن سیستم‌های فناوری اطلاعات و ارتباطات[۳۶] ایجاد کرده‌اند. میزان آسیبی که یک هکر فردی می تواند پس از نفوذ به یک سیستم وارد کند به خوبی درک شده است. بنابراین، سیستم‌های امنیت سایبری هوشمند به‌طور اجتناب‌ناپذیری برای بهبود حفاظت در برابر تهدیدات مخرب مهم شده‌اند. با این حال، از آنجایی که حملات بدافزار به طور چشمگیری در حجم و پیچیدگی افزایش می‌یابد، شناسایی و کاهش تهدیدها برای ابزارهای تحلیلی سنتی چالش برانگیزتر شده است. علاوه بر این، حجم عظیمی از داده های تولید شده توسط شبکه های بزرگ، کار شناسایی را پیچیده تر و چالش برانگیزتر کرده است.از این رو

[۳۴] Malware
[۳۵] Phishing
[۳۶] information and communication technology

ضرورت استفاده از الگورتیم های هوش مصنوعی برای کمک به متخصصان امنیت سایبری برای شناسایی و مقابله با تهدیدات سایبری بیشتر از قبل احساس می شود.

ابزار:

با توجه به اینکه با پایتون به راحتی می‌توان فرآیندهای دشوار را مدیریت کرد و استفاده از آن ساده است، در این پروژهش ما از زبان برنامه نویسی پایتون برای توسعه مدل ها خود استفاده میکنیم همچنین این زبان برنامه نویسی کتابخانه های فراوانی برای کار با الگورتیم های هوش مصنوعی و پردازش داده ها را دارا می باشد. پایتون مجموعه وسیعی از کتابخانه‌ها را برای توسعه هوش مصنوعی ارائه می‌دهد که شامل موارد پایه‌ای نیز هست که در زمان برنامه نویسی، صرفه جویی می‌کند. پایتون به دلیل کد جمع و جور و خواندنی‌اش مشهور است و از نظر قابلیت استفاده عملاً بی‌نظیر است. ساده و مختصر بودن پایتون دلیلی‌ست که آن را با سایرزبان‌های برنامه نویسی متفاوت می‌کند و به زمان کدنویسی کمتری نیاز دارد. همچنین به توسعه دهنده اجازه می‌دهد تا الگوریتم‌ها را بدون اجرا کردن، سریع آزمایش کند.

