Vol. 1, No. 4, Jan-Mar 2024, (52-68)
Journal of Applied Research in Electrical, Computer and Energy Systems (JARECE)
نشریه تحقیقات کاربردی در برق ، کامپیوتر و سیستم های انرژی
دوره ۱، شماره ۴، زمستان ۱۴۰۲ (۶۸-۵۲)
journal homepage: https://jarece.ir/

بررسی رویکردهای یادگیری ماشین در امنیت اینترنت اشیا

وصال فیروزی*[1] ، داود بهره پور[2]

[1] گروه کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران. V.firoozi@mshdiau.ac.ir
[2] گروه کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران. Bahrepour@mshdiau.ac.ir

چکیده

اینترنت اشیا بسیاری از جنبه های زندگی مدرن را پوشش داده است و از مراقبت های بهداشتی و حمل و نقل گرفته تا اتوماسیون خانگی و سیستم های کنترل صنعتی را متحول کرده است. با این حال، افزایش تعداد دستگاه‌های متصل منجر به افزایش تهدیدات امنیتی شده است. برای کاهش این تهدیدات، تکنیک‌های مختلف یادگیری ماشین و یادگیری عمیق بمنظور شناسایی حملات امنیتی اینترنت اشیا پیشنهاد شده‌اند. در این مطالعه تکنیک های یادگیری ماشین را دسته بندی کرده و به مرور اجمالی مطالعات انجام شده در رابطه با امنیت اینترنت اشیا در هر دسته می پردازیم. در نهایت موضوعات باز و چالش-هایی که نیاز به توجه محققان این رشته دارند، معرفی می‌شود. این تحقیق پتانسیل قابل‌توجه رویکردهای یادگیری ماشین را در تقویت امنیت اینترنت اشیا روشن می‌کند و در نتیجه بینش‌های ارزشمندی را به محققان حوزه امنیت اینترنت اشیا ارائه می‌دهد.

واژه‌های کلیدی: امنیت، اینترنت اشیا، یادگیری عمیق، یادگیری ماشین.

1. مقدمه

اینترنت اشیا[1](IoT) به شبکه‌ای از دستگاه‌های متصل به اینترنت، مانند تلفن‌های هوشمند، دستگاه‌های خانه هوشمند، حسگرهای صنعتی و دستگاه‌های پزشکی اشاره دارد[1]. اینترنت اشیا الگویی است که ارتباط طیف وسیعی از اشیاء و وسایل روزمره را در بر می گیرد. اشیا یا «چیزها» می‌توانند شامل حسگرها، پوشیدنی‌ها، لوازم خانگی، وسایل نقلیه و موارد دیگر باشند که همگی قادر به جمع‌آوری و تبادل داده‌ها با یکدیگر و با اینترنت هستند[2]. اینترنت اشیا در حوزه های مختلف کاربرد دارد و به طور مداوم با پیشرفت فناوری در حال گسترش است[3]. پیش‌بینی‌ها رشد قابل‌توجه در تعداد دستگاه‌های اینترنت اشیا در سرتاسر جهان را نشان می دهد، به طوری که تخمین‌ها حاکی از افزایش تقریباً سه برابری از 9/7 میلیارد دستگاه در سال 2020 به بیش از 29 میلیارد دستگاه تا سال 2030 است. طبق یک گزارش تحقیقات بازار، پیش‌بینی می‌شود که بازار جهانی امنیت اینترنت اشیا از سال 2022 تا 2027 رشد قابل توجهی داشته باشد. عواملی مانند افزایش تعداد دستگاه های اینترنت اشیا، تکثیر محاسبات ابری و نیاز به اقدامات امنیتی سختگیرانه باعث افزایش تقاضا برای راه حل های امنیتی اینترنت اشیا می‌شود[4] .

شکل 1- حوزه های مختلف کاربردی اینترنت اشیا

برنامه های کاربردی اینترنت اشیا در دامنه‌های مختلفی قرار دارند و تطبیق پذیری و پتانسیل خود را به نمایش می گذارند. شکل 1، نمونه هایی از این کاربردها را نشان می دهد. برنامه های کاربردی متنوع اینترنت اشیا نمونه ای از پذیرش و تأثیر گسترده فناوری اینترنت اشیا در بخش های مختلف است[5]. در خانه‌های هوشمند دستگاه‌های اینترنت اشیا می‌توانند به طور یکپارچه نور، دما، امنیت و سرگرمی را مدیریت کنند و راحتی و اتوماسیون را فراهم کنند[6]. در زمینه شهرهای هوشمند، حسگرهای اینترنت اشیا نقش مهمی در نظارت و بهینه‌سازی ترافیک، کیفیت هوا، مدیریت زباله و سایر سیستم‌های شهری ایفا می‌کنند و به افزایش کارایی و پایداری کمک می‌کنند. در حوزه مراقبت‌های بهداشتی از دستگاه های پوشیدنی اینترنت اشیا و دستگاه‌های پزشکی برای نظارت مستمر سلامت، مشاوره از راه دور، و تسهیل درمان، ترویج خدمات مراقبت‌های بهداشتی شخصی و از راه دور استفاده می‌کند[6]. در کشاورزی با استفاده از حسگرها و دستگاه‌های اینترنت اشیا بر شرایط خاک، رشد

[1] Internet of Things

محصول و الگوهای آب و هوا نظارت می‌کنند و اینترنت اشیا کشاورزان را قادر می‌سازد تا تکنیک‌های کشاورزی دقیق را پیاده‌سازی کنند و عملکرد را بهبود بخشند[7].

در حوزه اتوماسیون صنعتی، حسگرها و دستگاه‌های اینترنت اشیا در نظارت و کنترل ماشین‌آلات و تجهیزات، بهینه‌سازی عملیات و به حداقل رساندن زمان خرابی کمک می‌کنند[8]. علاوه بر این، ظهور خودروهای متصل و مجهز به اتصال به اینترنت، به وسایل نقلیه اجازه می دهد تا با سایر دستگاه ها، شبکه ها و خدمات ارتباط برقرار کنند. این خودروها داده‌ها را جمع‌آوری و انتقال می‌دهند، دسترسی از راه دور به کنترل‌های وسیله نقلیه ارائه می‌کنند و طیف وسیعی از خدمات را به رانندگان و مسافران ارائه می‌کنند و تجربه کلی رانندگی را بهبود می‌بخشند. همچنین صنایع از این فناوری برای به حداکثر رساندن عملکردهای تجاری خود با رویکردهای هوشمندسازی و هوش تجاری استفاده می کنند.

اساسی ترین نیاز در شبکه اینترنت اشیا محافظت از کل سیستم ها، برنامه ها و دستگاه های متصل است. حجم عظیم کارهای شبکه اینترنت اشیا چالش های جدیدی را در حوزه های مختلفی از جمله مدیریت دستگاه، مدیریت داده، محاسبات، امنیت و حریم خصوصی و غیره معرفی می کند. با رشد اینترنت اشیا، نگرانی های امنیتی و تهدیدات بالقوه مختلفی مطرح می‌شود[9] .

سیستم‌های اینترنت اشیا به دلیل ویژگی‌های منحصربه‌فرد خود، مانند تعداد زیاد دستگاه‌های درگیر، تنوع پروتکل‌های ارتباطی و قالب‌های داده، و نیاز به ارتباطات بلادرنگ، چالش‌های امنیتی متعددی را ارائه می‌کنند[10]. نادیده گرفته شدن حفره‌ها و قصورهای امنیتی در این فناوری، صنایع را با حملات سایبری مواجه می‌کند[11]. برخی از مهم‌ترین چالش‌های امنیتی در سیستم‌های اینترنت اشیا عبارتند از: امنیت دستگاه، امنیت داده‌ها، امنیت ارتباطات، حریم خصوصی، امنیت میان‌افزار و امنیت زنجیره تامین[12].

