به نام خدا

به کارگیری هوش مصنوعی در امنیت سایبری

مرضیه علیدادی ۸۱۰۱۰۱۲۳۶

مقدمه

امروزه کاربرد هوش مصنوعی در حوزه‌ی امنیت سایبری برای افزایش حفاظت از اطلاعات حساس و سیستم‌های حیاتی در حوزه‌ی مدیریت فناوری اطلاعات بسیار مورد توجه قرار گرفته‌است. راه‌حل‌های مبتنی بر هوش مصنوعی، طیف گسترده‌ای از مزایای بالقوه‌ای، از جمله تشخیص پیشرفته‌ی تهدید، واکنش سریع به حادثه، و مدیریت فعال ریسک ارائه می‌کند. با این حال، با توجه به این که سازمان‌ها به پذیرش هوش مصنوعی در امنیت سایبری فکر می‌کنند، با چالش مدیریت مؤثر ریسک‌های مرتبط و پیمایش در چشم‌انداز پیچیده‌ی پیامدهای مدیریتی و تجاری مواجه می‌شوند.

این مطالعه‌ی تحقیقاتی به دنبال بررسی مفاهیم چندوجهی استفاده از هوش مصنوعی در امنیت سایبری در زمینه‌ی مدیریت فناوری اطلاعات است. به طور خاص، هدف این مطالعه روشن کردن مزایای بالقوه‌ی استفاده از هوش مصنوعی، مانند بهبود دقت تشخیص تهدید، کاهش زمان پاسخ به حوادث امنیتی، و افزایش سازگاری با تهدیدات سایبری است. علاوه بر این، کاربردهای رایج هوش مصنوعی در مسائل امنیت سایبری، محدودیت‌های بالقوه‌ی ناشی از اتکا به هوش مصنوعی و چشم‌انداز حال و آینده‌ی این حوزه بررسی خواهد شد. و تعدادی از شرکت‌های فعال در این حوزه، مطالعه‌ی موردی خواهند شد.

۱ تعاریف اولیه

۱.۱ امنیت سایبری

امنیت سایبری عمل دفاع از رایانه‌ها، شبکه‌ها و داده‌ها در برابر حملات مخرب و دسترسی غیرمجاز است. امنیت سایبری به عنوان مجموعه‌ای از ابزارها، شیوه‌ها و دستورالعمل‌ها برای محافظت از شبکه‌های کامپیوتری، برنامه‌های نرم افزاری و داده‌ها در برابر حملات و دسترسی غیرمجاز تعریف می‌شود. این شامل جنبه‌های مختلفی از جمله امنیت شبکه، امنیت اطلاعات، امنیت برنامه‌ها، امنیت اینترنت اشیا و امنیت زیرساخت است. امنیت سایبری، سیاست‌ها، رویه‌ها و مکانیسم‌های فنی را برای محافظت، تشخیص، تصحیح و دفاع در برابر آسیب،

استفاده‌ی غیرمجاز یا اصلاح یا سوء استفاده از سیستم‌های اطلاعات و ارتباطی و اطلاعات موجود در آن قرار می‌دهد. امنیت سایبری به عنوان مجموعه‌ای از فرآیندها، رفتار انسانی و سیستم‌هایی تعریف می‌شود که به حفاظت از منابع الکترونیکی کمک می‌کند.

۲.۱ هوش مصنوعی

هوش مصنوعی کاربردهای گسترده‌ای در زمینه‌های مختلف از جمله امنیت سایبری دارد. هوش مصنوعی به این مسئله مربوط می‌شود که ماشین‌ها به درستی مانند انسان‌ها فکر کنند یا عمل کنند؛ یا اینکه نتایج را به حداکثر برسانند. این شامل حوزه‌هایی مانند پردازش زبان طبیعی، بازنمایی دانش، منطق، استدلال خودکار، یادگیری ماشین، ریاضیات و نظریه بازی می‌شود.
برنامه‌های کاربردی اولیه‌ی هوش مصنوعی شامل حل پازل‌ها و بازی‌ها بود، در حالی که برنامه‌های بعدی شامل ربات‌های اخلاقی برای موتورهای جستجو و ربات‌های مخرب برای تقلب، ارسال هرزنامه و انتشار بدافزار بود. تحقیقات امنیت سایبری بر شناسایی و محافظت در برابر ربات‌های مخرب با تجزیه و تحلیل رفتار و الگوهای ارتباطی آن‌ها متمرکز است. برنامه‌های کاربردی هوش مصنوعی در امنیت سایبری شامل سیستم‌های تشخیص نفوذ است که ترافیک اینترنت را تجزیه و تحلیل می‌کند تا آن را به عنوان قانونی یا مخرب طبقه‌بندی کند.
حوزه‌های اصلی هوش مصنوعی در امنیت سایبری شامل استدلال، برنامه ریزی، یادگیری، ارتباطات و ادراک است. این حوزه‌ها حوزه‌های علمی مختلف هوش مصنوعی مانند بازنمایی دانش، یادگیری ماشین، پردازش زبان طبیعی، بینایی ماشین و پردازش صوتی را در بر می‌گیرند. فناوری‌های هوش مصنوعی مورد استفاده در امنیت سایبری شامل منطق فازی، الگوریتم‌های ژنتیک، یادگیری عمیق، SVM، تحلیل احساسات، پردازش تصویر و پردازش گفتار است.
سیستم‌های مبتنی بر قوانین در ابتدا برای شناسایی حملات سایبری استفاده می‌شدند، اما با افزایش تعداد دستگاه‌ها و برنامه‌ها، تکنیک‌های یادگیری ماشین موثرتر شدند. راه حل‌های مبتنی بر یادگیری ماشین تشخیص حمله را خودکار می‌کنند و با یادگیری از ترافیک اینترنت جمع آوری شده در طول زمان بهبود می‌یابند. تکنیک‌های یادگیری ماشین می‌توانند حجم زیادی از داده‌ها و طیف گسترده‌ای از ویژگی‌ها را مدیریت کنند و آن‌ها را برای سیستم‌های تشخیص نفوذ در امنیت سایبری ارزشمند می‌سازند. سیستم‌های هوش مصنوعی در امنیت سایبری با تجزیه و تحلیل محیط و انجام اقداماتی برای دستیابی به اهداف خاص، رفتار هوشمندانه‌ای از خود نشان می‌دهند.