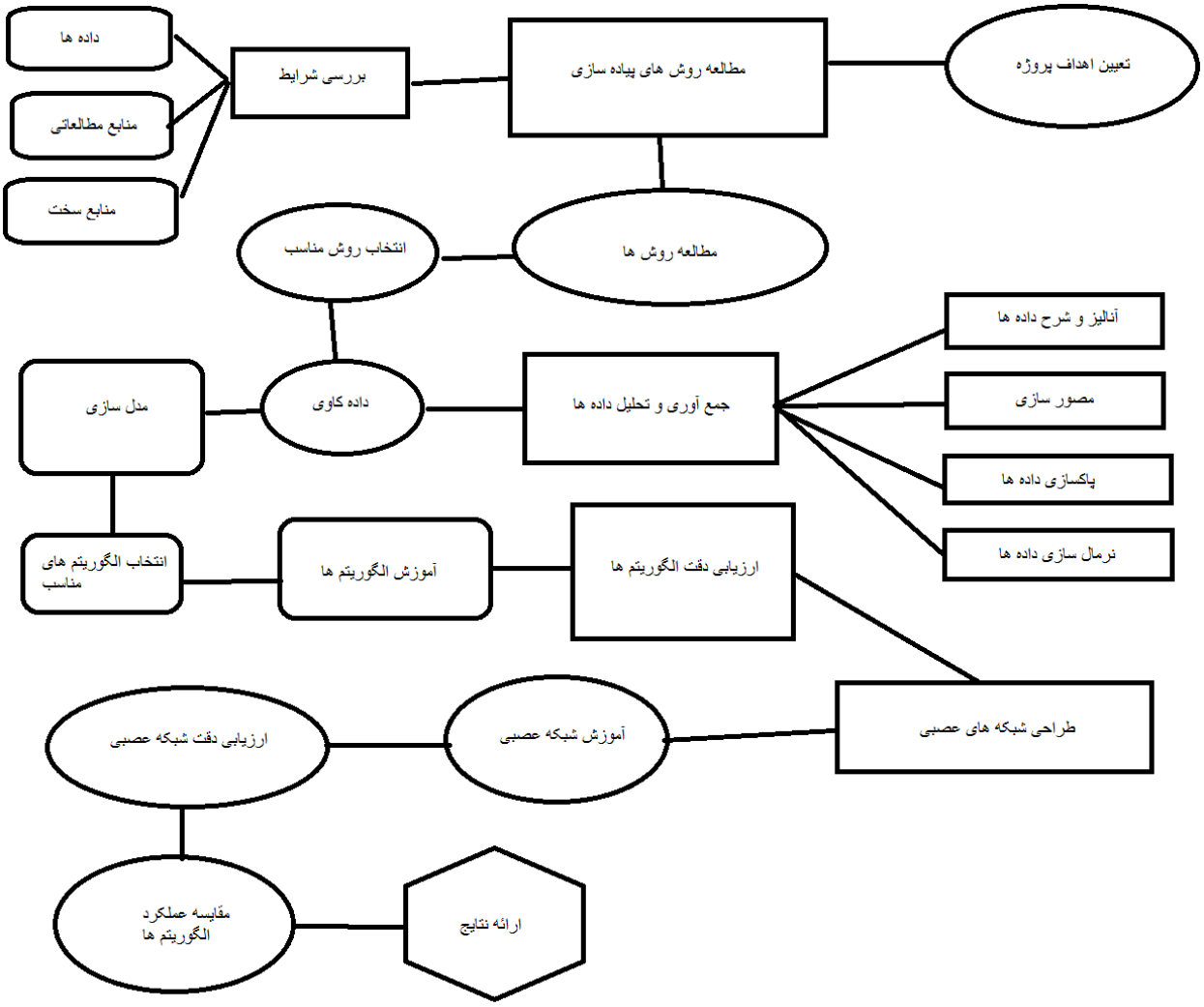
داده ها:

برای آموزش و ارزیابی روش پیشنهاد شده ما در این پژوهش از مجموعه داده ها کا دی دی ۹۹ استفاده میکنیم که شامل ٤٩٤٠٢٠سطر و ٤١ ستون ویژگی می باشد این مجموعه داده یکی از محبوب ترین و پرکاربرد ترین مجموعه داده ها در این زمینه می باشد.

روش کار:

در این پروژه ما ابتدا الگوریتم های یادگیری ماشین مانند ادابوست،جنگل تصادفی،درخت تصمیم ،نایو بیز و لجستیک رگرسیون را با داده های کادی دی ۹۹ آموزش داده و دقت آنها را مورد ارزیابی قرار میدهیم سپس یک شبکه عصبی کرده ایم و با استفاده از داده های که در اختیار داریم آن را

آموزش داده و دقت آن را میسنجیم.سپس نتایج حاصل از شبکه عصبی را بانتایج بدست آمده از الگوریتم های یادگیری ماشین مقایسه می کنیم.



شرح پروژه:

ابتدا کتابخونه های پانداز:برای خوندن فایل و تجزیه و تحلیل دیتافریم،نامپای:برای کار با آرایه های نامپای،مت پلات لیب:برای رسم نمودار،سیبورن:برای رسم نمودار،سایکیت لرن برای:استفاده از الگوریتم های یادگیری ماشینی،استاندارد کردن دیتا و اندازه گیری

خطا فراخوانی شده اند همچنین از کتابخانه های کراس و تنسرفلو برای ساخت شبکه های عصبی استفاده میکنیم.