بدون یک سیستم قابل اعتماد، برنامه های کاربردی اینترنت اشیا، نمی توانند نیازهای مردم و جامعه را برآورده کنند و ممکن است تمام کارایی خود را از دست بدهند. به طور معمول، سیستم های اینترنت اشیا در چندین لایه، از جمله لایه ادراک یا حس، شبکه و ارتباطات داده لایه میان افزار یا لایه پشتیبانی و لایه کاربردی کار می کنند. هر یک از این لایه‌ها دارای مجموعه منحصربه‌فردی از وظایف و فناوری‌های مرتبط برای انجام در یک برنامه اینترنت اشیا هستند و هر لایه مجموعه جدیدی از مسائل و خطرات امنیتی را به همراه دارد. به عنوان مثال، حمله انکار سرویس[۲](DDoS) ، حملات جعل سرویس، پارازیت، استراق سمع، دستکاری داده ها، حملات مخرب و غیره رایج ترین حملات اینترنت اشیا هستند[13] . بنابراین، بسته به ماهیت مسائل امنیتی، راه‌حل‌های بالقوه امنیتی اینترنت اشیا مانند احراز هویت، کنترل دسترسی، پیش‌بینی تهدید و خطر، تجزیه تحلیل بدافزار، تشخیص ناهنجاری یا نفوذ، و پیشگیری و غیره می‌تواند مفید باشد. پرداختن به این چالش ها نیازمند یک رویکرد چند لایه است که شامل پروتکل های امنیتی قوی، به روز رسانی مکرر نرم افزار، و نظارت و آزمایش مداوم برای شناسایی و رسیدگی به آسیب پذیری ها در صورت بروز می شود[14].

با توجه به ازدیاد تهدیدات و حملات امنیتی و پیچیدگی در حوادث امنیتی، تکنیک های مرسوم برای مقابله با آنها دیگر موثر نیستند. بنابراین یک سیستم امنیتی هوشمند مبتنی بر فناوری‌های مدرن که بتواند این نگرانی‌های امنیتی را برطرف کند، برای محافظت از نسل بعدی سیستم اینترنت اشیاء ضروری است.

[2] Distributed denial-of-service

هوش مصنوعی یکی از مهم‌ترین فناوری‌ها برای توسعه سیستم‌های هوشمند است و به عنوان بخشی از انقلاب صنعتی چهارم [15] نیز در نظر گرفته می‌شود. بنابراین، با استفاده از دانش هوش مصنوعی، به‌ویژه یادگیری ماشین و یادگیری عمیق، می‌توان با ناهنجاری‌ها یا فعالیت‌های مخرب نامطلوب در اینترنت اشیا مقابله کرد.

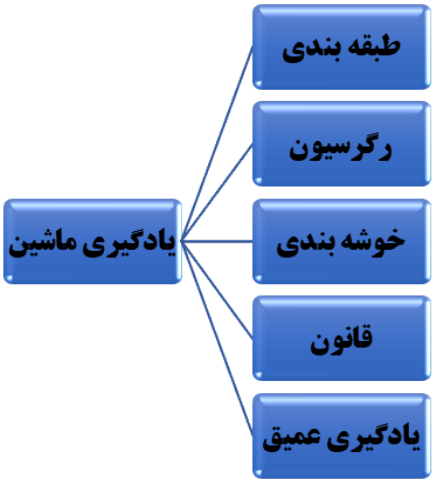
به طور معمول، مدل‌های یادگیری عمیق و یادگیری ماشین شامل مجموعه‌ای از قوانین، روش‌ها یا توابع انتقال پیچیده هستند که بینش‌های مفید یا الگوهای داده‌ای جالب را از داده‌های امنیتی استخراج می‌کنند. بنابراین، می‌توان از مدل‌های امنیتی حاصل برای آموزش ماشین‌ها برای پیش‌بینی تهدیدها یا خطرات در مراحل اولیه، یا شناسایی ناهنجاری‌ها در اینترنت اشیا برای توسعه یک سیاست دفاعی مناسب استفاده کرد. تکنیک‌های یادگیری ماشین که معمولاً برای جنبه های امنیتی و تشخیص حملات به کار می‌روند شامل درخت‌های تصمیم، جنگل‌های تصادفی، K نزدیک‌ترین همسایه‌ها و ماشین‌های بردار پشتیبان می‌شود. اثربخشی این رویکردها به شدت به کیفیت مجموعه داده اتخاذ شده برای اهداف آموزش و ارزیابی بستگی دارد. برای ارزیابی عملکرد مدل‌های یادگیری ماشین، معیارهای عملکرد متنوعی از جمله دقت، یادآوری، امتیاز F1 استفاده می‌شود[16] . در یادگیری عمیق معماری های مختلف یادگیری عمیق مانند پرسپترون چند لایه[۳](MLP)، شبکه های عصبی کانولوشن[۴] (CNN)، شبکه های عصبی تکراری[۵] (RNN)، شبکه های باور عمیق[۶] (DBN)، یا شبکه های ترکیبی می توانند برای مدل سازی امنیت اینترنت اشیا استفاده شوند[17].

با توجه به اهمیت روش های یادگیری ماشین در امنیت اینترنت اشیا، در این تحقیق، مطالعات انجام شده در زمینه استفاده از یادگیری ماشین برای افزایش امنیت اینترنت اشیا دسته بندی می شود و چالش های موجود در این زمینه معرفی می گردد. در ادامه این مقاله در بخش 2 مروری بر کارهای مرتبط انجام می شود. چالش های پیش روی، همچنین فرصت های مطالعاتی آینده دستورالعمل های آینده، در بخش 3 بیان می شود، و در بخش 4 مقاله جمع بندی می شود.

2. مرور کارهای پیشین

تکنیک‌های یادگیری ماشین و یادگیری عمیق به هوش مصنوعی معروف هستند که می‌توانند به دستگاه‌های اینترنت اشیا کمک کنند تا با کمک داده های آموزشی، بیاموزند و رفتار کنند. مدل‌های یادگیری اغلب از مجموعه‌ای از قوانین، رویه‌ها یا «عملکردهای انتقال» پیچیده تشکیل شده‌اند که ممکن است برای کشف روندهای مربوط به حوادث امنیتی در داده‌های اینترنت اشیا، و همچنین شناسایی و پیش‌بینی رفتار مورد استفاده قرار گیرند[18]. در نتیجه، در زمینه اینترنت اشیا، هم یادگیری ماشین و هم یادگیری عمیق می توانند در شبکه های پویا اینترنت اشیا بدون نیاز به دخالت انسان یا کاربر عمل کنند. تحقیقات اخیر به طور فزاینده ای بر اثربخشی الگوریتم های یادگیری ماشین و یادگیری عمیق برای مبارزه با این نفوذ و فعالیت بدخواهانه متمرکز شده است. در این بخش به بررسی این الگوریتم ها و همچنین کاربرد و کارایی آنها در امنیت اینترنت اشیا می پردازیم. برای این منظور مطابق شکل 2، تکنیک‌های یادگیری ماشین را به شش گروه دسته بندی کرده مطالعه نمودیم.

[3] Multi-layer perceptron
[4] Convolutional neural networks
[5] Recurrent neural networks
[6] Deep belief networks



شکل 2- دسته بندی تکنیک های یادگیری ماشین

2-1 طبقه بندی

به فرایند تشخیص، درک و دسته‌بندی اشیا و ایده‌ها به دسته‌های موجود و تعریف شده بـه عنـوان زیردسـته‌ای از جامعـه فعلی، در یادگیری ماشین طبقه‌بندی می‌گویند. به کمک مجموعه داده‌های آموزشی از پیش طبقه‌بندی شـده، برنامـه‌های طبقـه بندی در یادگیری ماشین، آموزش می‌بینند و با استفاده از گستره‌ی وسـیعی از الگوریتم‌هـا، مجموعـه داده‌هـا را می‌تواننـد بـه دسته‌های مرتبط و معنی‌دار، طبقه‌بندی کنند. در زمینه یادگیری ماشین، روشهای طبقه بندی به طور گسترده مورد استفاده قـرار می گیرند. از طبقه‌بندی در امنیت اینترنت اشیا معمولاً به برای پیش‌بینی یک مقدار/رده گسسته ثابت، مانند نتیجـه [ناهنجـاری، عادی] استفاده می‌شود.