۲ راه حل‌های هوش مصنوعی مورد استفاده در مسائل امنیت سایبری

مدیریت هوشمند امنیت سایبری، مبتنی بر هوش مصنوعی است و از روش‌های مختلف هوش مصنوعی برای تصمیم‌گیری هوشمند در برنامه‌های سایبری استفاده می‌کند. روش‌های یادگیری ماشین، یادگیری عمیق، NLP و سیستم‌های مبتنی بر قانون، از جمله تکنیک‌های رایج هوش مصنوعی هستند که در مدل‌سازی اطلاعات امنیتی استفاده می‌شوند.

مدل‌سازی مبتنی بر یادگیری ماشین از داده‌های گذشته‌ی امنیت سایبری برای ایجاد مدل‌های امنیتی مؤثر با استفاده از الگوریتم‌هایی مانند یادگیری بانظارت، یادگیری بدون نظارت و بهینه‌سازی ویژگی‌های امنیتی استفاده می‌کند. در یادگیری بانظارت، نمونه داده‌ها برچسب گذاری می‌شوند و برای ایجاد یک مدل ریاضی برای طبقه‌بندی داده‌های جدید استفاده می‌شوند. تکنیک‌های یادگیری بانظارت شامل درخت‌های تصمیم، SVM و روش‌های ensemble هستند که می‌توانند برای طبقه‌بندی و پیش‌بینی حملات بدافزار یا ناهنجاری‌های سایبری استفاده شوند. الگوریتم‌های یادگیری بدون نظارت، انسجام/پراکندگی بین نمونه داده‌ها را برای ایجاد کلاس‌ها تعیین می‌کنند. تکنیک‌های یادگیری بدون نظارت، مانند الگوریتم‌های خوشه‌بندی، می‌توانند برای یافتن الگوها و ساختارها در داده‌های امنیتی بدون برچسب استفاده شوند. تمایز بین یادگیری بانظارت و بدون نظارت مبهم است، زیرا الگوریتم‌های بدون نظارت می‌توانند داده‌های مورد استفاده توسط الگوریتم‌های بانظارت را برچسب گذاری کنند. بهینه‌سازی ویژگی‌های امنیتی شامل انتخاب ویژگی‌های امنیتی مهم و به حداقل رساندن پیچیدگی مدل‌های امنیتی است. Naïve Bayes یک تکنیک یادگیری ماشین است که برای طبقه‌بندی بر اساس قضیه بیزی استفاده می‌شود. در روش SVM صفحه‌ای که نمونه داده‌ها را به دو کلاس جدا تقسیم می‌کند، تشخیص داده می‌شود؛ و همچنین در صورت چند کلاسه بودن داده‌ها، با استفاده از بیش از یک صفحه، این تقسیم‌بندی انجام می‌شود.

درخت تصمیم با یافتن مکرر ویژگی‌هایی که نمونه داده‌ها را دسته‌بندی می‌کنند، ایجاد می‌شوند و در نتیجه ساختاری درخت‌مانند ایجاد می‌شود. درخت تصمیم روشی بصری برای تشخیص مسائل امنیت سایبری ارائه می‌دهند.

تکنیک‌های یادگیری مبتنی بر قوانین، مجموعه‌ای از ویژگی‌ها را در هر تکرار پیدا می‌کنند و در عین حال کیفیت نتایج طبقه‌بندی را به حداکثر می‌رسانند.

تکنیک K-Nearest Neighbor (k-NN) با استفاده از نمونه داده‌ها برای ایجاد کلاس‌ها یا خوشه‌ها آموزش داده می‌شود.

