سامانهٔ دوسطحی تشخیص نفوذ برای شبکهٔ اینترنت اشیا، مبتنی بر یادگیری عمیق

احمد تیموری [۱]، محمود دی‌پیر [۲]*

کارشناس‌ارشد گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی، واحد تهران جنوب، تهران، ایران[۱]

دانشیار، دانشکدهٔ مهندسی کامپیوتر، دانشگاه هوایی شهید ستاری، تهران، ایران[۲]

چکیده

به موازات رشد استفاده از شبکه‌های اینترنت اشیا برای کاربردهای مختلف، تهدیدات و حملات مربوط به این نوع شبکه‌ها نیز افزایش پیدا کرده‌است. سامانه‌های تشخیص نفوذ به‌منظور تشخیص و شناسایی حملات در این‌گونه شبکه‌ها طراحی و مورد استفاده قرار می‌گیرند و اقدام به شناسایی خرابکاری‌ها و نفوذها و یا سوءاستفاده‌هایی که از شبکه قرار است صورت بگیرد، کرده و این موضوع را به اطلاع مسئول مربوطهٔ شبکه می‌رسانند. در بیشتر سامانه‌های تشخیص نفوذ، روش‌ها و الگوریتم‌های مختلفی از جمله الگوریتم‌های مبتنی بر یادگیری ماشین و یادگیری عمیق استفاده می‌شود که هر کدام دارای مزایا و معایبی هستند، اما به طور معمول نسبت به روش‌های ترکیبی نرخ صحت کمتری دارند. در سال‌های اخیر در تشخیص مبتنی بر ناهنجاری از ایدهٔ ترکیب طبقه‌بندها استفاده شده‌است. ما در این پژوهش، برای افزایش سرعت الگوریتم در شناسایی و دستیابی به نرخ درستی و صحت بالاتر از ترکیب روش‌های تحلیل مؤلفهٔ اصلی یا (PCA) و شبکه‌های عصبی پیچشی(CNN) برای طراحی سامانهٔ تشخیص نفوذ پیشنهادی خود استفاده کرده‌ایم؛ از PCA به‌منظور کاهش ابعاد و حجم داده‌های ورودی بهره بردیم تا به افزایش کارایی الگوریتم اصلی ما کمک کند و دادهٔ جدید تولیدشده با این الگوریتم در اختیار طبقه‌بند CNN قرار می‌گیرد؛ همچنین ما از دو سطح از دسته‌بندی مبتنی بر شبکهٔ عصبی عمیق پیچشی دودویی و چندطبقه برای شناسایی حملات بهره بردیم. به این صورت که ابتدا حملات و داده‌های نرمال به‌وسیلهٔ طبقه‌بند عمیق دودویی از هم جداسازی می‌شوند؛ سپس به‌وسیلهٔ طبقه‌بند عمیق چندطبقه به شناسایی و تفکیک نوع حملات صورت‌گرفته پرداخته شده و دسته‌بندی حملات صورت می‌گیرد. بر اساس نتایج آزمایش‌های انجام‌شده روی داده‌های واقعی حملات، شاهد رشد نرخ صحت و درستی روش پیشنهادی نسبت به بسیاری از روش‌های مطرح دیگر بوده‌ایم.

واژگان کلیدی: سامانهٔ تشخیص نفوذ، شبکهٔ عصبی پیچشی، طبقه‌بند دودویی، طبقه‌بند چندطبقه، تحلیل مؤلفه‌های اصلی.

Two-level intrusion detection system for Internet of Things network based on deep learning

Ahmad Teymouri[1], Mahmood Deypir[2]*

Master, Computer Engineering Department, Islamic Azad University, Tehran, Iran[1]

Associate Professor, Shahid Sattari Aeronautical University of Science and Technology, Tehran, Iran [2]*

Abstract

Along with the growth in the use of Internet of Things networks for various applications, threats and attacks related to these types of networks have also increased. Intrusion detection systems are designed and used to detect and identify attacks in this type of networks, and to identify intrusions or abuses that are going to take place from the network, and to inform the relevant authorities about this issue. In most intrusion detection systems, various methods and algorithms are used, including deep neural networks

* نویسندهٔ عهده‌دار مکاتبات

* Corresponding author

• تاریخ ارسال مقاله: ۱۴۰۲/۴/۳۰ • تاریخ پذیرش: ۱۴۰۳/۵/۲۸ • تاریخ انتشار: ۱۴۰۳/۱۰/۲۸ • نوع مطالعه: پژوهشی

سال ۱۴۰۳ شمارهٔ ۳ پیاپی ۶۱

[DOI: 10.61186/jsdp.21.3.3]

(DNNs), support vector machines (SVM), or multilayer perceptron (MLP), and other traditional machine learning models. Each method has advantages and disadvantages, but it usually has a lower accuracy rate than combined methods. In recent years, the idea of combining classifications has been used for anomaly-based diagnosis. In this research, to reach better accuracy, we used the combination of principal component analysis (PCA) and convolutional neural network (CNN) algorithms to design our intrusion detection system. In the initial step of the proposed method, after preprocessing including conversions and normalizations, valuable features for classification are extracted. In this study, the NSL-KDD dataset, which has been mentioned in many scientific articles as a valid reference dataset in the field of intrusion detection, has been used. In fact, due to the high number of data dimensions and the high dispersion of feature values, we used a dimension reduction method. The dimensionality reduction method used in this research is principal component analysis (PCA). In the PCA method, the dimensions of the data are reduced in such a way that the reduced dimension data also includes the vital information of the dataset. We used PCA in order to reduce the size and volume of the input data to help increase the efficiency of our main algorithm and the new data generated with this algorithm is provided to the CNN classifier. A convolutional neural network is a special type of neural network with multiple layers that processes data that has a grid arrangement and then extracts important features from them. Here, accurate pattern learning and deep insight from the given data are our two main reasons for using CNN. In the proposed approach, we have two level classification including binary CNN and multi-class CNN, for detecting attacks and exact type of them, respectively. That is, firstly attacks and normal data are identified by binary classification and then by multi-class classification, the types of attacks are identified and separated. In fact, the type of attacks which includes one of DoS, U2R, R2L and Probe cases is determined using second convolutional neural network. Based on the obtained results, we have witnessed the growth of the accuracy rate of the proposed method compared to many other popular methods. In the evaluation of accuracy parameter values for different phases of training and testing, competitive results are observed for binary classification phase. Here we consider the number of 15 rounds. As it is clear from the graph related to training, the accuracy values in the final courses have reached 0.94. The accuracy of the test has also approached the value of 0.9 in the last round. Also, the results obtained in multi-class CNN are such that the accuracy value is 0.99 in the classification of the training data samples and 0.97 in the classification of the test data samples. Moreover, the cost graphs for training and testing courses of multi-class CNN are shown. The cost of training and testing in the final round is 0.06 and 0.09, respectively.

Keywords: Intrusion detection system, Convolutional neural network (CNN), Binary classifier, Multi-class classifier, Principal component analysis (PCA).