چندین تکنیک طبقه‌بندی محبوب، مانندk نزدیک‌ترین همسایه [19]، ماشین‌های بردار پشتیبان[20] ، تقویت تطبیقی [21] و درخت تصمیم[22] ، یادگیری مجموعه ای مانند جنگل های تصادفی [23]، وجود دارد. k نزدیک‌ترین همسایه یک الگوریتم یادگیری ماشین است که معمولاً در وظایف رگرسیون و طبقه بندی استفاده می شود. کارکرد این الگـوریتم بـر اسـاس اصـل شباهت است که در آن نمونه ها بر اساس شباهت ویژگی‌های آنها با نمونه های شـناخته شـده طبقـه بنـدی مـی شـوند. درk نزدیک‌ترین همسایه، کلاس یا مقدار یک نمونه معین بر اساس نزدیکترین همسایه ها تعیـین مـی شـود. مقـدار k معمـولاً بـه صورت تجربی انتخاب می شود و می تواند بر عملکرد الگوریتم تأثیر بگذارد. سپس کلاس نمونـه جدیـد بـا اکثریـت رای k نزدیکترین همسایه آن تعیین می شود [19].ماشین‌های بردار پشتیبان یک الگوریتم یادگیری نظارت شده معروف است کـه بـه طور گسترده در یادگیری ماشین برای کارهای طبقه بندی و رگرسیون استفاده می شود. ماشین‌های بـردار پشـتیبان بـر اسـاس اصول کمینه سازی ریسک ساختاری و بعد عمل می کند. هدف اصلی الگوریتم ماشین‌های بردار پشـتیبان شناسـایی یـک ابـر صفحه بهینه است که به طور موثر طبقات متمایز از داده ها را با به حداکثر رساندن حاشیه بین نزدیک ترین نقاط از هر کلاس، که به عنوان بردارهای پشتیبان نامیده می شوند، جدا می کند [20]. تقویت تطبیقی چندین یادگیرنده ضعیف را با تنظیم مکـرر وزن‌ها بر روی نمونه‌های طبقه‌بندی‌شده اشتباه به یادگیرندگان قوی ترکیب می‌کند [21]. درخت تصمیم از مدل‌های یـادگیری ماشینی همه کاره است که برای مسائل طبقه‌بندی و رگرسیون از جمله شناسایی باتنت اینترنت اشیا قابل استفاده مـی باشـد. الگوریتم به صورت بازگشتی داده های ورودی را بر اساس قوانین تصمیم گیری به زیرمجموعه های کوچکتر تقسیم می کنـد

تا زمانی که هر زیر مجموعه به یک کلاس یا مقدار منطبق شود. هدف درختان تصمیم، به حداکثر رساندن اطلاعات در طول انتخاب ویژگی است [22].

الگوریتم‌های طبقه‌بندی می‌توانند حوادث امنیتی را به منظور رسیدگی به مسائل مختلف امنیتی اینترنت اشیا، از جمله تشخیص نفوذ یا حمله، تجزیه و تحلیل بدافزار، و تشخیص ناهنجاری یا تقلب در اینترنت اشیا، دسته بندی کند. به عنوان مثال، تکنیک طبقه‌بندی ماشین بردار پشتیبان در پروفایل رفتار غیرعادی دستگاه‌های اینترنت اشیا [24] و برای شناسایی بدافزارهای اندرویدی و ارائه خدمات اینترنت اشیا قابل اعتماد [25] استفاده می‌شود. تکنیک جنگل تصادفی برای تشخیص ناهنجاری ها [26]، حمله انکار سرویس [27]، سرویس تشخیص نفوذ در اینترنت اشیا [28]، تشخیص ناهنجاری شهر هوشمند [29] و غیره استفاده می شود.

2-2 رگرسیون

رگرسیون یکی از اصولی‌ترین روش‌های آماری است و در تحلیل داده‌های آماری به‌عنوان ابزار مهم مورد استفاده قرار می‌گیرد. با استفاده از رگرسیون، می‌توانیم بهترین مدلی که توصیف کننده رابطه بین متغیرهاست را پیدا کنیم. این مدل به ما این امکان را می‌دهد تا پیش‌بینی‌های دقیق‌تری در مورد متغیرهای وابسته براساس متغیرهای مستقل داشته باشیم. یک کار رگرسیونی به عنوان پیش بینی یک مقدار پیوسته یا عددی، مانند تأثیر حملات تعریف می‌شود. مدل رگرسیون برای پیش‌بینی کمی حملات یا پیش‌بینی تأثیر یک حمله، مانند کرم‌ها، ویروس‌ها یا سایر نرم‌افزارهای مخرب مفید است [30]. به طور مشابه، یک مدل امنیتی کمی، به عنوان مثال، فیشینگ در یک دوره خاص یا پارامترهای بسته شبکه، تکنیک های رگرسیون می تواند مفید باشد [31]. چندین تکنیک رگرسیون رایج مانند خطی، لجستیک، چند جمله‌ای، ریج، کمند، درخت‌های رگرسیون، مؤلفه‌های اصلی، شبکه الاستیک، پواسون، دوجمله‌ای منفی، گام به گام، رگرسیون حداقل مربعات جزئی [32] و غیره وجود دارد که می‌توان از آنها برای ایجاد امنیت کمی استفاده کرد. با توجه به اصل کار آنها در یادگیری ماشین مدل کنید. به عنوان مثال، مدل مبتنی بر رگرسیون خطی برای شناسایی منشأ حمله سایبری [33] و تحلیل رگرسیون چندگانه برای همبستگی ویژگی‌های انسانی و اهداف رفتار امنیت سایبری استفاده می‌شود. به طور مشابه، روش‌های منظم‌سازی رگرسیون مانند Lasso، Ridge، یا ElasticNet، می‌توانند تجزیه و تحلیل حملات امنیتی را برای دستیابی به نتیجه بهتر با توجه به ابعاد بالای داده‌های امنیتی اینترنت اشیا تقویت کنند[34]. یک روش مبتنی بر رگرسیون لجستیک برای شناسایی بات نت‌های مخرب اینترنت اشیا [35] استفاده می شود. رگرسیون لجستیک یک الگوریتم یادگیری ماشینی اساسی است که به طور گسترده در برنامه های کاربردی مختلف از جمله شناسایی بات نت اینترنت اشیا استفاده می شود. به دلیل سادگی، کارایی و تفسیر پذیری آن مورد توجه قرار گرفته است. ایده اصلی رگرسیون لجستیک، پیش‌بینی احتمال یک نتیجه باینری بر اساس متغیرهای ورودی است، مانند تعیین اینکه آیا دستگاهی به یک بات‌نت آلوده شده است یا خیر. این پیش‌بینی با استفاده از تابع سیگموئید مدل‌سازی می‌شود. بنابراین، می‌توان نتیجه گرفت که تکنیک‌های رگرسیون را می‌توان برای ساخت مدل پیش‌بینی و طبقه‌بندی شده برای هوش امنیتی اینترنت اشیا استفاده کرد.

2-3 تکنیک های خوشه بندی

خوشه بندی یکی دیگر از کارهای رایج در یادگیری ماشین، برای تحلیل داده های امنیتی اینترنت اشیا است که یادگیری بدون نظارت بشمار می رود. دراین تکنیک گروه‌هایی از مجموعه‌ای از نقاط داده را بر اساس شباهت و عدم شباهت در داده‌های امنیتی تولید شده توسط دستگاه‌های اینترنت اشیا از منابع مختلف، خوشه‌بندی یا ایجاد کند. بنابراین، خوشه‌بندی می‌تواند به کشف الگوها و ساختارهای پنهان در داده‌ها کمک کند و امکان تشخیص ناهنجاری‌ها یا حملات در اینترنت اشیا را فراهم کند. پارتیشن، سلسله مراتب، نظریه فازی، توزیع، چگالی، نظریه گراف، گرید، نظریه فراکتال و سایر دیدگاه ها می توانند برای خوشه بندی داده ها استفاده شوند[36] . K-means[37]، K-medoids[38] ، پیوند تکی، پیوند کامل، خوشه بندی تجمعی، DBSCAN، OPTICS، مدل مخلوط گوسی [36]، مفاهیم رایج الگوریتم های خوشه بندی است و این تکنیک های خوشه بندی را می توان برای حل مشکلات مختلف امنیتی اینترنت اشیا استفاده کرد. الگوریتم K-Means ، مجموعه داده بدون برچسب را به عنوان ورودی می‌گیرد، مجموعه داده را به تعداد k خوشه تقسیم می‌کند و روند را تکرار می‌کند تا زمانی که بهترین خوشه ها را پیدا نکند الگوریتم ادامه پیدا می‌کند. مقدار k باید در این الگوریتم از پیش تعیین شده باشد این الگوریتم داده ها را به یک خوشه اختصاص می‌دهد به طوری که مجموع فاصله مربع شده بین نقاط داده و مرکز گروه (میانگین محاسبه تمام نقاط داده ای که به آن خوشه تعلق دارند) در حداقل باشد. هرچه تنوع کمتری در خوشه ها داشته باشیم، نقاط داده در یک خوشه همگن (مشابه) هستند[37] . الگوریتم k-Medoids که بهبود یافته الگوریتم k-Means است، عملکردی بسیار شبیه به الگوریتم k-Means دارد، با این تفاوت که در الگوریتم k-Medoids به جای استفاده از میانگین، از خود نمونه ها برای مرکز ثقل و نمایندگی خوشه ها استفاده می شود. با انتخاب نمونه های واقعی جهت نمایش یک خوشه، حساسیت روش نسبت به نمونه های نویز و خارج از محدوده کاهش می یابد[38] .

