Scientific Journal of Electronical & Cyber Defence
Vol. 11, No. 2, Summer 2023, Serial No. 42

Identify malicious traffic on IoT infrastructure using neural networks and deep learning

H. Tanha, M. Abbasi*
*Assistant Professor, Imam Hossein University (AS), Tehran, Iran
(Received: 27/11/2021, Accepted: 05/02/2023)

ABSTRACT

The Internet of Things is a network of physical devices and equipment that includes sensors, software, and other technologies for exchanging data with other devices and systems over the Internet. The spread of the Internet of Things in the fields of smart health, smart agriculture, smart city, smart home, has revolutionized human life. Given the importance of the Internet of Things, identifying anomalies and malicious traffic is essential to maintaining privacy, network stability, and blocking unwanted behaviors. Due to the limited resources on IoT devices, traditional methods cannot be used directly to secure IoT devices and networks. To solve this problem, an artificial neural network-based identification method and in-depth learning has been developed to identify malformations and malicious traffic about which there is no predefined information. The data set used in this method is a combination of malicious and healthy traffic collected from related sources and feature extraction manually. Deep artificial neural network was applied to the data set and preprocessed and the results were analyzed with some conventional machine learning algorithms. The results show that the model designed using neural network and deep learning is able to detect anomalies and malicious traffic in the Internet of Things with an accuracy rate of more than 98.9% and an accuracy rate of 99.3%. In addition, the detection speed is 1.7 times faster than machine learning algorithms.

Keywords: IoT, malware, network traffic, feature extraction, artificial neural network, deep learning.

*Corresponding Author Email: Moabbasi@ihu.ac.ir

This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

Publisher: Imam Hussein University © Authors

نشریه علمی "پدافند الکترونیکی و سایبری"
سال یازدهم، شماره ۲، تابستان ۱۴۰۲، ص۱-۱۳

علمی – پژوهشی

شناسایی ترافیک بدخواه در زیرساخت اینترنت اشیاء با استفاده از شبکه عصبی و یادگیری عمیق

حمید تنها[۱]، مصطفی عباسی[۲*]

۱- کارشناسی ارشد، ۲- استادیار، دانشگاه جامع امام حسین (ع)، تهران، ایران

(دریافت: ۱۴۰۰/۰۹/۰۶، پذیرش: ۱۴۰۱/۱۱/۱۶)

چکیده

اینترنت اشیاء شبکه‌ای از دستگاه‌ها و تجهیزات فیزیکی دربردارنده حسگرها، نرم‌افزارها و سایر فناوری‌ها به‌منظور تبادل داده با سایر دستگاه‌ها و سامانه‌ها از طریق اینترنت است. گسترش اینترنت اشیاء در حوزه‌های بهداشت و درمان هوشمند، کشاورزی هوشمند، شهر هوشمند، خانه هوشمند و سایر حوزه‌ها انقلابی در زندگی بشر ایجاد کرده است. با توجه به اهمیت اینترنت اشیاء شناسایی ناهنجاری و ترافیک مخرب در آن برای حفظ حریم خصوصی، پایداری شبکه و مسدودسازی رفتارهای ناخواسته ضروری است. به دلیل خاصیت محدودیت منابع در دستگاه‌های اینترنت اشیاء، شیوه‌های سنتی نمی‌توانند مستقیماً برای ایمن‌سازی دستگاه‌ها و شبکه اینترنت اشیاء مورداستفاده قرار گیرند. برای رفع این مشکل یک روش شناسایی مبتنی بر شبکه‌های عصبی مصنوعی و یادگیری عمیق برای شناسایی ناهنجاری و ترافیک مخربی که هیچ‌گونه اطلاعات از پیش تعیین‌شده‌ای درباره آن‌ها وجود ندارد، توسعه داده شده است. مجموعه داده‌های مورداستفاده در این روش ترکیبی از ترافیک مخرب و سالم جمع‌آوری‌شده از منابع مرتبط و استخراج ویژگی به‌صورت دستی است. شبکه عصبی مصنوعی عمیق بر روی مجموعه داده و پیش‌پردازش شده اعمال گردید و نتایج حاصل با برخی از الگوریتم‌های یادگیری ماشین مرسوم مورد بررسی قرار گرفت. نتایج به‌دست‌آمده نشان می‌دهد که مدل طراحی‌شده با استفاده از شبکه عصبی و یادگیری عمیق قادر به شناسایی ناهنجاری و ترافیک بدخواه در شبکه اینترنت اشیاء با نرخ صحت بیش از ۹۸,۹٪ و نرخ دقت ۹۹,۳٪ است. علاوه بر این، سرعت شناسایی در مقایسه با الگوریتم‌های یادگیری ماشین ۱,۷ برابر سریع‌تر است.

کلیدواژه‌ها: اینترنت اشیاء، بدافزار، ترافیک شبکه، استخراج ویژگی، شبکه عصبی مصنوعی، یادگیری عمیق

۱- مقدمه

اینترنت اشیاء سیستم به‌هم‌پیوسته‌ای از دستگاه‌ها، تجهیزات فیزیکی، رایانه‌ها و غیره است که با شناسه منحصربه‌فرد[۱] از یکدیگر متمایز می‌شوند و با استفاده از زیرساخت اینترنت از قابلیت انتقال داده بهره‌مند هستند. شمای کلی زیرساخت اینترنت اشیاء در شکل (۱) نشان داده شده است. در حال حاضر فناوری و گستره اینترنت اشیاء روزبه‌روز در حال گسترش است [۱] و در هر ساعت دستگاه‌های بیش‌تری به آن اضافه می‌شود. بر اساس پیش‌بینی‌های صورت‌گرفته تا سال ۲۰۲۵ بیش از ۴۱ میلیارد دستگاه اینترنت اشیاء وجود خواهد داشت، این در حالی است که این رقم در سال ۲۰۱۹ حدود ۸ میلیارد بوده است [۲], [۳].

بر اساس گزارش شرکت امنیتی کسپرسکی در نیمه اول سال ۲۰۱۹ بیش از ۱۰۰ میلیون حمله به دستگاه‌های اینترنت اشیاء صورت‌گرفته است که ۷ برابر بیش‌تر از نیمه نخست سال ۲۰۱۸ است [۴]. حمله به دستگاه‌های اینترنت اشیاء شامل ۴ دسته حمله فیزیکی، حمله به شبکه، حمله به نرم‌افزار و حمله به رمزنگاری است؛ [۵] که عمدتاً از نوع حمله به نرم‌افزار و حمله به شبکه است. بدافزار میرای[۲] نمونه‌ای از یک حمله گسترده به تجهیزات اینترنت اشیاء است که در سال ۲۰۱۶ بیش از ۱ میلیون دستگاه را آلوده کرد. به دلیل وجود نقایص امنیتی در دستگاه‌های اینترنت اشیاء، این دستگاه‌ها به‌عنوان یک هدف جذاب برای مهاجمین سایبری شناخته می‌شوند. این دستگاه‌ها اغلب باهدف کاهش هزینه‌ها بدون ملاحظات جدی امنیتی تولید می‌شوند و این باعث می‌شود تا در برابر حملات بسیار آسیب‌پذیر باشند؛ در بسیاری از موارد حتی نام کاربری و گذرواژه پیش‌فرض دستگاه‌های اینترنت اشیاء تغییر داده نمی‌شود. علاوه بر این، به‌روزرسانی‌های ارائه‌شده از سوی تولیدکنندگان دستگاه‌های اینترنت اشیاء بر روی دستگاه‌های مذکور اعمال نمی‌گردد که به‌نوبه خود منجر به ایجاد نقایص امنیتی جدی‌تری می‌گردد. در سال‌های اخیر تحقیقات زیادی برای شناسایی و مقابله با حملات مرتبط با دستگاه‌ها و شبکه اینترنت اشیاء صورت‌گرفته است اما حملات به دستگاه‌ها و شبکه‌های اینترنت اشیاء نیز به همان اندازه پیچیده و کارآمدتر شده‌اند.

* رایانامه نویسنده مسئول: Moabbasi@ihu.ac.ir

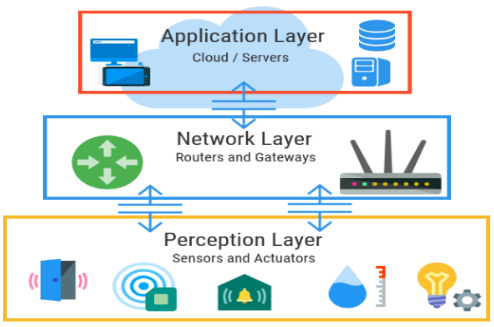
[1] Unique Identifier

[2] Mirai

* این مقاله یک مقاله با دسترسی آزاد است که تحت شرایط و ضوابط مجوز Creative Commons Attribution (CC BY) توزیع شده است.

ناشر: دانشگاه جامع امام حسین (ع)

© نویسندگان



شکل (۱): معماری کلی اینترنت اشیاء

مهاجمین در فازهای مختلف شناسایی، آلوده‌سازی، ماندگاری، عملیات و ماندگاری [۶]، نیازمند تعامل با دستگاه و شبکه‌های اینترنت اشیاء از طریق اینترنت و پروتکل‌های شبکه می‌باشند؛ لذا بررسی و پویش ترافیک شبکه اینترنت اشیاء می‌تواند در شناسایی حملات و دستگاه‌ها و شبکه‌های به خطر افتاده، کمک کند [۷]. اگرچه مبهم سازی ترافیک شبکه توسط مهاجمین می‌تواند در فرایند شناسایی حملات توسط متخصصین امنیتی اختلالاتی ایجاد کند اما بررسی‌های عمیق‌تر در ساختار و ماهیت بخش‌های مختلف ترافیک شبکه می‌تواند منجر به افزایش دقت و صحت در شناسایی گردد.

تحقیقات بسیاری باهدف شناسایی حملات به زیرساخت‌های اینترنت اشیاء به‌خصوص حملات مبتنی بر بدافزار با استفاده از تحلیل ترافیک شبکه اینترنت اشیاء صورت‌گرفته است. عباد حفیض [۸] و همکاران از یک روش ترکیبی خوشه‌بندی *c-means* فازی و طرح الحاق فازی برای تجزیه‌وتحلیل ترافیک شبکه و شناسایی ترافیک مخرب استفاده می‌کنند. آرونان سیوانتان [۹] با بهره‌برداری از الگوهای سیگنالینگ و به کمک ویژگی‌هایی نظیر چرخه فعالیت در ترافیک شبکه سعی در ایجاد یک موتور استنتاج مبتنی بر یادگیری ماشین دارد. آیوش کومار و تنگ جو لیم [۱۰] با تمرکز بر روی بدافزار میرای شیوه‌ای جهت شناسایی بدافزارهای اسکن‌کننده در زیرساخت اینترنت اشیاء مبتنی بر امضاهای منحصربه‌فرد ارائه کرده‌اند. بینگلای وانگ و همکاران [۱۱] بر اساس وجود ضعف‌های اعتبارسنجی در برخی از سرویس‌ها همانند *SSH* و *Telnet* و امکان تزریق دستور به آن‌ها، یک چارچوب ترکیبی ظرف عسل برای ضبط نمونه‌های مخرب در زیرساخت‌های اینترنت اشیاء پیشنهاد داده است.