۱-مقدمه

امروزه با رشد روزافزون ابزار و صنایع ارتباطی و مخابراتی، شاهد تأثیرات قابل توجه فناوری اطلاعات در بخش‌های مختلف هستیم. یکی از این بخش‌ها اینترنت اشیا (IOT) است. اینترنت اشیا عبارت است از شبکه‌ای از اشیای فیزیکی که به‌وسیلهٔ اینترنت به هم متصل شده‌اند. IOT نخستین بار توسط کوین اشتون در سال ۱۹۹۹ مورد استفاده قرارگرفت. اینترنت اشیا به ما اجازه می‌دهد که اشیای روزمره را به اشیا هوشمندی که می‌توانند بفهمند و به محیط واکنش نشان دهند، تبدیل کنیم. اینترنت اشیای ظهورکرده در نسل حاضر که میلیون‌ها دستگاه و اشیا را به هم متصل کرده، هدفی جذاب برای هکرهاست. با وجود توسعهٔ IOT در سال‌های اخیر، بااین‌حال فناوری‌های مبتنی بر IOT هنوز در مراحل ابتدایی‌اند که باید بسیاری از مشکلات فنی در IOT برطرف شود. یکی از مهم‌ترین چالش‌ها در IOT امنیت است که شامل امنیت زیرساخت‌ها، امنیت شبکهٔ ارتباطی، امنیت نرم‌افزار و امنیت عمومی سامانه است. تهدیداتی که می‌تواند بر نهادهای اینترنت اشیا تأثیر گذارد متعددند؛ مانند حملات با هدف کانال‌های ارتباطی مختلف، تهدیدات فیزیکی، محرومیت از خدمات، ساخت هویت و بسیاری موارد دیگر[۴].

یکی از کارآمدترین روش‌های تشخیص نفوذ در اینترنت اشیا، روش‌های مبتنی بر یادگیری ماشین است. یادگیری ماشین به تنظیم و اکتشاف شیوه‌ها و الگوریتم‌هایی می‌پردازد که بر اساس آن‌ها رایانه‌ها و سامانه‌ها توانایی تعلیم و یادگیری پیدا می‌کنند. هدف یادگیری ماشین این است که رایانه‌ها و سامانه‌ها بتوانند به‌تدریج و با افزایش داده‌ها کارایی بهتری در انجام وظیفهٔ موردنظر پیدا کنند. طیف پژوهش‌هایی که در حوزهٔ یادگیری ماشین انجام می‌شود، گسترده است. به لحاظ نظری پژوهش‌گران بر آن‌اند که روش‌های یادگیری تازه‌ای به وجود بیاورند و امکان‌پذیری و کیفیت یادگیری را برای روش‌های خود مطالعه کنند و در سوی دیگر عده‌ای از پژوهش‌گران سعی می‌کنند روش‌های یادگیری ماشینی را بر مسائل تازه‌ای اعمال کنند. یادگیری ماشین کمک فراوانی به صرفه‌جویی در هزینه‌های عملیاتی و بهبود سرعت عمل تجزیه و تحلیل داده‌ها می‌کند[۱۳].

[DOI: 10.61186/jsdp.21.3.3]

نتایج حاصل‌شده از پژوهش‌ها در حوزهٔ یادگیری ماشین و یادگیری عمیق در سال‌های اخیر نشان‌دهندهٔ کارایی بالای این روش‌ها در مقایسه با سایر روش‌هاست؛ درنتیجه ارائهٔ یک روش تشخیص نفوذ در اینترنت اشیا با استفاده از یادگیری عمیق یک موضوع پژوهشی جذاب و روش کارآمد در زمینهٔ امنیت اینترنت اشیا است. در ادامه به پیشینهٔ موضوع، بیان مسئله، معرفی روش پیشنهادی و اهمیت پژوهش و درنهایت اقدام به ارزیابی این روش و همچنین نتیجه‌گیری نهایی خواهیم پرداخت.

۲-پیشینه

در این بخش به بررسی برخی از روش‌های سنتی ارائه‌شده در پژوهش‌ها برای تشخیص نفوذ در IOT می‌پردازیم. در ادامهٔ بررسی مقالات با تمرکز بر روی معماری، مکانیسم تشخیص نفوذ و حملات رفع‌شده (درمان‌شده) انجام می‌گیرد؛ نخستین سامانهٔ NIDS در IOT توسط رضا شهید و همکاران در منبع [۱۸] تحت عنوان SVELTE طراحی و پیاده‌سازی شد. این سامانه یک سامانهٔ بلادرنگ[1] در تشخیص نفوذ بود که بر اساس hybrid signature و روش‌های تشخیص آنومالی طراحی شد. تمرکز کار در این پژوهش بر روی حملات مسیریابی از قبیل spoofing و sinkhole است. این سامانه سه ماژول را ادغام می‌کند: 6Mapper که وظیفهٔ فراهم‌کردن اطلاعات را برعهده دارد، یک مؤلفهٔ تشخیص نفوذ بر اساس تحلیل داده‌های نگاشت‌شده و یک دیوار آتش کوچک[2] که برای نودهای offload با استفاده از پالایهٔ ترافیک‌های ناخواسته قبل از ورود منابع توسعه داده شده‌است. SVELTE در سیستم عامل Contiki پیاده‌سازی شد. این سامانه موفق شد حملات sinkhole را با نرخ ۹۰٪ TPR[3] در یک شبکهٔ کوچک با اتلاف[4] و تقریباً ۱۰۰٪ TPR در شبکه بدون اتلاف[5] تشخیص دهد؛ باوجوداین، مشکل اصلی این سامانه در تشخیص حملات Dos بود.

کاسینتن و همکاران در منبع [۲] در یک پژوهش به مطالعه و بررسی حملات DOS در IOT پرداختند. با وجود IDS Probe های توزیع‌شده، معماری ارائه‌شده یک معماری متمرکز است. در حقیقت IDS Probe ها که ماژول‌های خارجی‌اند، شبکه را در حالت بی‌قاعده[6] اسنیف می‌کنند و سپس داده‌ها را از طریق یک ارتباط سیمی به سمت NIDS اصلی می‌فرستند. زمانی‌که ترافیک با امضای یک حمله مطابقت داده شد یک هشدار به سمت مدیریت حفاظت Dos ارسال می‌شود. مدیر شبکه، حفاظت حمله را با یک‌سری اطلاعات اضافی جمع‌آوری‌شده آنالیز کرده و نرخ هشدار اشتباه[7] را کاهش می‌دهد. این راه‌حل محدودیت موجود در SVELTE را از بین می‌برد؛ زیرا این تشخیص نفوذ به معماری وابسته نیست؛ درنتیجه حملات Dos در شبکهٔ IOT روی آن تأثیری نمی‌گذارد.

جان در منبع [۱۹] یک IDS برای سامانه‌های IOT بر اساس فناوری پردازش رویداد پیچیده[8] (CEP) که یک فناوری کارآمد و نوظهور در پالایه و پردازش رویدادهای بلادرنگ است، پیشنهاد داد. این یک راه‌حل ایده‌آل برای پیام‌های با حجم زیاد و با تأخیر کم بود. درنتیجه این فناوری می‌تواند برای نیازهای IOT نیز مورد استفاده قرار گیرد. درواقع آن‌ها یک عملکرد برخط را به جای خارج از خط ارائه کردند. این سامانه با جمع‌آوری داده از دستگاه‌های IOT شروع به کار، سپس رویدادها را از داده‌ها استخراج می‌کند و درنهایت، رویدادهای امنیتی را با استفاده از انبار پردازش رویداد[9] (EPR) و موتور CEP تشخیص می‌دهد. این رویکرد پیشنهادی موجب مصرف CPU زیاد و حافظهٔ کم می‌شود. این سامانه برای 800K داده، ۶۲٪ CPU مصرف و 730MB حافظه اشغال می‌کند. همچنین زمان پردازش آن ۴۲۲ میلی ثانیه است که در حالت کلی نسبت به یک سامانهٔ سنتی IDS عملکرد بهتری دارد.