از نمونه های خوشه بندی در امنیت اینترنت اشیا می توان به استفاده از الگوریتم k-Means در روش پیشنهادی بنام "پروفایل" اشاره کرد که رفتار غیرعادی دستگاه های اینترنت اشیا را تشخیص می داد [24]. در[39] الگوریتم k-Medoids را با استفاده از روشهای فراابتکاری بهبود دادند و از آن برای تشخیص نفوذ در ابزارهای اینترنت اشیا بهره بردند. در [40] یک رویکرد مبتنی بر آستانه پویا با استفاده از خوشه بندی داده ها را برای تشخیص موارد پرت یا نویز در داده ها پیشنهاد شده است. در [41]، یک رویکرد خوشه‌بندی فازی در تشخیص نفوذ اینترنت اشیا استفاده می‌شود. برای تجزیه و تحلیل داده های گزارش سیستم برای برنامه های کاربردی امنیت سایبری، رویکردهای خوشه بندی برای استخراج بینش یا دانش مفید مفید است. بنابراین، با کشف الگوها و ساختارهای پنهان در داده‌های امنیتی اینترنت اشیا، تکنیک‌های خوشه‌بندی می‌توانند نقش مهمی را از طریق اندازه‌گیری شباهت یا عدم تشابه رفتاری برای حل مشکلات امنیتی مختلف مانند تشخیص بیرونی، تشخیص ناهنجاری، استخراج امضا، تشخیص تقلب، تشخیص حمله و غیره در حوزه اینترنت اشیا سایبری ایفا کنند.

2-4 تکنیک های مبتنی بر قانون

یک سیستم مبتنی بر قانون، سیستمی است که قوانین را برای تصمیم گیری هوشمندانه اعمال می کند. این سیستم قوانین را از داده ها استخراج می کند و می‌تواند هوش انسانی را تقلید کند[42]. سیستم‌های مبتنی بر قانون می‌توانند نقش مهمی در امنیت اینترنت اشیا از طریق یادگیری قوانین امنیتی یا خط‌مشی از داده‌ها ایفا کنند. یادگیری قوانین انجمنی یک روش برجسته برای کشف ارتباط یا قوانین در میان مجموعه ای از ویژگی های موجود در یک مجموعه داده امنیتی در زمینه یادگیری ماشینی است. انواع مختلفی از قوانین تداعی در این حوزه پیشنهاد شده است، مانند الگوهای مکرر [43]، مبتنی بر درخت، مبتنی بر منطق، قوانین فازی[44] ، باور قانون [45] و غیره. تکنیک های یادگیری قوانین مانند AIS، AprioriTID ,[46] Apriori و Apriori-Hybrid،[47] FP-Tree، وجود دارند که می توانند برای حل مشکلات امنیتی اینترنت اشیا و تصمیم گیری هوشمند استفاده شود. به عنوان مثال، تشخیص نفوذ شبکه مبتنی بر الگوریتم قانون کاوی در [48] ارائه شده است. علاوه بر این، قوانین تداعی فازی برای ساختن یک سیستم تشخیص نفوذ مبتنی بر قانون استفاده می شود [49]. برای تجزیه و تحلیل فعالیت‌های بدافزار اینترنت اشیا، یک مطالعه مبتنی بر قوانین مرتبط با درخت FP در [50] انجام شده است. اگرچه اتخاذ یک رویکرد مبتنی بر قانون آسان است، اما به دلیل ایجاد تعداد زیادی تداعی یا الگوهای مکرر بسته به مقادیر حمایت و اطمینان، و در نتیجه، مدل را پیچیده می کند. یک مدل ارتباط موثر می تواند این موضوع را به حداقل برساند. به عنوان مثال، نویسندگان در [51]، یک رویکرد یادگیری قوانین را ارائه می کنند که به طور موثر قوانین ارتباطی را که غیر زائد و قابل اعتماد هستند کشف می‌کند. قوانین همچنین می توانند برای ساختن سیستم های مبتنی بر دانش یا سیستم های خبره مبتنی بر قانون برای حل مشکلات امنیتی پیچیده تر در اینترنت اشیا استفاده شوند. هر یک از این سیستم‌ها شامل مجموعه‌ای از قوانین خط‌مشی برای تعریف محدوده فعالیت‌هایی است که باید در یک شبکه مجاز باشند، که در آن هر قانون به طور صریح مجاز است یا رد می‌شود. حتی حملات روز صفر جدیدی که از کنترل‌های مبتنی بر قانون استفاده می‌کنند یا نظارت بر سیاست‌های امنیتی را فیلتر می‌کنند، مسدود می‌شوند.

.

2-5 رویکردهای مبتنی بر شبکه عصبی عمیق

یادگیری عمیق زیرمجموعه‌ای از یادگیری ماشینی است که از شبکه عصبی مصنوعی توسعه یافته است، که یک معماری محاسباتی برای یادگیری از داده‌ها با ترکیب سطوح پردازشی متعدد، مانند لایه‌های ورودی، پنهان و خروجی در یک واحد شبکه ارائه می‌دهد[52]. بنابراین، تکنیک‌های یادگیری عمیق قادر به یادگیری از داده‌های امنیتی اینترنت اشیا از طریق این لایه‌ها هستند و به دلیل ماهیت جذب دانش در معماری عمیق، به عنوان روش‌های یادگیری سلسله مراتبی شناخته می‌شوند. یادگیری عمیق در موقعیت‌های مختلف، به‌ویژه زمانی که از مجموعه داده‌های امنیتی عظیم یاد می‌گیرد، از الگوریتم‌های یادگیری ماشین معمولی بهتر عمل می‌کند. دستگاه های مبتنی بر اینترنت اشیا و برنامه‌ها یا سیستم‌های آنها مقدار زیادی داده امنیتی در محیط اینترنت اشیا تولید می‌کنند. در نتیجه، بسته به مجموعه داده‌ها، رویکردهای یادگیری عمیق ممکن است نتایج

بهتری ارائه دهند. بسته به ویژگی ها و ماهیت داده های امنیتی، معماری هـای مختلـف یـادگیری عمیـق ماننـدMLP ، CNN، RNN، DBN، یا شبکه های ترکیبی می توانند برای مدل سازی امنیت اینترنت اشیا استفاده شوند[17] .

MLP یا پرسپترون چند لایه: یک MLP که اغلب به عنوان یک شبکه عصبی مصنوعی پیشخور شناخته می شود، بلـوک اصلی ساختمان شبکه عصبی است. الگوریتم های یادگیری عمیق یک MLP معمولی شامل یک لایه ورودی، یک یا چند لایه پنهان و یک یا چند لایه خروجی است. هر گره در یک لایه از طریق زنجیره ای از اتصالات بـه وزن خاصـی در لایـه بعـدی متصل می شود. وزنها به‌طور داخلی توسط MLP به‌روزرسانی و تنظیم می‌شوند، زیـرا مـدل از طریـق فرآینـد پـس‌از انتشـار توسـعه می‌یابـد. از شـبکه MLP و LSTM بـرای تشـخیص نفـوذ در شـبکه اینترنـت اشـیا بـا اسـتفاده از مجموعـه داده CICDDoS2019 در [53] استفاده شده است. یک چارچوب برای تجزیه و تحلیل بدافزارهای اندرویدی در [54] با استفاده از یادگیری عمیق پیشنهاد شده است.در [55] برای شناسایی ترافیک مخرب بات نتها از یادگیری عمیق استفاده شد.