علی‌رغم تلاش‌های صورت‌گرفته در زمینه شناسایی و مقابله با حملات مرتبط با دستگاه‌ها و شبکه اینترنت اشیاء همچنان این دسته از مخاطرات امنیتی در حال گسترش روزافزون است. یکی از دلایل این امر عدم توانایی پوشش روش‌های شناسایی موجود و تعداد و حجم حملات جدید و ناشناس است. یک روش شناسایی کارآمد می‌بایست قابلیت تطابق با شرایط پویا جهت شناسایی حملات روز صفر و از پیش مشاهده نشده را داشته باشد.

در این مقاله شیوه جدیدی جهت شناسایی حملات به زیرساخت‌های اینترنت اشیاء با استفاده از شبکه عصبی مصنوعی و یادگیری عمیق و مبتنی بر تحلیل ترافیک شبکه ارائه گردیده است. روش پیشنهادی کاملاً منطبق بر محدودیت منابع در دستگاه‌های اینترنت اشیاء است. استفاده از شبکه عصبی مصنوعی و یادگیری عمیق مزایای زیادی ازلحاظ دقت پیش‌بینی نسبت به شیوه‌های سنتی دارد و موجب می‌گردد فرایند طبقه‌بندی بر روی داده‌های حجیم و پیچیده بدون نیاز به اعمال مهندسی ویژگی، صورت پذیرد. حذف فرایند مهندسی ویژگی و به دنبال آن، حذف عامل انسانی از آن، می‌تواند شیوه‌های دفاعی شناسایی را به طرق مختلف توسط توسعه‌دهندگان حملات سایبری علیه زیرساخت‌های اینترنت اشیاء مورداستفاده قرار می‌گیرد را کم‌اثر نماید. ازجمله این طرق می‌توان به ایجاد ترافیک شبکه سالم و خوش‌خیم در بین ترافیک اصلی و بدخواهانه اشاره کرد. مدل‌های یادگیری توسعه داده شده به روش یادگیری عمیق قادر به شناسایی و نادیده‌گرفتن داده‌های غیرمؤثر و وزن‌دهی مناسب به داده‌های مرتبط با خروجی نهایی می‌باشند.

در بخش ۲ مقاله، دانش پس‌زمینه در خصوص شبکه عصبی مصنوعی و یادگیری عمیق و پژوهش‌های مرتبط با تحلیل ترافیک و شناسایی ترافیک بدخواه در زیرساخت اینترنت اشیاء ارائه گردیده است. در بخش ۳، روش پیشنهادی شامل شیوه فیلترگذاری و استخراج ویژگی و مدل شبکه عصبی عمیق طراحی‌شده بیان شده است. در بخش ۴، نتایج و اعتبارسنجی روش پیشنهادی، بررسی شده است. در بخش ۵ به نتیجه‌گیری و کارهای آینده اختصاص‌یافته است.

۲- ادبیات موضوع و پیشینه تحقیق

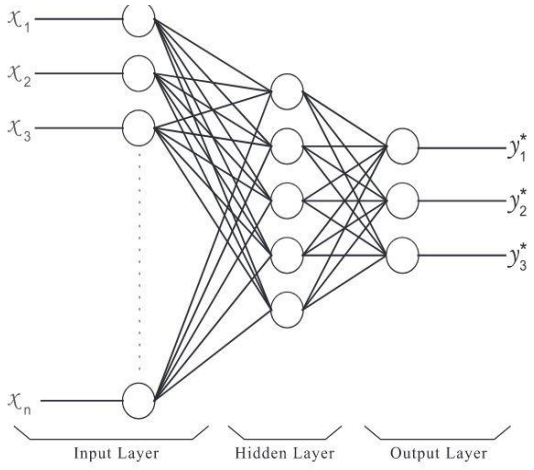
با توجه به موضوع مقاله، در این بخش مروری بر ادبیات موضوع شامل شبکه عصبی مصنوعی، یادگیری عمیق و شبکه عصبی کانوشنال و کارهای مرتبط انجام می‌گیرد.

۲-۱- شبکه عصبی مصنوعی

در حال حاضر شبکه‌های عصبی مصنوعی به یک مدل محبوب و مفید برای طبقه‌بندی، خوشه‌بندی، تشخیص الگو و پیش‌بینی در بسیاری از رشته‌های علمی تبدیل شده است. شبکه عصبی مصنوعی مدل جدیدی برای یادگیری ماشین با هدف پیش‌بینی پاسخ‌های خروجی از سامانه‌های پیچیده است. ایده اصلی این ساختار از سازوکار سیستم عصبی زیستی جهت پردازش داده‌ها

الهام گرفته شده است و نسبت به مدل‌های آماری و رگرسیون مرسوم برتری قابل‌ملاحظه‌ای دارند [۱۲].

انواع مختلفی از مدل‌های محاسباتی تحت عنوان شبکه عصبی مصنوعی توسعه داده شده است که هر یک پاسخگوی بخشی از فضای حالت مسائل و کاربردها است. تمامی مدل‌های محاسباتی پیشنهادشده دارای یک مدل ریاضی، مجموعه از پارامترها و عناصر تنظیم‌پذیر می‌باشند. بهینه‌سازی ساختار توسط الگوریتم یادگیری در انواع شبکه‌های عصبی موجب بروز رفتار مناسب توسط مدل محاسباتی می‌گردد [۱۳]. شبکه‌های عصبی مصنوعی شامل پرسپترون چندلایه، ماشین بردار پشتیبان، شبکه‌های عصبی شعاعی، نگاشت‌های خودسازمان‌ده، یادگیرنده رقمی‌ساز بردار و شبکه عصبی هاپفیلد است [۱۴].



شکل (۲): ساختار مدل شبکه عصبی پرسپترون چندلایه [۱۵]

شبکه عصبی پرسپترون چندلایه به دلیل عملکرد سریع، سهولت پیاده‌سازی و نیاز به داده‌های آموزشی کوچک‌تر متداول‌ترین نوع شبکه عصبی است. همان‌طور که در شکل (۱) نشان داده شده است، این دسته از شبکه‌های محلی از سه لایه متوالی تشکیل شده است: لایه ورودی، مخفی و خروجی. لایه مخفی اطلاعات ورودی را پردازش کرده و به لایه خروجی منتقل می‌کند. یک مدل شبکه عصبی پرسپترون با تعداد ناکافی یا بیش از اندازه تعداد نورون‌ها در لایه مخفی موجب بروز مشکلاتی نظیر تعمیم بد و بیش برازش می‌گردد [۱۶]. در روش پیشنهادی از شبکه عصبی پرسپترون چندلایه استفاده‌شده است.

۲-۲- یادگیری عمیق

روش‌های سنتی یادگیری ماشین به‌صورت گسترده‌ای به انتخاب ویژگی‌ها به‌صورت دستی وابسته می‌باشند، به این معنی که متخصص انسانی مرتبط با دامنه موضوع می‌بایست بر اساس دانش قبلی ویژگی‌های موجود در مسئله را که فرایندی چالش‌برانگیز و زمان‌بر است را شناسایی و استخراج کند.

یادگیری عمیق حوزه جدیدی در داده‌کاوی و یادگیری ماشین است که به‌صورت گسترده‌ای در تحقیقات صنعتی و دانشگاهی مورداستفاده قرار می‌گیرد. یک معماری یادگیری عمیق چندلایه از قابلیت برتری در یادگیری ویژگی برخوردار است. از همه مهم‌تر، یادگیری عمیق با پیش آموزش لایه‌ای، به معنی پیش آموزش لایه‌های متعدد آشکارسازهای ویژگی از پایین‌ترین سطح تا بالاترین سطح برای ساخت مدل طبقه‌بندی نهایی، بر دشواری‌های یادگیری غلبه می‌کند [۱۷]. در این روش مفاهیم پیچیده به مفاهیم ساده‌تری تقسیم می‌شوند و ادامه این روند به مفاهیم پایه‌ای ختم می‌شوند که قادر به تصمیم‌گیری می‌باشند. درنتیجه‌ی این فرایند نیازی به مهندسی ویژگی توسط عامل انسانی نخواهد بود.

یادگیری عمیق با نوع داده‌ای که با آن کار می‌کند و روش‌هایی که در آن یاد می‌گیرد، خود را از یادگیری ماشین کلاسیک متمایز می‌کند. مدل‌های یادگیری عمیق قادر به انواع مختلف یادگیری است که معمولاً به‌عنوان یادگیری تحت نظارت، یادگیری بدون نظارت و یادگیری تقویتی طبقه‌بندی می‌شوند. یادگیری تحت نظارت از مجموعه داده‌های دارای برچسب برای طبقه‌بندی یا پیش‌بینی استفاده می‌کند. این نیاز به‌نوعی مداخله انسانی برای برچسب‌زدن صحیح داده‌های ورودی دارد. در مقابل، یادگیری بدون نظارت نیازی به مجموعه داده‌های دارای برچسب ندارد و در عوض، الگوهای موجود در داده‌ها را تشخیص می‌دهد و آن‌ها را با هر ویژگی متمایز دسته‌بندی می‌کند. یادگیری تقویتی فرایندی است که در آن یک مدل یاد می‌گیرد که برای انجام یک عمل در یک محیط بر اساس بازخورد دقیق‌تر عمل کند تا پاداش را به حداکثر برساند.

یادگیری عمیق شبکه‌های عصبی یا شبکه‌های عصبی مصنوعی، سعی می‌کند مغز انسان را از طریق ترکیبی از ورودی‌های داده، وزن و بایاس تقلید کند. شبکه های عصبی عمیق از لایه های متعددی از گره‌های به‌هم‌پیوسته تشکیل شده است که هر یک بر اساس لایه قبلی برای اصلاح و بهینه‌سازی پیش‌بینی یا دسته‌بندی ساخته‌شده‌اند. این پیشرفت محاسبات از طریق شبکه را انتشار روبه جلو می نامند. لایه های ورودی و خروجی یک شبکه عصبی عمیق، لایه های قابل مشاهده نامیده می شوند. لایه ورودی جایی است که مدل یادگیری عمیق داده ها را برای پردازش وارد می کند و لایه خروجی جایی است که پیش‌بینی یا طبقه‌بندی نهایی انجام می شود. فرایندی دیگر به نام *backpropagation* از الگوریتم هایی مانند گرادیان نزول برای محاسبه خطاها در پیش‌بینی‌ها استفاده می کند و سپس وزن و بایاس‌های عملکرد را با حرکت به عقب در لایه‌ها در تلاش برای آموزش مدل تنظیم می‌کند. انتشار رو به جلو و انتشار رو به عقب به‌صورت هم‌زمان به یک شبکه عصبی اجازه می‌دهد تا پیش‌بینی‌ها را انجام داده و بر

این اساس هرگونه خطا را تصحیح کند [۱۸]. با گذشت زمان، الگوریتم به‌تدریج دقیق‌تر می‌شود. دو نوع شبکه عصبی پرکاربرد در پیاده‌سازی یادگیری عمیق شامل شبکه عصبی کانولوشن[1] و مکرر[2] وجود دارد که در پژوهش جاری از شبکه عصبی کانولوشن استفاده‌شده است.