یادگیری عمیق برای غلبه بر محدودیت‌های یادگیری ماشین با تقلید از فرآیند نورون‌های انسانی و ساختن معماری‌های عصبی پیچیده پیشنهاد شد. یادگیری عمیق به طور گسترده در سناریوهای صنعتی و حوزه‌های تحقیقاتی مختلف استفاده می‌شود که به یادگیری بانظارت، یادگیری بدون نظارت و یادگیری تقویتی طبقه بندی می‌شود. کاربردهای آن شامل تشخیص تصویر و ویدئو با استفاده از شبکه‌های عصبی کانولوشن عمیق (CNN)، تجزیه و تحلیل متن و پردازش زبان طبیعی، و امور مالی، اقتصاد و تحلیل بازار است. این روش، در تشخیص تصویر و ویدئو، اندازه‌ی تصویر را از طریق کانولوشن و ادغام کاهش می‌دهد و امکان تشخیص سریع‌تر اشیا را در زمان واقعی فراهم می‌کند. همچنین، در تجزیه و تحلیل متن و پردازش زبان طبیعی برای ترجمه و تعامل انسان و ماشین با گفتار طبیعی استفاده می‌شود. روش‌های یادگیری عمیق، مانند شبکه‌های عصبی مصنوعی (ANN) و معماری‌های یادگیری عمیق مانند CNN و LSTM، می‌توانند برای تشخیص نفوذ شبکه، طبقه‌بندی ترافیک بدافزارها و تجزیه و تحلیل ناهنجاری‌های سایبری استفاده شوند. تکنیک یادگیری شبکه‌های عصبی مصنوعی (ANN) نورون ها را بر اساس یک معادله ریاضی مدل می‌کند. ANN ها می‌توانند الگوهای مختلف

در نمونه داده‌ها، حتی نمونه داده‌های دارای نویز یا ناقص را تشخیص دهند. شبکه عصبی Cascade Correlation یا به اختصار (CCNN) گام به گام واحدهای پنهان جدیدی را به لایه‌ی پنهان اضافه می‌کند. ANN ها می‌توانند برخی حملات سایبری را شناسایی کرده و از حوادث اخیر درس بگیرند. ANN ها برای برنامه‌های امنیت سایبری مناسب هستند که در آن‌ها کلاس حمله می‌تواند هنگام وقوع حادثه برچسب گذاری شود.

پردازش زبان طبیعی (NLP) شاخه‌ی مهمی از هوش مصنوعی است که برای درک و پردازش داده‌های بدون ساختار در امنیت سایبری استفاده می‌شود. تجزیه و تحلیل لغوی (lexical) متن را به پاراگراف‌ها، جملات، عبارات یا نشانه‌ها تقسیم می‌کند و می‌تواند برای طبقه‌بندی دامنه‌های مخرب استفاده شود. تجزیه و تحلیل نحوی (syntactic) تعیین می‌کند که چگونه زبان طبیعی با قواعد دستوری همسو می‌شود و می‌تواند به مدل‌های مبتنی بر (NLP) برای پیش‌بینی حملات سایبری کمک کند. تجزیه و تحلیل معنایی (semantic) شامل درک زمینه و درک کلمات است و می‌تواند برای کارهایی مانند طبقه‌بندی رمزگیری (حمله‌ی phishing یا رمزگیری: تلاش برای به دست آوردن اطلاعاتی مانند نام کاربری، گذرواژه، اطلاعات حساب بانکی، IP و مانند آن‌ها از طریق جعل یک وبگاه، آدرس ایمیل و مانند آن‌ها؛ یا به بیان ساده‌تر، تلاش شخصی برای فریب شخصی دیگر، برای در اختیار گرفتن اطلاعات شخصی او) و تشخیص وضعیت امنیت سایبری در شبکه‌های (IoT) استفاده شود.

۳ کاربرد هوش مصنوعی در امنیت سایبری

راه حل‌ها و روش‌های مختلف هوش مصنوعی در مسائل متعددی از امنیت سایبری به کار گرفته شده‌اند. تعدادی از این مسائل در ادامه معرفی و شرح داده شده است.

۱.۳ احراز هویت دسترسی کاربر

احراز هویت دسترسی کاربر، جنبه‌ی مهمی از امنیت سایبری است و نیاز به شناسایی دقیق رفتارهای استتار و شناسایی اهداف غیرقانونی یا مخرب دارد. سیستم باید از احراز هویت کاربر اطمینان حاصل کند و محرمانه بودن داده‌های کاربر را حفظ کند، تا از خطراتی مانند جمع‌آوری مخرب اطلاعات کاربر جلوگیری کند.

۱.۱.۳ احراز هویت چندگانه

احراز هویت یک چالش در تضمین امنیت با تطبیق رمزهای عبور و ترکیب ویژگی‌های کاربر است. احراز هویت یک حالته، مانند کدهای پین، برای تضمین امنیت احراز هویت کافی نیست. فناوری‌های احراز هویت چندگانه، برای رفع محدودیت‌های احراز هویت یک‌حالته توسعه یافته‌اند. این فناوری‌ها از روش‌هایی مانند جنگل تصادفی و شبکه‌های عصبی برای افزایش امنیت استفاده می‌کنند. روش‌های دیگر، مانند استفاده از Support Vector Regression و SVM یک کلاسه، برای احراز هویت مورد بررسی قرار گرفته‌اند.