CNN یا شبکه های عصبی کانولوشن: CNN طراحـی سـنتی شـبکه عصـبی را بهبـود م یبخشـد و شـامل لایـه هـای کانولوشن، لایه های ادغام و لایه های کاملاً متصل است. هر یک از این سطوح پارامترهای بهینه شده را در نظـر مـی گیـرد و پیچیدگی را کاهش می دهد. CNN همچنین برای رفع مشکل برازش بیش از حد که می تواند در شبکه MLP اتفاق بیفتـد، از انصراف استفاده می کند. در سال‌های اخیر معمولاً در زمینه‌های متعددی مانند پردازش زبان طبیعـی، تجزیـه و تحلیـل صـدا، پردازش تصویر و سایر داده‌های همبسته خودکار استفاده می‌شود، زیرا از ساختار دوبعدی داده‌های ورودی بهره می‌برد. CNN در حوزه امنیت اینترنت اشیا نیز مورد استفاده قرار گرفته است. استفاده از یک مـدل یـادگیری عمیـق مبتنـی بـر CNN بـرای تشخیص نفوذ، مانند حملات انکار سرویس[56] ، برای شناسایی بدافزار [57]، تشخیص بدافزار اندرویـد [58] اسـتفاده شـده است. در محیط اینترنت اشیا، برخی از مدل‌های یادگیری عمیق مبتنی بر CNN با معماری سبک می‌توانند محاسبات را کاهش داده و عملکرد بالاتری را با منابع محدود ارائه دهند.

RNN یا شبکه عصبی بازگشتی: یک RNN نوع دیگری از شبکه عصبی است که در آن اتصالات بین گره ها یک نمودار جهتدار را در امتداد یک دنباله زمانی تشکیل می دهند. مدل RNN که از شبکه های عصبی پیشـخور مشـتق شـده اسـت، مـی تواند توالی های با طول ورودی های متغیر را با استفاده از حالت داخلی یا حافظه آنها پردازش کنـد. اسـتفاده از مـدل RNN برای امنیت اینترنت اشیا و همچنین پردازش زبان طبیعی و تشخیص صدا به دلیل ظرفیت آن برای مـدیریت مـوثر داده هـای متوالی امکان پذیر است. دستگاه های اینترنت اشیا مقدار قابل توجهی از داده های متوالی را از چندین منبع تولیـد مـی کننـد، مانند جریان های ترافیک شبکه، داده های وابسته به زمان و غیره. هنگامی که الگوهای رفتاری تهدید وابسته به زمـان هسـتند، استفاده از اتصالات مکرر می تواند به شبکه های عصبی کمک کند تا نگرانی های امنیتی را شناسایی کنند. دلیل این امـر ایـن است که دارای مشخصه ای به نام حافظه کوتاه مدت طولانی[7](LSTM) است که به آن اجازه می دهـد ورودی هـای قبلـی را حفظ کند و آن را به یک مدل بسیار مفید برای پیش بینی سری های زمانی تبدیل می کند. چنین شبکه بازگشتی مبتنی بر مدل

[7] Long Short Term Memory

LSTM می تواند برای چندین هدف در حوزه امنیت، مانند تشخیص نفوذ [53]، برای شناسایی و طبقه بندی برنامه های مخرب [59] و غیره استفاده شود.

علاوه بر این مدل‌های یادگیری عمیق، مدل‌های شبکه ترکیبی مانند مجموعه طبقه‌بندی‌کننده‌ها، شبکه LSTM با ترکیب CNN نیز می‌تواند برای شناسایی حملات اینترنت اشیا مانند شناسایی بدافزار، فیشینگ و شناسایی و کاهش حملات بات‌نت استفاده شود. سایر مدل‌های یادگیری عمیق، مانند مدل امنیتی مبتنی بر شبکه باور عمیق، ممکن است برای امنیت اینترنت اشیا استفاده شود[60] . در جدول 1، نحوه استفاده از روش‌های مختلف یادگیری ماشین از جمله یادگیری عمیق برای حل مسائل امنیتی مختلف در حوزه اینترنت اشیا را خلاصه کرده‌ایم. بنابراین، ما می‌توانیم استنباط کنیم که تکنیک‌های ماشینی یا یادگیری عمیق ذکر شده در بالا، و همچنین انواع آن‌ها یا رویکردهای سبک وزن اصلاح‌شده، می‌توانند نقش مهمی در تحلیل‌های امنیتی مبتنی بر داده در محیط اینترنت اشیا ایفا کنند.

جدول 1- خلاصه ای از الگوریتم های یادگیری ماشین در امنیت اینترنت اشیا

منبع	هدف	الگوریتم	تکنیک
[24]	طبقه بندی رفتار غیرعادی دستگاه‌های اینترنت اشیا	ماشین بردار پشتیبان	طبقه بندی
[25]	شناسایی بدافزارهای اندرویدی و ارائه خدمات اینترنت اشیا قابل اعتماد	ماشین بردار پشتیبان	
[26]	تشخیص ناهنجاری ها	جنگل تصادفی	
[27]	حمله انکار سرویس	جنگل تصادفی	
[28]	سرویس تشخیص نفوذ در اینترنت اشیا	جنگل تصادفی	
[29]	تشخیص ناهنجاری شهر هوشمند	جنگل تصادفی	
[34]	تحلیل حملات امنیتی	منظم‌سازی رگرسیون	رگرسیون
[35]	برای شناسایی بات نت های مخرب	رگرسیون لجستیک	
[24]	پروفایل رفتار غیرعادی دستگاه های اینترنت اشیا	k-Means	خوشه بندی
[39]	تشخیص نفوذ در ابزارهای اینترنت اشیا	k-medois	
[40]	تشخیص موارد پرت یا نویز در داده ها	آستانه پویا	
[41]	تشخیص نفوذ اینترنت اشیا	خوشه‌بندی فازی	
[48]	تشخیص نفوذ در شبکه	قانون کاوی	قانون
[49]	سیستم تشخیص نفوذ	قوانین تداعی فازی	
[51]	کشف قوانین ارتباطی قابل اعتماد	یادگیری قوانین	
[54]	تحلیل بدافزارهای اندرویدی	MLP	شبکه عصبی عمیق
[55]	شناسایی ترافیک مخرب بات نتها	MLP	
[56]	تشخیص حملات انکار سرویس	CNN	
[57]	شناسایی بدافزار	CNN	
[58]	تشخیص بدافزار اندروید	CNN	
[53]	تشخیص نفوذ	LSTM	
[59]	برای شناسایی و طبقه بندی برنامه های مخرب	LSTM	

3. موضوعات باز و چالش ها

در این بخش، ما چالش‌های موجود و همچنین جهت‌های آینده تحقیقات برای ایمن‌سازی شبکه‌ها و سیستم‌های اینترنت اشیا تحلیل می شود. کارایی یک راه‌حل امنیتی اینترنت اشیا مبتنی بر یادگیری ماشین یا یادگیری عمیق اساساً توسط ماهیت و ویژگی‌های داده‌ها و عملکرد الگوریتم‌های یادگیری تعیین می‌شود. تکنیک‌های یادگیری ماشین و یادگیری عمیق گوناگونی برای ارزیابی داده‌ها و استخراج بینش‌ها وجود دارد. بنابراین، انتخاب یک الگوریتم یادگیری مناسب برای برنامه موردنیاز در امنیت اینترنت اشیا ممکن است چالش‌برانگیز باشد. دلیل این موضوع این است که بر اساس کیفیت داده، نتایج الگوریتم‌های یادگیری مختلف ممکن است متفاوت باشد. اگر الگوریتم یادگیری نادرست انتخاب شود، ممکن است نتایج غیرمنتظره‌ای به دست آید که منجر به هدر رفتن زحمت و دقت مدل می‌شود. به همین ترتیب، داده‌های امنیتی غیرضروری اینترنت اشیا و نویزها و داده های پرت، ممکن است موجب پردازش های زاید و نتایج نادرست شود. اگر داده‌های اینترنت اشیا نامناسب باشند، مانند نماینده نبودن، کیفیت پایین، ویژگی‌های نامربوط، یا مقدار نامناسب برای آموزش، مدل‌های امنیتی یادگیری ماشین یا یادگیری عمیق ممکن است بی‌ارزش شود یا دقت کمتری داشته باشند. فرصت‌ها و جهت‌های تحقیق آینده در حوزه امنیت اینترنت اشیا شامل موارد زیر است:

- در دنیای اینترنت اشیا، جمع‌آوری داده‌های امنیتی آسان نیست. ویژگی‌های پویای اینترنت اشیا، مانند ناهمگنی، حجم بزرگ داده ها و فراوانی از حوزه‌های مختلف کار جمع اوری داده ها را پیچیده می کند. برای تحلیل بیشتر، جمع‌آوری و مدیریت داده‌های مرتبط تولیدشده توسط اینترنت اشیا برای برنامه‌های هدف، مانند امنیت در برنامه‌های شهر هوشمند، برای تسهیل تحقیقات بیشتر حیاتی است. بنابراین، هنگام کار با داده‌های تولیدشده توسط اینترنت اشیا، نیاز به تجزیه و تحلیل عمیق‌تری از روش‌های جمع‌آوری داده وجود دارد.

- مقادیر مبهم بسیار، مقدارهای گم‌شده، داده های پرت، و داده‌های نادرست ممکن است در داده‌های امنیتی تاریخی یا خام اینترنت اشیا کشف شود. متدهای یادگیری ماشین یا یادگیری عمیق در امنیت اینترنت اشیا تأثیر قابل توجهی بر کیفیت داده و دسترسی به آموزش دارند. بنابراین، تمیزکردن و پیش‌پردازش داده‌های مختلف امنیتی تولیدشده در محیط اینترنت اشیا کاری چالش‌برانگیز است. برای استفاده کارآمد از الگوریتم‌های یادگیری در حوزه امنیت اینترنت اشیا، بهبود روش‌های فعلی یا توسعه روش‌های جدید آماده‌سازی داده مورد انتظار است.

- برای یک راه‌حل امنیتی اینترنت اشیا موثر باید محدودیت‌ها یا قابلیت‌های دستگاه‌ها و سیستم‌های اینترنت اشیا که مدل‌های امنیتی مبتنی بر یادگیری استفاده می‌شود، در نظر گرفته شود. بنابراین، لازم است که یک توازن میان امنیت و قابلیت‌های دستگاه‌ها در زمینه ذخیره‌سازی داده، محاسبه، پردازش داده، تصمیم‌گیری، و منابع ارتباطی وجود داشته باشد. بنابراین، یک بررسی عمیق برای کشف مهمترین روش‌های یادگیری ماشین یا یادگیری عمیق مورد نیاز است.

- توجه به این نکته مهم است که انتخاب تکنیک اغلب به ویژگی های مجموعه داده و مبادله مطلوب بین دقت و پیچیدگی محاسباتی بستگی دارد. به دلیل تعداد زیاد فرایندهای تکراری، تکنیک‌های یادگیری کلاسیک به صورت مستقیم برای دستگاه‌های اینترنت اشیا در شرایط مختلف قابل اجرا نیست. به عنوان مثال، روش یادگیری قانون انجمن، در یک سیستم مبتنی بر قواعد، ممکن است تولید مجدد زائد از داده‌های امنیتی اینترنت اشیا را استخراج کند که فرایند تصمیم‌گیری را پیچیده و ناکارآمد می‌کند. بنابراین، نیاز به درک بهتر از مزایا و محدودیت‌های روش‌های یادگیری موجود وجود دارد، که باعث به وجود آمدن روش‌های بهبود یافته جدید یا توسعه روش‌های جدید یادگیری می‌شود.

- علیرغم پیشرفت قابل توجهی که در تکنیک های تشخیص مبتنی بر یادگیری ماشین به دست آمده است، اذعان به چالش های مداوم در این حوزه مهم است. ماهیت پویا محیط‌های اینترنت اشیا، پیچیدگی روزافزون حملات و مسائل امنیتی و محدودیت‌های منابع دستگاه‌های اینترنت اشیا همچنان موانعی را برای دستیابی به تشخیص دقیق و بلادرنگ ایجاد می‌کنند.

- با توجه به پیشرفت هایی که در بدافزارها و حملات رخ می دهد، یک روند رفتاری جدید و کارا برای پیش‌بینی یا شناسایی حملات در امنیت اینترنت اشیا مورد نیاز است. بنابراین، به جای مدنظر گرفتن تحلیل داده‌های سنتی، ایده تحلیل داده های اخیر، یعنی بینش یا دانش استخراج‌شده بر اساس الگوهای فعلی ممکن است در موارد مختلف مناسب‌تر باشد. بنابراین، یک چالش دشوار دیگر، پیشنهاد راه‌حل‌های سبک‌وزن جدید برای دستگاه‌های اینترنت اشیا است که الگوهای داده فعلی را در نظر بگیرند و در نهایت یک مدل امنیتی اینترنت اشیا بر پایه داده های جدید بسازند.

-با توجه به مزایایی که هر کدام از روشها دارند، ترکیب روشها و ارائه راه حلها و روشهای ترکیبی و قوی‌تر برای افزایش امنیت در اینترنت اشیا پیشنهاد می شود.

از آنجایی که محققان و متخصصان به کشف رویکردها و استراتژی‌های نوآورانه یادگیری ماشین ادامه می‌دهند، پرداختن به این چالش‌ها برای افزایش بیشتر امنیت و انعطاف‌پذیری سیستم‌های اینترنت اشیا ضروری است. تحقیقات آینده باید بر روی توسعه مدل‌های یادگیری ماشین تطبیقی و مقیاس‌پذیر تمرکز کند که می‌تواند به طور موثر موضوعات امنیتی در حال تکامل را شناسایی و کاهش دهد و در عین حال محدودیت‌های منابع دستگاه‌های اینترنت اشیا را در نظر بگیرد. علاوه بر این، تلاش‌های مشترک بین محققان، متخصصان صنعت و سیاست‌گذاران برای ایجاد چارچوب‌های ارزیابی استاندارد، اشتراک‌گذاری مجموعه داده‌های معیار، و ترویج اتخاذ راه‌حل‌های موثر تشخیص مبتنی بر یادگیری ماشین در استقرار اینترنت اشیا در دنیای واقعی مورد نیاز است.

تکنیک‌های تشخیص مبتنی بر یادگیری ماشین و یادگیری عمیق برای افزایش امنیت و انعطاف‌پذیری اکوسیستم‌های اینترنت اشیا با افزایش تعداد دستگاه‌های اینترنت اشیا ضروری هستند. این روش‌ها در حل مسائل امنیتی مؤثر هستند، زیرا تشخیص تهدید، شناسایی ناهنجاری‌ها و تشخیص الگو را بطور بلادرنگ ارائه می‌دهند. انعطاف پذیری آنها اثربخشی مداوم در برابر تهدیدات جدید را تضمین می کند و کاهش مثبت کاذب از استفاده قانونی از دستگاه محافظت می کند. علاوه بر این، آنها مسائل مربوط به حریم خصوصی را حل می کنند و به راحتی متناسب با سناریوی توسعه اینترنت اشیا مقیاس می شوند. راه‌حل‌های امنیتی مبتنی بر یادگیری ماشین نقشی کلیدی در تضمین امنیت و طول عمر دستگاه‌های اینترنت اشیا با ارائه روشهای نگهداری پیش‌بینی‌شده، قابلیت همکاری و اطمینان کاربر دارند. برای پیشگیری از تهدیدهای امنیتی جدید، تحقیق و توسعه مداوم ضروری است.

