بررسی امنیت اینترنت اشیاء به کمک تکنیک های یادگیری ماشین و بلاکچین

ریحانه رخشانی
کارشناسی ارشد مهندسی نرم افزار، دانشکده فنی و مهندسی دانشگاه آزاد اسلامی واحد زاهدان، زاهدان، ایران

امین شهرکی مقدم
استادیار گروه مهندسی نرم افزار، دانشکده فنی و مهندسی دانشگاه آزاد اسلامی واحد زاهدان، زاهدان، ایران

چکیده

با افزایش چشمگیر داده ها از طریق دستگاه های موجود در بستر اینترنت اشیاء روز به روز تامین امنیت اطلاعات نقش پررنگی در این حوزه ایفا می کند. حملات مخرب به سرعت در حال ارتقاء می باشند و فعالان حوزه ی امنیت باید برای مقابله با آن ها از روش های جدید با دقت و کارایی بالاتر استفاده کنند، چرا که دیگر روش های سنتی برای برقراری امنیت شبکه ها عملکرد قبل را ندارند. یادگیری ماشین به عنوان یک ابزار هوشمند میتواند به تشخیص و پیش بینی حملات مختلف کمک شایانی کند. الگوریتم های یادگیری ماشین با آموزش دیدن و استفاده از ابزارهای مختلف می توانند دقت و کارایی بسیار بالایی را ارائه دهند. یکی از مسائلی که دغدغه ی همیشگی این حوزه می باشد پایگاه داده های سنتی و آسیب پذیر بودنشان در برابر تغییر و حذف داده ها توسط هکرها است، که می توان با استفاده از الگوی بلاکچین برای ذخیره سازی داده ها این مشکل را برطرف نمود. در این پژوهش با استفاده از دو تکنیک یادگیری ماشین و بلاکچین روشی جدید ارائه شده است تا امنیت و دقت بالاتری در دستگاه های اینترنت اشیاء شاهد باشیم.

واژگان کلیدی: امنیت اینترنت اشیاء، یادگیری ماشین، بلاکچین، اینترنت اشیاء

مقدمه

پیشرفت اخیر در فناوری های ارتباطی، مانند اینترنت اشیاء (IoT) ، به طرز چشمگیری از سنجش سنتی محیط های اطراف فراتر رفته است. فناوری های IoT می توانند مدرن سازی هایی را که باعث بهبود کیفیت زندگی می شوند و توانایی جمع آوری، کمیت و درک محیط های اطراف را دارند، امکان پذیر کنند.اجرای اقدامات امنیتی، مانند رمزگذاری، احراز هویت، کنترل دسترسی، امنیت شبکه و کاربرد برای دستگاه های IoT و آسیب پذیری های ذاتی آنها بی اثر است. بنابراین، روشهای امنیتی موجود باید برای ایمن سازی مؤثر اکوسیستم IoT افزایش یابد. (الغرادی و همکاران، ۲۰۲۰)

این واقعیت که اینترنت اشیا از فناوری‌های توانمندی مانند شبکه‌های مبتنی بر نرم‌افزار (SDN)، محاسبات ابری (CC) و محاسبات مه استفاده می‌کند، همچنین چشم‌انداز تهدیدات را برای مهاجمان افزایش می‌دهد. دستگاه‌های اینترنت اشیا مقدار زیادی داده تولید می‌کنند و بنابراین، تکنیک‌های سنتی جمع‌آوری، ذخیره‌سازی و پردازش داده‌ها ممکن است در این مقیاس کار نکنند. علاوه بر این، مقدار زیادی از داده ها همچنین می تواند برای الگوها، رفتارها، پیش بینی ها و ارزیابی استفاده شود.

علاوه بر این، ناهمگونی داده های تولید شده توسط اینترنت اشیا، جبهه دیگری را برای مکانیسم های پردازش داده فعلی ایجاد می کند. بنابراین، برای مهار ارزش داده های تولید شده توسط اینترنت اشیا، مکانیسم های جدیدی مورد نیاز است. در این زمینه، یادگیری ماشین (ML) به عنوان یکی از مناسب‌ترین پارادایم‌های محاسباتی برای ارائه هوش تعبیه‌شده در دستگاه‌های IoT در نظر گرفته می‌شود. همچنین می‌توان آن را به عنوان توانایی یک دستگاه هوشمند برای تغییر یا خودکار کردن موقعیت یا رفتار بر اساس دانش که به عنوان بخشی ضروری برای راه‌حل اینترنت اشیا در نظر گرفته می‌شود، تعریف کرد(حسین و همکاران، ۲۰۲۰)

اهمیت موضوع

برای تجزیه و تحلیل داده های بزرگ تولید شده، یک هوش مصنوعی (AI) نقش مهمی را به عنوان یک ابزار تحلیلی قوی ایفا می کند و تجزیه و تحلیل مقیاس پذیر و دقیق داده ها را در بلادرنگ ارائه می دهد. با این حال، طراحی و توسعه یک ابزار موثر تجزیه و تحلیل داده‌های بزرگ با استفاده از هوش مصنوعی دارای چالش‌هایی مانند معماری متمرکز، امنیت و حریم خصوصی، محدودیت‌های منابع، کمبود داده‌های آموزشی کافی است. در مقابل، به عنوان یک فناوری در حال ظهور، یک بلاک چین از یک معماری غیرمتمرکز پشتیبانی می کند، که در آن اشتراک امن داده ها و منابع در میان گره های مختلف شبکه اینترنت اشیا برای حذف کنترل متمرکز پشتیبانی می شود و می تواند بر چالش های موجود در هوش مصنوعی غلبه کند. بلاک چین یک فناوری پایگاه داده ایمن، غیرمتمرکز و توزیع شده است.

تمام گره‌ها در این فناوری در جایی استفاده می‌شوند که تمام تراکنش‌ها و مهر زمانی به سرعت ثبت می‌شوند و تراکنش بدون استفاده از شخص ثالث به اشتراک گذاشته می‌شود. داده های ذخیره شده در بلوک ها به صورت زنجیره ای از طریق یک تابع هش به هم متصل می شوند (ساختار رمزنگاری شامل مهر زمانی و پیوند به بلوک قبلی است). از آنجایی که هر بلوک به آخرین بلوک متصل می شود، امکان هک تراکنش توسط هیچ سیستم مخربی در شبکه فناوری بلاک چین وجود ندارد(سینگ و همکاران، ۲۰۲۰). بلاک چین، اینترنت اشیا و هوش مصنوعی، فناوری‌های کلیدی هستند که موج بعدی تحول دیجیتال را پیش می‌برند(سندنر و همکاران، ۲۰۲۰).

با توجه به بررسی تحقیقات صورت گرفته در زمینه مورد مطالعه، تولید انبوه داده ها توسط بستر اینترنت اشیاء و همچنین پیشرفت و تنوع حملات سایبری، نیاز به امنیت، دغدغه ای ضروری و با اهمیت می باشد بطوریکه که با روش های سنتی قادر به رفع یا پیش بینی آن ها نخواهیم بود. نیاز به امنیت بیشتر، همواره ضروری بوده و هیچ زمانی نمی توان ادعا کرد که به امنیت کامل دست پیدا کرده ایم. بطورمثال در سازمان های اطلاعاتی، صنعت برق، بهره برداری نفت و ارتش که مستقیما با دفاع سایبری ملی مرتبط هستند،

نمی توان از روش های ستنی و همیشگی برقراری امنیت استفاده کرد، چرا که پیشرفت حملات و داده های مخرب آنقدر سریع هستند که باید همواره در پی ارائه ی مدل هایی با عملکرد و دقت بیشتر بود. به روز نشدن مدل های امنیتی سبب ناپایداری و فروپاشی شبکه های مهم هر کشور می شود. در سال های اخیر استفاده از روش های یادگیری ماشین برای بهبود امنیت اینترنت اشیاء تاثیرگذار بوده است و روز به روز الگوریتم های یادگیری ماشین با بهبود عملکردشان نتایج بهتری را ارائه می دهند. علاوه بر استفاده از یادگیری ماشین در این مساله، از فناوری نوظهور بلاکچین هم استفاده شده است که امنیت و اعتبارسنجی داده ها را چندین برابر بهبود می بخشد. در اکثر منابع بررسی شده این دو تکنیک در سطح تئوری یا بصورت جداگانه مورد ارزیابی قرار گرفته اند که با توجه به رشد سریع الگوریتم های یادگیری ماشین و همچنین بسترهای بلاکچین(بیت کوین، اتریوم)، این حوزه فضای تحقیقاتی و کاربردی زیادی برای افزایش امنیت به همراه خواهد داشت.