۲.۱.۳ احراز هویت زیست‌سنجی

احراز هویت زیست‌سنجی biometric به دلیل منحصر به فرد بودن، غیرقابل تکرار بودن، وراثت و تغییر ناپذیری آن به طور گسترده مورد استفاده قرار می‌گیرد. فرآیند شناسایی در این نوع احراز هویت، بر اساس ویژگی‌های ذاتی بدن انسان (اثر انگشت، عنبیه) و ویژگی‌های رفتاری (صدا، راه رفتن) است.
روش‌های مختلفی برای تشخیص اثر انگشت، از جمله sparse proximity، تطبیق feature point، و توصیف‌گر هیستوگرام گرادیان‌های جهت‌یافته (HOG) پیشنهاد شده‌است.
روش‌های تشخیص چهره شامل چارچوب‌های مبتنی بر CNN، حالت باینری محلی (local binary mode) و شبکه یادگیری ویژگی‌های ژنتیکی ترکیبی است.
روش‌های تشخیص عنبیه شامل اندازه‌گیری فاصله، تبدیل ویژگی ثابت مقیاس (SIFT)، کانولوشن منبسط شده و شبکه عصبی پیچشی عمیق (DCNN) است.
تشخیص الگوی رگ‌های انگشت را می‌توان با استفاده از روش‌هایی از جمله ماشین یادگیری افراطی (ELM) چند لایه، CNN چند لایه، Fully CNN (FCN) و آموزش انتقالی به دست آورد.
روش‌های تشخیص صدا شامل روش‌هایی از جمله شبکه‌های عصبی بازگشتی (RNN)، شبکه‌های نردبانی، شبکه‌های باور عمیق (DBN) و proximal SVM است.
روش‌های تشخیص راه رفتن شامل استخراج ویژگی از سایه‌های عمقی، CNN، و ترکیبی از RNN، CNN و شبکه عصبی RBF است.

۲.۳ آگاهی از وضعیت شبکه

آگاهی از وضعیت شبکه برای شناسایی آسیب‌پذیری‌ها و لینک‌های ضعیف در توپولوژی شبکه مهم است. مدل‌ها و تکنیک‌های مختلفی مانند شبکه‌های بیزی Multi-entity، شبکه عصبی فازی، جنگل تصادفی و CNN می‌توانند برای آگاهی از موقعیت شبکه استفاده شوند. برخی از مدل‌ها بر اساس سیستم ایمنی و نظریه‌ی پیش‌بینی (grey) هستند؛ در حالی که برخی دیگر، از شبکه عصبی wavelet و شبکه بیزی پویا استفاده می‌کنند. بهینه‌سازی پیکربندی سخت‌افزار، الگوریتم استنتاج، ساختار نرم‌افزار، پارامترهای مشخصه‌ی امنیتی و سازوکار عملیات همزمان برای سیستم آگاهی از وضعیت امنیت اطلاعات مهم هستند. با اسکن خودکار سیستم‌ها برای آسیب‌پذیری‌ها و اولویت‌بندی آن‌ها بر اساس تأثیر احتمالی، به مدیریت آسیب‌پذیری کمک می‌شود.

۳.۳ نظارت بر رفتارهای خطرناک

هکرها به طور مداوم در حال توسعه‌ی روش‌های تهاجمی و یافتن آسیب‌پذیری در شبکه‌ها هستند؛ که نظارت بر رفتارهای خطرناک و انواع حملات را در زمان واقعی ضروری می‌کند. محققان سیستم‌های تشخیص نفوذ را برای انطباق با ویژگی‌های شبکه بهبود داده‌اند و آن‌ها را مقیاس‌پذیر می‌کنند. روش‌های مختلفی برای تشخیص رفتارهای غیرعادی مانند استخراج ویژگی عمیق، SVM، شبکه‌های عصبی مصنوعی و الگوریتم‌های یادگیری ماشین پیشنهاد شده‌اند. برخی از سیستم‌ها بر نظارت بر رفتارهای خطرناک خاص مانند حملات DDoS (حمله‌ی DDoS یا distributed denial-of-service: سرازیر کردن تعداد زیادی درخواست

به سرور قربانی یا هدف و استفاده‌ی بیش از حد از منابع، به‌طوری‌که سرویس‌دهی عادی آن به کاربرانش دچار اختلال شده یا از دسترس خارج شود) تمرکز می‌کنند. با ظهور فناوری 5G، محققان شروع به مطالعه‌ی تشخیص ناهنجاری در شبکه‌های 5G با استفاده از مدل‌های یادگیری عمیق تطبیقی کرده‌اند. این مدل‌ها از تکنیک‌هایی مانند تشخیص تجمع جریان شبکه و LSTM برای شناسایی سریع و رسیدگی به ناهنجاری‌های شبکه استفاده می‌کنند.

۴.۳ شناسایی ترافیک غیرعادی

شناسایی ترافیک غیرعادی برای حفظ امنیت کلی سایبری و پاسخ شبکه بسیار مهم است. روش‌های مختلفی مانند طبقه‌بندی، آمار، خوشه‌بندی و تئوری اطلاعات می‌تواند برای تشخیص جریان غیرعادی استفاده شود. تکنیک‌های یادگیری عمیق، مانند شبکه‌های عصبی کانولوشن (CNN) و LSTM، می‌توانند برای تشخیص ناهنجاری ترافیک و شناسایی ترافیک شبکه استفاده شوند. ترکیبی از شناسایی ترافیک غیرعادی و هوش مصنوعی، از جمله استفاده از روش‌های K-means و SVM، می‌تواند به شناسایی و طبقه‌بندی ترافیک حملات چندگانه کمک کند.