مجموعه داده ما داری ٤٢ ستون و ٤٩٤٠٢٠سطر می باشد، در این مجموعه داده هیچ سطری با مقادی نامعلوم[٣٧]وجود ندارد.قطعه کد زیر پنج سطر ابتدای مجموعه داده ما را نشان می دهد:

```
[10] data.head()
```

	duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent	hot	num_failed_logins	logged_in	lnum_compromised	lroot_shell
0	0	tcp	http	SF	181	5450	0	0	0	0	0	1	0	0
1	0	tcp	http	SF	239	486	0	0	0	0	0	1	0	0
2	0	tcp	http	SF	235	1337	0	0	0	0	0	1	0	0
3	0	tcp	http	SF	219	1337	0	0	0	0	0	1	0	0
4	0	tcp	http	SF	217	2032	0	0	0	0	0	1	0	0

طبق جدول زیر حملات سایبری به ٤ دسته تقسیم می شوند:

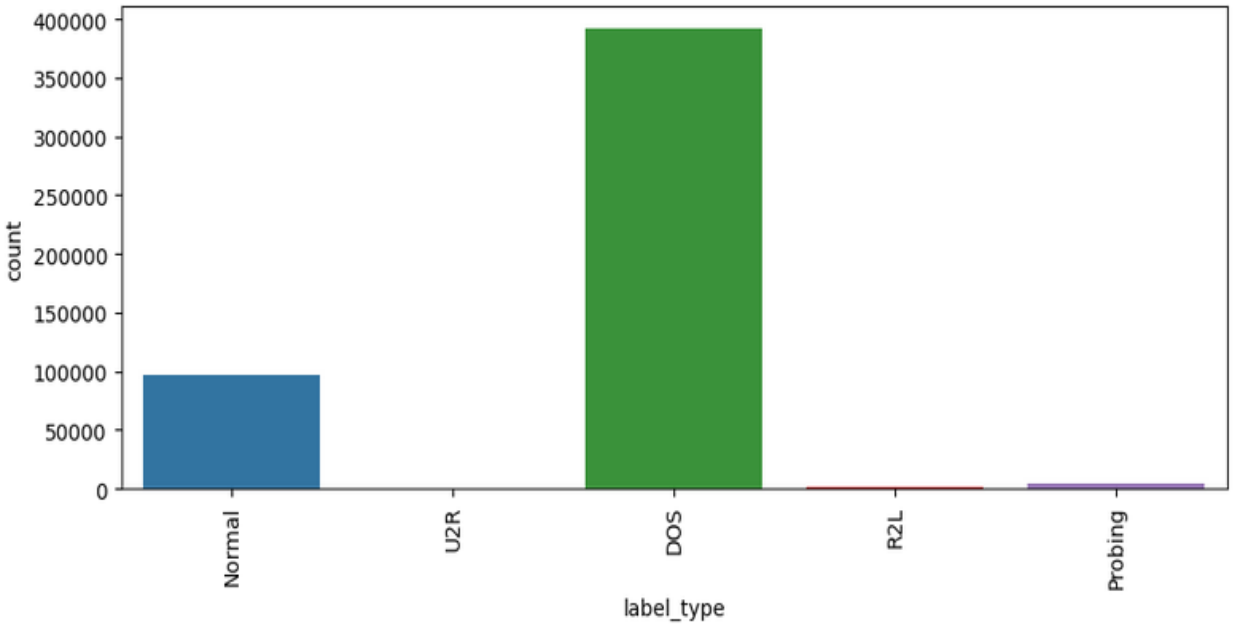
Attack class	Attack type
Dos	back, land, neptune, pod, smurf, teardrop
R2L	ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster
U2R	buffer_overflow, loadmodule, perl, rootkit
Probe	ipsweep, nmap, portsweep, satan

ما با قطعه کد زیر هر نوع حمله را به کلاس مربوطه خود نسبت داده و در ستونی با نام لیبل تیپ ذخیره میکنیم:

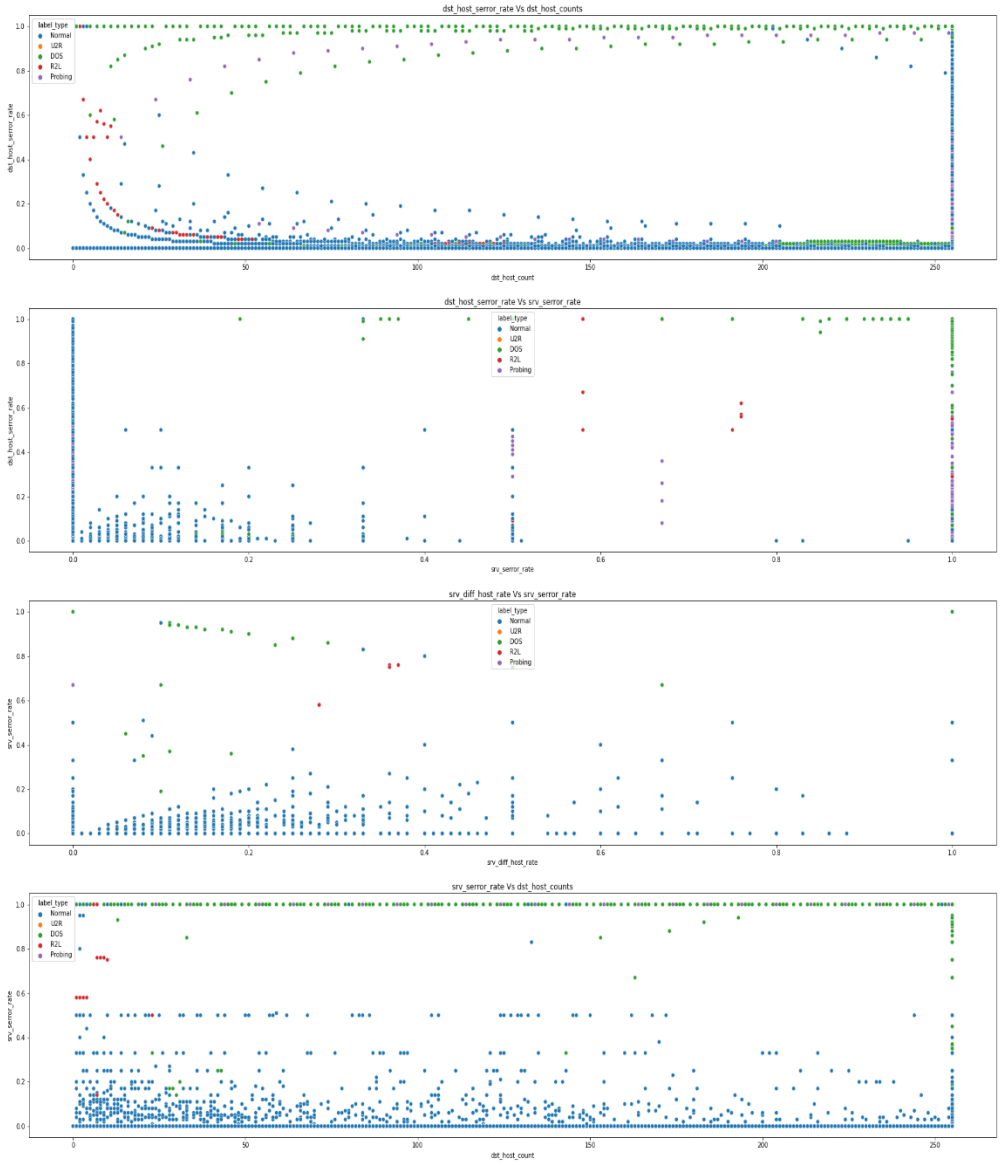
```
[16] data.loc[(data['label'].isin(['back','land','neptune','pod','smurf','teardrop'])),'label_type']='DOS'
     data.loc[data['label'].isin(['ipsweep','nmap','portsweep','satan']),'label_type']='Probing'
     data.loc[data['label'].isin(['ftp_write','guess_passwd','imap','multihop','phf','spy','warezclient','warezmaster']),
     data.loc[data['label'].isin(['buffer_overflow','loadmodule','perl','rootkit']),'label_type']='U2R'
     data.loc[data['label']=='normal','label_type']='Normal'
```

نمودار زیر سهم هرکدام از حملات حالت عادی را در داده ها موجودرا نشان می دهد:

[٣٧]NAN



نمودار زیر وضعیت ستون های مختلف را نسبت به یکدیگر نشان میدهد و همچنین برچسب هر داده با رنگ آن مشخص شده است:



قطعه کد زیر ستون های کت گوریکال را به ستون های عددی تبدیل می کند:

```
data=pd.get_dummies(data,prefix=['protocol_type'], columns = ['protocol_type'], drop_first=True)
data=pd.get_dummies(data,prefix=['service'], columns = ['service'], drop_first=True)
data=pd.get_dummies(data,prefix=['flag'], columns = ['flag'], drop_first=True)
```

کد های زیر به ترتیب این کار ها را انجام می دهند:۱-ویژگی ها را از لیبل ها جدا می کند-۲-لیبل ههها را با لیبل انکدور نامریک میکند که این روش مناسب الگوریتم های بادگیری ماشین می باشد که فقط میتوانند یک خروجی داشته باشند_۳_فرایند ترین تست اسپلیت را انجام میدهیم و داده ها را به دو دسته ترین ئ تست تقسیم میکنیم-٤-شیپ دیتافریم ها ایجاده شده را چاپ می کند_٥_داده ها را نرمالیز می کند :

```
train_test_split and LabelEncoders

x=data.drop("label_type",axis=1)
y=data.label_type

[92] le=LabelEncoder()
     y_ml=le.fit_transform(y)

[93] y_ml=y_ml.reshape(-1,1)

[97] xtrain,xtest,ytrain,ytest=train_test_split(x,y_ml,test_size=0.25,random_state=42)

[98] print("xtrain shape is",xtrain.shape)
     print("ytrain shape is",ytrain.shape,'\n')
     print("xtest shape is",xtest.shape)
     print("ytest shape is",ytest.shape)

normalizetion

[99] normalizer=Normalizer()
     xtrain_norm=normalizer.fit_transform(xtrain.values)
     xtest_norm=normalizer.transform(xtest.values)
```

کد ها زیر به ترتیب الگوریتم های یادگیری ماشین را ساخته و روی مجموعه داده ها آموزش داده و دقت مدل های ساخته شده را با معیار های مختلفی اعتبارسنجی می کنند:

```
#Machine Learning Algorithms
lr=LogisticRegression(random_state=42)
nb = GaussianNB()
dt=DecisionTreeClassifier(criterion="entropy",max_depth=5,random_state=42)
dt_gini=DecisionTreeClassifier(criterion="gini",max_depth=5,random_state=42)
rf=RandomForestClassifier(n_estimators=100,max_depth=5,random_state=42)
rf_entropy=RandomForestClassifier(criterion="entropy",n_estimators=100,max_depth=5,random_state=42)
ad=AdaBoostClassifier(n_estimators=50,random_state=42)
model_list=[lr,nb,dt,dt_gini,rf,rf_entropy,ad]
```

```
train_list=list()
test_list=list()
for model in model_list:
    model.fit(xtrain_norm,ytrain)
    train_score=model.score(xtrain_norm,ytrain)
    test_score=model.score(xtest_norm,ytest)
    print("train score: ",train_score,"and test score is: ",test_score)
    test_list.append(test_score)
    train_list.append(train_score)
    predict_test=model.predict(xtest_norm)
    print('\n',classification_report(ytest,predict_test),'\n')
    cm=confusion_matrix(ytest,predict_test)
    ax= plt.subplot()
    sb.heatmap(cm, annot=True, fmt='g', ax=ax);
    ax.set_xlabel('Predicted labels');ax.set_ylabel('True labels');
    ax.set_title('Confusion Matrix');
    plt.show()
    print('\n'+10*"*_* "+'\n')
```

