یادگیری ماشین در امنیت اینترنت اشیا

راه حل های فعلی و چالش های آینده

مقدمه

iotبه عنوان یک شبکه به‌هم‌پیوسته و توزیع‌شده از سیستم‌های تعبیه‌شده در نظر گرفته می‌شود که از طریق تکنولوژی‌های ارتباطی بی‌سیم یا سیمی ارتباط برقرار می‌کنند [۱] .همچنین به عنوان شبکه اشیا فیزیکی یا چیزهایی که با محاسبات، ذخیره‌سازی و قابلیت‌های ارتباطی محدود توانمند شده‌اند و همچنین با الکترونیک (مانند حسگرها و فعال‌کننده‌ها)، نرم‌افزار و اتصال شبکه که این اشیا را قادر به جمع‌آوری، پردازش و تبادل داده می‌کند، تعریف می‌شود .

اشیا در IoT به اشیا زندگی روزمره ما از دستگاه‌های هوشمند خانگی مانند لامپ هوشمند، آداپتور هوشمند، کنتور هوشمند، یخچال هوشمند، فر هوشمند، AC، سنسور دما، آشکارساز دود، دوربین IPگرفته تا دستگاه‌های پیچیده‌تر مانند دستگاه‌های تشخیص فرکانس رادیویی) (RFID، آشکارسازهای ضربان قلب، شتاب‌سنج، حسگرها اشاره دارد .

عنوان مقاله ما یادگیری ماشین در امنیت اینترنت اشیا هست که در ادامه به بررسی آن میپردازیم.

تعریف مسئله و هدف اصلی مقاله

داده‌های تولید شده توسط دستگاه‌های IoT عظیم هستند و بنابراین، تکنیک‌های جمع‌آوری، ذخیره‌سازی و پردازش داده‌های سنتی ممکن است در این مقیاس کار نکنند .علاوه بر این، مقدار مطلق داده‌ها می‌تواند برای الگوها، رفتارها، پیش‌بینی‌ها و ارزیابی نیز مورد استفاده قرار گیرد .علاوه بر این، ناهمگونی داده‌های تولید شده توسط IoT جبهه دیگری را برای مکانیزم‌های پردازش داده فعلی ایجاد می‌کند .

ضرورت تحقیق

برای کنترل ارزش داده‌های ایجاد شده توسطIoT ، به مکانیزم‌های جدیدی نیاز است .در این زمینه، یادگیری ماشین machin learning می‌تواند به ماشین‌ها و دستگاه‌های هوشمند کمک کند تا دانش مفید را از داده‌های تولید شده توسط انسان استنباط کنند. همچنین می‌تواند به عنوان توانایی یک دستگاه هوشمند برای تغییر یا خودکار کردن موقعیت یا رفتار براساس دانش که به عنوان یک بخش ضروری برای یک راه‌حل IoT در نظر گرفته می‌شود، تعریف شود. این حقیقت که اینترنت اینترنت از فن‌آوری‌های توانا مانند شبکه سازی تعریف‌شده نرم‌افزار (SDN)، محاسبات ابری (CC)و محاسبات مه استفاده می‌کند نیز چشم‌انداز تهدیدها برای مهاجمان را افزایش می‌دهد.

MLمی‌تواند به ماشین‌ها و دستگاه‌های هوشمند کمک کند تا دانش مفید حاصل از داده‌های تولید شده انسان را استنباط کنند .همچنین می‌تواند به عنوان توانایی یک دستگاه هوشمند برای تغییر یا خودکار کردن وضعیت یا رفتار مبتنی بر دانش تعریف شود که به عنوان یک بخش ضروری برای راه‌حل IoTمحسوب می‌شود.

شاخه های حل پیشین:

شاخه حل جاری

MLمی‌تواند در اینترنت برای ارائه خدمات هوشمند به کار رود .با این حال، در این مقاله، ما بر روی برنامه‌های MLدر ارائه خدمات امنیتی و حریم خصوصی به شبکه‌های اینترنت متمرکز می‌شویم.