4. جمع بندی و نتیجه گیری

در حال حاضر، اینترنت اشیا در صنایع مختلف، استفاده می شود و توسعه راه‌حل‌های جدید را امکان‌پذیر می‌کند. تلاش‌های متعددی برای استفاده از این فناوری در حوزه های مختلف صورت گرفته و انتظار می‌رود راه‌حل‌های جدید تا چند سال آینده سیستم‌های موجود را بهبود بخشند. تکنیک‌های یادگیری ماشین و یادگیری عمیق با دقت بهبود یافته می‌توانند حجم زیادی از داده‌ها را تجزیه و تحلیل کنند و الگوها و ناهنجاری‌هایی را که ممکن است توسط تکنیک‌های سنتی نادیده

گرفته شوند، شناسایی کنند، که در نتیجه باعث بهبود دقت و افزایش کارایی آنها در افزایش امنیت اینترنت اشیا می شود. این تکنیک‌ها مزایای قابل‌توجهی را برای شناسایی و پیشگیری از حملات اینترنت اشیا ارائه می‌دهند و امکان شناسایی و پاسخ سریع‌تر، دقیق‌تر و کارآمدتر به تهدیدات امنیتی را فراهم می‌کنند. این تحقیق یک مرور اجمالی و بررسی از راه‌حل‌های یادگیری ماشین برای امنیت اینترنت اشیا ارائه کرد. تمرکز اصلی بر روشها، منابع، برنامه‌ها، و چالش‌های باز در این زمینه بود. در نهایت، چالش های موجود بیان گردید و جهت های آینده تحقیقاتی مشخص شد. بنابرآنچه ذکر شد، کارهای آینده باید به داده های جمع آوری شده از دستگاه های متعدد، حجم داده ها و ویژگی‌های توصیفی متعدد، و حمله‌های مختلف توجه کنند. در طولانی مدت، نیاز به بررسی حملات با توجه به عملکرد الگوریتم ها و ابزارها و امکانات دستگاه های اینترنت اشیا وجود دارد. علاوه بر این، یک تجزیه و تحلیل عمیق در مورد اینکه چگونه پلتفرم‌های آزمایشی واقع‌گرا می‌توانند باعث نمایان‌سازی، تحلیل، یکپارچگی‌های بیشتر، و جمع‌آوری معیارهای عملیاتی شوند، بنیانی برای تحقیقات آینده است.

منابع

[1] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W., "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications.," *IEEE Internet Things J.* , vol. 4, no. 5, p. 1125–1142, 2017.

[2] Alabdulatif, Ali, Thilakarathne, Nalin N., Lawal, Zulkarnain K., Fahim, Kareem E., Zakari, Rabiu Y., "Internet of nano-things (IoNT): A comprehensive review from architecture to security and privacy challenges.," *Sensors* , vol. 23, no. 5, p. 2807, 2023.

[3] Plageras, Andreas P, Psannis, Kostas E, Stergiou, Christos, Wang, Haoxiang, Gupta, Brij B,, "Efficient IoT-based sensor BIG data collection–processing and analysis in smart buildings.," *Future Gener. Comput. Syst.* , vol. 82, p. 349–357, 2018.

[4] Statista Research Department, "Global IoT Security Market Size 2022–2027.," Statista, , Retrieved from https://www.statista.com/statistics/1362333/global-iotsecurity-market-value/., 2023.

[5] Nazir, A., He, J., Zhu, N., Wajahat, A., Ma, X., Ullah, F., ... & Pathan, M. S. , "Advancing IoT security: A systematic review of machine learning approaches for the detection of IoT botnets.," *Journal of King Saud University-Computer and Information Sciences*, 2023.

[6] Almazrouei, Essa, Shubair, Raed M., Saffre, Fabrice,, "Internet of nanothings: Concepts and applications," *arXiv preprint arXiv:1809.08914.*, 2018.

[7] Maksimović, Milica,, "The roles of nanotechnology and internet of nano things in healthcare transformation.," *Tecnológicas* , vol. 20, no. 40, p. 139–153., 2017.

[8] Miraz, Mahdi H., Ali, Md S., Excell, Peter S., Picking, Richard,, "Internet of nano-things, things and everything: future growth trends.," *Future Internet* , vol. 10, no. 8, p. 68, 2018.

[9] Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F., "Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. ," *Mobile Networks and Applications*, vol. 28, no. 1, pp. 296-312, 2023.

[10] Zafar, Saad, Nazir, Muhammad, Sabah, Ali, Jurcut, Anca Daniela,, "Securing biocyber interface for the internet of bio-nano things using particle swarm optimization and artificial neural networks-based parameter profiling.," *Comput. Biol. Med.* , vol. 136, 2021.

[11] Memos, Vasileios A, Psannis, Kostas E, Ishibashi, Yutaka, Kim, Byung-Gyu, Gupta, Brij B,, "An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city

framework.," *Future Gener. Comput. Syst.* , vol. 83, p. 619–628, 2018.

[12] Zheng, Shijun, Yang, Xiaowei,, "Dynashield: Reducing the cost of DDoS defense using cloud services.," *In: Proceedings of the 11th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 19). USENIX, Boston, MA, USA,* 2019.

[13] Syeda Manjia Tahsien, Hadis Karimipour, and Petros Spachos., " Machine learning based solutions for security of internet of things (iot): A survey.," *Journal of Network and Computer Applications,* vol. 161, 2020.

[14] Hu, Jui-Wen, Yeh, Li-Yuan, Liao, Shih-Wei, Yang, Chia-Shiang,, "Autonomous and malware-proof blockchain-based firmware update platform with efficient batch verification for Internet of Things devices.," *Comput. Secur.* , vol. 86, p. 238–252, 2019.

[15] Iqbal H Sarker, Md Hasan Furhad, and Raza Nowrozy, "Ai-driven cybersecurity: an overview, security intelligence modeling and research directions.," *SN Computer Science,* vol. 2, no. 3, 2021.

[16] Mao, Jiaxin, Bian, Jiang, Tian, Wei, Zhu, Shuyuan, Wei, Tingting, Li, An, Liang, Zhong,, "Phishing page detection via learning classifiers from page layout feature.," *EURASIP J. Wireless Commun. Networking* , vol. 1, pp. 1-14, 2019.

[17] I. H. Sarker., " Deep learning: A comprehensive overview on techniques, taxonomy, applications and research directions.," *SN Computer Science,* 2021.

[18] Sumeet Dua and Xian Du. , "Data mining and machine learning in cybersecurity.," *CRC press,* 2016.

[19] David W Aha, Dennis Kibler, and Marc K Albert., "Instance-based learning algorithms.," *Machine learning,* vol. 6, no. 1, pp. 37-66, 1991.

[20] Leevy, Jennifer L., Khoshgoftaar, Taghi M., Hancock, Jeffrey,, "Feature evaluation for IoT botnet traffic classification.," *Int. J. Internet Things Cyber-Assur.* , vol. 2, no. 1, pp. 87-102, 2022.

[21] Ferreira, A. J., & Figueiredo, M. A. , "Boosting algorithms: A review of methods, theory, and applications.," *Ensemble machine learning: Methods and applications,* pp. 35-85, 2012.

[22] Charbuty, B., & Abdulazeez, A., "Classification based on decision tree algorithm for machine learning.," *Journal of Applied Science and Technology Trends,* vol. 2, no. 1, pp. 20-28, 2021.

[23] Sun, Z., Wang, G., Li, P., Wang, H., Zhang, M., & Liang, X. , "An improved random forest based on the classification accuracy and correlation measurement of decision trees.," *Expert Systems with Applications,* vol. 237, 2024.

[24] Soo-Yeon Lee, Sa-rang Wi, Eunil Seo, Jun-Kwon Jung, and Tai-Myoung Chung., "Profiot: Abnormal behavior profiling (abp) of iot devices based on a machine learning approach.," *In 2017 27th International Telecommunication Networks and Applications Conference,* 2017.

[25] Hyo-Sik Ham, Hwan-Hee Kim, Myung-Sup Kim, and Mi-Jung Choi. , "Linear svm-based android malware detection for reliable iot services.," *Journal of Applied Mathematics,* 2014.

[26] Biswas, P., & Samanta, T. , "Anomaly detection using ensemble random forest in wireless sensor network.," *International Journal of Information Technology,* vol. 13, no. 5, pp. 2043-2052, 2021.