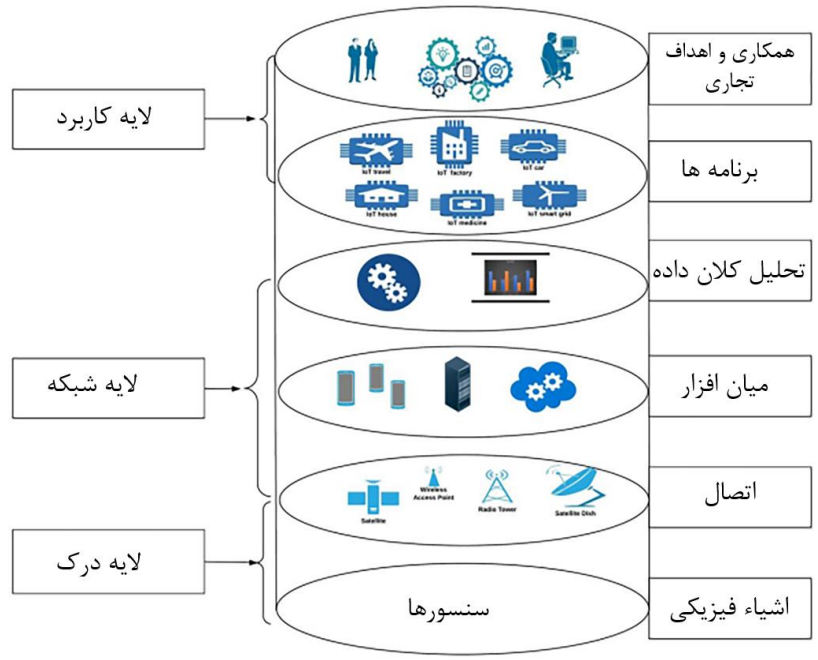
سیستم اینترنت اشیاء

اینترنت اشیا با استفاده از فناوری‌هایی مانند فناوری‌های ارتباطی، پروتکل‌های اینترنت و برنامه‌های کاربردی، شبکه‌های حسگر و محاسبات فراگیر، یک شی فیزیکی را از یک شی معمولی به یک شی هوشمند تبدیل می‌کند. مدل اینترنت اشیا را می توان به عنوان ارتباط متقابل دستگاه ها و سیستم های ناهمگن عظیم در الگوهای ارتباطی متنوع، مانند شی به شی انسان به انسان یا انسان به شی تعریف کرد(الفقها و همکاران، ۲۰۱۵).

رشد اینترنت اشیا در دهه گذشته به گونه‌ای است که همه چیز را از حسگرها گرفته تا محاسبات ابری و محاسبات مه/لبه را در خود جای داده است. اینترنت اشیا انواع مختلفی از یک شبکه مانند شبکه های توزیع شده، همه جا حاضر، شبکه ای و خودرویی دارد. کاربردهای اینترنت اشیاء تأثیر زیادی در زندگی روزمره مانند سنسورهای مستقر در بدن بیمار برای نظارت در شرایط بحرانی، نظارت بر نشت گاز در آشپزخانه هوشمند، زمینه کشاورزی، پارکینگ هوشمند خودرو، حمل و نقل هوشمند، ردیابی جزئیات کالا در سیستم زنجیره تامین داشته است. استفاده از سنسورهای داخل خودرو حسگرها دستگاه های محدودیت منابع هستند که از طریق سیم یا بی سیم در شبکه های ناهمگن متصل می شوند. شبکه‌های اینترنت اشیا دارای امنیت، حریم خصوصی و آسیب‌پذیری در برابر مهاجم هستند. زیرساخت اینترنت اشیا نه تنها از حسگرها تشکیل شده است، بلکه با برخی از فناوری های نوظهور نیز ادغام می شود. برنامه IoT بر اساس IoT Cloud یا IoT Fog Cloud است. معماری اینترنت اشیا ممکن است ساختار متمرکز، توزیع شده و غیرمتمرکز باشد. در اینترنت اشیا، پردازش و محاسبات در بلادرنگ یکی از چالش برانگیزترین مسائل است(موهانتا و همکاران، ۲۰۲۰).

معماری اینترنت اشیا

معماری اینترنت اشیا شامل اشیاء فیزیکی است که در یک شبکه ارتباطی ادغام شده و توسط تجهیزات محاسباتی با هدف ارائه خدمات هوشمند به کاربران پشتیبانی می شود. معماری اینترنت اشیا به طور کلی دارای سه لایه است: کاربرد، شبکه و ادراک. همانطور که در شکل ۱ نشان داده شده است، می توان این معماری را برای سادگی و تحلیل بهبودیافته، طبقه بندی کرد.



شکل ۱: معماری اینترنت اشیاء (الغرادی و همکاران، ۲۰۲۰)

امنیت اینترنت اشیاء

همانطور که گفته شد اینترنت اشیاء از فناوری‌های ارتباطی مختلفی مانند IPv6، Zigbee، 6LoWPAN، بلوتوث، Wave Z، WiFi و ارتباطات میدان نزدیک (NFC) استفاده می‌کند. فن‌آوری‌هایی مانند شبکه‌های اطلاعات محور (ICN) و شبکه‌های تعریف‌شده نرم‌افزار (SDN) برای خدمت به عنوان زیرساخت‌های ارتباطی زیربنایی برای IoT استفاده شده‌اند. این فناوری های ارتباطی فوق از نظر امنیتی دارای کاستی ها و محدودیت های خاص خود هستند و این محدودیت ها در حوزه اینترنت اشیا نیز به ارث رسیده است. استقرار فراگیر تعداد زیادی دستگاه، سطح حمله را در یک سیستم اینترنت اشیا افزایش می دهد (حسین و همکاران، ۲۰۲۰).