امنیت و حریم خصوصی دو عامل اصلی در درک تجاری خدمات و برنامه‌های اینترنت IoT هستند. اینترنت کنونی یک زمین‌بازی فریبنده برای حملات امنیتی است که از hacksساده تا سطح شرکت وجود دارد. شکاف‌های امنیتی هماهنگ که به طور زیان‌آور بر صنایع مختلف از قبیل مراقبت‌های بهداشتی و کسب‌وکار تاثیر می‌گذارد. محدودیت‌های تجهیزات اینترنت و محیطی که آن‌ها در آن فعالیت می‌کنند، چالش‌های اضافی برای امنیت هر دو برنامه و وسایل ایجاد می‌کنند.

Gaps in the Existing Security Solution for IoT Networks

شکاف‌ها در راه‌حل امنیت موجود برای شبکه‌های IoT . برای تحقق موفقیت‌آمیز اینترنت IoT مهم است که ریشه‌های مسایل امنیت و حریم خصوصی را آنالیز کنیم. به طور دقیق‌تر واژه اینترنت IoT از فن‌آوری‌های موجود به پایین پرتاب شده‌است و بنابراین ضروری است که بدانیم آیا چالش‌های امنیتی در اینترنت اشیا جدید یا ترکیبی از ارث از تکنولوژی‌های قدیمی هستند یا خیر

نگرانی اولیه از اینترنت اشیا -محدودیت‌های مربوط به منابع است که مانع محدودیت‌ها هستند. علاوه بر این، راه‌حل‌هایی برای مسایل امنیت و حریم خصوصی در اینترنت به طراحی لایه متقاطع و الگوریتم‌های بهینه نیاز دارند. به عنوان مثال به دلیل محدودیت‌های محاسباتی، وسایل اینترنت IoT ممکن است به نژاد جدیدی از رمزنگاری بهینه نیاز داشته باشند.

D. Machine Learning: A Solution to IoT Security Challenges

یادگیری ماشینی: راه حلی برای چالش‌های امنیتی IoT . یادگیری ماشینی به روش‌های هوشمندی اشاره دارد که برای بهینه‌سازی معیارهای عملکرد با استفاده از داده‌های نمونه یا تجربیات گذشته از طریق یادگیری مورد استفاده قرار می‌گیرند ML همچنین توانایی (برای دستگاه‌های هوشمند)برای یادگیری بدون برنامه‌ریزی صریح را ممکن می‌سازد .

یادگیری ماشینی زمانی به کار می‌رود که تخصص انسان وجود نداشته باشد و یا نمی‌تواند مورد استفاده قرار گیرد، مانند هدایت یک مکان خصمانه که در آن انسان‌ها قادر به استفاده از تخصص خود نیستند، برای مثال روباتیک، تشخیص گفتار و غیره. همچنین در شرایطی که در آن انسان‌ها قادر به استفاده از تخصص خود نیستند . علاوه بر این، در سیستم‌های هوشمند عملی استفاده می‌شود، به عنوان مثال، گوگل از ML برای تجزیه و تحلیل تهدیدات در برابر نقاط پایانی تلفن همراه و برنامه‌های کاربردی در حال اجرا بر روی اندروید استفاده می‌کند .همچنین از آن برای شناسایی و حذف بدافزار از هندست‌های آلوده استفاده می‌شود . بنابراین، تکنیک‌های ML نیاز به راهنمایی و اصلاح برای مدل دارد اگر پیش‌بینی نادرست ایجاد شود .برعکس، در یادگیری عمیق) (DL، نوع جدیدی ازML ، این مدل می‌تواند دقت پیش‌بینی را خودش تعیین کند . تولید مقدار زیادی از داده‌ها که توسط روش‌های ML و DL برای آوردن هوش به سیستم‌ها مورد نیاز است .علاوه بر این، سودمندی داده‌های تولید شده توسط IoT بهتر با تکنیک‌های ML و DL استفاده می‌شود که

سیستم‌های IoT را قادر به تصمیم‌گیری‌های آگاهانه و هوشمند می‌سازد ML .و DL عمدتا برای امنیت، حریم خصوصی، تشخیص حمله و تجزیه و تحلیل malware استفاده می‌شوند .