۵.۳ تجزیه و تحلیل رفتاری

هوش مصنوعی می‌تواند رفتار کاربر و ترافیک شبکه را برای شناسایی فعالیت‌های مشکوک و شناسایی تهدیدات داخلی تجزیه و تحلیل کند. همچنین می‌تواند الگوهای رفتاری عادی را یاد بگیرد و در صورت بروز انحراف و شناسایی تهدیدهای بالقوه، هشدار دهد.

۶.۳ طبقه‌بندی بدافزارها

فناوری‌های هوش مصنوعی، مانند یادگیری عمیق، می‌توانند برای ساخت مدل‌های هوشمند برای پیاده‌سازی طبقه‌بندی بدافزارها استفاده شوند.

۷.۳ تشخیص نفوذ

هوش مصنوعی می‌تواند برای تشخیص نفوذ در امنیت سایبری استفاده شود.

۸.۳ تشخیص و پیشگیری از تهدید

هوش مصنوعی می‌تواند برای سنجش و تحلیل تهدیدات سایبری برای ارائه اطلاعات تهدید استفاده شود. تکنیک‌های هوش مصنوعی، مانند یادگیری ماشینی و یادگیری عمیق، می‌توانند حجم زیادی از داده‌ها را برای شناسایی الگوها و ناهنجاری‌هایی که نشان‌دهنده تهدیدات سایبری بالقوه هستند، تجزیه و تحلیل کنند و امکان شناسایی و پیشگیری فعالانه از حملات را فراهم کنند.

۹.۳ مبارزه با حملات سایبری

هوش مصنوعی را می‌توان با اتخاذ روش‌های سنتی یادگیری ماشینی و راه حل‌های یادگیری عمیق موجود برای مبارزه با حملات سایبری استفاده کرد. سرعت تشخیص و پاسخ به تهدید، با تجزیه و تحلیل حجم زیادی از داده‌ها و شناسایی الگوهای نشان‌دهنده‌ی حملات سایبری با استفاده از الگوریتم‌های هوش مصنوعی، افزایش می‌یابد.

۱۰.۳ مدیریت آسیب‌پذیری

هوش مصنوعی می‌تواند با تجزیه و تحلیل داده‌ها از منابع مختلف، مانند پایگاه‌های اطلاعاتی آسیب‌پذیری و اسکن‌های شبکه، به شناسایی آسیب‌پذیری‌ها در سیستم‌ها و شبکه‌ها کمک کند. همچنین می‌تواند آسیب‌پذیری‌ها را بر اساس شدت آن‌ها اولویت‌بندی کند و اقدامات اصلاحی توصیه کند. با ارائه‌ی تجزیه و تحلیل در زمان واقعی و توصیه‌هایی برای کاهش تأثیر حوادث سایبری، مدیریت آسیب‌پذیری‌ها تسهیل و بهبود می‌یابد.

۱۱.۳ یادگیری ماشین تخاصمی

هوش مصنوعی را می‌توان برای توسعه مدل‌های قوی که می‌توانند در برابر حملات متخاصم مقاومت کنند، استفاده کرد. همچنین می‌تواند حملاتی را که هدف آن‌ها دستکاری یا فریب سیستم‌های هوش مصنوعی است، شناسایی و کاهش دهد و از یکپارچگی و قابلیت اطمینان راه‌حل‌های امنیت سایبری اطمینان حاصل کند.

۴ مطالعات موردی و شرکت‌های پیشتاز

در ادامه تعدادی از شرکت‌های فعال در این حوزه معرفی خواهند شد.

۱.۴ Palo Alto Networks

وقتی صحبت از ارائه دهندگان امنیت سایبری به میان می‌آید، Palo Alto Networks یکی از برجسته‌ترین‌هاست و با مشتریانی مانند Salesforce و Accenture کار می‌کند. محصولات آن از طیف وسیعی از نیازها، از فایروال‌ها و امنیت ابری گرفته تا تشخیص تهدید و محافظت از endpoint، با راه حل‌هایی که از یادگیری ماشین و یادگیری عمیق استفاده می‌کنند، پشتیبانی می‌کنند.

۲.۴ Crowdstrike

Crowdstrike محافظت از endpoint را ارائه می‌دهد. پلتفرم این شرکت، Falcon، شکار پیشگیرانه‌ی تهدید را به مشتریان در صنایعی مانند مالی، مراقبت‌های بهداشتی و خرده فروشی ارائه می‌دهد. این پلتفرم که فراتر از تشخیص ساده کار می‌کند، به طور خودکار تهدیدها را بررسی می‌کند و حدس و گمان را از تجزیه و تحلیل تهدید حذف می‌کند.