۲-۳- شبکه عصبی کانوشنال

در یادگیری عمیق، یک شبکه عصبی کانولوشن، یک کلاس از شبکه عصبی مصنوعی است که بیشتر برای تجزیه‌وتحلیل تصاویر بصری استفاده می‌شود [۱۹]. شبکه کانولوشن همچنین به‌عنوان شبکه عصبی مصنوعی تغییرناپذیر یا تغییرناپذیر فضا (*SIANN*) شناخته می‌شوند که بر اساس معماری وزن مشترک هسته‌های کانولوشن یا فیلترهایی است که در امتداد ویژگی‌های ورودی متغیر هستند و پاسخ‌های معادل تفسیر ارائه‌شده به‌عنوان نقشه ویژگی‌ها را ارائه می‌دهند [۲]، [۳]. این دسته از شبکه‌های عصبی کانولوشن دارای کاربردهایی در زمینه تشخیص تصویر و ویدئو، سیستم‌های توصیه گر [۵]، طبقه‌بندی تصویر، تقسیم‌بندی تصویر، تجزیه‌وتحلیل تصویر پزشکی، پردازش زبان طبیعی [۸]، رابط مغز و کامپیوتر [۹]، سری‌های زمانی مالی [۱۰]، تحلیل شبکه‌های اجتماعی [۲۰] و تشخیص بدافزار [۲۱] هستند.

در پژوهش نگوین و همکاران [۲۲]، سه رویکرد مبتنی بر CNN را برای شناسایی بدافزار اینترنت اشیا بر روی ۱۰۰۰ نمونه بدافزار اینترنت اشیا بر روی معماری ۳۲ بیتی با مقایسه نمایش داده‌های مختلف از جمله توالی‌ها، تصاویر و کد اسمبلی بررسی شده است. این مقایسه برای تشخیص فایل‌های مخرب و فایل‌های بی خطر انجام می‌گردد. بر اساس ادعای نویسندگان نتایج تجربی نشان می‌دهد که هر یک از رویکردها کاملاً خوب کار می‌کند.

در پژوهش باک و همکاران [۲۳]، یک طرح تشخیص بدافزار ترکیبی دو مرحله‌ای برای محافظت از دستگاه‌های اینترنت اشیاء در برابر بدافزار مبهم در یک محیط شهر هوشمند پیشنهاد می‌کنیم. این رویکرد شامل دو مرحله شناسایی بدافزار اینترنت اشیا است. ابتدا پس از انجام تحلیل ایستا، کدهای عملیاتی استخراج شده و با استفاده از اطلاعات آموخته شده از طریق مدل حافظه کوتاه مدت دو جهته، فایل‌های خوش خیم شناسایی می‌شوند. در مرحله بعد، تجزیه و تحلیل پویا بر روی فایل‌هایی که در یک محیط مجازی تودرتو به عنوان خوش خیم طبقه بندی می‌شوند، انجام می‌شود. پس از استخراج اطلاعات رفتار و حافظه پردازش از گزارش رفتار بر اساس تغییرات سیستم، بدافزار را می‌توان از طریق مدل آموزش دیده شناسایی کرد.

در پژوهش آزموده و همکاران [۲۴]، بدافزارهای اینترنت اشیا را در حوزه نظامی مورد بررسی قرار می‌دهد. یک بردار حمله رایج استفاده از بدافزار است. در این مقاله، یک روش مبتنی بر یادگیری عمیق برای شناسایی بدافزار از طریق دنباله کد عملیاتی دستگاه ارائه دهد. روش پیشنهادی کدهای عملیاتی را به یک فضای برداری تبدیل می‌کند و یک رویکرد یادگیری عمیق فضای ویژه را برای طبقه بندی برنامه‌های مخرب و مخرب اعمال می‌نماید. علاوه بر این استحکام رویکرد پیشنهادی در تشخیص بدافزار و پایداری آن در برابر حملات درج کد ناخواسته مورد بررسی قرار گرفته است.

شبکه‌های عصبی کانولوشن نسخه‌های منظم پرسپترون‌های چندلایه هستند. پرسپترون‌های چندلایه معمولاً به معنی شبکه‌های کاملاً متصل هستند، یعنی هر نورون در یک‌لایه به همه نورون‌های لایه بعدی متصل است [۲۵]. "اتصال کامل[3]" این شبکه‌ها آن‌ها را مستعد بیش برازش[4] می‌کند [۲۶]. روش‌های معمول منظم سازی یا جلوگیری از بیش برازش شامل موارد زیر است: جریمه کردن پارامترها در طول تمرین (مانند کاهش وزن) یا کاهش اتصال (حذف ارتباطات، حذف تصادفی و غیره) [۲۷]. شبکه‌های عصبی کانولوشن رویکرد متفاوتی نسبت به منظم سازی دارند: آن‌ها از الگوی سلسله مراتبی در داده‌ها استفاده می‌کنند و الگوهای افزایش پیچیدگی را با استفاده از الگوهای کوچک‌تر و ساده‌تر که در فیلترهای آن‌ها نقش بسته است، جمع‌آوری می‌کنند؛ بنابراین، در مقیاس اتصال و پیچیدگی، شبکه‌های عصبی کانولوشن در حد پایین قرار دارند [۲۸].

شبکه‌های عصبی کانولوشن نسبت به سایر الگوریتم‌های طبقه‌بندی از پیش‌پردازش نسبتاً کمی استفاده می‌کنند [۲۹]. این بدان معنی است که شبکه یاد می‌گیرد که فیلترها (هسته‌ها) را از طریق یادگیری خودکار بهینه کند، درحالی‌که در الگوریتم‌های سنتی این فیلترها به‌صورت دستی طراحی‌شده‌اند. این استقلال از دانش قبلی و مداخله انسان در استخراج ویژگی یک مزیت بزرگ است [۳۰].

۲-۴- کارهای مرتبط

به‌موازات ظهور و فراگیری اینترنت اشیاء در سال‌های اخیر و به دنبال آن بروز مخاطرات امنیتی، پژوهش‌های متعددی در حوزه شناسایی و مقابله با این تهدیدات سایبری به‌خصوص با استفاده از بررسی و تحلیل ترافیک شبکه انجام‌شده است که هر یک با میزان دقت، صحت و سرعت‌های تشخیص متفاوتی این حملات را شناسایی کرده‌اند. در ادامه به برخی از این پژوهش‌ها اشاره‌شده است.

[1] Convolutional Neural Networks
[2] Recurrent Neural Networks
[3] Fully-connected
[4] Overfitting

آزکا وانی و ریواتی [۳۱] روشی را با هدف شناسایی باج افزارها، متمرکز بر روی ترافیک بین تجهیزات اینترنت اشیاء و جهان خارج توسعه داده‌اند. روش پیشنهادی که *IoTSDN_RAN* نامیده می‌شود در *SDN* مقیم می‌شود و سرآیند بسته‌های *CoAP* و *TCP/IP* را تجزیه‌وتحلیل می‌کند. روش پیشنهادشده در سه مرحله اجرا می‌شود. مرحله اول که جمع‌آوری نمونه‌ها است شامل گردآوری نمونه‌های ترافیک مخرب و سالم است. مرحله دوم آموزش *IoTSDN_RAN* است که در آن ویژگی‌های خاص ترافیک جمع‌آوری‌شده در مرحله قبل، استفاده‌شده است. ترکیبی از *Naive Bayes* و تحلیل مؤلفه‌های اصلی برای شناسایی باج افزار در مرحله دوم و سوم پیشنهادشده است. سومین مرحله تشخیص و تعدیل است که در آن حملات باج افزار با استفاده از دانش مراحل قبل شناسایی می‌شود.

نادرا گویزانی و عاریف غفور [۳۲] یک معماری نرم‌افزاری به‌عنوان مجازی ساز عملکرد شبکه را جهت مقابله با گسترش بدافزار در شبکه‌های مبتنی بر اینترنت اشیاء پیشنهاد می‌دهند. برای ایجاد یک سیستم تشخیص نفوذ[1] مقیاس‌پذیر و تعمیم‌یافته از یک معماری شبکه عصبی بازگشتی تحت عنوان مدل یادگیری حافظه طولانی کوتاه‌مدت *LSTM* استفاده‌شده است. مدل‌های تعریف‌شده در این معماری شامل مدل مستعد، در معرض خطر، آلوده‌شده و مقاوم است. مجموعه داده ورودی شامل *BoT-IoT*[۳۳] است که پس از پیش‌پردازش به لایه‌های ورودی شبکه عصبی مصنوعی بازگشتی داده می‌شود. بر اساس داده‌های پیش‌پردازش شده مدل آموزش داده می‌شود و از آن در شناسایی ترافیک‌های مخرب استفاده می‌شود.

نای فو و همکاران [۳۴] یک چارچوب نرم‌افزاری جهت دسته‌بندی بدافزارهای مبتنی بر معماری *MIPS* در دستگاه‌های اینترنت اشیاء توسعه داده‌اند که از *F-Sandbox* منفعل و یادگیری ماشین استفاده می‌کند. رویکرد پیشنهادی علاوه بر فراخوانی‌های واسط‌های برنامه‌نویسی کاربردی، ردیابی دستورالعمل‌ها، تغییرات رجیستری، نوشتن حافظه و غیره، از رفتار مبتنی بر شبکه نیز جهت جمع‌آوری اطلاعات استفاده می‌کند. الگوریتم یادگیری ماشین استفاده‌شده شامل ماشین بردار پشتیبان به همراه روش استخراج ویژگی *n-gram* است و وزن مدل پیشنهادی آموزش داده شده برای دسته‌بندی پنج خانواده بدافزار ۹۷٫۴۴٪ است.

فی دینگ و همکاران [۳۵]،*DeepPower* یک رویکرد غیرتهاجمی برای استنباط فعالیت‌های مخرب بدافزارها در سطح شبکه اینترنت اشیاء از طریق تجزیه‌وتحلیل سیگنال‌های کانال جانبی با استفاده از یادگیری ماشین ارائه کرده‌اند. *DeepPower* در ابتدا سیگنال‌های خام دستگاه‌های اینترنت اشیاء را فیلتر می‌کند تا سیگنال‌های مشکوک را به دست آورد. سپس با انجام یک تحلیل *fine-grained* بر روی این سیگنال‌ها سعی در استنباط فعالیت‌های انجام‌شده درون دستگاه‌ها دارد. روش پیشنهادی با انجام تجزیه‌وتحلیل همبستگی در مورد فعالیت‌های شناسایی‌شده، تعیین می‌کند که آیا آلودگی به بدافزار رخداده است یا خیر.