[27] Najar, A. A., & Manohar Naik, S. , "DDoS attack detection using MLP and Random Forest Algorithms.," *International Journal of Information Technology,* vol. 14, no. 5, pp. 2317-2327, 2022.

[28] Pramilarani, K., & Kumari, P. V., "Cost based Random Forest Classifier for Intrusion Detection System in Internet of Things.," *Applied Soft Computing*, 2023.

[29] Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. , "Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning.," *In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference* , 2019.

[30] Venkatesh Jaganathan, Priyesh Cherurveettil, and Premapriya Muthu Sivashanmugam., " Using a prediction model to manage cyber security threats.," *The Scientific World Journal*, 2015.

[31] Iqbal H Sarker, ASM Kayes, Shahriar Badsha, Hamed Alqahtani, Paul Watters, and Alex Ng. , "Cybersecurity data science: an overview from machine learning perspective," .*Journal of Big Data*, vol. 7, no. 1, pp. 1-29, 2020.

[32] Ian H Witten, Eibe Frank, Leonard E Trigg, Mark A Hall, Geo_rey Holmes, and Sally Jo Cunningham. , "Weka: Practical machine learning tools and techniques with java implementations.," 1999.

[33] Lalou, M., Kheddouci, H., & Hariri, S. , "Identifying the cyber attack origin with partial observation: a linear regression based approach.," *In 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W)* , 2017.

[34] Desta Haileselassie Hagos, Anis Yazidi, _ivind Kure, and Paal E Engelstad. , "Enhancing security attacks analysis using regularized machine learning techniques.," *In 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (A*, 2017.

[35] Gatea, M. J., & Hameed, S. M., "An Internet of Things Botnet Detection Model Using Regression Analysis and Linear Discrimination Analysis," *Iraqi Journal of Science*, pp. 4534-4546, 2022.

[36] Ezugwu, A. E., Ikotun, A. M., Oyelade, O. O., Abualigah, L., Agushaka, J. O., Eke, C. I., & Akinyelu, A. A., "A comprehensive survey of clustering algorithms: State-of-the-art machine learning applications, taxonomy, challenges, and future research," *Engineering Applications of Artificial Intelligence*, vol. 110, 2022.

[37] N. Wiroonsri, "Clustering performance analysis using a new correlation-based cluster validity index. ," *Pattern Recognition*, vol. 145, 2024.

[38] Lenssen, L., & Schubert, E. , "Medoid Silhouette clustering with automatic cluster number selection.," *Information Systems*, vol. 120, 2024.

[39] Garg, S., Kaur, K., Batra, S., Kaddoum, G., Kumar, N., & Boukerche, A., " A multi-stage anomaly detection scheme for augmenting the security in IoT-enabled applications. ," *Future Generation Computer Systems*, vol. 104, pp. 105-118, 2020.

[40] I. H. Sarker, "A machine learning based robust prediction model for real-life mobile phone data.," *Internet of Things*, vol. 5, pp. 180-193, 2019.

[41] Liqun Liu, Bing Xu, Xiaoping Zhang, and Xianjun Wu., " An intrusion detection method for internet of things based on suppressed fuzzy clustering.," *EURASIP Journal on Wireless Communications and Networking*, vol. 1, no. 113, 2018.

[42] I. H. Sarker., " Data science and analytics: An overview from data-driven smart computing, decision-making and applications perspective.," *SN Computer Science*, 2021.

[43] Arora, P., Saxena, S., & Chopra, D., " Generalized association rules for er models by using mining operations on fuzzy datasets. ," *Recent Progress in Science and Technology,*, vol. 6, 2023.

[44] Soni, H. K., Sharma, S., & Jain, M. , "Frequent pattern generation algorithms for Association Rule Mining: Strength and challenges.," *In 2016 International conference on electrical, electronics, and optimization techniques (ICEEOT)* , 2016.

[45] Lajoie, S. P., & Poitras, E., "Technology-Rich Learning Environments: Theories and Methodologies for Understanding Solo and Group Learning. ," *In Handbook of educational psychology (pp. 630-653). Routledge.*, 2024.

[46] Lu, Y., & Sarmiento, E., "Apriori Optimization Model for the Intervention Strategies in Educational Model with Sentimental-Based Learning Analytics.," *International Journal of Intelligent Systems and Applications in Engineering*, , vol. 12, no. 6, pp. 466-480., 2024.

[47] Jiawei Han, Jian Pei, and Yiwen Yin. , "Mining frequent patterns without candidate generation.," *In ACM Sigmod Record*, vol. 29, pp. 1-12, 2000.

[48] Mayank Swarnkar and Neminath Hubballi., " Ocpad: One class naive bayes classi_er for payload based anomaly detection.," *Expert Systems with Applications*, vol. 64, pp. 330-339, 2016.

[49] Arman Tajbakhsh, Mohammad Rahmati, and Abdolreza Mirzaei., " Intrusion detection using fuzzy association rules.," *Applied Soft Computing*, vol. 9, no. 2, pp. 462-469, 2009.

[50] Seiichi Ozawa, Tao Ban, Naoki Hashimoto, Junji Nakazato, and Jumpei Shimamura. , "A study of iot malware activities using association rule learning for darknet sensor data.," *International Journal of Information Security*, vol. 19, no. 1, pp. 83-92, 2020.

[51] Iqbal H Sarker and ASM Kayes, "Abc-ruleminer: User behavioral rule-based machine learning method for context-aware intelligent services.," *Journal of Network and Computer Applications*, vol. 168, 2020.

[52] Bhalodia, R., Elhabian, S., Adams, J., Tao, W., Kavan, L., & Whitaker, R. , "DeepSSM: A blueprint for image-to-shape deep learning models. ," *Medical Image Analysis, 91, 103034.*, vol. 91, 2024.

[53] Shewale, Y., Kumar, S., & Banait, S., "Machine Learning Based Intrusion Detection in IoT Network Using MLP and LSTM.," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 7, pp. 210-223., 2023.

[54] ElMouatez Billah Karbab, Mourad Debbabi, Abdelouahid Derhab, and Djedjiga Mouheb., " Maldozer: Automatic framework for android malware detection using deep learning.," *Digital Investigation, 24:S48{S59, 2018.*, vol. 24, pp. 548-S59, 2018.

[55] Kornyo, O., Asante, M., Opoku, R., Owusu-Agyemang, K., Tei-Partey, B., Baah, E. K., & Boadu, N., "Botnet Attacks Classification in AMI Networks with Recursive Feature Elimination (RFE) and Machine Learning Algorithms. ," *Computers & Security*, 2023.

[56] Bambang Susilo and Riri Fitri Sari., "Intrusion detection in iot networks using deep learning algorithm.," *Information*, vol. 11, no. 5, 2020.

[57] Khan, S. H., Alahmadi, T. J., Ullah, W., Iqbal, J., Rahim, A., Alkahtani, H. K., ... & Almagrabi, A. O., " A new deep boosted CNN and ensemble learning based IoT malware detection.," *Computers & Security*, vol. 133, 2023.

[58] Yuan, Z., Lu, Y., Wang, Z., & Xue, Y., "Droid-sec: deep learning in android malware detection.," *In Proceedings of the 2014 ACM conference on SIGCOMM*, 2024.

[59] Jeon, J., Jeong, B., Baek, S., & Jeong, Y. S., "Hybrid malware detection based on bi-lstm and spp-net for smart iot. ," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, pp. 4830-

4837, 2021.

[60] Balakrishnan, N., Rajendran, A., Pelusi, D., & Ponnusamy, V., "Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things.," *Internet of things,* vol. 14, 2021.

[61] George H John and Pat Langley., " Estimating continuous distributions in bayesian classifiers.," *In Proceedings of the Eleventh conference on Uncertainty in artificial intelligence,*, pp. 338-345. , 1995.

[62] S. Sathiya Keerthi, Shirish Krishnaj Shevade, Chiranjib Bhattacharyya, and Karuturi Radha Krishna Murthy., "Improvements to platt's smo algorithm for svm classifier design.," *Neural computation,* vol. 13, no. 3, pp. 637-649, 2001.

[63] Mayank Swarnkar and Neminath Hubballi. , "Ocpad: One class naive bayes classifier for payload based anomaly detection.," *Expert Systems with Applications,* vol. 64, pp. 330-339, 2016.