برخی از برنامه‌های مربوط به امنیت دنیای واقعی ML به شرح زیر هستند:

- ✓ **تشخیص چهره در پزشکی قانونی: ژست، نورپردازی، انسداد (عینک، ریش)، آرایش، سبک مو و غیره .**
- ✓ **تشخیص هویت برای رمزنگاری امنیتی: سبک‌های مختلف نگارش .**
- ✓ **شناسایی کد مخرب: شناسایی کد مخرب در برنامه‌ها و نرم‌افزار.**
- ✓ **انکار توزیع‌شده سرویس (DDoS)تشخیص: حملات DDoS به زیرساخت از طریق تجزیه و تحلیل رفتار.**

ادبیات تحقیق حاضر امنیت در IoT را با بررسی راه‌حل‌های سنتی موجود و راه‌حل‌های ارائه‌شده از طریق تکنولوژی‌های نوظهور جدید پوشش می‌دهد. اگرچه ML و DL در چند نظرسنجی پوشش داده شده‌اند اما اطلاعات کلی در مورد کاربرد جامع ML و DL کمیاب است .برای پر کردن شکاف‌ها، ما یک بررسی جامع از تکنیک‌های ML و DL مورد استفاده در امنیت IoT انجام می‌دهیم .

حملات فیزیکی

در حملات فیزیکی، مهاجمان به دستگاه‌ها دسترسی مستقیم دارند و جنبه‌های مختلف دستگاه‌ها را دستکاری می‌کنند .برای دسترسی به دستگاه‌های فیزیکی، مهندسی اجتماعی یکی از برجسته‌ترین روش‌ها است که در آن حمله کنندگان به دستگاه‌ها دسترسی دارند و حمله واقعی را انجام می‌دهند که در محدوده آسیب فیزیکی به دستگاه تا استراق‌سمع، کانال‌های جانبی، و دیگر حملات مرتبط قرار دارد

علاوه بر این، برای شروع حملات فیزیکی، حمله کنندگان باید در نزدیکی دستگاه‌ها / سخت‌افزار با مقاصد مختلف مانند تخریب فیزیکی سخت‌افزار، محدود کردن طول عمر آن، به خطر انداختن مکانیزم ارتباطی، دستکاری در منبع انرژی و غیره باشند .همچنین شایان‌ذکر است که حملات فیزیکی ممکن است سنگ بنای سایر حملات باشند، به عنوان مثال از کار انداختن زنگ خطر در خانه می‌تواند منجر به سرقت یا سایر آسیب‌های مرتبط در محیط خانه هوشمند شود . تزریق گره مخرب به شبکه نیز می‌تواند باعث حمله انسان در میانه شود که به مهاجم این امکان را می‌دهد تا امتیازات را افزایش داده و حملات دیگری را آغاز کند .علاوه بر این، چنین دستکاری در دستگاه‌ها نیز ممکن است مهاجمان را قادر به ایجاد تغییراتی در جداول مسیریابی و کلیدهای امنیتی کند که بر ارتباط با لایه‌های بالاتر تاثیر خواهد گذاشت . دیگر حملات فیزیکی شامل مسدود کردن فرکانس‌های رادیویی است که ارتباط در محیط IoT را انکار می‌کند.

مسائل فیزیکی (PHY)و امنیت لایه پیوند

IoTفن‌آوری‌های ارتباطی مختلف را در لایه‌های پایین‌تر پشته پروتکل TCP / IP ترکیب می‌کند و بنابراین یک شبکه ناهمگن پیچیده فراهم می‌کند .این تکنولوژی‌ها عبارتند از:

اما محدود بهZig هایی، WSN، MANET، WiFi، RFID، NFCو غیره نمی‌شود و علاوه بر آن این تکنولوژی‌ها مسائل امنیتی خاص خود را دارند. همانطور که قبلا ذکر شد، ناهمگونی در لایه فیزیکی IoT معرفی می‌شود و سپس اصلاحات مختلفی در لایه لینک داده ایجاد می‌شود، برای مثال طراحی کانال خاص و غیره، بسته به تکنولوژی لایه فیزیکی اساسی . برای این منظور، مکانیزم‌های امنیتی IoT باید ناهمگونی در لایه پیوند داده و فیزیکی را در بر بگیرد . علاوه بر این، تشخیص اختلال در سخت‌افزار نیز از اهمیت بالایی برخوردار است و باید برای جلوگیری از ناهنجاری در لایه بالایی کنترل شود . شایان‌ذکر است که حتی برای تشخیص نفوذ در لایه‌های بالایی، به عنوان مثال حمله مسیریابی، بردارهای حمله بسیاری وجود دارند برای این منظور، IEEEیک استاندارد شناخته‌شده به نام IEEE ۸۰۲,۱۱ ۱۵,۴ را اجباری کرده‌است تا اجازه دهد دستگاه محدود به طور موثر ارتباط برقرار کند

حملات لایه شبکه

در سطح شبکه، حملات با هدف مسیریابی، داده‌ها و تجزیه و تحلیل ترافیک، جعل و راه‌اندازی حمله با دخالت انسان انجام می‌شوند . علاوه بر این، حملات سیبیل نیز در لایه شبکه امکان پذیر است که در آن هویت‌های جعلی / هویت‌های سیبیل برای ایجاد توهم در شبکه مورد استفاده قرار می‌گیرند

از سوی دیگر، نفوذ از طریق ابزارهای مختلف، راهی را برای مهاجم به سیستمی فراهم می‌کند که در آن حمله کنندگان می‌توانند حملات دیگری را انجام دهند و بنابراین، امنیت شبکه برای مهار حملات در مراحل اولیه ضروری است . در لایه شبکه، مهاجم همچنین می‌تواند یک‌گره در معرض خطر را برای استفاده از آن به عنوان گره ارسال جعلی و ایجاد حفره سینکویل نفوذ کند .

حملات لایه حمل و نقل

لایه حمل و نقل مسئول فرآیند تحویل است که در آن پروتکل‌های حمل و نقل امکان تبادل داده‌ها را فراهم می‌کنند . در زمینهIoT ، مسائل امنیتی لایه حمل و نقل سنتی همچنان ادامه دارند .

جدی‌ترین حمله در این لایه، حمله انکار سرویس است که شبکه را خفه می‌کند و منجر به انکار سرویس به برنامه‌های کاربردی می‌شود .لازم به ذکر است که به دلیل ماهیتIoT ، پروتکل‌های TCP و UDP سنتی با دستگاه‌های منابع محدود مقیاس بندی نمی‌شوند، و بنابراین نسخه‌های سبک پروتکل‌های حمل و نقل در مقالات پیشنهاد شده‌اند

لازم به ذکر است که به دلیل ماهیتIoT ، پروتکل‌های TCP و UDP سنتی با دستگاه‌های منابع محدود مقیاس بندی نمی‌شوند، و بنابراین نسخه‌های سبک پروتکل‌های حمل و نقل در مقالات پیشنهاد شده‌اند با این حال، امنیت این پروتکل‌ها برای کاهش حملات DDoS و DoS در IoT از اهمیت ویژه‌ای برخوردار است .