آیوش کومار و تنگ جون لیم [۷] یک راه‌حل ماژولار توزیع‌شده را تحت عنوان *EDIMA* ارائه می‌دهند که می‌تواند برای شناسایی فعالیت‌های مبتنی بر شبکه در زیرساخت اینترنت اشیاء و در مقیاس بزرگ پیش از حمله و در مرحله اسکن / آلوده‌سازی مورداستفاده قرار بگیرد. *EDIMA* از الگوریتم‌های یادگیری ماشین برای دسته‌بندی ترافیک دستگاه‌های لبه، پایگاه داده بردار ویژگی‌های ترافیک شبکه و ماژول سیاست‌های امنیتی استفاده می‌کند. مدل یادگیری ماشین برای طبقه‌بندی ترافیک شبکه دروازه‌های دسترسی با استفاده از بردار ویژگی و برچسب‌های کلاس بازیابی شده از پایگاه داده ویژگی ترافیک بسته به‌عنوان ورودی به الگوریتم‌های طبقه‌بندی نظارت‌شده همانند *Naive Bayes*، درخت تصمیم‌گیری و ماشین بردار پشتیبان داده می‌شود. سپس مدل به دسته‌بندی کننده یادگیری ماشین ارسال می‌شود. در صورت کشف بدافزار جدید مدل دوباره آموزش داده می‌شود و برای بررسی عملکرد با طبقه‌بندی کننده کنونی مقایسه می‌شود، اگر پیشرفت چشمگیری حاصل نشده باشد، مدل یادگیری ماشین فعلی همچنان مورداستفاده قرار می‌گیرد.

۲-۵- ترافیک شبکه اینترنت اشیاء

چندین پروتکل اینترنت اشیا در دسترس است که هر کدام قابلیت‌ها یا ترکیبی از ویژگی‌ها را ارائه می‌دهند که آن‌ها را نسبت به سایر پروتکل‌های رایج شبکه متمایز می‌کند. هر پروتکل اینترنت اشیا ارتباط دستگاه به دستگاه، دستگاه به دروازه یا دستگاه به ابر/مرکز داده، یا ترکیبی از این ارتباطات را فعال می‌کند. عواملی مانند موقعیت جغرافیایی، نیازهای مصرف انرژی، گزینه‌های باتری‌دار، وجود موانع فیزیکی و هزینه تعیین می‌کنند که کدام پروتکل در استقرار اینترنت اشیا بهینه است. علاوه بر معماری‌های سه‌لایه، چهارلایه و پنج‌لایه، پروتکل‌های خاص منظوره اینترنت اشیا ترافیک کاملاً متفاوتی با پروتکل‌ها رایج شبکه ایجاد می‌کند. از جمله این پروتکل‌ها می‌توان به AMQP[2]، MQTT[3]، CoAP[4]، DDS[5] و غیره اشاره نمود [۳۶]، [۳۷].

۲-۶- جمع‌بندی کارهای پیشین

بررسی مبانی نظری و کارهای پیشین مقاله نشان داد که از یادگیری عمیق در تحلیل و شناسایی ترافیک بدخواه در زیرساخت اینترنت اشیاء با مهندسی ویژگی‌ها به‌صورت محدود

[1] IDS

[2] Advanced Message Queue Protocol
[3] Message Queue Telemetry Transport
[4] Constrained Application Protocol
[5] Data Distribution Service

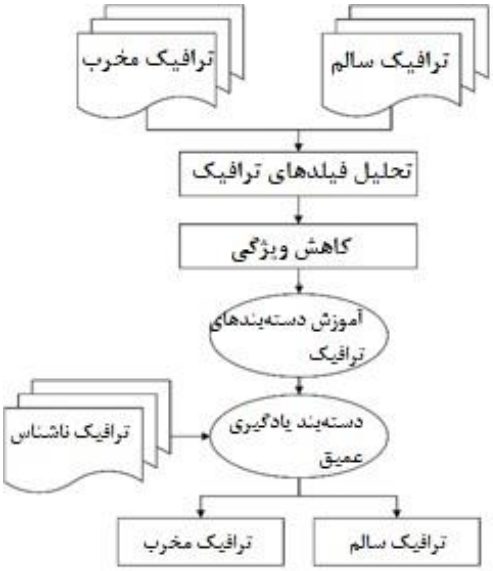
استفاده شده است. بهبود صورت‌گرفته در این مقاله مبتنی بر یادگیری عمیق، شامل ۱) تعریف و تبیین ویژگی‌های ترافیک ۲) تولید ترافیک شبیه‌سازی شده ۳) توسعه مدل و بهینه‌سازی پارامترها ۴) بهبود در دقت تشخیص ترافیک مخرب است.

۳- روش پیشنهادی

وجود محدودیت‌های جدی منابع در تجهیزات اینترنت اشیا موجب عدم اعمال بسیاری از سیاست‌های امنیتی حتی در سطح ابتدایی بر روی آن‌ها گردیده است. ضعف‌های امنیتی متعدد موجب گردیده است تا تجهیزات اینترنت اشیا به‌عنوان یک هدف محبوب و دست‌یافتنی برای مهاجمان سایبری بدل گردد. به دلیل افزایش چشمگیر این نوع از حملات، لزوم برخورد بیش‌ازپیش با آن‌ها احساس می‌گردد. در این مقاله یادگیری عمیق جهت شناسایی ترافیک بدخیم در حوزه اینترنت اشیا استفاده‌شده است. جهت ارزیابی روش پیشنهادی الگوریتم‌های سنتی یادگیری ماشین و یادگیری عمیق بر اساس مجموعه داده واقعی و مجموعه داده شبیه‌سازی‌شده باهدف طبقه‌بندی ترافیک خوش‌خیم و بدخیم مورد مقایسه قرار می‌گیرد. روش پیشنهادی مبتنی بر استخراج ویژگی‌های مؤثر، حذف موارد غیر ضروری در قالب فرایند پیش‌پردازش و بررسی میزان کارایی استفاده از آن‌ها در سامانه‌های تشخیص ترافیک بدخواه و ناسالم است. در شکل (۳) طرح روش پیشنهادی نشان داده شده است.

روش پیشنهادی از یک شبکه عصبی عمیق استفاده می‌کند. از آن جهت که در دستگاه‌های اینترنت اشیاء علاوه بر پروتکل‌های معمول شبکه از پروتکل‌های مدیریتی و انتقال داده اختصاصی نیز استفاده می‌شود، ویژگی‌های منحصربه‌فرد مربوط به اتصال، تبادل اطلاعات، کنترل و مدیریت و سایر تعاملات استخراج گردیده است. رویکرد پیشنهادی از طریق بهینه‌سازی معماری مدل و توسعه پارامترها جهت بهبود شبکه عصبی در شناسایی ترافیک سالم از مخرب استفاده می‌کند. روش پیشنهادی شامل دو مرحله اساسی آموزش و تشخیص است. فاز آموزش شامل شناسایی ویژگی‌ها، طراحی معماری مدل، تعیین پارامتر و وزن‌دهی به اتصالات است. در فاز شناسایی از مدل آموزش داده شده جهت تعیین ترافیک‌های ورودی به‌عنوان خوش‌خیم و بدخیم بهره‌برداری می‌شود.

پیکربندی مناسب یادگیری عمیق پیشنهادی، موجب افزایش دقت، صحت و سایر پارامترهای ارزیابی در مقایسه با الگوریتم‌های کلاسیک یادگیری ماشین می‌گردد. در بخش‌های بعدی مجموعه‌های داده مورداستفاده، ویژگی‌های استخراج‌شده و معماری و پیکربندی شبکه عصبی عمیق مورد بررسی قرار گرفته است.



شکل (۳): طرح روش پیشنهادی

۳-۱- مجموعه داده

مجموعه داده‌های استفاده‌شده در این پژوهش شامل ترافیک واقعی و ترافیک شبیه‌سازی‌شده است.

مجموعه داده واقعی:

IOT23 مجموعه داده واقعی و غیر شبیه‌سازی‌شده‌ای از ترافیک شبکه دستگاه‌های اینترنت اشیاء است و دارای ۲۰ سناریو بدخواه از بدافزارهایی است که در دستگاه‌های اینترنت اشیا اجرا می‌شوند و ۳ سناریو برای ترافیک خوش‌خیم دستگاه‌های اینترنت اشیاء است [۳۸]. این مجموعه داده در بازه زمانی ۲۰۱۸ تا ۲۰۱۹ جمع‌آوری شده و اولین بار در ژانویه ۲۰۲۰ منتشر شد. این ترافیک شبکه اینترنت اشیا در آزمایشگاه استراتوسفر، گروه *AIC*، *FEL*، دانشگاه *CTU*، جمهوری چک، ثبت شده است. این مجموعه داده و تحقیقات مرتبط با آن توسط نرم‌افزار *Avast*، در پراگ تأمین مالی می‌شود.

در هر سناریو مخرب، یک نمونه بدافزار خاص که از چندین پروتکل استفاده می‌کرده است و اقدامات متفاوتی را انجام می‌داده است بر روی تراشه رزبری‌پای[1] اجراشده است. از جمله ویژگی‌های سناریوهای بدافزارهای موردمطالعه می‌توان به بیش از ۷۶۴ میلیون بسته شبکه که شامل پروتکل‌های *HTTP*، *DNS*، *DHCP*، *Telnet*، *SSL*، *SSH* و *IRC* است اشاره کرد. ترافیک شبکه‌ای که برای سناریوهای خوش‌خیم ثبت‌شده است، با ضبط ترافیک شبکه سه دستگاه مختلف اینترنت اشیا به‌دست‌آمده است شامل لامپ ال‌ای‌دی[2] هوشمند فیلیپس[3]، دستیار شخصی هوشمند آمازون[4] و قفل هوشمند سومفی[5] است. مزیت ترافیک

[1] Raspberry Pi
[2] LED
[3] Philips HUE
[4] Amazon Echo home
[5] Somfy

ضبط‌شده در سناریوهای خوش‌خیم این است که این سه دستگاه اینترنت اشیا، سخت‌افزار واقعی هستند و شبیه‌سازی نشده‌اند؛ که این امکان را فراهم می‌کند رفتار واقعی شبکه ضبط و تحلیل گردد. هر دو سناریوی مخرب و خوش‌خیم در یک محیط شبکه کنترل‌شده با اتصال به اینترنت بی‌قیدوشرط مانند سایر دستگاه‌های واقعی اینترنت اشیا اجرا می‌شوند. داده‌های شبکه سناریوهای خوش‌خیم *IoT* نیز شامل بیش از ۴۲۷ هزار بسته شبکه است که از پروتکل‌های *HTTP*، *DNS*، *DHCP* و *SSL* استفاده می‌کنند [۳۸]. در این مجموعه داده بیش از ۹۹ درصد داده‌ها شامل ترافیک بدخیم و کم تر از ۱ درصد داده‌ها را داده‌های خوش خیم تشکیل داده است.