قطعه کد های زیر داده ها را برا یادگیری شبکه عصبی آماده می کنند :

```
[108] y_deep=pd.get_dummies(y).values

[110] xtrain,xtest,ytrain,ytest=train_test_split(x,y_deep,test_size=0.25,random_state=42)

[111] print("xtrain shape is",xtrain.shape)
      print("ytrain shape is",ytrain.shape,'\n')
      print("xtest shape is",xtest.shape)
      print("ytest shape is",ytest.shape)

      xtrain shape is (370515, 115)
      ytrain shape is (370515, 5)

      xtest shape is (123505, 115)
      ytest shape is (123505, 5)

[112] normalizer=Normalizer()
      xtrain_norm=normalizer.fit_transform(xtrain.values)
      xtest_norm=normalizer.transform(xtest.values)
```

کد های زیر یک شبکه عصبی شامل۶ لایه دنس[۳۸]که ۵ لایه آن با تابع فعاسازی رلو[۳۹]را ساخته , و لایه آخر آن داری تابع فعالسازی سافت مکس[۴۰]می باشد در آموزش این شبکه از تابع بهینه ساز آدام و برای تابع هزینه از کت گوریکال کراس انتروپی استفاده شده است خلاصه ای از شبکه را ارائه می دهند در پایان نیز دقت آن سنجیده و چاپ می شود:

[۳۸] dense
[۳۹] relu
[۴۰] softmax

```
[113] dnn=Sequential()
      dnn.add(Dense(115,activation="relu"))
      dnn.add(Dropout(0.3))
      dnn.add(Dense(50, activation="relu"))
      dnn.add(Dropout(0.01))
      dnn.add(Dense(500,activation='relu'))
      dnn.add(Dense(250,activation='relu'))
      dnn.add(Dropout(0.1))
      dnn.add(Dense(100,activation='relu'))
      dnn.add(Dropout(0.2))
      dnn.add(Dense(5,activation='softmax'))

[114] dnn.compile(optimizer='adam',loss=tf.keras.losses.CategoricalCrossentropy(),metrics=["accuracy"])

[116] dnn.fit(xtrain_norm,ytrain,batch_size=64,epochs=20,shuffle = True)

      dnn.summary()

[120] y_pred_dnn=dnn.predict(xtest_norm)
      train_score=dnn.evaluate(xtrain_norm,ytrain)
      test_score=dnn.evaluate(xtest_norm,ytest)
      print("train score: ",train_score[1],"and test score is: ",test_score[1])
```

نتایج:

با پیشرفت روز افزون تکنولوژی مهاجمان از تکنیک های پیچیده‌تر و هوشمندانه‌تری برای هک کردن سیستم‌های استفاده میکنند، میزان آسیبی که یک هکر فردی می تواند پس از نفوذ به یک سیستم وارد کند بسیار زیاد است پس شناسایی به موقع حملات سایبری می تواند به میزان قابل توجهی صدمه وارد شده را کاهش دهد و یا در مواردی به صفر برساند، در آینده هوش مصنوعی زندگی بشر را متحول می سازد.ابزار های مبتنی بر هوش مصنوعی می توانند به متخصصین در شناسایی حملات سایبری کمک بسزای بکنند،ابزار های مبتنی بر هوش مصنوعی میتوانند با سرعت بیشتر اطلاعات در ابعاد وسیع را پردازش کرد و نتایج را در اختیار متخصصین قرار دهند.بنابراین امروزه استفاده از هوش مصنوعی در امنیت سایبری نه تنها مفید بلکه یک امر کاملا ضروری می باشد ما در این پژوهش تلاش کردیم تا عملکرد الگوریتم های مختلف یادگیری ماشین در تشخیص حملات سایبری را ارزیابی و ارائه کنیم که نتایج حاصل بدین شرح می باشد:الگوریتم های یادگیری ماشین نایوبیز ،لجستیک رگرسیون،جنگل تصادفی،درخت تصمیم و آدابوست به ترتیب به دقت

های ۹۹,۲۲،۹۹,۵۷،۹۹,۱۳،۹۸,۲۸،۹۵و۸۸,۵۹رو داده های تست دست یافته اند وعملکرد خوبی داسته اند اما شبکه های عصبی مصنوعی با دقت ۹۹,۸۷دقت عملکرد بهتری نسبت به این الگوریتم های یادگیری ماشین داشته است.