در ادامه به بررسی روش‌های تشخیص نفوذ در IOT مبتنی بر یادگیری ماشین می‌پردازیم. نوبخت و همکاران در منبع [۵] یک IDS مبتنی بر میزبان تحت عنوان IOT-IDM برای دستگاه‌های هوشمند در محیط‌های یک خانهٔ هوشمند ارائه کردند. IOT-IDM به منظور تشخیص حملات، ترافیک در جریان بین دستگاه‌ها را پایش می‌کند. این سامانه از معماری شبکهٔ نرم‌افزار محور[10] (SDN) بهره می‌برد و همچنین از روش‌های یادگیری ماشین برای حفاظت از میزبان‌ها و کاهش حملات استفاده می‌کند. IOT-IDM درکل از پنج ماژول مجزا تشکیل می‌شود که عبارت‌اند از: مدیریت دستگاه‌ها[11]، حس‌گر، استخراج‌کنندهٔ ویژگی،

[1] Real time
[2] Mini firewall
[3] True positive rate
[4] Lossy
[5] Lossless
[6] Promiscuous mode
[7] False alarm rate
[8] Complex Event Processing
[9] Event Processing Repository
[10] Software defined networking
[11] Device Manager

[DOI: 10.61186/jsdp.21.3.3]

واحد تشخیص و واحد کاهش[1]. در این رویکرد پیشنهادی از روش‌های ماشین بردار پشتیبان[2] (SVM) و رگرسیون ترابری[3] برای تشخیص نفوذ استفاده شده‌است. نتایج به‌دست‌آمده برای روش رگرسیون ترابری شامل مقدار دقت ۹۴/۲۵ ٪ و صحت ۸۵/۰۵٪ است. همچنین به ازای روش SVM مقدار دقت و صحت به‌ترتیب ۹۸/۵۳ ٪ و ۹۵/۹۴ ٪ گزارش شده‌است.

بستانی و شیخانی در منبع [۶] یک IDS بلادرنگ ترکیبی و مبتنی بر آنومالی ارائه کردند؛ این IDS قادر به تشخیص حملات Sinkhole و حمل‌ونقل[4] در شبکه‌های 6LowPAN است. این IDS دارای دو گام اصلی است: تشخیص مشخصات در سطح مسیریاب‌ها و تشخیص آنومالی در سطح ریشه. در گام نخست مسیریاب‌ها ویژگی‌های شبکه مانند ترافیک و نودهای میزبان را آنالیز می‌کنند. نتایج گام نخست به سمت نود ریشه برای گام دوم ارسال و به‌منظور کاهش مصرف حافظه و پردازنده، اطلاعات آن‌ها از مسیریاب‌ها حذف می‌شود. در گام دوم، تشخیص حمله انجام می‌گیرد به‌طوری‌که بر اساس داده‌های واردشده به نود ریشه تشخیص آنومالی انجام می‌گیرد. در این مرحله از الگوریتم مسیر بهینهٔ جنگل بدون نظارت برای ساخت مدل خوشه‌بندی استفاده می‌شود. همچنین از معماری نگاشت - کاهش[5] برای پیاده‌سازی موازی و توزیع‌شدهٔ خوشه‌ها بهره گرفته می‌شود. نویسندگان پس از شبیه‌سازی این IDS نتایج خود را در سه آزمایش اصلی گزارش کردند: در آزمایش نخست تمرکز آن‌ها روی معیارهای ارزیابی بود، در آزمایش دوم بر روی مقیاس شبکه‌ها از نظر اندازه و در نهایت در آزمایش سوم بر روی توسعهٔ روش خود برای تشخیص دیگر حملات تمرکز کردند.

از دیگر روش‌های تشخیص نفوذ مبتنی بر یادگیری ماشین می‌توان به روش تینگ در منبع [۷] که یک روش تشخیص نفوذ و طبقه‌بندی حملات در شبکه‌های بی‌سیم است، اشاره کرد. در این روش نیز از یک خودرمزنگار عمیق با معماری شامل دو و سه لایهٔ پنهان استفاده شده‌است. نویسنده از توابع فعال‌ساز[6] مختلفی در لایه‌های پنهان استفاده کرده‌است. او به منظور آزمایش و ارزیابی روش خود، یک دادگان را با استفاده از یک آزمایشگاه شبیه‌سازی‌شده در SOHO[7] تولید کرد. طبق نتایج گزارش ادعا شده که به دقت ۹۸/۶۶ ٪ در طبقه‌بندی چهارکلاسه رسیده‌است.

یک IDS دیگر مبتنی بر محاسبات مه[8] با استفاده از ماشین فرایادگیری متوالی برخط توسط پراباواتی و همکاران در منبع [۱] ارائه شد. سازوکار پیشنهادی جنبه‌هایی از IOT از قبیل: قابلیت انعطاف، مقیاس‌پذیری و ناهمگنی را مورد توجه قرار داده‌است. این روش از دو بخش اصلی تشکیل شده‌است: بخش نخست تشخیص حمله در نودهای مه است که نویسندگان از الگوریتم OS-ELM برای تشخیص نفوذ نودهای مه استفاده کردند. در اینجا شبکهٔ IOT به خوشه‌های مجازی تقسیم می‌شود، به‌طوری‌که هر خوشه متعلق به گروهی از دستگاه‌ها و تحت نظارت یک نود مه است. OS-ELM پکت‌ها را در دو دستهٔ نرمال و حمله طبقه‌بندی می‌کند. ELM یک لایهٔ پنهان شبکهٔ عصبی با یک گام یادگیری سریع است. بخش دوم خلاصه‌سازی در سرور ابر است که در این ایده تشخیص نفوذ، حملات تشخیص داده شده از سمت نود مه به سمت نود سرور ارسال می‌شوند. پس از تحلیل حملات، نویسندگان دو اقدام را پیشنهاد دادند: ۱)پیش‌بینی حملات بعدی با استفاده از یک رویکرد تشخیص حمله یا ۲)تشخیص موقعیت جغرافیایی نود مه چندمرحله‌ای و حملاتDDOS.

راتور و پارک در منبع [۸] یک NIDS مبتنی بر الگوریتم C-Means فازی و ELM، با استفاده از یک تشخیص‌دهندهٔ مه جدید ارائه کردند. این IDS توزیع‌شده، توزیع جغرافیایی و تأخیر پایین در تشخیص را با وجود محدودیت‌های منابع و شبکه، با محاسبات مه کنترل می‌کند. با وجود دقت خوب در الگوریتم‌های یادگیری ماشین با نظارت، اما این الگوریتم‌ها قادر به تشخیص حملات ناشناخته و جدید نیستند. الگوریتم‌های بدون نظارت نیز با وجود تشخیص حملات ناشناخته، دارای دقت پایین‌تری هستند؛ لذا یک روش یادگیری نیمه‌نظارتی[9] با استفاده از الگوریتم‌های با نظارت و بدون نظارت برای داده‌های ورودی با برچسب و بدون برچسب ارائه شده‌است.