مجموعه داده شبیه‌سازی‌شده:

مجموعه داده شبیه‌سازی‌شده نوع دیگری از مجموعه داده استفاده‌شده در این پژوهش است که شامل ۱۵ سناریوی بدخیم از ترافیک شبکه بدافزارهایی است که بر روی دستگاه‌های اینترنت اشیاء نصب می‌شوند و ۵ سناریوی خوش‌خیم از ترافیک شبکه دستگاه‌های اینترنت اشیاء است و از طریق دریافت بسته‌های شبکه دستگاه‌های اینترنت اشیاء شبیه‌سازی‌شده تولید گردیده است. شبیه‌سازی از طریق اجرای میان‌افزار دستگاه‌های سونیک وال[۱]، دی لینک[۲]، یرلینک[۳] و هیک ویژن[۴] در محیط کیو ایمیو[۵] انجام گردیده است.

در هر سناریو مخرب یک نمونه بدافزار از مجموعه بدافزارهای اینترنت اشیاء بر روی یک دستگاه اینترنت اشیاء اجرا گردیده است. از جمله ویژگی‌های این مجموعه داده می‌توان به بیش از ۲۰ میلیون بسته شبکه شامل پروتکل‌های *HTTP*، *DNS*، *DHCP*، *Telnet*، *SSL*، *SSH*، *IRC*، *MQTT* و *LwM2M* است، اشاره کرد. ترافیک شبکه خوش‌خیم شامل دستگاه‌های اینترنت اشیاء بیان‌شده در بالا بدون آلودگی است که بلافاصله پس از شبیه‌سازی و قبل از آلوده‌سازی ذخیره گردیده‌اند. هر دو سناریو خوش‌خیم و بدخیم در یک محیط شبیه‌سازی شده بااتصال به اینترنت بی‌قیدوشرط مانند سایر دستگاه‌های واقعی اینترنت اشیا اجراشده‌اند. داده‌های سناریو خوش‌خیم نیز شامل ۲۰۰ هزار بسته شبکه است که از پروتکل‌های *HTTP*، *DNS*، *DHCP*، *Telnet*، *SSL*، *SSH*، *MQTT*، *LwM2M* و *AMQP* استفاده می‌کنند.

بدافزارهای میرای[۶]، کیوبات[۷]، هجیم[۸]، کایتن[۹] و ورم وار[۱۰] در بازه‌های زمانی ۵ تا ۲۴ ساعت جهت تولید سناریوهای بدخواه مورداستفاده قرارگرفته است. در این مجموعه داده پروتکل‌های اختصاصی اینترنت اشیاء همانند *MQTT*، *LwM2M* و *AMQP* مشاهده و دریافت شده‌اند. در این مجموعه داده نیز بیش از ۹۹ درصد داده‌ها شامل ترافیک بدخیم و کم تر از ۱ درصد داده‌ها را داده‌های خوش خیم تشکیل داده است.

۳-۲- فیلتر گذاری و استخراج ویژگی

در این پژوهش داده‌های موجود در پروتکل‌های شبکه به دو بخش داده‌های ثابت و داده‌های متغیر دسته بندی شده است. منظور از داده‌های ثابت داده‌هایی هستند که برای تمامی حالات و موقعیت‌ها مقدار ثابت و یکسانی دارند. از جمله این ویژگی‌ها می‌توان به نام پروتکل، نسخه پروتکل، واژه‌های رزرو شده پروتکل و غیره اشاره نمود که از آن‌ها به عنوان داده‌های مانا یاد می‌شود. در مقابل ویژگی‌های متغیر آن دسته از داده‌هایی هستند که متناسب با وضعیت‌های گوناگون حاوی مقادیر مختلفی می‌باشند. فیلتر گذاری در این بخش شامل حذف داده‌های مانا و انتخاب داده‌های متغیر بر روی پروتکل‌های شبکه می‌باشد که در مرحله استخراج ویژگی مورد استفاده قرار می‌گیرند. مرحله استخراج ویژگی‌ها شامل خواندن داده‌ها و رکوردهای متغیر مجموعه داده آموزشی و استخراج ویژگی‌های مبتنی بر جریان است. یک ویژگی مقداری عددی یا غیر عددی است که به مشخصه‌ای از جریان بسته در پنجره زمانی خاص، اشاره می‌کند. پیش‌پردازش بر روی مجموعه داده انجام گردیده و دو سناریو با دو حجم متفاوت از ویژگی‌ها تهیه گردید. سناریوی شماره ۱ شامل تمامی ویژگی‌های استخراج‌شده و سناریو شماره ۲ شامل ۶۰ درصد ویژگی‌ها است. جهت استخراج ویژگی، پس از تبدیل داده‌های مجموعه داده به یک جدول ساخت‌یافته، به‌عنوان ورودی به الگوریتم استخراج گر مورداستفاده قرار می‌گیرد. جدول (۱) در پیوست مقاله وضعیت ویژگی‌های استخراج‌شده و دسته‌بندی آن‌ها را نشان می‌دهد.

لیست ویژگی‌های استخراج‌شده از بین مجموعه ویژگی‌های موجود با هدف کاهش مشکل بیش برازش و رفع مشکل جمع‌آوری داده‌های نامتوازن مور استفاده قرار می‌گیرد. کاهش جزئی عملکرد الگوریتم یادگیری عمیق در مقایسه با افزایش ملموس سرعت به دلیل حذف سایر ویژگی‌ها قابل‌چشم‌پوشی است. در این پژوهش جهت حذف ویژگی‌های کم‌اثر و انتخاب ویژگی‌های مؤثر از مجموعه داده اولیه و کاهش پیچیدگی مدل یادگیری عمیق از درخت طبقه‌بندی و رگرسیون [۳۹] استفاده‌شده است. درخت طبقه‌بندی و رگرسیون از سرعت بالا و برخوردار از مقیاس‌پذیری برای مجموعه داده‌های بسیار بزرگ است که گزینه مناسبی برای انتخاب مجموعه داده هدف در پژوهش جاری است.

[1] SonicWall
[2] D-Link
[3] Yealink
[4] HikVision
[5] QEMU
[6] Mirai
[7] Qbot
[8] Hajime
[9] Kaiten
[10] Worm war

۳-۳- ساختار مدل یادگیری عمیق پیشنهادی

طراحی مدل یادگیری عمیق مبتنی بر ویژگی‌های استخراج‌شده و انتخاب‌شده در مرحله قبل است. مجموعه داده‌های ارائه‌شده به مدل یادگیری عمیق جهت آموزش و ارزیابی به دو مجموعه آموزش و آزمون تقسیم می‌شود. مجموعه آموزش که شامل ۷۰ درصد از کل مجموعه داده اولیه است جهت یادگیری و مجموعه آزمون شامل ۳۰ درصد باقی‌مانده از کل مجموعه داده اولیه است که جهت ارزیابی مدل مورداستفاده قرار می‌گیرند که در هر دو مجموعه ۹۹ درصد از حجم مجموعه را داده‌های بدخیم و ۱ درصد را داده‌های خوش خیم تشکیل داده اند. مجموعه داده آموزشی به طور تصادفی به ۷۰ درصد آموزش و ۳۰ درصد اعتبارسنجی تقسیم می‌شود. داده‌های اعتبارسنجی به مشاهده دقت آموزش در دوره‌های مختلف کمک می‌کند. انتخاب مجموعه آموزش و اعتبارسنجی به‌صورت تصادفی صورت‌گرفته است.

همان‌طور که پیش‌تر بیان‌شده مدل شبکه عصبی کانوشنال شامل سه لایه ورودی، مخفی و خروجی است. با توجه به این‌که تعداد ویژگی‌های استخراج‌شده شامل *40* ویژگی است، تعداد گره‌های ورودی *40* در نظر گرفته‌شده است (جدول (۲)). لایه‌های ۲ تا ۲۱ شامل لایه‌های مخفی و لایه ۲۲ تا ۲۳ لایه‌های خروجی را تشکیل می‌دهند.

برای یافتن میزان یادگیری مناسب، ۲ آزمایش آزمایشی برای نرخ یادگیری متنوع در بازه *[0.01-0.5]* اجرا شد. آزمایش‌ها با نرخ یادگیری *0.2* عملکرد بهتری داشتند. آزمایش‌هایی با نرخ یادگیری پایین‌تر در مقایسه با نرخ یادگیری بالاتر در زمانی که آزمایش‌ها تا ۱۰۰ دوره اجرا می‌شدند دقت کمتری نشان دادند.

در مدل پیشنهادی لایه‌های کاملاً متصل از تابع فعال‌ساز *ReLU* استفاده می‌کند که در جلوگیری از مسئله محوشدگی و انفجار گرادیان مؤثر است. جهت وزن دهی اولیه از کلاس *HeUniform* استفاده شده است*[*]*. تابع فعال سازی *ReLU* به وسیله این مدل مقداردهی اولیه، بسیار خوب عمل می‌کند. تنها پارامتری که در مقداردهی اولیه *He* درنظر گرفته می‌شود، تعداد ورودی‌هاست. از لایه‌های *Batch Normalization* جهت نرمال‌سازی داده‌ها در درون شبکه و مدل استفاده می‌شود. نرمال‌سازی دسته‌ای یک مرحله از فراعامل‌های γ و β که دسته‌ی $\{X_i\}$ را نرمال می‌کند در معادله ۱ نشان داده شده است. نماد μ_B و σ_B^2 به میانگین و واریانس دسته‌ای که میخواهیم آن را اصلاح کنیم اشاره دارد.

$$X_i \longleftarrow \gamma \frac{X_i - \mu_B}{\sqrt{\sigma_B^2 + \epsilon}} \qquad (۱)$$

لایه‌های نرمال‌سازی پس از لایه‌های کاملاً متصل تعبیه گردیده است تا تغییرات مرتبط با توزیع داده‌ها را خنثی نماید. جهت جلوگیری از بیش برازش از لایه‌های *Dropout* استفاده‌شده است. در فرایند اعمال *Dropout* بر روی شبکه، در هر مرحله از آموزش، گره‌هایی از شبکه، با احتمال p-۱ کنار گذاشته‌شده و گره‌های دیگری با احتمال p، نگه‌داشته می‌شوند درنتیجه این کار سرعت یادگیری در طول آموزش افزایش می‌یابد. در پژوهش جاری میزان $p = ۰,۶$در نظر گرفته‌شده است که به‌صورت تجربی نتیجه بهتری را در مقایسه با سایر مقادیر تولید می‌کند. تابع *Sigmoid* در لایه خروجی استفاده‌شده است که نتیجه آن ۰ یا ۱ است که ۰ نشان‌دهنده خوش‌خیم و ۱ نشان‌دهنده بدافزار است. جزئیات پیاده‌سازی مدل پیشنهادی در جدول (۲)، نشان داده شده است.

جهت یافتن ساختار بهینه شبکه عصبی عمیق، توپولوژی‌های شبکه مختلف به میزان ۵۰۰ دور اجراشده‌اند. در مدل یادگیری عمیق نهایی از بهینه‌ساز *adam*، تابع فعال‌سازی غیرخطی *Sigmoid* و تابع هزینه آنتروپی دودویی متقاطع[1] استفاده‌شده است. *ReLU* به‌عنوان تابع فعال‌سازی در لایه‌های کانولوشنال و کاملاً متصل به‌کاررفته است. توابع *Sigmoid* و آنتروپی دودویی متقاطع ازنظر ریاضی به‌صورت معادلات (۱)و(۲) تعریف می‌شوند:

$$Sigmoid(x) = \frac{1}{1+e^{-x}} \qquad (۲)$$

$$loss(pd, ed) = -\frac{1}{N}\sum_{i=1}^{N}[ed_i \log pd_i + (1-ed_i)log(1-pd_i)] \qquad (۳)$$

که در آن X به‌عنوان ورودی، pd احتمال پیش‌بینی‌شده و ed برچسب کلاس مورد انتظار است. جدول (۲)، جزییات پیکربندی مدل پیشنهادی را نشان می‌دهد.