پیشنهادات کاربردی:

می توان سیستمی جهت شناسایی حملات سایبری توسعه داد که به متخصصین در حوزه امنیت کم کند تا در زمان کمتری این حملات را شناسایی کنند و راهکار دفاعی مناسب جهت خنثی سازی این حملات را به سرعت اتخاذ کنند و امنیت کاربران و شرکت های تجاری را افزایش دهیم،استفاده از هوش مصنوعی در امنیت سایبری علاوه بر اینکه میتواند خسارت ناشی از این حملات را کاهش دهد می تواند از وقئع این حملات جلوگیری کند و سبب تشخیص به موقع این حملات گردد.

پیشنهادات آتی:

دو سیستم مجزا توسعه داده شود یکی برای تشخیص اینکه حمله سایبری را شناسایی کند اگر سامانه اول حمله را تشخیص داد مشخصات به سامانه دوم فرستاده شود تا نوع دقیق حمله را سامانه دوم تشخیص دهد.از الگوریتم های یادگیری عمیق برای توسعه این سامانه ها استفاده شود همچنین از روش های انتخاب ویژگی جهت انتخاب ویژگی های مهم استفاده شود تا از دادن اطلاعات اضافه به الگوریتم ها جلوگیری شود.

محدودیت:

در این پروژه با محدودیت خاصی رو به رو نشدیم

References:

1- Al-Abassi, A., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2020). An ensemble deep learning-based cyber-attack detection in industrial control system. *IEEE Access*, *8*, 83965-83973.

2- Abu Al-Haija, Q., & Zein-Sabatto, S. (2020). An Efficient Deep-Learning-Based Detection and Classification System for Cyber-Attacks in IoT Communication Networks. *Electronics*, *9*(12), 2152.

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

٤-https://www.tpbin.com/article/٦٣٥١٩

٥-Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. *Information*, *10*(4), 122.

٦- Komar, M., Sachenko, A., Golovko, V., & Dorosh, V. (2018, May). Compression of network traffic parameters for detecting cyber attacks based on deep learning. In *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 43-47). IEEE.

٧- Taormina, R., & Galelli, S. (2018). Deep-learning approach to the detection and localization of cyber-physical attacks on water distribution systems. *Journal of Water Resources Planning and Management*, *144*(10), 04018065.

٨- ماروسی, علی, ذباح, عطایی خباز, & حسین. (٢٠٢٠). تشخیص نفوذ در شبکه با استفاده از ترکیب شبکه‌های عصبی مصنوعی به‌صورت سلسله مراتبی. *پدافند الکترونیکی و سایبری*, ٨(١), ٨٩-٩٩.

٩- Dasgupta, D. (2006, October). Computational intelligence in cyber security. In *2006 IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety* (pp. 2-3). IEEE.

١٠- Ford, V., & Siraj, A. (2014, October). Applications of machine learning in cyber security. In *Proceedings of the 27th international conference on computer applications in industry and engineering* (Vol. 118). Kota Kinabalu: IEEE Xplore.

١١- Teoh, T. T., Chiew, G., Jaddoo, Y., Michael, H., Karunakaran, A., & Goh, Y. J. (2018, July). Applying RNN and J48 deep learning in android cyber security space for threat analysis. In *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)* (pp. 1-5). IEEE.

١٢- Kozik, R., & Choraś, M. (2014). Machine learning techniques for cyber attacks detection. In *Image Processing and Communications Challenges 5* (pp. 391-398). Springer, Heidelberg.

١٣- Choraś, M., & Kozik, R. (٢٠١٥). Machine learning techniques applied to detect cyber attacks on web applications. *Logic Journal of the IGPL*, *23*(1), 45-56.

١٤- Wang, D., Wang, X., Zhang, Y., & Jin, L. (2019). Detection of power grid disturbances and cyber-attacks based on machine learning. *Journal of information security and applications*, *46*, 42-52.

15- Suresh, M., & Anitha, R. (2011, July). Evaluating machine learning algorithms for detecting DDoS attacks. In *International Conference on Network Security and Applications* (pp. 441-452). Springer, Berlin, Heidelberg.