دیرو و همکاران در منبع [۹] از محاسبات مه برای تشخیص نفوذ در IOT استفاده کردند. در حقیقت آن‌ها لایهٔ مه را به یک پردازش اطلاعات هوشمند مجهز کردند؛ این فناوری توانایی تشخیص حملات به صورت توزیع‌شده را دارد و از نظر مقیاس‌پذیری، تشخیص حملات محلی، یادگیری داده‌ها در نزدیکی منابع و اشتراک‌گذاری پارامترهای همسایگان، کارایی بالایی دارد. نویسندگان یک

[1] Mitigation
[2] Support Vector Machine
[3] Logistic Regression
[4] Forwarding
[5] Map-Reduce
[6] Activation functions
[7] Small Office Home Office
[8] Fog Computing
[9] Semi-Supervised

[DOI: 10.61186/jsdp.21.3.3]

رویکرد مبتنی بر یادگیری عمیق برای تشخیص حملات شناخته‌شده و ناشناخته ارائه کردند.

ناصری و همکاران در منبع [۲۰] به انتخاب ویژگی بر اساس الگوریتم باروری مزرعه برای سامانه‌های تشخیص نفوذ بهبودیافته پرداختند. در این مقاله، یک نسخهٔ دودویی از الگوریتم باروری زمین‌های کشاورزی به نام BFFA در طبقه‌بندی IDSها به FS ارائه شده‌است. در روش پیشنهادی از تابع V شکل برای جابه‌جایی فرایندهای FFA در فضای باینری استفاده می‌شود که در نتیجه تابع V شکل، موقعیت پیوستهٔ راه حل‌ها را در الگوریتم FFA به حالت باینری تغییر می‌دهد. یک رویکرد ترکیبی برای طبقه‌بندی‌کننده‌ها و BFFA به‌عنوان یک IDS سریع و قوی ارائه شده‌است. روش پیشنهادی بر روی دو مجموعه‌دادهٔ IDS معتبر، یعنی NSL-KDD و UNSW-NB15 آزمایش می‌شود و در معیارهای دقت، دقت، یادآوری و امتیاز F1 با K- نزدیک‌ترین همسایه KNN، ماشین بردار پشتیبانی SVM تصمیم مقایسه می‌شود. طبقه‌بندی‌کننده‌های Tree، Random Forest، Adaboost و Naive Bayes نتایج شبیه‌سازی نشان داد که روش پیشنهادی بهتر از طبقه‌بندی‌کننده‌ها در معیارهای دقت، دقت و یادآوری عمل می‌کند؛ علاوه‌براین، روش پیشنهادی زمان اجرای بهتری در عملیات FS دارد.

املاپوران و همکاران در منبع [۲۱] به یادگیری مستمر برای تشخیص نفوذ شبکهٔ مبتنی بر ناهنجاری پرداختند. برای دفاع از سامانه‌های محاسباتی در برابر حملات سایبری روبه‌رشد، سامانه‌های تشخیص نفوذ شبکه مبتنی بر ناهنجاری باید مداوم تکامل یابند. شبکه‌های عصبی(NN) زمانی که بر روی داده‌های متوالی آموزش داده می‌شوند، مستعد فراموشی فاجعه‌بار(CF) هستند. پیشرفت‌های اخیر در پرداختن به این اشکال NN منجر به الگویی به نام یادگیری مستمر (CL) شده‌است که با معرفی محدودیت‌های مناسب در طول آموزش متوالی این NNها، CF را کاهش می‌دهد. CL در بهبود عملکرد NN در وظایف بینایی کامپیوتر بسیار مؤثر است. در این مقاله، مناسب‌بودن CL را برای رسیدگی به چالش‌های مطرح‌شده در طراحی IDS ارزیابی کرده‌است؛ برای این منظور، دو الگوریتم محبوب CL در این مقاله استفاده شده‌است. Elastic Weight Consolidation (EWC) و Gradient Episodic Memory (GEM) روی دو مجموعه‌داده یعنی CICIDS و KDD Cup'99، ارزیابی شده‌است.

تیکسیریا و همکاران در منبع [۲۲] به معماری مبتنی بر رأی برای تولید مجموعه‌داده‌های طبقه‌بندی‌شده و بهبود عملکرد سامانه‌های تشخیص نفوذ بر اساس یادگیری نظارت‌شده پرداختند. سامانهٔ تشخیص نفوذ ابزار مهمی برای جلوگیری از تهدیدات احتمالی برای سامانه‌ها و داده‌هاست. این مقاله یک معماری مبتنی بر رأی را برای تولید مجموعه‌داده‌های طبقه‌بندی‌شده و بهبود عملکرد IDS های مبتنی بر یادگیری نظارت‌شده پیشنهاد می‌کند. به طور منظم، چندین IDS در مکان‌های مختلف، گزارش‌های خود را به یک سامانهٔ مرکزی ارسال می‌کنند که آن‌ها را با استفاده از مدل‌های مختلف یادگیری ماشینی و سامانهٔ رأی اکثریت ترکیب و طبقه‌بندی می‌کند. سپس یک مجموعه‌دادهٔ جدید و طبقه‌بندی‌شده تولید می‌کند که برای به‌دست‌آوردن بهترین مدل به‌روزشده برای ادغام در IDS شرکت‌های درگیر آموزش داده می‌شود. معماری پیشنهادی چندین‌بار با چندین الگوریتم آموزش می‌بینند. برای کوتاه‌کردن زمان اجرای کلی، معماری پیشنهادی منابع موجود خود را به صورت توزیع‌شده استفاده می‌کند. مجموعه‌ای از الگوریتم‌های یادگیری ماشین در معماری پیشنهادی مورد ارزیابی قرار گرفته‌است. در مقایسه با سناریوی مقالهٔ پایهٔ خود، معماری پیشنهادی امکان افزایش دقت را تا ۱۱٪ فراهم کرده‌است.

غروی و همکاران در منبع [23] از شبکه‌های عصبی عمیق برای بهبود بازنمایی متن استفاده کرده‌اند. یافتن یک بازنمایی معنایی غنی با ابعاد کم برای متون طولانی یکی از چالش‌های اساسی در فعالیت‌های مختلف پردازش زبان طبیعی به شمار می‌رود؛ این بازنمایی باید اطلاعات معنایی و نحوی متن را دربرگیرد و همچنین، بر حسب وظیفهٔ مدنظر ارتباط و تشابه متون را در ابعاد کم الگوسازی کند. در این مقاله تلاش بر آن است تا با بهره‌گیری از نظریهٔ ساختار بلاغی و شبکه‌های عصبی عمیق چالش‌های مطرح‌شده مرتفع شود.