جدول (۲): جزییات پیکربندی مدل پیشنهادی

Layers	Type	Output Shape	Number of units	Activation function
0-1	Fully-connected	(None,40)	40	ReLU
1-2	Batch Normalization	(None,40)		
2-3	Dropout (0.6)	(None, 40)		
3-4	Fully-connected	(None,38)	38	ReLU
4-5	Batch Normalization	(None, 38)		
5-6	Dropout (0.6)	(None,38)		
6-7	Fully-connected	(None,32)	32	ReLU
7-8	Batch Normalization	(None,32)		
8-9	Dropout (0.6)	(None,32)		
9-10	Fully-connected	(None,26)	26	ReLU
10-11	Batch Normalization	(None,26)		
11-12	Dropout (0.6)	(None,26)		
12-13	Fully-connected	(None,14)	14	ReLU
13-14	Batch Normalization	(None, 14)		
14-15	Dropout (0.6)	(None,14)		
15-16	Fully-connected	(None,10)	10	ReLU
16-17	Batch Normalization	(None,10)		
17-18	Dropout (0.01)	(None,10)		
18-19	Fully-connected	(None,5)	5	ReLU
19-20	Batch Normalization	(None,5)		
20-21	Dropout (0.01)	(None,5)		
21-22	Fully-connected	(None,1)	1	ReLU
22-23	Activation	(None,1)	1	Sigmoid

[1] Binary-Cross Entropy

۳-۴- جزییات پیاده‌سازی

سامانه به کار گرفته‌شده جهت آموزش مدل پیشنهادی دارای پردازنده *Intel Core i7-2670QM*، ۲/۲ گیگاهرتز، حافظه اصلی ۱۶ گیگابایت و پردازنده گرافیکی *NVIDIA GeForce GT540* با ۴ گیگابایت حافظه اصلی است. سیستم‌عامل مورداستفاده ویندوز ۷ نسخه ۶۴ بیتی است.

مدل پیشنهادی با استفاده از زبان برنامه‌نویسی پایتون نسخه ۳,۶ و در محیط ژوپیتر نوت بوک با بهره‌گیری از تنسورفلو کراس ۲,۲,۲ آموزش داده شده است.

۴- ارزیابی روش پیشنهادی و تحلیل نتایج

در این پژوهش برای ارزیابی عملکرد مدل طبقه‌بندی کننده، از معیارهای استاندارد صحت (*Accuracy* $\mathcal{E}2\ [0;\ 1]$)، بیان‌کننده درصد پیش‌بینی‌های صحیح تمام نمونه‌ها، دقت (*Precision* $\mathcal{E}\ [0;\ 1]$)، نشان‌دهنده درصد نمونه‌هایی که به‌درستی به‌عنوان نمونه مثبت طبقه‌بندی‌شده‌اند، بازخوانی (*Recall* $\mathcal{E}\ [0;\ 1]$)، نشان‌دهنده درصد نمونه‌های جریان ترافیک که به‌عنوان یک جریان ترافیک بدخواه پیش‌بینی‌شده است و میانگین هارمونی (*F1 _ score* $\mathcal{E}\ [0;\ 1]$)، معیاری از دقت آزمون، استفاده‌شده است. این معیارها بر اساس مثبت واقعی (*TP*)، منفی واقعی (*TN*)، مثبت کاذب (*FP*) و منفی کاذب (*FN*) برآورد می‌شوند. مثبت واقعی نشان‌دهنده تعداد نمونه جریان ترافیک بدخواه که به‌درستی به‌عنوان جریان ترافیک بدخواه شناسایی‌شده‌اند، منفی واقعی نشان‌دهنده تعداد نمونه‌های جریان ترافیک خوش‌خیم است که به‌درستی به‌عنوان نمونه جریان‌های ترافیک خوش‌خیم شناسایی‌شده‌اند، مثبت کاذب نشان‌دهنده تعداد نمونه‌های جریان ترافیک خوش‌خیم است که به‌عنوان نمونه جریان‌های ترافیک بدافزار طبقه‌بندی‌شده‌اند، منفی کاذب نشان‌دهنده تعدادی از نمونه‌های جریان ترافیک بدافزار است که به‌اشتباه به‌عنوان نمونه جریان‌های ترافیک خوش‌خیم طبقه‌بندی‌شده‌اند. معیارهای صحت، دقت، بازخوانی و میانگین هارمونی با استفاده از معادلات (۳) تا (۶) محاسبه می‌شود.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (۴)$$

$$Precision = \frac{TP}{TP+FP} \quad (۵)$$

$$Recall = \frac{TP}{TP+FN} \quad (۶)$$

$$F1-score = 2\left(\frac{Precision*Recall}{Precision+Recall}\right) \quad (۷)$$

یکی از رایج‌ترین ابزارهای تشخیصی برای شناسایی تفسیر طبقه‌بندی کننده‌های دودویی، منحنی ویژگی عملکرد گیرنده (*ROC*) است. در درجه اول، منحنی‌های *ROC* زمانی استفاده می‌شوند که نمونه‌های هر کلاس متعادل باشند. به‌طورمعمول، مساحت زیر منحنی (*AUC*) برای مقایسه منحنی‌های *ROC* استفاده می‌شود. *AUC*، همان‌طور که از نامش مشخص است، فقط مساحت زیر منحنی *ROC* است. این به‌طور خاص میزان فاصله بین کلاس‌ها را اندازه‌گیری می‌کند. *AUC* به‌صورت معادله (۷) تعریف می‌شود:

$$AUC = \int_0^1 \frac{TP}{TP+FN}\, d\, \frac{FP}{TN+FP} \quad (۸)$$

مقدار بالاتر *AUC* نشان‌دهنده این است که مدل، کلاس‌ها را با دقت بیش‌تر پیش‌بینی می‌کند. برای تولید *ROC*، مساحت بین نرخ مثبت واقعی (*TPR* $\mathcal{E}\ [0;\ 1]$) بر روی محور Y و نرخ مثبت کاذب (*FPR 2* $[0;\ 1]$) در محور X در بازه متغیر [۰؛۱] مورد ارزیابی قرار می‌گیرد. جهت محاسبه نرخ مثبت واقعی و نرخ مثبت کاذب از معادلات (۸) و (۹) استفاده می‌شود.

$$TPR = \frac{TP}{TP+FN} \quad (۹)$$

$$FPR = \frac{FP}{FP+TN} \quad (۱۰)$$

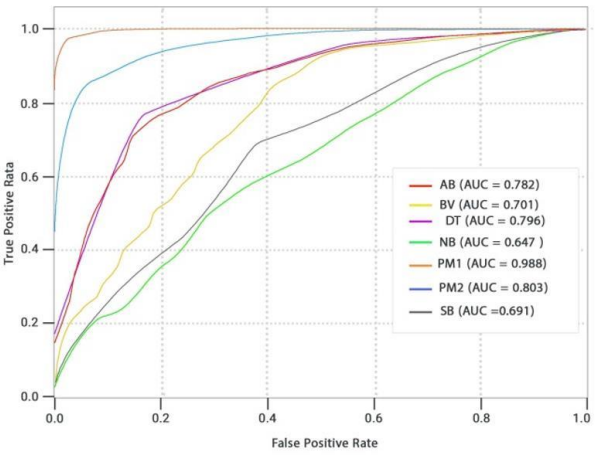
جدول (۳) صحت، دقت، بازخوانی، میانگین هارمونی و نرخ مثبت کاذب روش پیشنهادی را در مقایسه با الگوریتم‌های کلاسیک طبقه‌بندی همانند درخت تصمیم‌گیری، نزدیک‌ترین همسایه، هرس آلفا بتا و بردار پشتیبان را برای هر دو مجموعه داده نشان می‌دهد.

جدول (۳): مقایسه مدل پیشنهادی با الگوریتم‌های کلاسیک طبقه‌بندی

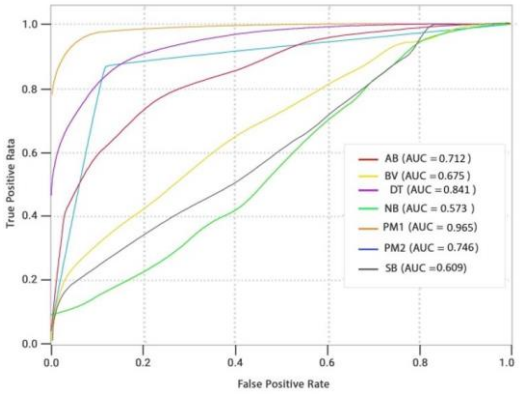
مدل	صحت	دقت	بازخوانی	هارمونی
مجموعه داده *IOT23*				
روش پیشنهادی، سناریو ۱*	**۹۸/۹**	**۹۹/۳**	**۹۹/۷**	**۹۸/۸**
روش پیشنهادی، سناریو ۲[1]	۹۷/۵	۹۶	۹۵/۱	۹۴/۶
درخت تصمیم[2]	۹۶/۲	۹۷/۳	۹۶/۷	۹۶/۹
نزدیک‌ترین همسایه[3]	۸۴/۳	۸۷/۵	۷۹/۶	۸۲/۲
هرس آلفا بتا[4]	۹۶/۸	۹۷/۲	۹۶/۷	۹۶/۹
بردار پشتیبان[5]	۹۷/۲	۹۸/۴	۹۵/۱	۹۶/۸
بیز ساده[6]	۹۶/۱	۹۶/۵	۹۵/۸	۹۶/۳
مجموعه داده شبیه‌سازی‌شده				
روش پیشنهادی، سناریو ۱*[7]	**۹۸/۶**	**۹۸/۹**	**۹۸/۶**	**۹۸/۱**
روش پیشنهادی، سناریو ۲	۹۷/۲	۹۶/۵	۹۳/۴	۹۵/۱
درخت تصمیم	۹۵/۱	۹۵/۵	۹۴/۷	۹۵/۱
نزدیک‌ترین همسایه	۸۵/۲	۸۶/۱	۷۸/۹	۸۲/۶
هرس آلفا بتا	۹۷/۳	۹۸/۰	۹۷/۴	۹۷/۷
بردار پشتیبان	۹۶/۵	۹۶/۱	۹۴/۹	۹۵/۸
بیز ساده	۹۴/۳	۹۴/۹	۹۳/۱	۹۵/۸

[1] Proposed Method(PM2)
[2] Decision Tree(DT)
[3] Nearest Neighbor(NB)
[4] Alpha Beta(AB)
[5] Backup Vector(BV)
[6] Simple Bayes(SB)
[7] Proposed Method(PM1)

منحنی *ROC* برای مجموعه داده ۱ و مجموعه داده ۲ به ترتیب در شکل (۴) و (۵)، نشان داده شده است. در این بخش الگوریتم‌های کلاسیک یادگیری ماشین و الگوریتم پیشنهادی بر روی *Dataset 1* و *Dataset 2* مورد ارزیابی قرارگرفته‌اند. همان‌طور که مشاهده می‌شود روش پیشنهادی دارایی عملکرد بهتری نسبت به الگوریتم‌های کلاسیک یادگیری ماشین است. بر اساس نتایج جدول (۳)، روش پیشنهادی در سناریو ۱ در هر دو مجموعه داده بهترین نتایج را نشان داده است.