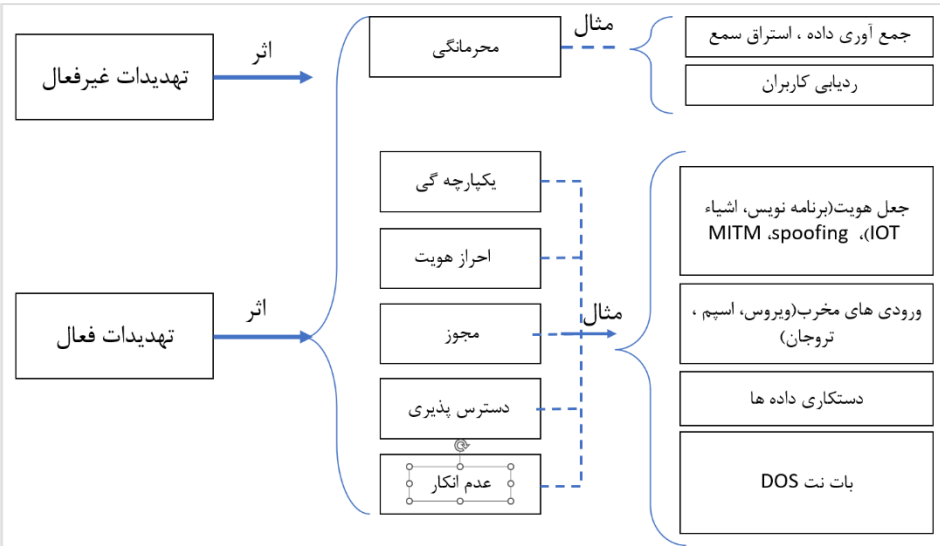
برنامه های کاربردی مختلف اینترنت اشیا انواع استانداردها و مشخصات صنعتی مختلفی دارند، اما هیچ استاندارد امنیتی یکپارچه اینترنت اشیا ایجاد نشده است. ویژگی های کلیدی که مسائل امنیتی IoT را از موارد سنتی متمایز می کند، فراگیر بودن و استقرار گسترده آن به عنوان یک شبکه توزیع شده است. این ویژگی های ناهمگونی و پیچیدگی منجر به مشکلاتی در تضمین امنیت اینترنت اشیا می شود. سازمان‌های مختلفی مانند IEEE و ETSI تلاش می‌کنند استانداردهای IoT را برای امنیت ایجاد کنند. چارچوب‌های مبتنی بر اینترنت اشیا فعلی در شبکه‌های کوچک مستقل هستند، در حالی که چارچوب‌های نسبتا کمی برای شبکه‌های مقیاس بزرگ شناخته شده‌اند. همانطور که توسعه اینترنت اشیا به بلوغ می رسد، شبکه های کوچک به یک شبکه بزرگ همگرا می شوند. یک شبکه بزرگ اینترنت اشیا به اقدامات پیچیده ای برای امنیت نیاز دارد. حل این چالش های امنیتی برای توسعه پایدار اینترنت اشیا بسیار مهم خواهد بود (الغرادی و همکاران، ۲۰۲۰).

تهدیدات امنیتی در اینترنت اشیاء

مفاهیم اساسی امنیت و حریم خصوصی حول سه گانه محرمانه بودن داده ها، یکپارچگی داده ها و در دسترس بودن شبکه (CIA) می چرخد. در اینترنت اشیا، داده ها می توانند هر چیزی باشند، به عنوان مثال، اطلاعات هویتی کاربر، بسته های ارسال شده از دوربین مداربسته به سرور مقصد، فرمانی که کاربر با استفاده از جاکلیدی به خودروی خود داده یا مکالمه چند رسانه ای بین دو نفر. هر گونه افشای غیرمجاز داده ها ممکن است منجر به نقض محرمانه بودن، یکپارچگی یا در دسترس بودن شود. اگر تهدیدی بر محرمانگی تأثیر بگذارد، یک تهدید حریم خصوصی است. تهدیدات امنیتی بر یکپارچگی داده ها و در دسترس بودن شبکه تأثیر می گذارد.

تهدیدات اینترنت اشیا با شبکه های معمولی متفاوت است که به طور قابل توجهی به دلیل منابع موجود دستگاه های نهایی است. دستگاه های اینترنت اشیا حافظه و قدرت محاسباتی محدودی دارند، در حالی که اینترنت معمولی شامل سرورها و رایانه های قدرتمند با منابع فراوان است. به همین دلیل، یک شبکه سنتی را می توان با لایه های امنیتی چند عاملی و پروتکل های پیچیده ایمن کرد، این چیزی است که یک سیستم اینترنت اشیا بلادرنگ نمی تواند از عهده آن برآید. در نهایت، به دلیل عملکرد خاص برنامه و عدم وجود سیستم‌عامل مشترک، دستگاه‌های IoT دارای محتویات و قالب‌های داده متفاوتی هستند که توسعه یک پروتکل امنیتی استاندارد را به چالش می‌کشد که نیاز به یک شخص ثالث قابل اعتماد دارد تا به عنوان یک پل عمل کند (مخدوم و همکاران، ۲۰۱۹). همه این محدودیت‌ها باعث می‌شود اینترنت اشیا مستعد چندین تهدید امنیتی و حریم خصوصی باشد، بنابراین مکان‌هایی برای انواع مختلف حملات باز می‌شود. علاوه بر این، چندین مطالعه نگرانی از به روز رسانی منظم نرم افزار را برای میلیاردها دستگاه هوشمند مطرح کرده است.

با توجه به اینکه هدف اصلی سیستم اینترنت اشیا دسترسی به هر کسی، در هر مکان و هر زمان است، بردارها یا سطوح حمله نیز برای مهاجمان قابل دسترسی می‌شوند. در نتیجه، باعث می شود که تهدیدهای بالقوه محتمل تر شوند. تهدید عملی است که می تواند از ضعف های امنیتی در یک سیستم سوء استفاده کند و بر آن تأثیر منفی بگذارد (آبومهارا، ۲۰۱۵). تهدیدهای متعدد، مانند حملات غیرفعال (مانند استراق سمع) و تهدیدهای فعال (مانند جعل، Sybil، MITM، ورودی های مخرب و DoS)، ممکن است بر سیستم اینترنت اشیا تأثیر بگذارد. شکل ۲ حملات بالقوه ای را نشان می دهد که می تواند بر الزامات امنیتی اصلی (احراز هویت، عدم انکار یکپارچگی، در دسترس بودن محرمانه بودن و مجوز) تأثیر بگذارد.



شکل ۲-۲: حملات بالقوه در سیستم اینترنت اشیاء (الغرادی و همکاران، ۲۰۲۰)

یادگیری ماشین

الگوریتم های یادگیری به دلیل ماهیت منحصر به فردشان در حل مسائل در بسیاری از کاربردهای دنیای واقعی به طور گسترده مورد استفاده قرار گرفته اند. چنین الگوریتم‌هایی ساخت ماشین‌هایی را مدیریت می‌کنند که به‌طور خودکار از طریق تجربه پیشرفت می‌کنند (جردن و میچل، ۲۰۱۵). اخیراً الگوریتم های یادگیری به طور گسترده در عمل به کار گرفته شده اند. پیشرفت فعلی الگوریتم‌های یادگیری با توسعه الگوریتم‌های جدید و در دسترس بودن داده‌های بزرگ، علاوه بر ظهور الگوریتم‌های کم هزینه محاسباتی انجام شده است (الغرادی و همکاران، ۲۰۲۰).

الگوریتم های اصلی یادگیری ماشین

الگوریتم های ML را می توان به چهار دسته طبقه بندی کرد. الگوریتم های یادگیری تحت نظارت، بدون نظارت، نیمه نظارت شده و تقویتی.

یادگیری نظارت شده: یادگیری تحت نظارت زمانی انجام می شود که اهداف خاصی برای دستیابی از مجموعه مشخصی از ورودی ها تعریف شده باشد. برای این نوع یادگیری ابتدا داده ها برچسب گذاری می شوند و سپس آموزش با داده های برچسب دار (دارا بودن ورودی ها و خروجی های دلخواه) انجام می شود.

یادگیری بدون نظارت: در یادگیری بدون نظارت، محیط تنها ورودی هایی را بدون اهداف مورد نظر ارائه می دهد. نیازی به داده های برچسب دار ندارد و می تواند شباهت بین داده های بدون برچسب را بررسی کند و داده ها را در گروه های مختلف طبقه بندی کند.

یادگیری نیمه نظارت شده: در دو نوع قبلی، یا هیچ برچسبی برای همه مشاهدات در مجموعه داده وجود ندارد یا برچسب هایی برای همه مشاهدات وجود دارد. یادگیری نیمه نظارت شده بین این دو قرار می گیرد. در بسیاری از موقعیت‌های عملی، هزینه برچسب‌گذاری بسیار زیاد است، زیرا برای انجام این کار به متخصصان انسانی ماهر نیاز دارد.

یادگیری تقویتی: در یادگیری تقویتی (RL) هیچ پیامد خاصی تعریف نمی شود و عامل پس از تعامل با محیط از بازخورد یاد می گیرد. برخی از اقدامات را انجام می دهد و بر اساس پاداش به دست آمده تصمیم می گیرد. این تا حد زیادی از رفتارهای یادگیری انسان و حیوانات الهام گرفته شده است. چنین رفتارهایی آن را به یک رویکرد جذاب در کاربردهای بسیار پویا رباتیک تبدیل می کند که در آن سیستم یاد می گیرد که وظایف خاصی را بدون برنامه نویسی صریح انجام دهد (دابنی و همکاران، ۲۰۱۷). همچنین انتخاب تابع پاداش مناسب بسیار مهم است زیرا موفقیت و شکست عامل به پاداش کل انباشته شده بستگی دارد (ویرث و همکاران، ۲۰۱۷).