حملات لایه برنامه

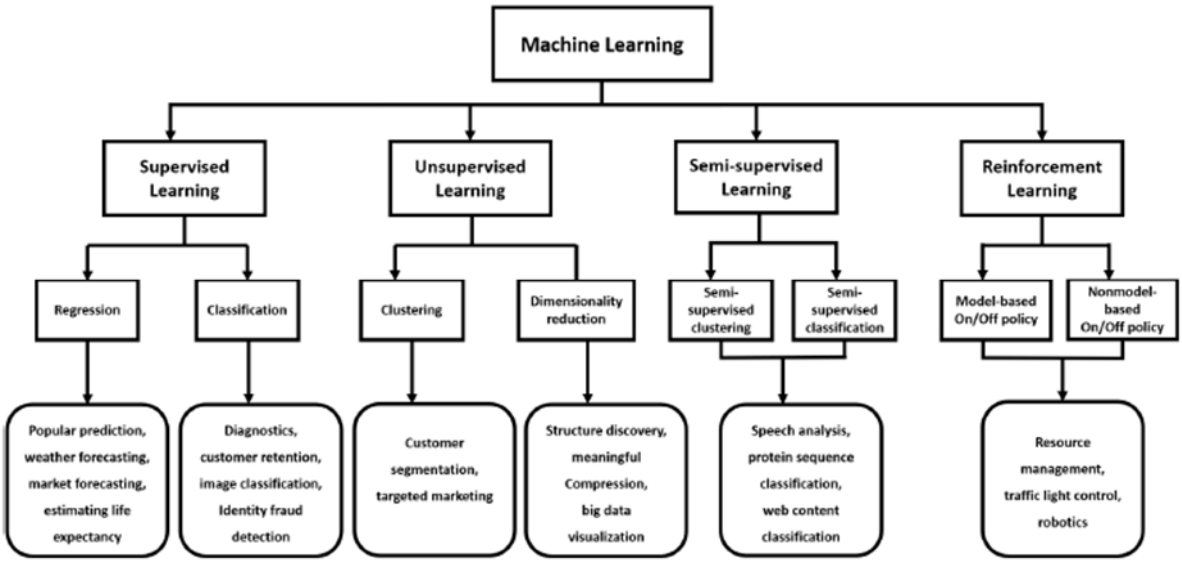
برنامه‌های کاربردی IoT اهداف نسبتا سودمندی برای حمله کنندگان هستند، زیرا راه‌اندازی حملات در سطح برنامه‌ها نسبتا آسان است . برخی از حملات شناخته‌شده شامل حملات سرریز بافر، حملات بدافزار، انکار خدمات، فیشینگ، بهره‌برداری از آسیب‌پذیری‌هایWebApp ، حملات رمزنگاری، حملات کانال جانبی، و حملات انسان در موضوع هستند اما محدود به آن‌ها نمی‌شوند . تکنیک‌های موجود برای کاهش مکانیزم سرریز بافر شامل تجزیه و تحلیل کد استاتیک و دینامیک و دیگر مکانیزم‌های پیچیده مانند اشکال‌زدایی نمادین است. با این حال، به دلیل محدودیت منابع نمی توان از این تکنیک‌ها در IoT استفاده کرد . برنامه‌های کاربردیIoT همچنین در اثر سرریز بافر در معرض تزریق کد مخرب قرار دارند و سایر آسیب‌پذیری‌ها مانند تزریقSQL ، کدنویسی در محل متقابل، ارجاع به شی و ... نیز در معرض

تزریق کد مخرب قرار دارند .پروژه امنیت برنامه وب باز) (OWASP۱۰ آسیب‌پذیری برتر را شناسایی کرد که باعث حملات مختلف به برنامه‌ها می‌شوند .

IOT SECURITY AND MACHINE LEARNING

الگوریتم‌های یادگیری ماشین پایه

الگوریتم های ML می‌توانند به چهار دسته طبقه‌بندی شوند؛ الگوریتم های نظارت شده، بدون نظارت، نیمه نظارت شده و یادگیری تقویتی



یادگیری بدون نظارت: در یادگیری بدون نظارت، محیط تنها ورودی‌هایی را بدون اهداف مطلوب فراهم می‌کند .به داده‌های برچسب دار نیاز ندارد و می‌تواند تشابه بین داده‌های برچسب دار نشده را بررسی کند و داده‌ها را به گروه‌های مختلف طبقه‌بندی کند .

یادگیری با نظارت و تکنیک‌های بدون نظارت عمدتا بر مشکلات تجزیه و تحلیل داده‌ها تمرکز دارند در حالی که یادگیری تقویتی برای مقایسه و مشکلات تصمیم‌گیری ترجیح داده می‌شود .این طبقه‌بندی و انتخاب تکنیک ML به ماهیت داده‌های موجود بستگی دارد .