Check Point ۳.۴

Check Point راه حل‌های امنیتی کامپیوتر و شبکه را برای دولت‌ها و شرکت‌ها در سراسر جهان ارائه می‌دهد. راه‌حل اطلاعاتی تهدیدات آن به تیم‌های امنیتی این امکان را می‌دهد که تهدیدها را کنترل کنند، شبکه‌ها را رصد کنند، سرویس‌های امنیتی را مدیریت کنند و به حملات پاسخ دهند. از آن‌جا که تهدیدها به سرعت تکامل می‌یابند، Check Point اطلاعات قابل تنظیم تهدیدات را برای برآورده کردن نیازهای سازمان‌ها در زمان واقعی فراهم می‌کند.

Fortinet ۴.۴

Fortinet راه حل‌های امنیتی را برای هر بخش از زیرساخت فناوری اطلاعات ارائه می‌دهد. از امنیت شبکه و برنامه‌های کاربردی وب گرفته تا حفاظت از تهدید و دسترسی یکپارچه ایمن، محصولات امنیت سایبری Fortinet توسط بسیاری از شرکت‌های Fortune 500 استفاده می‌شود. محصول مبتنی بر هوش مصنوعی این شرکت، FortiWeb، یک فایروال تحت وب است که از یادگیری ماشین و دو لایه احتمالات آماری برای شناسایی دقیق تهدیدها استفاده می‌کند.

LogRhythm ۵.۴

LogRhythm یک راه حل امنیتی انتهابه‌انتها برای شرکت‌ها و سازمان‌ها برای شناسایی و پاسخ سریع به تهدیدات امنیت سایبری ارائه می‌دهد. این شرکت از یادگیری ماشین برای شناسایی تهدیدها، حساب‌های در معرض خطر، سوء استفاده از امتیازات و سایر ناهنجاری‌ها استفاده می‌کند.

FireEye ۶.۴

FireEye به طور مداوم در نوآوری امنیت سایبری با فناوری‌های مبتنی بر هوش مصنوعی، هوش و فناوری‌های پیشگیری پیشرفته، مدیریت امنیت یکپارچه و اتوماسیون امنیت ابری برای کمک به محافظت از سازمان‌ها در برابر حملات سایبری نسل ششم پیشرو است. این شرکت هم از طریق نوآوری و هم از طریق خرید به این مهم دست یافت، اکنون می‌تواند از ابزارهای امنیت سایبری استفاده کند که از هوش مصنوعی برای نظارت بر شبکه‌ها و شناسایی ناهنجاری‌ها استفاده می‌کند.

Sophos ۷.۴

Sophos با محافظت از بیش از ۵۰۰۰۰۰ سازمان و میلیون‌ها مصرف کننده در بیش از ۱۵۰ کشور، یک رهبر جهانی در امنیت سایبری نسل بعدی است. این شرکت دارای مجموعه‌ای قوی و گسترده از محصولات و خدمات پیشرفته برای ایمن‌سازی کاربران، شبکه‌ها و endpointها در برابر باج‌افزار، بدافزار، سوء استفاده و رمزگیری است. این مجموعه با هوش تهدید، هوش مصنوعی و یادگیری ماشین از SophosLabs و SophosAI پشتیبانی می‌کند.

Symantec ۸.۴

اگرچه Symantec معمولاً به دلیل کار خود در محصولات فایروال و آنتی ویروس شناخته شده است، اما در سال‌های اخیر از قدرت هوش مصنوعی برای گسترش کار خود در تشخیص تهدید و پیشگیری استفاده کرده است. Symantec که همچنان به کار خود در زمینه‌ی امنیت ادامه می‌دهد، به عنوان یک رهبر جهانی در امنیت endpoint، امنیت وب، امنیت اطلاعات، امنیت ایمیل و مدیریت دسترسی ممتاز معرفی شده است.

Google ۹.۴

Google از یادگیری عمیق در پلتفرم Cloud Video Intelligence خود استفاده می‌کنند. ویدیوهای ذخیره شده در سرور ابری آن‌ها توسط الگوریتم‌های هوش مصنوعی بر اساس محتوا و زمینه‌ی آن‌ها تجزیه و تحلیل می‌شوند. اگر ناهنجاری پیدا شود که احتمال تبدیل به تهدید داشته باشد، الگوریتم‌های هوش مصنوعی یک هشدار ارسال می‌کنند. همچنین در Gmail از یادگیری ماشین برای فیلتر کردن هرزنامه‌ها spam از ایمیل استفاده می‌کند.

IBM ۱۰.۴

IBM Watson، محصول شرکت IBM، از یادگیری ماشین برای شناسایی تهدیدها و ایجاد راه حل‌های امنیت سایبری استفاده می‌کند. قابلیت‌های آن به عنوان یک بستر پیشرو هوش مصنوعی، آن را قادر می‌سازد تا حجم وسیعی از داده‌های امنیتی را تجزیه و تحلیل کرده، تهدیدهای بالقوه را شناسایی کرده و به سرعت پاسخ‌های آگاهانه را فرموله کند. IBM Watson با بهره‌گیری از تجزیه و تحلیل مبتنی بر هوش مصنوعی و زمینه‌سازی داده‌های امنیتی، شناسایی پیشگیرانه‌ی تهدید و پاسخ به حادثه را تسهیل می‌کند و در نهایت انعطاف‌پذیری سایبری کلی سازمان را تقویت می‌کند

Darktrace ۱۱.۴

Darktrace به هزاران شرکت در صنایع مختلف کمک کرده است تا تهدیدات سایبری را در زمان واقعی شناسایی و با آن‌ها مبارزه کنند. پلتفرم هوش مصنوعی آن، داده‌های شبکه را برای انجام محاسبات و شناسایی الگوها تجزیه و تحلیل می‌کند. فناوری یادگیری ماشین از داده‌ها برای کمک به سازمان‌ها برای شناسایی انحرافات از رفتار معمولی و شناسایی تهدیدها استفاده می‌کند.