انگیزه استفاده از ML در امنیت IOT

در این بخش، ما در مورد مزایای استفاده از یادگیری ماشین و اینکه چرا یک فناوری عالی برای ادغام با اینترنت اشیا و امنیت است، بحث خواهیم کرد. اگرچه رویکردهای سنتی به طور گسترده برای جنبه‌های مختلف اینترنت اشیا (مانند برنامه‌های کاربردی، خدمات، معماری‌ها، پروتکل‌ها، تجمیع داده‌ها، تخصیص منابع، خوشه‌بندی، تجزیه و تحلیل) از جمله امنیت استفاده می‌شوند، اما استقرار گسترده اینترنت اشیا از تکنیک‌های هوشمند، قوی و قابل اعتماد حمایت می‌کند. . برای این منظور، ML و DL به دلایل مختلف، تکنیک‌های امیدوارکننده‌ای برای شبکه‌های IoT هستند، به عنوان مثال، شبکه‌های اینترنت اشیا حجم زیادی از داده‌ها را تولید

می‌کنند که توسط رویکردهای ML و DL برای آوردن هوشمندی به سیستم‌ها مورد نیاز است. علاوه بر این، داده‌های تولید شده توسط اینترنت اشیا با تکنیک‌های ML و DL بهتر مورد استفاده قرار می‌گیرند که سیستم‌های اینترنت اشیا را قادر می‌سازد تا تصمیمات آگاهانه و هوشمندانه بگیرند. ML و DL تا حد زیادی برای امنیت، حفظ حریم خصوصی، شناسایی حملات و تجزیه و تحلیل بدافزار استفاده می شود. برخی از کاربردهای دنیای واقعی ML مربوط به امنیت به شرح زیر است:

- تشخیص چهره برای پزشکی قانونی: نورپردازی، عینک، ریش، آرایش، مدل مو و غیره.
- تشخیص کاراکتر برای رمزگذاری امنیتی: سبک های مختلف دست خط.
- شناسایی کدهای مخرب: شناسایی کدهای مخرب در برنامه ها و نرم افزارها.
- تشخیصDDoS : شناسایی حملات DDoS به زیرساخت از طریق تجزیه و تحلیل رفتار

فناوری بلاکچین

بلاک چین (BC) برای اولین بار در سال ۱۹۹۱ توسط استوارت هاربر و دبلیو اسکات استورنتتا اختراع شد و اساساً زنجیره ای از داده ها از نظر رمزنگاری محافظت شده بود که به عنوان زنجیره جعبه نیز شناخته می شود. بعداً در سال ۱۹۹۸، نیک سابو که یک دانشمند کامپیوتر و رمزنگار است، شروع به کار بر روی بیت طلا کرد که چیزی جز یک ارز دیجیتال غیرمتمرکز نبود. . در سال ۲۰۰۰، استفان کنست نظریه خود را در مورد بلوک های متصل از طریق یک زنجیره ایمن پیشنهاد کرد. سرانجام در سال ۲۰۰۸ مدل بلاک چین ساخته شد و سال بعد اولین لیگ عمومی توسط ناکاموتو ساخته شد. ناکاموتو شخصی است که برای توسعه بیت کوین با استفاده از اصول بلاکچین زیر اعتبار دارد. این تنها یکی از نمونه هایی است که به توسعه یک اکوسیستم سایبری ایمن کمک کرده است. این را می توان برای بسیاری از فناوری های دیگر اعمال کرد تا انواع مختلفی از سیستم های هوشمند را اضافه کند که می توانند برای محافظت از داده های شما نیز ساخته شوند. (سندنر و همکاران، ۲۰۲۰).

بلاک چین یک شبکه مش ایمن است که قابل تحمل خطا، شفاف، قابل تأیید و ممیزی است. این ویژگی ها یک BC را قابل اعتمادتر از یک مدل سرور مشتری مرکزی غیرقابل اعتماد می کند. فناوری بلاک چین این قابلیت را دارد که تراکنش الکترونیکی از یک فرد به فرد دیگر را در قالب ارزهای دیجیتال (بیت کوین، اتریوم، مونرو، زی کش، شفق قطبی و غیره) فعال کند. این امکان را فراهم می کند تا تراکنش ها یا دفتر کل داده ها را به شکل غیرمتمرکز، توزیع شده، ایمن و قابل اعتماد به اشتراک بگذارید. بلاک چین مجموعه ای از بلوک ها است. هر بلوک دارای چهار بخش است: جزئیات تراکنش یا مبادلات دارایی (بیت کوین یا اتریوم)، ارزش هش بلاک فعلی و ارزش هش بلوک قبلی و مهر زمانی. ذخیره سازی غیرمتمرکز روش بلاک چین است و برای ذخیره مقدار زیادی داده استفاده می شود که بلوک فعلی را با کد قرارداد هوشمند به بلوک قبلی مرتبط می کند. Swarm، LitecoinDB، MoneroDB، SiacoinDB، IPFS، BigchainDB و غیره برای پایگاه داده غیرمتمرکز در سناریوی فعلی امروزی استفاده می شوند. سیستم فایل بین سیاره ای (IPFS) یک پایگاه داده نقطه به نقطه، غیرمتمرکز و توزیع شده است که به یکدیگر متصل شده و فایل های مشترک را انتقال می دهد (سینگ و همکاران، ۲۰۲۰). IPFS یک رسانه ذخیره‌سازی قابل‌توجه است که توسط فناوری بلاک چین برای برنامه‌های IoT برای توان عملیاتی بالا استفاده می‌شود.

انواع بلاکچین

در این بخش، انواع مختلف بلاک چین را بررسی و تفاوت هر یک از آنها با دیگری در جدول ۳ ارائه شده است. به طور عمده سه نوع بلاک چین وجود دارد:

بلاک چین عمومی: بلاک چین عمومی یکی از محبوب ترین و رایج ترین انواع بلاک چین است. نمونه های بلاک چین عمومی شامل بیت کوین و اتریوم است.

بلاک چین خصوصی: بلاک چین خصوصی بسیار متفاوت از بلاک چین عمومی است به این معنا که باید قبل از استفاده درخواست شود و پس از آن فقط شما می توانید به داده ها دسترسی داشته باشید و روی آن کار کنید، در حالی که هر کسی می تواند به بلاک چین عمومی بپیوندد. این یک اکوسیستم بسیار بهم گره خورده است و برای پیوستن به مجوز نیاز دارد.

بلاک چین کنسرسیوم: بلاک چین کنسرسیوم بیشتر شبیه بلاک چین خصوصی است. تنها تفاوت عمده این است که آنها تحت مالکیت و اداره گروهی از نهادها هستند.

جدول ۳: انواع بلاکچین و نحوه ی عملکرد آن ها(گوپتا و همکاران، ۲۰۲۱)

بلاک چین عمومی	بلاک چین خصوصی	بلاک چین کنسرسیوم
بدون مالکیت	تک مالکیتی	متعلق به گروهی از افراد
توکن های اعطا شده	توکن ها ممکن است اعطا شوند	توکن ها ممکن است اعطا شوند
غیر متمرکز	متمرکز	متمرکز
بدون سانسور	سانسور شده	سانسور شده
مثال: بیت کوین	مثال :hyperledge	مثال: زنجیر اژدها

مزایای فناوری بلاک چین

فناوری بلاک چین دارای مزایای مختلفی است که برخی از آنها در زیر آورده شده است:

جلوگیری از نشت اطلاعات: از آنجایی که دستکاری یک جعبه منجر به تغییر هش در تمام کادرهای زیر به صورت دومینو می شود، تغییر و تغییر آن دشوار می شود که تضمین می کند هیچ اطلاعات شخصی به بیرون درز نمی کند یا به هیچ وجه تغییر نمی کند. به نحوی از لو رفتن هر نوع داده ای جلوگیری می کند

زمان تراکنش کمتر: این یک فناوری بسیار سریعتر است که در مقایسه با سایر فناوری‌های موجود وجود دارد، زیرا دارای یک رابط داده بسیار ساده است که امن است، بنابراین زمان هر تراکنش کم است زیرا این فایل‌ها خیلی سنگین نیستند و به راحتی قابل پردازش هستند.