الگوریتم هایی مانندSVR ، شبکه‌های عصبی، و نایو بیز برای مدل‌سازی پیش‌بینی استفاده می‌شوند.

یادگیری نیمه نظارت شده: در دو نوع قبلی، یا هیچ لیبل برای تمام مشاهدات در مجموعه داده وجود ندارد یا لیبل برای تمام مشاهدات وجود دارد . در بسیاری از موقعیت‌های عملی، هزینه برچسب زدن بسیار بالا است، زیرا برای انجام این کار به متخصصان ماهر انسانی نیاز است. بنابراین، در غیاب برچسب‌ها در اکثر مشاهدات، اما در تعداد کمی از آن‌ها، الگوریتم های نیم عمقی بهترین گزینه برای ساخت مدل هستند.

یادگیری تقویتی: در یادگیری تقویتی) (RL، هیچ نتیجه خاصی تعریف نشده است و نماینده پس از تعامل با محیط از بازخورد یاد می‌گیرد . برخی اقدامات را انجام می‌دهد و براساس پاداش به‌دست‌آمده تصمیم‌گیری می‌کند . یک نماینده را می توان برای انجام اقدامات خوب یا مجازات برای اقدامات بد و استفاده از معیارهای بازخورد برای به حداکثر رساندن پاداش‌های بلند مدت پاداش داد . همچنین انتخاب تابع پاداش مناسب بسیار مهم است زیرا موفقیت و شکست عامل به پاداش کل انباشته بستگی دارد

در ادامه، همان طور که در جدول ۳ نشان‌داده شده‌است، الگوریتم های مختلف ML با تمرکز بر مسائل امنیتی و حریم خصوصی اساسی در شبکه‌های IoT را مورد بحث قرار می‌دهیم . به طور دقیق‌تر، ما احراز هویت، تشخیص و کاهش حمله، حملات انکار سرویس توزیع‌شده) (DDoS،

تشخیص ناهنجاری و نفوذ، و تجزیه و تحلیل malware را در نظر می‌گیریم .

Machine Learning Algorithm	Description
Naive Bayes	It is the classification algorithm used with binary and multi-class environment. It is named as "Naive", as over-simplified assumptions are made for the calculation of probabilities for specific hypothesis. All the attributes are assumed to be conditionally independent instead of calculating the actual values [74].
K-Nearest Neighbour	It is simple and effective supervised learning algorithm and is used for associating new data points to the existing similar points by searching through the available dataset. The model is trained and grouped according to some criteria and incoming data is checked for similarity within K neighbours [75].
K-Means Algorithm	The most commonly used well know technique is K-means clustering algorithm belonging to the unsupervised category of ML family. K-Means clustering is used to classify or group devices based on attributes or parameters, into K number of groups, where K is a positive integer number and its value has to be known for the algorithm to work [76].
Random Forest and Decision Tree (DT)	It is a supervised learning method. It defines a model by implementing certain rules inferring from the data features. Afterwards, this model is used to predict the value of new targeted variable. Decision tree is used in classification and as well as regression problems. Essentially, these trees are used to split dataset into several branches based on certain rules [77].
Support Vector Machines (SVM)	SVM is a supervised ML algorithm with low computational complexity, used for classification and regression. It has the ability to work with binary as well as with multi-class environments [78], [79]. It classifies input data into n dimensional space and draws $n-1$ hyperplane to divide the entire data points into groups.
Recurrent Neural Networks (RNN)	This is a supervised learning algorithm used to develop a cascaded chain of decision units for solving the complex problems [80]. It essentially constructs network with certain number of inputs to trigger outputs. Various types of neural networks have been proposed in the literature, e.g. Multi-Layer Perceptron (MLP), Convolutional Neural Networks (CNNs), and Recurrent Neural Networks (RNNs) [81], [82], [83].
Principal Component Analysis	It is an unsupervised ML algorithm and is multivariate technique for data compression. It performs dimensionality reduction in large data sets and extracts useful information in the form of set comprised of orthogonal variables known as "principal components". These components are organized in an increasing order of variance where first component is associated with highest variance of the data and it continues to the last. The least variance components having least information can be discarded [84].
Q-Learning	It is used for resource scheduling in spectrum management in addition to security in IoT. Q-learning belongs to reinforcement learning (RL) class of the ML. In RL, an agent learns by trial and error that how its actions effect the environment. It estimates the reward after each action and moves to the new state accordingly [76]. It will get reward for good action and penalty for bad actions.
Deep Learning	It is essentially a feed forward Neural Network (NN) in which each neuron is connected to another layer and no connection exists within the layer. The term deep learning refers to multiple layers holding multiple levels of perception such that each layer receives input from the previous layer and feeds the result to following layer [85].