Framework Security ۱۲.۴

Framework Security به شرکت‌های مشتری خود درباره‌ی ترکیب ابزارها و استراتژی‌هایی برای مقابله با تهدیدات دیجیتال در عملیات روزانه آن‌ها مشاوره می‌دهد. حوزه‌های تخصص آن شامل ریسک و انطباق همراه با آموزش امنیت سایبری است و این شرکت یک پلتفرم تست نفوذ مجهز به قابلیت‌های هوش مصنوعی ارائه می‌دهد.

Tessian ۱۳.۴

پلتفرم امنیتی هوش مصنوعی Tessian از نفوذ، رمزگیری و از دست دادن داده‌ها توسط ایمیل‌های خطرناک جلوگیری می‌کند. این شرکت فیلترهای قابل تنظیم ایمیل ایجاد می‌کند که فعالیت‌های مخرب و مشکوک را در ایمیل‌های ورودی و خروجی از بین می‌برد. این پلتفرم همچنین دارای داشبورد بی‌درنگ است تا تیم‌های امنیتی بتوانند فوراً از سلامت زیرساخت خود مطلع شوند.

۵ چالش‌ها و محدودیت‌ها

۱.۵ دفاع در برابر یادگیری ماشین تخاصمی

یادگیری ماشین تخاصمی، فریب یادگیری ماشین یا مدل‌های هوش مصنوعی است که اغلب با نیت مخرب انجام می‌شود. این ترفند که به آن هوش مصنوعی متخاصم نیز می‌گویند، با دستکاری جزئی ورودی‌ها رخ می‌دهد که می‌تواند الگوریتم‌های یادگیری ماشین را دور بزند یا فریب دهد. مدل‌های هوش مصنوعی با تهدیدات سایبری مختلفی روبرو هستند و برای مبارزه با یادگیری ماشینی تخاصمی به فناوری‌های دفاعی و حفاظتی امنیتی سایبری خاصی نیاز است. احتمال دستکاری نمونه‌های آموزش و آزمایش در حملات خصمانه وجود دارد.

۲.۵ حفظ حریم خصوصی در یادگیری ماشینی

مدل‌های هوش مصنوعی به تکنیک‌های حفظ حریم خصوصی برای محافظت از داده‌های حساس در طول فرآیندهای یادگیری ماشین نیاز دارند.

۳.۵ تنظیم هوش مصنوعی برای الزامات امنیت سایبری

فناوری‌های هوش مصنوعی باید برای پاسخگویی به نیازها و الزامات خاص حوزه امنیت سایبری تطبیق داده شوند.

Human-in-the-Loop ۴.۵

ادغام تخصص انسانی و تصمیم گیری در سیستم‌های هوش مصنوعی برای امنیت سایبری موثر مهم است. این رویکرد محدودیت‌های هوش مصنوعی را تشخیص می‌دهد و بر همکاری بین انسان‌ها و هوش مصنوعی برای مقابله با چالش‌های پیچیده امنیت سایبری تأکید می‌کند. امکان جایگزینی کامل هوش انسانی با هوش ماشینی وجود ندارد.

۵.۵ راه‌حل‌های سنتی هوش مصنوعی

راه‌حل‌های سنتی هوش مصنوعی برای شناسایی و کاهش حملات سایبری در حال ظهور ناکافی هستند و نیاز به تکنیک‌های پیشرفته‌تر را برجسته می‌کنند. فناوری و نرم‌افزارهای سنتی با پیاده‌سازی ثابت برای محافظت در برابر تهدیدات امنیتی کافی نیستند.

۶.۵ حملات سایبری پیچیده‌تر

مجرمان سایبری همچنین از هوش مصنوعی برای راه‌اندازی حملات سایبری پیچیده‌تر استفاده می‌کنند و در عین حال ردپای خود را پنهان می‌کنند، که این امر را به چالشی دائمی برای کارشناسان امنیت سایبری تبدیل می‌کند. نقش هوش مصنوعی در امنیت سایبری در حال گسترش است زیرا در برنامه‌های کاربردی حیاتی مرتبط با امنیت ملی و رفاه انسان به کار می‌رود. با این حال، این بدان معناست که عواقب حملات سایبری مبتنی بر هوش مصنوعی می تواند شدید باشد.