تراکنش بدون واسطه: با اضافه کردن مستقیم اطلاعات و تراکنش های خود، نیاز شخص ثالث منسوخ می شود. بنابراین، این سیستم می تواند به صرفه جویی در منافع شخص ثالث کمک کند و دیگر لازم نیست اطلاعات شخصی خود را با طرف مقابل به اشتراک بگذارید

خطر تقلب پایین: احتمال کلاهبرداری و کلاهبرداری به دلیل شبکه امن آن بسیار کمتر است. از آنجایی که داده ها به تنهایی توسط کاربر نهایی اضافه می شوند، احتمال کلاهبرداری و کلاهبرداری کم است. دلیل استفاده از آن در بیت کوین نیز به همین دلیل بود

معاملات بلادرنگ: دلیل اصلی این است که این روزها ترجیح داده می شود زیرا معاملات در بلادرنگ انجام می شود و استفاده از آنها را جایگزین بسیار مناسب تر می کند.

انگیزه استفاده از فناوری بلاک چین در اینترنت اشیا

بلاک چین یکپارچگی و اعتبار داده ها را تضمین می کند و آن را به راه حلی مناسب برای محافظت در برابر دستکاری داده ها در دستگاه های اینترنت اشیا تبدیل می کند(وحید و همکاران، ۲۰۲۰). فناوری بلاک چین می‌تواند مدیریت داده‌های دستگاه‌های IoT را به دلیل شفافیت، اعتماد، صداقت، تغییرناپذیری، امنیت و ویژگی‌های حفظ حریم خصوصی بهبود بخشد. در ترکیب با هوش مصنوعی، می‌تواند محدودیت‌های فعلی داده‌های اینترنت اشیا را برطرف کند. فناوری بلاک چین وقتی با هوش مصنوعی ترکیب می‌شود، از نظر تئوری یک سیستم هوشمند خودکفا وجود دارد که می‌تواند در بخش‌های بانکی و بخش‌های فناوری اطلاعات نیز مورد استفاده قرار گیرد. این ترکیب می تواند انتقال پول و پرداخت ها را بسیار ایمن تر و محتاطانه تر کند و از هرگونه تقلب جلوگیری کند زیرا نمی توان آن را تغییر داد زیرا هش با تغییر داده ها در بلوک تغییر ایجاد می کند. ترکیب فناوری بلاک چین با دستگاه‌های اینترنت اشیا و هوش مصنوعی می‌تواند مدل‌های تجاری جدیدی را برای کسب درآمد از دستگاه‌های اینترنت اشیا باز کند (سندنر و همکاران، ۲۰۲۰).

مروری بر ادبیات

(یانگ و همکاران، ۲۰۱۸) به منظور تعیین متجاوزان احتمالی در شبکه ، یک سیستم تشخیص فعال در شبکه های IoT بی سیم را بر اساس یادگیری ماشین و تکنیک های یادگیری فعال پیشنهاد می کنند. مشاهده می شود که روش یادگیری فعال می تواند به طور موثر عملکرد را نسبت به تکنیک های یادگیری نظارت شده سنتی برای تشخیص نفوذ بهبود بخشد.

در پژوهشی نویسندگان یک مدل تشخیص نفوذ را بر اساس الگوریتم ژنتیک و شبکه باور عمیق پیشنهاد می کنند(ژانگ و همکاران، ۲۰۱۹). آنها برای تشخیص چهار نوع حمله از مجموعه داده NSL KDD استفاده می کنند: DOS ، R2L ، Probe و U2R.
این روش دارای مزایای بسیاری است: از یک طرف، ساختار شبکه خاص تولید شده برای انواع حملات خاص از نظر دقت طبقه بندی، بالاتر از سایر ساختارهای شبکه است که می تواند به بیش از ۹۹ درصد نرخ تشخیص برسد. از سوی دیگر، برای مجموعه های آموزشی کوچک، مانند U2R، دقت طبقه بندی الگوریتم پیشنهاد شده نیز به طور قابل توجهی بالاتر از روش های دیگر است.

در مقاله ی دیگری با استفاده از یک الگوریتم یادگیری ماشین برای شناسایی و کاهش حملات توزیع توزیع شده مبتنی بر DDOS در شبکه های IoT ، یک مدل پیشنهاد شده است که از الگوریتم های مختلف یادگیری ماشین مانند K نزدیکترین همسایه (KNN) ، مدل بیز ساده و شبکه عصبی مصنوعی درک چند لایه (MLP ANN) استفاده می کند. این تحقیق نشان داد که چگونه و چرا مجموعه داده‌های نامتعادل بلادرنگ بهینه نیستند، چگونه بر معیارهایی مانند دقت، یادآوری، صحت، امتیاز f1 و ROC AUC تأثیر می‌گذارد و چگونه مجموعه داده باید بهبود یابد(پوهرل و همکاران، ۲۰۲۱).

محققان به دنبال ادغام راه‌حل‌های قبلی برای ایجاد یک مکانیسم حفاظتی یکپارچه برای شبکه‌های دستگاه اینترنت اشیا بودند که امکان شناسایی تهدیدات، فعال کردن مکانیسم‌های انتقال اطلاعات امن و سازگاری با قابلیت‌های محاسباتی اینترنت اشیاء صنعتی را فراهم می‌آورد. در این مقاله از الگوریتم KNN و بلاکچین برای تشخیص حملات DOS و داده های نامعتبر استفاده شده است(بارگاس و همکاران، ۲۰۲۱). همچنین راه حل پیشنهادی بلاک چین از بار بالایی پشتیبانی می کند و زمان های بسیار خوبی را مدیریت می کند. افزایش تعداد گره های همزمان و/یا بارگذاری بیش از حد زنجیره با تراکنش های متعدد بر زمان پاسخگویی راه حل تاثیری نمی گذارد، بنابراین مقیاس پذیری را تضمین می کند.

روش تحقیق

مدل پیشنهادی که در این پژوهش ارائه شده است ، داده های بدست آمده از دستگاه های مختلف اینترنت اشیاء را با استفاده از الگوریتم knn که الگوریتم انتخابی تحقیق می باشد پردازش می کند و تشخیص می دهد که آیا جریان داده ها طبیعی و معتبر است یا خیر. اگر الگوریتم داده را مشکوک و نامعتبر تشخیص دهد آن را حذف کرده و اجازه ی دسترسی به سیستم مورد نظر را نمی دهد. در غیر اینصورت داده ها را بر روی پایگاه داده ای مبتنی بر شبکه ی بلاکچین ذخیره می کند تا تغییر و حذف داده ها امکان پذیر نباشد. همچنین کاربران سامانه های امنیتی در اینترنت اشیاء و فعالیت های آنان می تواند از طریق بلاکچین احراز هویت و اعتبارسنجی شوند. در نتیجه انتظار می رود با ادغام دو تکنیک قید شده، دقت تشخیص حملات و داده های مخرب را افزایش داده و در نتیجه امنیت قابل قبولی ارائه شود.