نظریهٔ ساختار بلاغی با ارائهٔ یک ساختار سلسله‌مراتبی به توصیف اهمیّت عبارات موجود در متن و روابط بین آن‌ها می‌پردازد. در اینجا تأثیر به‌کارگیری این ساختار درختی بر دو وظیفهٔ بازیابی اطلاعات و تحلیل احساسات بررسی شده‌است. در وظیفهٔ بازیابی اطلاعات، جهت الگوسازی وابستگی معنایی بین مستندات، یادگیری بازنمایی سند با شبکه‌های عصبی بازگشتی عمیق بازگشتی عمیق تشکیل دوقلو انجام شد؛ به‌طوری که ذخیره و بازیابی مستندات متنی تسهیل شود؛ این شبکه از دو زیرشبکه تشکیل شده‌است و این شبکه‌های بازگشتی، مبتنی بر ساختار درختی حاصل از تجزیهٔ متن با نظریهٔ ساختار بلاغی هستند.

[DOI: 10.61186/jsdp.21.3.3]

عباسی و همکاران در منبع[24] از الگوریتم‌های بهینه‌سازی برای خوشه‌بندی ترکیبی با بیشینه‌سازی ترکیبی استفاده کرده‌اند. خوشه‌بندی داده‌ها یکی از مراحل اصلی در داده‌کاوی است که وظیفهٔ کاوش الگوهای پنهان در داده‌های بدون برچسب را بر عهده دارد. به خاطر پیچیدگی مسئله و ضعف روش‌های خوشه‌بندی پایه، امروزه بیشتر مطالعات به‌سمت روش‌های خوشه‌بندی ترکیبی هدایت شده‌است. پراکندگی در نتایج اولیه یکی از مهم‌ترین عواملی است که می‌تواند در کیفیت نتایج نهایی اثرگذار باشد؛ همچنین، کیفیت نتایج اولیه نیز عامل دیگری است که در کیفیت نتایج حاصل از ترکیب مؤثر است. هر دو عامل در پژوهش‌های اخیر خوشه‌بندی ترکیبی مورد توجه قرار گرفته‌اند. در اینجا یک چارچوب جدید برای بهبود کارایی خوشه‌بندی ترکیبی پیشنهاد شده که مبتنی بر استفاده از زیرمجموعه‌ای از خوشه‌های اولیه است. روش ارائه‌شده نشان می‌دهد که استفاده از زیرمجموعه‌ای از نتایج خوشه‌بندی‌های اولیه می‌تواند بهتر از استفاده از کل نتایج باشد همچنین معیاری را پیشنهاد می‌دهد که چگونه نتایج اولیه نسبت به هم ارزیابی شوند. این پژوهش معیاری ارائه می‌دهد که به وسیلهٔ آن می‌توان تشخیص داد کدام زیرمجموعه از نتایج اولیه می‌تواند منجر به بهبود عملکرد خوشه‌بندی ترکیبی شود.

۳-بیان مسئله

اینترنت اشیا یا IoT، سامانه‌ای به‌هم‌پیوسته از تجهیزات رایانه‌ای، ماشین‌های مکانیکی و دیجیتال، اشیا، حیوانات یا افرادی است که با شناسه‌های منحصربه‌فرد (UID) هویت یافته‌اند و از قابلیت انتقال داده‌ها روی یک شبکه بدون نیاز به تعامل انسان-با-انسان یا انسان-با-رایانه برخوردارند. یک شی در اینترنت اشیا می‌تواند انسانی باشد که یک دستگاه پایش قلب در بدنش نصب شده‌است؛ یا دامی با یک ترانسپوندر بیولوژیک، یا خودرویی که با حس‌گرهای تعبیه‌شده در آن، راننده را از فشار کم لاستیک‌ها آگاه می‌کند یا هر شی طبیعی یا انسان‌ساخت دیگر که می‌تواند با اختصاص یک نشانی IP داده‌ها را روی یک شبکه انتقال دهد[۱۲].

دستگاه‌های IOT که از شبکه‌های بی‌سیم برای ارسال و دریافت اطلاعات استفاده می‌کنند، همواره در معرض حملات مختلف قرار دارند. برخلاف حملات معمول به شبکه‌های محلی که در بخش‌ها و دامنه‌های خاصی محدود می‌شوند، حملات در IOT طیف گسترده‌تری را دربرگرفته و منجر به بروز مشکل در بخش‌های متعددی از قبیل تارنماها، برنامه‌ها، شبکه‌های اجتماعی و سرورهای IOT می‌شوند. با توجه به رشد و تأثیرگذاری IOT در حوزه‌های مختلف مانند آموزش، توزیع انرژی، اقتصاد، مراقبت پزشکی، حمل‌ونقل، سرگرمی و ... باید این مسئله مورد توجه ویژه قرار گیرد. در مواجهه با این چالش ضروری است که دستگاه‌ها و تجهیزات IOT از نظر آسیب‌پذیری مورد توجه ویژه‌ای قرار گیرند. امروزه در دنیای تجارت، داده‌ها یکی از سرمایه‌های بسیار مهم برای ذی‌نفعان تلقی می‌شوند؛ ازاین‌رو، تشخیص نفوذ در IOT می‌تواند تضمین حفاظت از اطلاعات را به همراه داشته باشد.

طبق پژوهش‌های انجام‌شده در سال ۲۰۲۲، پانزده میلیارد دستگاه هوشمند در دنیا وجود داشت که با توجه به پیشرفت فناوری این مقدار به ارقام بسیار بالاتری خواهد رسید. در این راستا تعدادی از چالش‌ها و مسائل مربوط به IoT، از ایجاد امنیت تا یکپارچه‌سازی ارتباطات وجود دارند که ادغام بسیاری از این مسائل با هم، پیچیدگی‌ها و چالش‌هایی را ایجاد کرده‌است. بر همین اساس ما با ماهیت چالش‌برانگیز نقص‌های امنیتی جدیدی در برابر اینترنت اشیا مواجهیم. پروتکل‌های مسیریابی در اینترنت اشیا همیشه با چالش‌های امنیتی مواجه بوده‌است. اینترنت اشیا مزایای زیادی برای کاربران به ارمغان آورده‌است؛ بااین‌حال، برخی از چالش‌ها همراه آن است. امنیت سایبری و خطرات مربوط به حفظ حریم خصوصی مهم‌ترین نگرانی پژوهش‌گران و متخصصان امنیتی است که به آن‌ها اشاره شده‌است. این دو موضوع چالش‌های قابل توجهی برای بسیاری از سازمان‌های تجاری و همچنین سازمان‌های عمومی به وجود آورده‌است. حملات رایج و شایع امنیت سایبری، آسیب‌پذیری فناوری‌های اینترنت اشیا را نشان می‌دهد. این آسیب‌پذیری فقط به این دلیل است که ارتباط متقابل شبکه‌ها در اینترنت اشیا امکان دسترسی از طریق فرد یا دستگاه ناشناس و غیرقابل اعتماد را فراهم می‌کند که نیاز به راه حل‌های جدید امنیتی دارد. از بین تمام چالش‌هایی که شناخته شده‌است، هیچ‌یک از آن‌ها تأثیر قابل توجهی در سازگاری اینترنت اشیا، مانند امنیت و حریم خصوصی ندارند. با نقض مداوم امنیت که حریم خصوصی کاربران را به خطر انداخته است، اکنون تمایل مصرف‌کنندگان برای افزایش امنیت سامانه‌ها بیشتر شده‌است[۳].