۷.۵ سیستم هوش مصنوعی ایمن

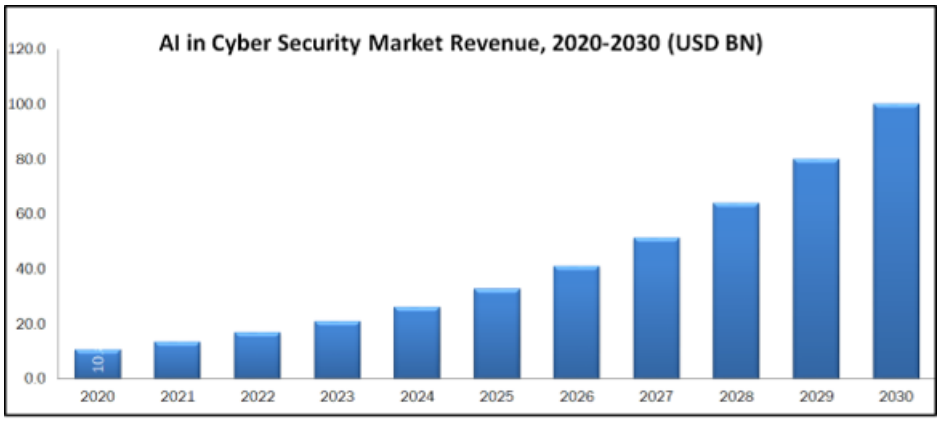
تحقیقات در مورد ساخت شبکه‌های عصبی رمزگذاری شده و تحقق یادگیری عمیق فدرال ایمن برای ایجاد یک سیستم هوش مصنوعی ایمن در حال انجام است.

۶ چشم‌انداز

در این بخش، پیشینه و چشم‌انداز حال و آینده‌ی این حوزه بررسی خواهد شد.

در تصویر زیر، نمودار heatmap جهانی که حدوداً مربوط به سال ۲۰۲۰ است، را مشاهده می‌کنید. کشورهای فعال در زمینه‌ی به کار گیری هوش مصنوعی در امنیت سایبری، با رنگ سبز نشان داده شده‌اند. و کشورهایی که بیشترین فعالیت را در این زمینه دارند، نیز با رنگ قرمز مشخص شده‌اند. فعال‌ترینِ آن‌ها، کشورهای آمریکا، چین، آلمان، ژاپن، هند و استرالیا هستند.

نمودار زیر توسط Decision Foresight که یک سازمان تحقیقاتی با محتوای قابل اعتماد و معتبر است و برآورد بازار و بهترین تحلیل‌ها را برای ارائه گزارش‌های با کیفیت بالا به مشتریان خود طراحی می‌کند، ارائه شده است. در این نمودار، اندازه‌ی بازار نشان داده شده است. اندازه بازار، کل حجم بالقوه مصرف کنندگان یا مشتریان در یک بخش محصول خاص است. و نقش مهمی برای شرکت‌ها در تصمیم گیری استراتژی‌های بازاریابی، بودجه و نیروی کار مورد نیاز برای یک محصول خاص ایفا می‌کند. بهترین راه برای محاسبه آن، ضرب تقاضای محصول در قیمت هر محصول است.
این بررسی از سال ۲۰۲۰ تا ۲۰۲۳ انجام شد. اندازه‌ی بازار در سال ۲۰۲۰ برابر ۱۰.۷۵ بود و تا سال ۲۰۲۳، ۲۵ درصد افزایش یافت و پیشبینی صعودی بودن آن تا سال ۲۰۳۰ به شرح زیر ارائه شد.



Source: Decision Foresight

مراجع

[١] Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K. R. (2021). *"Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artificial Intelligence Review,"* 55(2), 1029–1053. https://doi.org/10.1007/s10462-021-09976-0

[٢] I. H. Sarker, H. Furhad, and R. Nowrozy, *"AI-Driven Cybersecurity: An Overview, security intelligence modeling and research directions,"* SN Computer Science, vol. 2, no. 3, Mar. 2021, doi: 10.1007/s42979-021-00557-0.

[٣] N. Abbas, T. Ahmed, S. H. U. Shah, M. Omar, and H. W. Park, *"Investigating the applications of artificial intelligence in cyber security,"* Scientometrics, vol. 121, no. 2, pp. 1189–1211, Sep. 2019, doi: 10.1007/s11192-019-03222-9.

[٤] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). *"Artificial intelligence for cybersecurity: Literature review and future research directions."* Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804

[٥] J. Li, *"Cyber security meets artificial intelligence: a survey,"* Frontiers of Information Technology & Electronic Engineering, vol. 19, no. 12, pp. 1462–1474, Dec. 2018, doi: https://doi.org/10.1631/fitee.1800573.

[٦] Zeadally, S., Adi, E., Baig, Z. A., & Khan, I. A. (2020). *"Harnessing artificial intelligence capabilities to improve cybersecurity."* IEEE Access, 8, 23817–23837. https://doi.org/10.1109/access.2020.2968045

[٧] Das, R., Sandhane, R. (2021). *"Artificial intelligence in cyber security."* Journal of Physics: Conference Series, 1964(4), 042072. https://doi.org/10.1088/1742-6596/1964/4/042072

[٨] A. Singh and S. Choudhary, *"Leveraging IBM Watson for Cyber Security: A Case Study in AI-Driven Threat Detection,"* Journal of Cybersecurity and Information Assurance, vol. 6, no. 2, pp. 112–125, 2020.

[٩] IBM Security. *"IBM Security: Cognitive Security with Watson."* [Online]. Available: https://www.ibm.com/security/cognitive. Accessed on: Sep. 2019.