شکل (۴): منحنی *ROC* برای مجموعه داده ۱

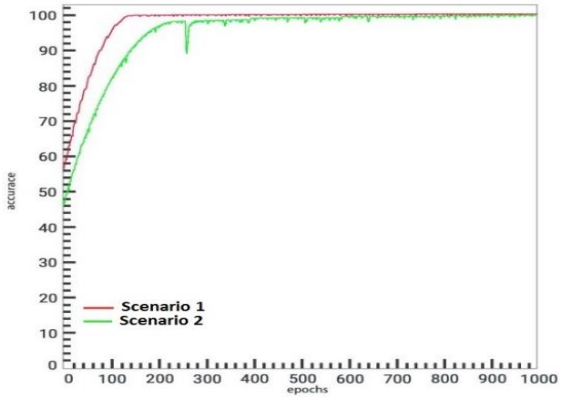


شکل (۵): منحنی *ROC* برای مجموعه داده ۲

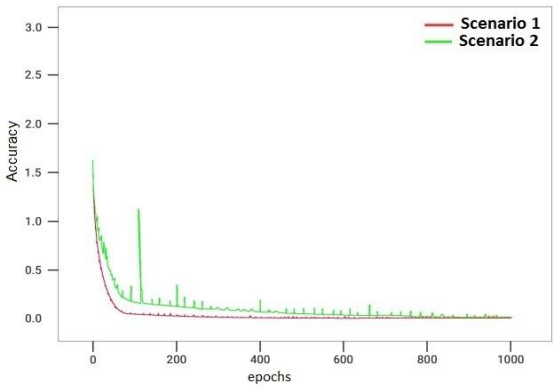
الگوریتم‌های یادگیری ماشین و یادگیری عمیق از دو فاز تشکیل‌شده است. تمامی این الگوریتم‌ها با داده‌های آموزشی، آموزش داده می‌شوند و با استفاده از داده‌های آزمون مورد ارزیابی قرار می‌گیرند. در این پژوهش تابع هزینه در خلال فاز آموزش مورد نظارت قرار گرفت و درصورتی‌که $c+1$ موجب ایجاد بهبود در تابع هزینه نسبت به c گردد، آن مدل در اجرای جاری ذخیره می‌گردد. دقت آموزش مدل یادگیری عمیق پیشنهادی اعمال‌شده بر روی مجموعه داده ۱ و ۲ در ۱۰۰۰ دور اجرا در شکل (۶) نشان داده شده است. نرخ خطای ۰ که از طریق معادله (۱۱) محاسبه شده است نشان می‌دهد که مدل دارای عملکردی به دور از بیش برازش شده است.

$$Error\ rate = \left(1 - \left(\frac{corrected\ predictions}{total\ predictions}\right)\right) * 100 \quad (۱۱)$$

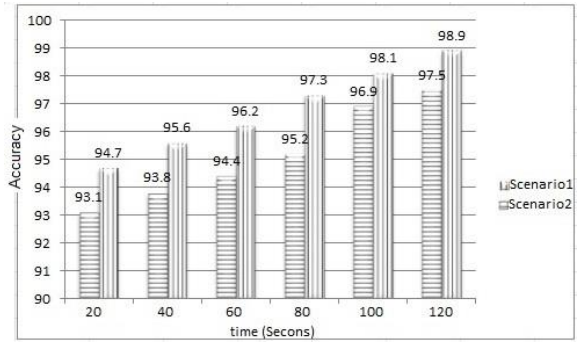
هزینه آموزش مدل یادگیری عمیق پیشنهادی نیز در شکل (۷)، نشان داده شده است. همان‌طور که مشاهده می‌شود مدل پیشنهادی با تعداد ویژگی‌های بیشتر در اجرای ۱۴۰ به‌دقت بهینه دست می‌یابد. این امر نشان می‌دهد که ویژگی‌های انتخاب‌شده از کیفیت بسیار بالایی برخوردار می‌باشند و تعداد بیشتر ویژگی‌های مؤثر، به‌دقت بالاتر مدل کمک خواهد نمود. مدل یادگیری عمیق پیشنهادشده قادر به شناسایی ترافیک خوش‌خیم و بدخیم در یک بازه زمانی کم‌تر از ۵ ثانیه است.



شکل (۶): دقت یادگیری الگوریتم پیشنهادی در سناریو شماره ۱ و سناریو شماره ۲

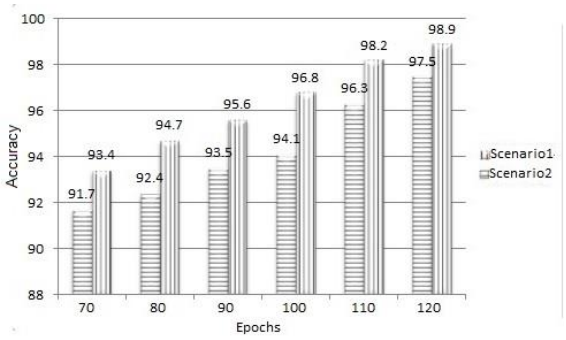


شکل (۷): تابع هزینه مدل پیشنهادی با مجموعه ویژگی کم‌حجم و پرحجم



شکل (۸): نرخ صحت روش پیشنهادی در سناریو شماره ۱ و ۲ مربوط به مجموعه داده واقعی در محدوده زمانی ۲۰ تا ۱۲۰ ثانیه

آزمون‌های متعددی جهت بررسی میزان تأثیر زمان تشخیص (برحسب ثانیه) و دوره اجرا (تعداد اجرا) شبکه عصبی عمیق بر روی نرخ صحت صورت‌گرفته است که در شکل‌های (۸) و (۹) نشان داده شده است. نتایج به‌دست‌آمده بیان‌کننده افزایش نرخ صحت در مدت زمان اجرای طولانی‌تر شبکه عصبی عمیق بر روی سناریوی شماره ۱ نسبت به سناریوی شماره ۲ در مجموعه داده واقعی است.



شکل (۹): نرخ صحت روش پیشنهادی در سناریو شماره ۱ و ۲ مربوط به مجموعه داده واقعی در محدوده اجرای ۷۰ تا ۱۲۰

۵- نتیجه‌گیری

گسترش روزافزون دستگاه‌های اینترنت اشیاء و عدم تعبیه سیاست‌های امنیتی مناسب در زمان تولید بر روی آن‌ها، این دسته از تجهیزات را به اهداف بالقوه‌ای برای مهاجمین سایبری و توسعه‌دهندگان بدافزارهای رایانه‌ای تبدیل کرده است. محدودیت منابع در دستگاه‌های اینترنت اشیا چالش اصلی در پیاده‌سازی سازوکارهای امنیتی است. در پژوهش انجام‌شده روشی پیشنهادشده است که با تحلیل ترافیک شبکه دستگاه‌های اینترنت اشیاء یک مدل یادگیری عمیق که قادر است در بازه زمانی کم‌تر از ۵ ثانیه ترافیک خوش‌خیم را از ترافیک بدخیم تشخیص دهد توسعه داده شده است. در این روش ویژگی‌ها به‌صورت دستی استخراج‌شده است و از دو مجموعه داده ترافیک شبکه اینترنت اشیاء جهت آموزش مدل شبکه عصبی عمیق پیشنهادی استفاده‌شده است. جهت ارزیابی عملکرد، مدل مذکور با تعدادی از الگوریتم‌های یادگیری ماشین مطرح همانند درخت تصمیم، نزدیک‌ترین همسایه، هرس آلفا بتا، بردار پشتیبان و بیز ساده مورد مقایسه قرارگرفته است و نشان داده شد که در تمامی سنجه‌های عملکردی دارای عملکرد بهتری است. بررسی‌های عملی نشان داد که مدل یادگیری عمیق با تعداد بیشتر ویژگی قادر به رسیدن به نقطه بهینه یادگیری در زمان بسیار کم‌تری است. با توجه به‌سرعت بالای روش پیشنهادی و نرخ بالای صحت، دقت، بازخوانی و هارمونی می‌توان از آن به‌عنوان یک روش کارآمد در شناسایی ترافیک بدخواه اینترنت اشیاء استفاده کرد. در کارهای آینده می‌توان با استفاده از سایر ویژگی‌های بسته‌های شبکه و توسعه مدل‌های یادگیری عمیق به همراه الگوریتم‌های فعال‌ساز و توابع هزینه مختلف می‌توان ترافیک بدخواه موجود در شبکه‌های اینترنت اشیاء را مورد ارزیابی قرارداد.

۶- مراجع

[1] B. Kaur and V. Dhir, “Internet of things: Vision, challenges and future scope,” Int. J. Adv. Res. Comput. Sci., vol. 8, no. 4, pp. 40–43, 2017.

[2] T. Fougeroux, A. Douyere, P. O. L. de Peslouan, N. Murad, S. Oree, and J.-L. Dubard, “Circuit Model of Rectennas Array for Estimating Microwave Energy Harvesting in Presence of Mutual Coupling Between Elements,” in 10ième Journées Nationales sur la Récupération et le Stockage de l’Energie (JNRSE 2021), 2021, p. 2.

[3] “Internet of Things Report.” https://www.businessinsider.com/internet-of-things-report (accessed Nov. 13, 2021).

[4] “Things just got real: 61% of businesses already use IoT platforms despite security risks | Kaspersky.” https://www.kaspersky.com/about/press-releases/2020_things-just-got-real-61-of-businesses-already-use-iot-platforms-despite-security-risks (accessed Nov. 13, 2021).

[5] J. Deogirikar and A. Vidhate, “Security attacks in IoT: A survey,” in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017, pp. 32–37.

[6] C. McCormack, “Five stages of a web malware attack.” Abingdon. Retrieved from https://www. sophos. com/en-us/medialibrary/Gated …, 2016.

[7] A. Kumar and T. J. Lim, “EDIMA: early detection of IoT malware network activity using machine learning techniques,” in 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), 2019, pp. 289–294.

[8] I. Hafeez, M. Antikainen, A. Y. Ding, and S. Tarkoma, “IoT-KEEPER: Detecting malicious IoT network activity using online traffic analysis at the edge,” IEEE Trans. Netw. Serv. Manag., vol. 17, no. 1, pp. 45–59, 2020.

[9] A. Sivanathan, “Iot behavioral monitoring via network traffic analysis,” arXiv Prepr. arXiv2001.10632, 2020.