انواع چالش‌های امنیتی اینترنت اشیا را می‌توان به حریم خصوصی، امنیت سایبری، ارتباطات و پروتکل‌های مسیریابی، چالش‌های سخت‌افزاری و امنیت داده

[DOI: 10.61186/jsdp.21.3.3]

تقسیم‌بندی کرد. برای غلبه بر این چالش‌های امنیتی، نیازمند سامانه‌های تشخیص و مقابله با نفوذ هستیم[۱۴]؛ بنابراین مسئلهٔ پژوهش ما ایجاد یک سامانهٔ تشخیص نفوذ هوشمند برای اینترنت اشیا است که بتواند حملات امنیتی و نفوذهای شبکه را از ترافیک نرمال تشخیص دهد. علاوه بر تشخیص حمله باید بتوانیم نوع حمله را نیز تشخیص دهیم تا راهکار مناسب هر حمله یا چالش امنیتی را برای مقابله با آن درنظر بگیریم. سامانهٔ تشخیص نفوذی که برای اینترنت اشیا طراحی و پیاده‌سازی می‌شود باید علاوه بر اینکه دقت لازم را داشته باشد، توان پردازشی و انرژی محدود دستگاه‌های موجود در این نوع شبکه‌ها را درنظر بگیرد؛ بنابراین باید بتواند با تعداد ویژگی‌های محدود، نرخ تشخیص مناسب و قابل قبولی داشته باشد.

۴-روش پیشنهادی

در این بخش به معرفی کلی روش ارائه‌شده در این پژوهش در قالب نمودار جعبه‌ای و روندنما می‌پردازیم. شکل‌های (۱ و ۲) به ترتیب نمودار جعبه‌ای و روندنما روش پیشنهادی را توصیف می‌کنند. همان‌طور که نمودار جعبه‌ای شکل (۱) نشان داده شده‌است، مرحلهٔ نخست پیش‌پردازش دادگان است؛ در این مرحله، نوع حملات نمونه داده‌های مجموعه‌داده دسته‌بندی و مقادیر ویژگی‌های رسته‌ای[1] به مقادیر عددی تبدیل می‌شوند؛ همچنین در این مرحله دادگان نرمال‌سازی می‌شوند. در مرحلهٔ بعد با استفاده از روش کاهش بعد PCA [۱۶] ابعاد دادگان کاهش یافته و آمادهٔ استفاده برای یادگیری ماشین می‌شوند. در ادامه با استفاده از یک طبقه‌بند (CNN) [۱۷] دودویی[2] که از نوع شبکهٔ یادگیری عمیق است، تشخیص داده می‌شود که آیا نمونهٔ ورودی یک حمله است یا خیرY سپس در صورتی‌که حمله تشخیص داده شود، از یک طبقه‌بند (CNN) چندطبقه[3] برای تشخیص نوع حمله استفاده می‌شود؛ درنهایت نوع حمله که شامل یکی از موارد DoS[4]، U2R[5]، R2L[6] و Probe است تعیین می‌شود؛ بنابراین، در روش پیشنهادی دو سطح یا مرحلهٔ دسته‌بندی داریم؛ سطح نخست دسته‌بندی برای تشخیص حمله یا عدم‌حمله در ترافیک ورودی و سطح دوم که نوع حملهٔ انجام‌شده در صورت تشخیص حمله در سطح نخست را مشخص می‌کند. در بخش‌های بعد هر یک از مراحل روش پیشنهادی به طور کامل شرح داده می‌شوند.

شکل (۲) روندنمای مراحل روش پیشنهادی را نشان می‌دهد. همان‌طورکه در این شکل پیداست، پس از ورود داده ابتدا پیش‌پردازش داده‌ها به‌منظور دسته‌بندی نمونه‌های ورودی و نرمال‌سازی داده‌ها صورت می‌گیرد، پس از آن با استفاده از روش تحلیل مؤلفه‌های اساسی، عملیات کاهش ابعاد داده‌ها با استفاده از الگوریتم PCA انجام و مجموعه‌دادهٔ جدیدی تشکیل می‌شود که در آن ویژگی‌های کم‌اهمیت حذف می‌شوند.

این ویژگی‌ها تأثیر چندانی در شناسایی حملات یا نوع آن‌ها ندارند و حذف آن‌ها سبب افزایش سرعت کار خواهد شد؛ درواقع این الگوریتم موجب کاهش ابعاد دادگان و حذف برخی ویژگی‌های کم‌اهمیت شده و باعث می‌شود الگوریتم اصلی ما به این داده‌ها نپردازد و همین امر سرعت کار الگوریتم را در شناسایی حملات افزایش خواهد داد و همچنین اثر مثبتی بر روی صحت و دقت کار الگوریتم دارد؛ زیرا وجود ویژگی‌های بیشتر در دادگان می‌تواند موجب خطای الگوریتم در شناسایی حملات شده و برخی داده‌ها به‌عنوان ورودی‌های نرمال شناسایی شوند. پس از آن بخشی از داده‌ها به صورت Train و بخشی هم به صورت Test در اختیار الگوریتم CNN قرار می‌گیرد. مرحلهٔ بعدی انجام آموزش و آزمایش برای ساخت مدل دسته‌بند دودویی CNN به منظور شناسایی ترافیک حمله از ترافیک نرمال است. که خروجی الگوریتم CNN دودویی حملات شناسایی‌شده از داده‌های ورودی است، تا این خروجی در اختیار الگوریتم CNN چندطبقه قرار گیرد. مرحلهٔ بعدی ساخت مدل چندکلاسهٔ CNN برای شناسایی نوع حمله است. برای ساخت این مدل، تنها داده‌هایی که از نوع ترافیک حمله در مرحلهٔ قبلی شناسایی شده‌اند، به‌کار می‌روند. به دلیل وجود چهار نوع دسته‌بندی حملات که در شکل (۱) مشخص‌اند، نیاز به دسته‌بند چندطبقه وجود دارد. در بخش بعد مراحل مربوط به پیش‌پردازش دادگان شرح داده می‌شود. در ادامه به بیان کاهش بعد دادگان پرداخته می‌شود. در دو بخش پایانی نیز طبقه‌بندهای دودویی و چندطبقه بیان می‌شوند.