انتخاب مجموعه داده ها

برای پیاده سازی مدل مورد نظر نیاز به انتخاب نوع خاصی از حملات مهم در اینترنت اشیاء می باشد، به همین منظور مجموعه داده ای از حملات DDOS که شامل http, tcp, udp است انتخاب و پس از آن به الگوریتم یادگیری ماشین آموزش داده و تست شد. از این مجموعه داده ها ویژگی های مهم و تاثیرگذار در یادگیری الگوریتم انتخاب شده است که در جدول ۱ مشاهده می شود. همچنین جدول شماره ۲ نوع حملات موجود در هر دیتاست و مقادیر آن ها را نشان می دهد.

جدول ۳-۱: مشخصات مجموعه داده ها

ردیف	نام ویژگی	شرح ویژگی
۱	pkSeqID	شناسه ردیف
۲	stime	ضبط زمان شروع
۳	flgs_number	نمایش عددی پرچم های ویژگی
۴	proto_number	نمایش عددی پرتکل ویژگی
۵	pkts	تعداد کل بسته ها در تراکنش
۶	bytes	تعداد کل بایت در تراکنش
۷	state_number	وضعیت تراکنش
۸	ltime	ضبط آخرین زمان
۹	seq	شماره دنباله
۱۰	dur	ضبط کل مدت زمان
۱۱	mean	میانگین مدت رکوردهای جمع آوری شده
۱۲	stddev	انحراف استاندارد رکوردهای تجمیع شده
۱۳	sum	مجموع مدت رکوردهای تجمیع شده
۱۴	min	حداقل مدت رکوردهای تجمیع شده
۱۵	max	حداکثر مدت رکوردهای تجمیع شده
۱۶	spkts	تعداد بسته مبدا به مقصد
۱۷	dpkts	تعداد بسته مقصد به مبدا
۱۸	sbytes	تعداد بسته مبدا به مقصد
۱۹	dbytes	تعداد بسته مقصد به مبدا
۲۰	rate	مجموع بسته ها بر ثانیه در تراکنش

۲۱	srate	بسته ها از مبدا به مقصد در ثانیه
۲۲	drate	بسته ها از مقصد به مبدا در ثانیه
۲۳	TnBPSrcIP	تعداد کل بایت ها در هر IP مبدا
۲۴	TnBPDstIP	تعداد کل بایت ها در هر IP مقصد
۲۵	TnP_PSrcIP	تعداد کل بسته ها در هر IP مبدا
۲۶	TnP_PDstIP	تعداد کل بسته ها در هر IP مقصد
۲۷	TnP_PerProto	تعداد کل بسته ها در IP مقصد
۲۸	TnP_Per_Dport	تعداد کل بسته ها در هر پروتکل
۲۹	AR_P_Proto_P_SrcIP	میانگین نرخ هر پروتکل بر IP مبدا
۳۰	AR_P_Proto_P_DstIP	میانگین نرخ هر پروتکل بر IP مقصد
۳۱	N_IN_Conn_P_DstIP	تعداد اتصالات ورودی در هر IP مبدا
۳۲	N_IN_Conn_P_SrcIP	تعداد اتصالات ورودی به ازای IP مقصد
۳۳	AR_P_Proto_P_Sport	میانگین نرخ هر پروتکل در هرsport
۳۴	AR_P_Proto_P_Dport	میانگین نرخ هر پروتکل در هر dport
۳۵	Pkts_P_State_P_Protocol_P_DestIP	تعداد بسته های گروه بندی شده بر اساس وضعیت جریان ها و پروتکل ها بر هر IP مقصد
۳۶	Pkts_P_State_P_Protocol_P_SrcIP	تعداد بسته های گروه بندی شده بر اساس وضعیت جریان ها و پروتکل ها بر هر IP مبدا
۳۷	Attack	0 برای ترافیک عادی، ۱ برای ترافیک حمله

همچنین جدول شماره ۳-۲ نوع حملات موجود در هر دیتاست و مقادیر آن ها را نشان می دهد.

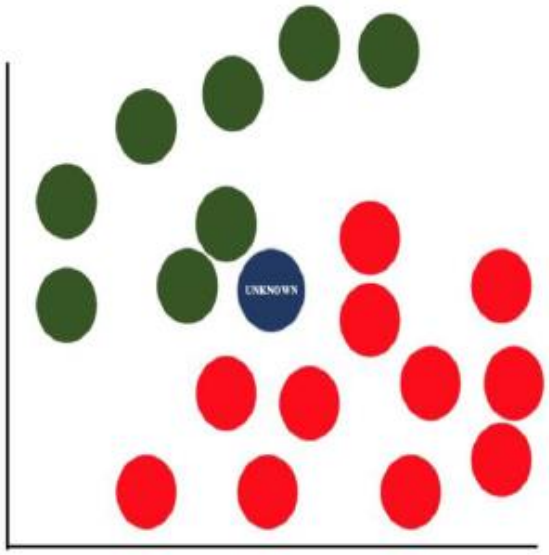
جدول ۳-۲: مشخصات مجموعه داده ها

ردیف	مجموعه داده	نوع حملات	حجم مجموعه داده
۱	DDoS1.CSV	HTTP	1K
۲	DDoS2.CSV	HTTP, TCP	10K
۳	DDoS3.CSV	HTTP, TCP, UDP	100K

پیاده سازی الگوریتم k نزدیک ترین همسایه (knn)

الگوریتم KNN یکی از الگوریتم های یادگیری ماشین بر اساس تکنیک یادگیری نظارت است. شکل ۳-۲ طبقه بندی KNN را نشان می دهد که در آن نمونه های ورودی جدید طبقه بندی می شوند. در شکل، دایره های قرمز نشان دهنده رفتارهای مخرب و دایره های سبز نشان دهنده رفتارهای عادی سیستم هستند. نمونه جدید ناشناخته (دایره آبی) باید به عنوان رفتار مخرب یا عادی طبقه بندی شود. طبقه‌بند KNN نمونه جدید را بر اساس آرای تعداد منتخب نزدیک‌ترین همسایگانش دسته‌بندی می‌کند. یعنی KNN کلاس نمونه های ناشناخته را با اکثریت آرای نزدیکترین همسایگان خود تعیین می کند. به عنوان مثال، در شکل۳-۲، اگر طبقه بندی KNN بر اساس یک همسایه نزدیک باشد (k = 1)، کلاس نمونه دیده نشده را به عنوان رفتار عادی طبقه بندی می کند (زیرا نزدیکترین چرخه یک چرخه سبز است). اگر طبقه‌بندی KNN بر اساس دو همسایه نزدیک (k = 2) باشد،

طبقه‌بندی‌کننده KNN کلاس نمونه دیده نشده را به‌عنوان رفتار عادی دسته‌بندی می‌کند، زیرا دو نزدیک‌ترین دایره سبز هستند (رفتار عادی). اگر طبقه‌بندی KNN بر اساس سه و چهار همسایه نزدیک (k = 3)، (k = 4) باشد، طبقه‌بندی‌کننده KNN کلاس نمونه ناشناخته را به عنوان رفتار مخرب دسته‌بندی می‌کند زیرا سه و چهار نزدیکترین دایره‌ها دایره‌های قرمز هستند (رفتار مخرب). آزمایش مقادیر مختلف k در طول فرآیند اعتبار سنجی متقاطع، گام مهمی برای تعیین مقدار بهینه k برای یک مجموعه داده معین است. اگرچه الگوریتم KNN یک الگوریتم طبقه بندی ساده و موثر برای مجموعه داده های آموزشی بزرگ است، بهترین مقدار k همیشه بسته به مجموعه داده ها متفاوت است. طبقه بندی کننده های KNN برای تشخیص نفوذ شبکه و تشخیص ناهنجاری استفاده شده است.