[10] A. Kumar and T. J. Lim, “Early detection of Mirai-like IoT bots in large-scale networks through sub-sampled packet traffic analysis,” in Future of Information and Communication Conference, 2019, pp. 847–867.

[11] B. Wang, Y. Dou, Y. Sang, Y. Zhang, and J. Huang, “IoTCMal: Towards a hybrid IoT honeypot for capturing and analyzing malware,” in ICC 2020-2020 IEEE International Conference on Communications (ICC), 2020, pp. 1–7.

[12] O. I. Abiodun, A. Jantan, A. E. Omolara, K. V. Dada, N. A. Mohamed, and H. Arshad, “State-of-the-art in artificial neural network applications: A survey,” Heliyon, vol. 4, no. 11, p. e00938, 2018.

[13] S. Chatterjee, S. Sarkar, S. Hore, N. Dey, A. S.

"Architectures and accuracy of artificial neural network for disease classification from omics data," BMC Genomics, vol. 20, no. 1, pp. 1–12, 2019.

[26] S. Ni, Q. Qian, and R. Zhang, "Malware identification using visualization images and deep learning," Comput. Secur., vol. 77, pp. 871–885, 2018.

[27] S. Arvinth, A. Balakrishnan, M. Harikrishnan, and J. Jeydheepan, "WEED DETECTION USING CONVOLUTION NEURAL NETWORK", 2021.

[28] V. Sze, Y.-H. Chen, T.-J. Yang, and J. S. Emer, "Efficient processing of deep neural networks: A tutorial and survey," Proc. IEEE, vol. 105, no. 12, pp. 2295–2329, 2017.

[29] D. Perna, "Convolutional neural networks learning from respiratory data," in 2018 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), 2018, pp. 2109–2113.

[30] C. Modarres, N. Astorga, E. L. Droguett, and V. Meruane, "Convolutional neural networks for automated damage recognition and damage type identification," Struct. Control Heal. Monit., vol. 25, no. 10, p. e2230, 2018.

[31] A. Wani and S. Revathi, "Ransomware protection in loT using software defined networking," Int. J. Electr. Comput. Eng., vol. 10, no. 3, pp. 3166–3175, 2020.

[32] N. Guizani and A. Ghafoor, "A network function virtualization system for detecting malware in large IoT based networks," IEEE J. Sel. Areas Commun., vol. 38, no. 6, pp. 1218–1228, 2020.

[33] "The Bot-IoT Dataset | UNSW Research." https://research.unsw.edu.au/projects/bot-iot-dataset (accessed Nov. 13, 2021).

[34] T. N. Phu, K. H. Dang, D. N. Quoc, N. T. Dai, and N. N. Binh, "A novel framework to classify malware in mips architecture-based iot devices," Secur. Commun. Networks, vol. 2019, 2019.

[35] F. Ding et al., "DeepPower: Non-intrusive and deep learning-based detection of IoT malware using power side channels," in Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, 2020, pp. 33–46.

[36] S. Elhadi, A. Marzak, N. Sael, and S. Merzouk, "Comparative study of IoT protocols," Smart Appl. Data Anal. Smart Cities, 2018.

[37] S. Zamfir, T. Balan, I. Iliescu, and F. Sandu, "A security analysis on standard IoT protocols," in 2016 international conference on applied and theoretical electricity (ICATE), 2016, pp. 1–6.

[38] A. Parmisano, S. Garcia, and M. J. Erquiaga, "A labeled dataset with malicious and benign iot network traffic," Stratos. Lab. Praha, Czech Repub., 2020.

[39] M. Toğaçar, B. Ergen, and Z. Cömert, "Detection of lung cancer on chest CT images using minimum redundancy maximum relevance feature selection method with convolutional neural networks," Biocybern. Biomed. Eng., vol. 40, no. 1, pp. 23–39, 2020.

Ashour, and V. E. Balas, "Particle swarm optimization trained neural network for structural failure prediction of multistoried RC buildings," Neural Comput. Appl., vol. 28, no. 8, pp. 2005–2016, 2017.

[14] M. Skowron, M. Wolkiewicz, T. Orlowska-Kowalska, and C. T. Kowalski, "Effectiveness of selected neural network structures based on axial flux analysis in stator and rotor winding incipient fault detection of inverter-fed induction motors," Energies, vol. 12, no. 12, p. 2392, 2019.

[15] Q. Li et al., "A Novel High-Speed and High-Accuracy Mathematical Modeling Method of Complex MEMS Resonator Structures Based on the Multilayer Perceptron Neural Network," Micromachines, vol. 12, no. 11, p. 1313, 2021.

[16] U. Orhan, M. Hekim, and M. Ozer, "EEG signals classification using the K-means clustering and a multilayer perceptron neural network model," Expert Syst. Appl., vol. 38, no. 10, pp. 13475–13481, 2011.

[17] W. Hardy, L. Chen, S. Hou, Y. Ye, and X. Li, "DL4MD: A deep learning framework for intelligent malware detection," in Proceedings of the International Conference on Data Science (ICDATA), 2016, p. 61.

[18] D. Utomo, "Stock price prediction using back propagation neural network based on gradient descent with momentum and adaptive learning rate," J. Internet Bank. Commer., vol. 22, no. 3, pp. 1–16, 2017.

[19] A. Qayyum, S. M. Anwar, M. Awais, and M. Majid, "Medical image retrieval using deep convolutional neural network," Neurocomputing, vol. 266, pp. 8–20, 2017.

[20] mohammadreza mohammadrezaei, "Detecting Fake Accounts on Social networks using Principal Components Analysis and Algorithm Kernel Density Estimation (A case study on the Twitter social network)," Electron. Cyber Def., 2021, [Online]. Available: https://ecdj.ihu.ac.ir/article_205996.html

[21] M. Karami and M. Mosleh, "Providing a behavioral malware detection system based on the function of hardware counters using a neural network optimized with a dragonfly algorithm," Electron. Cyber Def., vol. 9, no. 2, pp. 9–16, 2021, [Online]. Available: https://ecdj.ihu.ac.ir/article_205749.html

[22] K. D. T. Nguyen, T. M. Tuan, S. H. Le, A. P. Viet, M. Ogawa, and N. Le Minh, "Comparison of three deep learning-based approaches for IoT malware detection," in 2018 10th international conference on Knowledge and Systems Engineering (KSE), 2018, pp. 382–388.

[23] S. Baek, J. Jeon, B. Jeong, and Y.-S. Jeong, "Two-stage hybrid malware detection using deep learning," Human-centric Comput. Inf. Sci., vol. 11, no. 27, pp. 10–22967, 2021.

[24] A. Azmoodeh, A. Dehghantanha, and K.-K. R. Choo, "Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning," IEEE Trans. Sustain. Comput., vol. 4, no. 1, pp. 88–95, 2018.

[25] H. Yu, D. C. Samuels, Y. Zhao, and Y. Guo,

۷- پیوست

جدول (۱): لیست ویژگی‌های ترافیک شبکه استخراج‌شده از مجموعه داده

ردیف	ویژگی	نوع ویژگی	دسته پرحجم	دسته کم‌حجم	توضیح
۱	*src-ip*	متنی	بلی	بلی	آدرس آی پی مبدأ
۲	*dst-ip*	متنی	بلی	بلی	آدرس آی پی مقصد
۳	*src-port*	عددی	بلی	بلی	شماره پورت مبدأ
۴	*dst-port*	عددی	بلی	بلی	شماره پورت مقصد
۵	*fr-len*	عددی	بلی	خیر	طول فریم
۶	*fr-no*	عددی	بلی	خیر	شماره فریم
۷	*protocol*	متنی	بلی	بلی	پروتکل
۸	*protocol type*	متنی	بلی	خیر	نوع پروتکل
۹	*bytes*	عددی	بلی	خیر	بایت‌های بسته
۱۰	*client to server packets*	متنی	بلی	بلی	بسته کلاینت به سرور
۱۱	*client to server bytes*	عددی	بلی	خیر	بایت‌های کلاینت به سرور
۱۲	*server to client packets*	متنی	بلی	بلی	بسته سرور به کلاینت
۱۳	*server to client bytes*	عددی	بلی	خیر	بایت‌های سرور به کلاینت
۱۴	*duration*	عددی	بلی	خیر	میانگین بازه زمانی بین بسته‌ها
۱۵	*Inter arrival time*	عددی	بلی	خیر	میانگین زمان پاسخ
۱۶	*num-get/post*	عددی	بلی	بلی	تعداد بسته‌های *get* و *post*
۱۷	*count-serv-src*	عددی	بلی	خیر	تعداد سرورها به‌عنوان مبدأ
۱۸	*count-serv-dst*	عددی	بلی	خیر	تعداد سرورها به‌عنوان مقصد
۱۹	*num-packets-src-dst*	عددی	بلی	بلی	تعداد بسته‌های مبدأ به مقصد
۲۰	*num-packets-dst-src*	عددی	بلی	بلی	تعداد بسته‌های مقصد به مبدأ
۲۱	*Up bytes*	عددی	بلی	خیر	تعداد بسته‌های آپ لینک
۲۲	*Down bytes*	عددی	بلی	خیر	تعداد بسته‌های داون لینک
۲۳	*uppkgnum*	عددی	بلی	خیر	تعداد بسته‌های آپستریم
۲۴	*downpkgnum*	عددی	بلی	خیر	تعداد بسته‌های داون استریم
۲۵	*upbytesmean*	عددی	بلی	خیر	میانگین تعداد بسته‌های آپ لینک
۲۶	*downbytesmean*	عددی	بلی	خیر	میانگین تعداد بسته‌های داون لینک
۲۷	*MQTT_ctl_len*	عددی	بلی	بلی	طول فیلد کنترل پروتکل
۲۸	*MQTT_Pkt_len*	عددی	بلی	بلی	طول فلید بسته پروتکل
۲۹	*MQTT_Hdr_len*	عددی	بلی	بلی	طول فیلد سرایند بسته پروتکل
۳۰	*MQTT_pld_len*	عددی	بلی	بلی	طول فیلد پیلود پروتکل
۳۱	*CoAP_Request/ResponseCode*	متنی	بلی	بلی	کد درخواست / پاسخ پروتکل
۳۲	*CoAP_MessageID*	متنی	بلی	بلی	شناسه پیام پروتکل
۳۳	*CoAP_Options_len*	عددی	بلی	بلی	طول فیلد اختیارهای پروتکل
۳۴	*CoAP_payload_len*	عددی	بلی	بلی	طول فیلد پیلود پروتکل
۳۵	*AMQP_type*	متنی	بلی	بلی	نوع بسته پروتکل
۳۶	*AMQP_channel*	متنی	بلی	بلی	محتوای فیلد کانال پروتکل
۳۷	*AMQP_size*	عددی	بلی	بلی	اندازه بسته پروتکل به بایت
۳۸	*AMQP_payload_byte_len*	عددی	بلی	بلی	طول فیلد پیلود پروتکل به بایت
۳۹	*LwM2M_ payload_byte_len*	عددی	بلی	بلی	طول فیلد پیلود پروتکل
۴۰	*LwM2M _size*	عددی	بلی	بلی	طول بسته پروتکل