۴-۱-پیش‌پردازش دادگان

در این مرحله مطابق شکل (۳) که گام ابتدایی روش ارائه‌شده در این پژوهش است، دادگان مورد استفاده پیش‌پردازش می‌شوند. در این پژوهش از دادگان NSL-KDD [۱۵] که به عنوان یک دادگان مرجع معتبر در زمینهٔ تشخیص نفوذ، در بسیاری از مقالات علمی به آن اشاره شده، استفاده شده‌است. پیش‌پردازش دادگان شامل سه مرحلهٔ دسته‌بندی نمونه‌ها بر اساس نوع کلاس، تبدیل

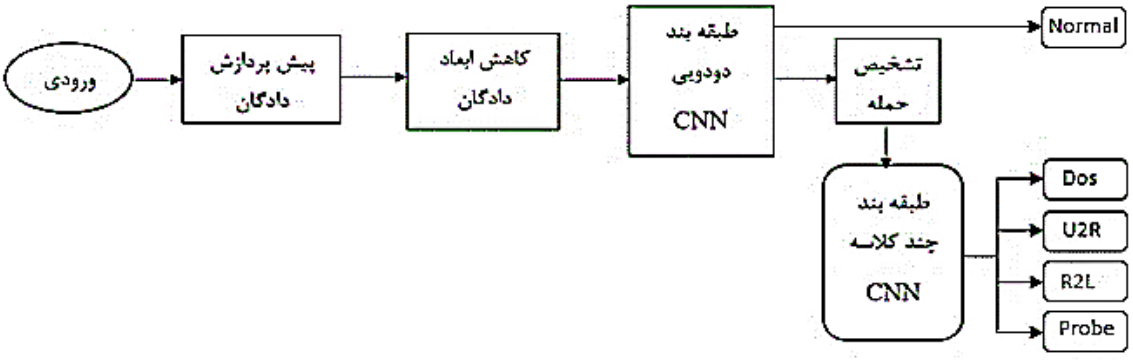
[1] Categorical
[2] Binary Classifier
[3] Multi-class Classifier
[4] Denial-of-Service
[5] User to Root
[6] Root to Local

[DOI: 10.61186/jsdp.21.3.3]

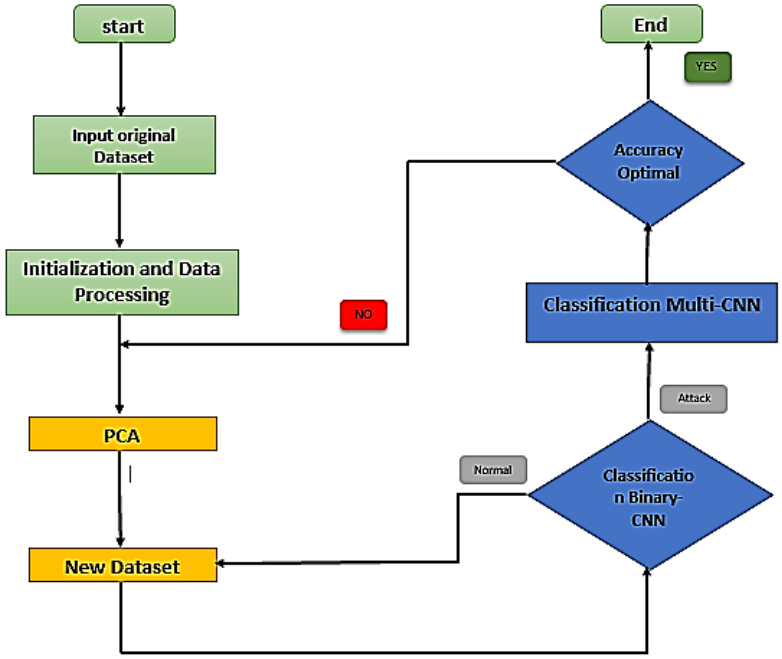
مقادیر رسته‌ای به عددی و نرمال‌سازی است. در ادامه به بررسی هر یک از این مراحل می‌پردازیم.

۱-۱-۴-دسته‌بندی نمونه‌ها

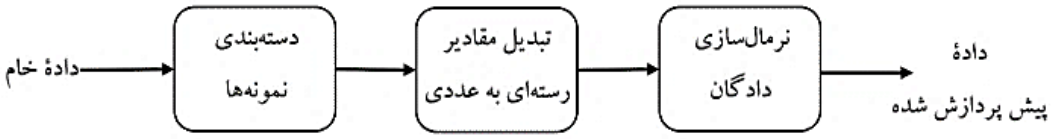
نمونه‌های موجود در دادگان را می‌توان از نظر نوع حمله به چند دستهٔ کلی تقسیم کرد. این دسته‌ها را مطابق آنچه در مقالات معتبر انجام شده‌است، به صورت حملات DoS، U2R، R2L و Probe دسته‌بندی می‌کنیم.



(شکل-۱): نمودار جعبه‌ای روش پیشنهادی
(Figure-1): Block diagram of the proposed method



(شکل-۲): روندنمای روش پیشنهادی
(Figure-2): Flowchart of the proposed method



(شکل-۳): پیش‌پردازش داده‌ها
(Figure-3): Data preprocessing

[DOI: 10.61186/jsdp.21.3.3]

مطابق جدول (۱) هر مجموعه از حملات مشابه نیز در طبقه واحدی قرار گرفته و برچسب زده می‌شوند.

۲-۱-۴-تبدیل مقادیر رسته‌ای به عددی

در این مرحله آن دسته از ویژگی‌هایی که دارای مقادیر رسته‌ای هستند را به عددی تبدیل می‌کنیم؛ بدین منظور از یک روش کدگذاری تحت عنوان LabelEncoder که در کتابخانهٔ SKLearn زبان برنامه‌نویسی پایتون موجود است، استفاده شد. این روش مقادیر غیرعددی ویژگی‌های دادگان را به مقادیر عددی در بازه [0 , n_classes] تبدیل می‌کند، به‌طوری که n_classes تعداد طبقه‌های آن ویژگی است.

(جدول-۱): دسته‌بندی حملات دادگان NSL-KDD
(Table-1): Classification of NSL-KDD data attacks

طبقه حمله	حمله
DoS	netun, back, land, pod, smurf, teardrop
U2R	Buffer-overflow, loadmodule, perl, rootkit
R2L	ftp-write, Guess-passwd, imap, multihop, phf, spy, warezclient, warezmaster
Probe	ipsweep, nmap, portsweep, satan

۳-۱-۴-نرمال‌سازی دادگان

در آخرین گام پیش‌پردازش دادگان که نرمال‌سازی است، تمامی دادگان را نرمـال می‌کنیم. بدین منظور مقادیر دادگان در بازه [۰ و ۱] نرمال می‌شوند. این نرمال‌سازی در رابطهٔ (۱) نشان داده شده‌است.

در این رابطه $x = (x_1 , \dots , x_n)$ نمونه‌داده و z_i i امین مقدار نرمال‌شده هستند.

$$z_i = \frac{x_{i-min(x)}}{\max(x) - \min(x)} \qquad (۱)$$

۲-۴- کاهش بعد دادگان

دادگان NSL-KDD که در این پژوهش مورد استفاده قرار گرفته‌است دارای ۴۱ بعد هستند؛ به عبارت دیگر هر نمونه داده در این دادگان دارای ۴۱ ویژگی است. بالابودن تعداد ابعاد در دادگان، بیشتر الگوریتم‌های یادگیری ماشین را با مشکل مواجه می‌کند. از جمله روش‌های یادگیری ماشین که به‌طورکامل به تعداد ابعاد دادگان حساس‌اند روش‌های مبتنی بر شبکه‌های عصبی مصنوعی و یادگیری عمیق‌اند. در این دسته از روش‌های یادگیری، افزایش ابعاد دادگان (تعداد ویژگی‌ها) موجب کاهش کارایی و در مقابل افزایش تعداد نمونه‌ها منجر به افزایش کارایی می‌شود.