شکل ۳: طبقه بندی knn

طبقه بندی کننده های KNN اغلب از فاصله اقلیدسی به عنوان متریک فاصله استفاده می کنند(رابطه ۱).

$$ECU_D = \sqrt{\sum_{h=1}^{d}\left(train_{f_h} - test_{f_h}\right)} \qquad \text{رابطه (۱)}$$

رابطه (۱) $htrain\_f_h$ و $htest\_f_h$ به ترتیب یک تک ویژگی در یک نمونه خاص از داده های آموزش و تست هستند. h یک متغیر است(h=1, ⋯ , d) و d تعداد ویژگی های هر نمونه است. برای آموزش طبقه بندی، یک روش معمول این است که بخشی از داده ها به عنوان داده های آزمایشی و داده های باقیمانده برای آموزش طبقه بندی استفاده میشود. با این حال وقتی این کار انجام شود، ممکن است مشکل overfitting رخ دهد. این مشکل زمانی اتفاق میافتد که طبقه بند به جای داده های آزمایشی دقت بیشتری را برای داده های آموزش انجام دهد. یکی از راه های کاهش مشکل overfitting استفاده از cross-validation است. در روش اعتبارسنجی متقابل که از این به بعد آن را به اختصار (CV) می‌نامیم، طی یک فرآیند تکرار شونده، قسمت داده‌های آموزشی (Training set) که به منظور مدل‌سازی به کار می رود، خود به دو بخش تفکیک می‌شود. در هر بار تکرار فرآیند CV، بخشی از داده‌ها برای آموزش و بخشی دیگر برای آزمایش مدل به کار می‌رود. اگر مجموعه داده‌های آموزشی را به طور تصادفی به k زیرنمونه یا «لایه» (Fold) با حجم یکسان تفکیک کنیم، می‌توان در هر مرحله از فرایند CV، تعداد k-1 از این لایه‌ها را به عنوان مجموعه داده آموزشی و یکی را به عنوان مجموعه داده اعتبارسنجی در نظر گرفت. شکل ۴ مراحل روش k-Fold را به خوبی نشان می‌دهد.

شکل ۴: مراحل روش k-Fold

در پیاده سازی این الگوریتم سعی شده است مقادیر متفاوت k برای دیتاست های مختلف با حجم های متفاوت بررسی شود تا بهترین دقت الگوریتم در تشخیص حملات حاصل شود.

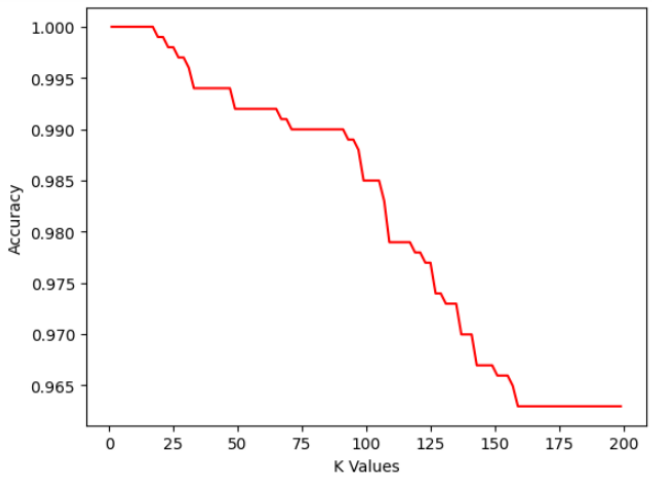
بلاکچین

ایده ی اصلی و جدید مطرح شده در این رویکرد، استفاده از تکنیک بلاکچین برای پیاده سازی پایگاه داده ای امن می باشد که اخیرا در مقالات به آن اشاره شده است و هنوز در مرحله ی بررسی می باشد. هدف استفاده از ساختار بلاکچین در این روش، افزایش شفافیت و غیر متمرکز بودن آن است، چرا که غیر متمرکز بودن آن باعث می شود که دیگر یک master/server وجود نداشته باشد و همه ی کاربران بطور یکسان از مزیت های شبکه بهره مند شوند. به دلیل ماهیت غیر متمرکز بلاکچین، همه تراکنش ها را می‌توان با داشتن یک نود شخصی یا با استفاده از کاوشگران بلاکچین که به هر کسی امکان می‌دهد تراکنش ها را به صورت زنده مشاهده کند، بصورت شفاف مشاهده کرد. هر نود دارای نسخه خاص خود از زنجیره است که با تأیید و اضافه شدن بلوک های جدید به روز می‌شود.

یافته ها

نتایج پیاده سازی الگوریتم knn

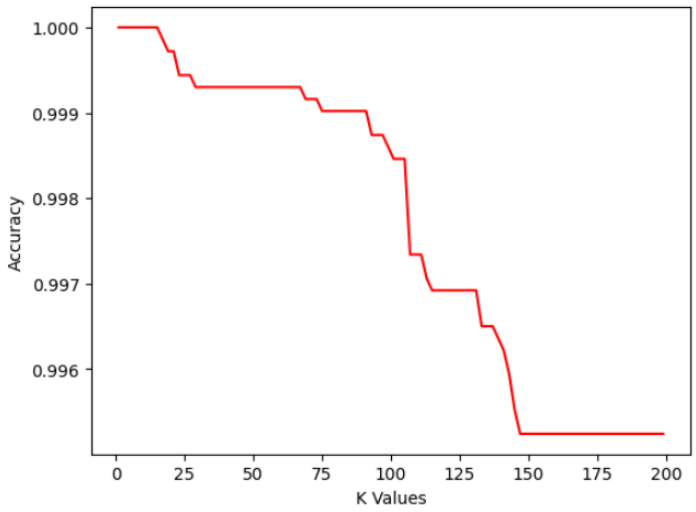
پس از اجرای کد پیاده سازی شده با پایتون، آن را با مجموعه داده های مختلف مورد آزمایش قرار دادیم که در ادامه نتایج بدست آمده ارائه شده است. شکل ۵ دقت بدست آمده با استفاده از پردازش مجموعه داده ی DDoS1.CSV که شامل 1K از اطلاعات حملات می باشد را نشان می دهد.



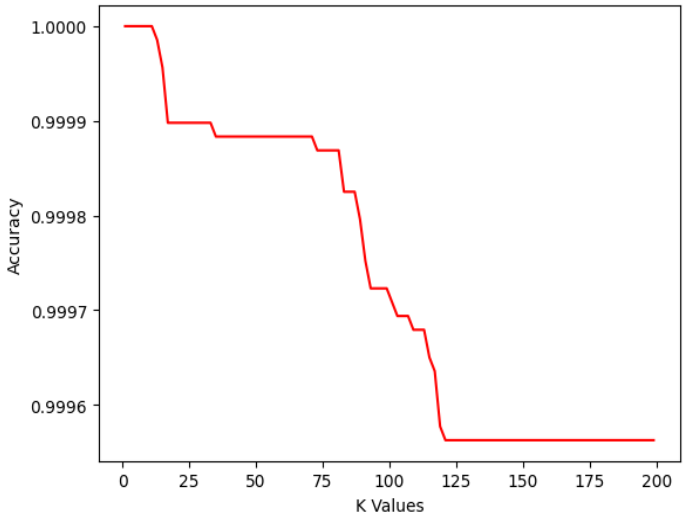
شکل ۵: بررسی دقت بدست آمده با مقادیر مختلف k برای مجموعه داده DDoS با حجم 1k

نمودار بالا نشان دهنده ی دقت الگوریتم با مقادیر K متفاوت می باشد. در کد اجرا شده فقط K با مقادیر فرد نظر گرفته شده است و همانطور که در فصل قبل هم اشاره شد اگر داده ها به درستی به مجموعه های آموزشی و آزمایشی تقسیم نشده باشند احتمال وقوع Over fitting می باشد. این احتمال با انتخاب مقادیر K خیلی کوچک یا خیلی بزرگ بیشتر می شود در نتیجه با بررسی کردن محدوده ای از مقادیر K می توان بهترین مقدار K را انتخاب کرد. بطو مثال در نمودار بالا بهترین دقت بدست آمده ۱ می باشد که طبق پردازش الگوریتم به ازای مقدار ۱ برای K، دقت ۱۰۰٪ حاصل می شود اما برای جلوگیری از وقوع Over fitting می توان با تحلیل نمودار مقادیر منطقی تری را برای K انتخاب کرد.