MLبرای ایجاد مدل‌ها استفاده می‌شود، که برای طراحی، تست، و آموزش مجموعه داده‌ها استفاده می‌شود .این الگوریتم های ML برای تشخیص الگوها و شباهت‌های ممکن در مجموعه داده‌های بزرگ استفاده می‌شوند و می‌توانند در داده‌های جدید پیش‌بینی کنند .

ارزیابی و بررسی

در این مطالعه ما یادگیری ماشین در امنیت اینترنت اشیا را مورد بحث و برسی قرار دادیم همچنین درباره ی انواع حملات مختلف در لایه های مختلف را مورد بحث و برسی قرار دادیم.همچنین ما در مورد چالش‌های امنیتی و حریم خصوصی درIoT ، بردارهای حمله، و الزامات امنیتی بحث کرده‌ایم.

جمع بندی

امنیت IoT و حریم خصوصی از اهمیت بالایی برخوردار هستند و نقشی محوری در تجاری سازی فن‌آوری IoT ایفا می‌کنند .راه‌حل‌های امنیتی و حریم خصوصی سنتی از تعدادی از مسائل رنج می‌برند که به ماهیت پویای شبکه‌های IoT مربوط می‌شوند .تکنیک‌های ML و DL و DRL به طور خاص‌تر می‌توانند برای قادر ساختن دستگاه‌های IoT برای انطباق با محیط پویای خود مورد استفاده قرار گیرند .این تکنیک‌های یادگیری می‌توانند عملیات خود سازماندهی را پشتیبانی کنند و همچنین عملکرد کلی سیستم را با یادگیری و پردازش اطلاعات آماری از محیط بهینه کنند) برای مثال کاربران انسانی و دستگاه‌های(IoT .این تکنیک‌های یادگیری ذاتا توزیع شده‌اند و نیازی به ارتباط متمرکز بین دستگاه و کنترلر ندارند .با این حال، مجموعه داده‌های مورد نیاز برای الگوریتم های ML و DL هنوز هم کمیاب هستند، که باعث تعیین معیار می‌شوند

کارهار آینده

اندازه برای همه مناسب نیست: تکنیک‌های DL بسیار خاص کاربرد هستند که در آن یک مدل آموزش‌دیده برای حل یک مساله ممکن است نتواند برای مساله دیگری در دامنه مشابه به خوبی عمل کند . این مدل‌ها معمولا نیاز به آموزش مجدد با داده‌های مربوطه دارند تا برای مشکلات مشابه دیگر مورد استفاده قرار گیرند .

شبکه‌های عصبی عمیق مانند یک جعبه سیاه عمل می‌کنند، همانطور که نمی‌دانیم چگونه هر مدل DL با دستکاری پارامترها و داده‌های ورودی به نتیجه می‌رسد . همانند مغز انسان، غیر ممکن است که بدانیم مغز چگونه کار می‌کند و راه‌حل به‌دست‌آمده نتیجه نورون‌های جاسازی‌شده در لایه‌های به‌هم‌پیوسته پیچیده است . بنابراین، پیش‌بینی لایه دقیق برای شکست احتمالی دشوار است و از این رو برای کاربردهایی که صحت سنجی در آن‌ها مهم است نامناسب می‌شود .