در ادامه نتیجه ی پردازش الگوریتم با مجموعه داده های DDoS1.CSV، DDoS2.CSV و DDoS3 با حجم های1K، 10Kو 100Kارائه شده است.



شکل ۶: بررسی دقت بدست آمده با مقادیر مختلف k برای مجموعه داده DDoS با حجم 10k



شکل ۷ : بررسی دقت بدست آمده با مقادیر مختلف k برای مجموعه داده DDoS با حجم 100k

همانطور که مشاهده می شود الگوریتم KNN توانسته است در این مسئله و با مجموعه داده های DDoS عملکرد و دقت خوبی را ارائه دهد. نتایج فوق نشان دهنده ی این مهم است که با افزایش حجم داده ها دقت الگوریتم کاهش پیدا نمی کند و کاملا برای پیاده سازی در سازمان های اطلاعاتی و امنیتی که در هر ساعت حجم زیادی از اطلاعات را بصورت بلادرنگ دریافت می کنند، مناسب می باشد. زمان پردازش هر کدام از مجموعه داده ها ۱۰ برابر مجموعه داده ی قبلی می باشد که بهبود آن می تواند برای تحقیقات آینده کارآمد باشد اما از آنجایی که پیاده سازی این پژوهش با رایانه ای به مشخصات(CPU COREI7,RAM 8) انجام شده است انتظار می رود در سازمان ها با سیستم های پیشرفته تر، بصورت بلادرنگ زمان پردازش قابل قبولی داشته باشد.

بحث و نتیجه‌گیری

در جدول ۴ نتایج مقایسه ی الگوریتم knn پیاده سازی شده با تحقیقات دیگر بطور خلاصه ارائه شده است.

جدول ۴: مقایسه ی عملکرد تحقیقات گذشته با الگوریتم های یادگیری ماشین

ردیف	شماره رفرنس	نوع حمله	الگوریتم	دقت
۱	۱	DDoS	Knn	۹۹.۸۹٪
			Decision Tree	۹۹.۵۰٪
			Random Forest	۹۹.۹۰٪
			ANN	۹۹.۹۵٪
۲	۲۰	DDoS	Naïve Bayes	۹۳.۹۵٪
			knn	۹۸.۵۱٪
۳	۲۶	DDoS	MLP ANN	۸۷.۴٪

				۹۹.۴٪ Naïve Bayes
				۸۷.۴٪ knn
۴	این پژوهش	DDoS	Knn	۹۹.۹۰٪

همانطور که از نتایج بالا مشخص است، الگوریتم های یادگیری ماشین دقت بالایی برای تشخیص حملات DDoS ارائه می دهند که نشان دهنده ی افزایش امنیت و تشخیص حملات در بستر اینترنت اشیاء می باشد. همچنین استفاده از بستر بلاکچین برای ذخیره سازی انداع داده های مهم و امنیتی می تواند گام جدیدی برای سیستم های ذخیره سازی اطلاعات باشد، چرا که دیگر فقط یک master برای ثبت و حفظ اطلاعات تصمیم گیری نمی کند بلکه همه ی افراد می توانند در این امر شریک باشند و اعتبار آن ها را بسنجند.

همانطور که بیان شد اینترنت اشیا می تواند نقش مهمی در توسعه فناوری های جدید ایفا کند، به همین علت برقراری امنیت یکی از فاکتورهای مهم در این موضوع می باشد. چرا که روز به روز حملات جدیدتری از طرف هکرها طراحی و اجرا می شود. مدل پیاده سازی شده به دقت بالای ۹۹ درصد برای تشخیص و کاهش حملات DDoS دست یافت. الگوریتم های یادگیری ماشین تنوع بسیار زیادی دارند و هر کدام از آن ها را برای انواع مختلف حملات میتوان پیاده سازی کرد. بطور مثال الگوریتم knn در عین سادگی برای مجموعه داده های بزرگ بسیار خوب عمل می کند و می توان با ارتقاء آن به نتایج بهتری هم رسید. در کنار آن، پایگاه داده ها همیشه در معرض حملات می باشند که با پیاده سازی آن ها بر اساس شبکه بلاکچین، افزایش فاکتورهایی مثل مقیاس پذیری، شفافیت و عدم تغییر یا حذف دشوار داده ها را به همراه دارد. در نتیجه مکمل بودن این دو تکنیک راه حلی جدید برای بهبود امنیت و حریم خصوصی می باشد. هرچند که این مدل هنوز در مرحله ی تحقیق و بررسی می باشد اما در آینده ای نزدیک به یکی از بهترین روش ها در امنیت اینترنت اشیاء تبدیل خواهد شد.

منابع

Al-Garadi, Mohammed Ali, et al. (2020). "A survey of machine and deep learning methods for internet of things (IoT) security." *IEEE Communications Surveys & Tutorials*, 22(3), 1646-1685.

Hussain, Fatima, et al. (2020). "Machine learning in IoT security: Current solutions and future challenges." *IEEE Communications Surveys & Tutorials*, 22(3), 1686-1721.

Singh, Sushil Kumar, Shailendra Rathore, and Jong Hyuk Park. (2020). "Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence." *Future Generation Computer Systems*, 110, 721-743.

Sandner, Philipp, Jonas Gross, and Robert Richter. (2020). "Convergence of blockchain, IoT, and AI." *Frontiers in Blockchain*, 42.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). "Internet of things: A survey on enabling technologies, protocols, and applications." *IEEE communications surveys & tutorials*, 17(4), 2347-2376.

Mohanta, Bhabendu Kumar, et al. (2020). "Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology." *Internet of Things*, 11, 100227.

I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni. 2019. "Anatomy of threats to the Internet of Things". *IEEE Communications Surveys Tutorials* (2019) 21, 2.

M. Abomhara, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security and Mobility,* (2015)vol. 4, no. 1, pp. 65-88.

W. Dabney, M. Rowland, M. G. Bellemare, and R. Munos, “Distributional reinforcement learning with quantile regression,” CoRR, vol. abs/1710.10044, 2017.

Yang, Kai, et al. (2018). "Active learning for wireless IoT intrusion detection." *IEEE Wireless Communications*, 25(6), 19-25.

Zhang, Ying, Peisong Li, and Xinheng Wang. (2019). "Intrusion detection for IoT based on improved genetic algorithm and deep belief network." *IEEE Access*, 7, 31711-31722.

Pokhrel, S.; Abbas, R.; Aryal, B. 2021, "Botnet detection in IoT using Machine learning." *IoT Security*. arXiv.

22 th International Conference on
Information Technology,
Computer and Telecommunication
Event Place: Tbilisi,Georgia
www.itctconf.ir
بیست و دومین کنفرانس بین المللی
فناوری اطلاعات، کامپیوتر و مخابرات | گرجستان
22th International Conference on Information Technology,Computer and Telecommunication
مجلات معتبر بین المللی ——— ۲۶ اسفندماه ۱۴۰۲

Examining the security of the Internet of Things using machine learning and blockchain techniques

Reyhaneh Rakhshani

Master of Software Engineering, College of Engineering and Technology, Islamic Azad University, Zahedan Branch, Zahedan, Iran

Amin Shahraki Moghadam

Assistant Professor, Department of Software Engineering, Faculty of Engineering and Technology, Islamic Azad University, Zahedan Branch, Zahedan, Iran

Abtract

With the significant increase of data through the devices available in the Internet of Things platform, information security plays a prominent role in this field day by day. Malicious attacks are increasing rapidly, and security activists must use new methods with higher accuracy and efficiency to deal with them, because traditional methods for establishing network security no longer function as before. Machine learning as an intelligent tool can help to detect and predict various attacks. Machine learning algorithms can provide high accuracy and efficiency by learning to see and use different tools. One of the issues that is a constant concern of this field is the traditional databases and their vulnerability to change and deletion of data by hackers, which can be solved by using the blockchain model for data storage.

Key words: Internet of Things Security**,** Machine Learning, Blockchain, iot