در این پژوهش با توجه به بالابودن تعداد ابعاد دادگان و همچنین پراکندگی[1] بالای مقادیر ویژگی‌ها، از یک روش کاهش بُعد بهره گرفته شده‌است. روش کاهش بُعد مورد استفاده در این پژوهش تحلیل مؤلفه‌های اصلی (PCA) است. در روش PCA ابعاد دادگان به‌گونه‌ای کاهش می‌یابد که دادگان کاهش بُعدیافته همچنان شامل اطلاعات حیاتی و لازم باشند. در ادامه مراحل کاهش بعد دادگان تشخیص نفوذ در IOT به روش PCA را شرح می‌دهیم.

گام نخست در این روش کاهش بعد، نرمال‌سازی دادگان است. از آنجاکه در مرحلهٔ پیش‌پردازش روش پیشنهادی دادگان نرمال‌سازی شد؛ لذا به سراغ گام دوم می‌رویم. در این گام ماتریس کواریانس دادگان را محاسبه می‌کنیم. هدف از انجام این مرحله این است که متوجه شویم داده‌ها چقدر با مقدار میانگین متفاوت است و چه ارتباطی بین آن‌ها وجود دارد. ماتریس کواریانس یک ماتریس متقارن با ابعاد P × P است که P نشان‌دهندهٔ تعداد ابعاد دادگان است؛ این ماتریس مقدار کواریانس بین تمام جفت متغیرها را نشان می‌دهد. ماتریس کواریانس دادگان ما در رابطهٔ شمارهٔ (۲) نشان داده شده‌است. در این رابطه $(x_1 , x_2 , \dots , x_{42})$ نشان‌دهندهٔ بردار ویژگی دادگان هستند. ماتریس Cov دارای ۴۱ سطر و ۴۱ ستون است که این تعداد نشان‌دهندهٔ تعداد ابعاد دادگان NSL-KDD است.

$$Cov = \begin{vmatrix} Cov(x_1x_1) & Cov(x_1x_2)\dots & Cov(x_1x_{42}) \\ Cov(x_2x_1) & Cov(x_2x_2)\dots & Cov(x_2x_{42}) \\ \dots & \dots & \dots \end{vmatrix} \qquad (۲)$$

در ماتریس کواریانس، مقدار مثبت نشان می‌دهد که دو متغیر به هم وابسته[2] هستند؛ به عبارت دیگر، با افزایش و یا کاهش یک متغیر، دیگری نیز به همان صورت تغییر می‌کند؛ همچنین در صورتی که مقدار کواریانس بین دو متغیر منفی باشد، بدین معنی است که دو متغیر وابستگی معکوس[3] به هم دارند؛ یعنی با افزایش یک متغیر، دیگری به همان صورت کاهش می‌یابد و بالعکس.

در مرحلهٔ بعد مقادیر ویژه و بردار ویژهٔ ماتریس کواریانس را محاسبه می‌کنیم. سپس ماتریس مقادیر ویژه (ماتریسی که درایه‌ها قطری آن مقادیر ویژه‌اند) را مطابق رابطهٔ (۳) به دست می‌آوریم. در این رابطه V ماتریس بردارهای ویژه و Cov ماتریس کواریانس است.

$$D = V^{-1}\mathrm{CovV} \qquad (۳)$$

[1] sparseness
[2] correlated
[3] Inverse correlated

[DOI: 10.61186/jsdp.21.3.3]

در ادامه بردارهای ویژه بر اساس مقادیر ویژه متناظر با آن‌ها به صورت کاهشی مرتب می‌شوند. در پایان نیز زیرمجموعه‌ای از بردارهای ویژه به‌عنوان مؤلفه‌های اصلی و بر اساس همان ترتیب مرتب‌شده انتخاب می‌شوند.

۳-۴-طبقه‌بندی دودویی

در روش پیشنهادی ارائه‌شده در این پژوهش ابتدا با استفاده از یک طبقه‌بند دودویی، حمله و یا نرمال‌بودن نمونهٔ ورودی تشخیص داده می‌شود. در این بخش به بررسی این طبقه‌بند دودویی می‌پردازیم. در این طبقه‌بند از شبکه CNN[1] استفاده شده‌است. در ادامه معماری این شبکه را شرح می‌دهیم.

در شکل (۴) معماری شبکهٔ CNN به کار رفته در طبقه‌بند دودویی نشان داده شده‌است. در اینجا نیز نمونهٔ ورودی با چهار ویژگی به صورت (x_1 , x_2 , x_3 , x_4) در لایهٔ ورودی قرار دارد؛ همان‌طور که در شکل مشخص است، در ساختار لایه‌های پنهان این شبکهٔ سه لایهٔ کانولوشن[2]، دو لایهٔ MaxPooling، یک لایهٔ Flatten و در نهایت یک لایهٔ Dense شامل ۳۲ نورون وجود دارد؛ این لایه خروجی لایه‌های قبل را دریافت و اقدام به مرتب‌کردن، تفکیک و ساده‌سازی حملات شناسایی‌شده به‌وسیلهٔ لایه‌های کانولوشنالی کرده و یک بردار ستونی از این داده‌ها تشکیل می‌دهد. اندازهٔ لایه‌های کانولوشن به ترتیب ۱۲۸، ۶۴ و ۳۲ است. لایه‌های کانولوشنالی وظیفهٔ شناسایی و کشف داده‌های سطح بالا را دارند که در روش ما حملات به‌عنوان داده‌های سطح بالا شناسایی می‌شوند و در واقع این لایه‌ها اقدام به بررسی و تجزیه و تحلیل تمام ابعاد داده‌های ورودی کرده و حملات موجود در داده‌های ورودی را شناسایی و یک جدول وضعیت از آن‌ها تشکیل می‌دهد. در لایهٔ خروجی این مدل نیز یک نورون وجود دارد که نشان‌دهندهٔ طبقه نرمال و یا طبقه حمله است.

۴-۴-طبقه‌بند چندطبقه

در بخش قبل معماری طبقه‌بند دودویی شرح داده شد؛ همان‌طور که اشاره شد، این طبقه‌بند برای تشخیص اینکه نمونهٔ ورودی یک حمله است یا یک ورودی نرمال، به‌کار گرفته می‌شود. در صورتی که حمله تشخیص داده شود در مرحلهٔ بعد با توجه به جدول (۱) باید نوع یا طبقه حمله تشخیص داده شود. تشخیص نوع حمله در این روش پیشنهادی به‌وسیلهٔ طبقه‌بند چندطبقه انجام می‌شود. در این طبقه‌بند نیز مشابه طبقه‌بند دودویی از شبکهٔ CNN استفاده می‌شود. در ادامه به بررسی این شبکه می‌پردازیم.

در شکل (۵) معماری شبکهٔ CNN در طبقه‌بند چندطبقه نشان داده شده‌است. همان‌طور که در شکل مشخص است، در این شبکه چهارلایهٔ کانولوشن به‌ترتیب با اندازه‌های ۲۵۶، ۱۲۸، ۶۴ و ۳۲ به‌کار گرفته شده‌است. در این الگوریتم نیز لایه‌های کانولوشنالی وظیفهٔ تحلیل و بررسی داده‌های ورودی که شامل حملات شناسایی‌شده به‌وسیلهٔ CNN دودویی بود را بر عهده دارند و خروجی این لایه‌ها انواع حملاتی هستند که به‌وسیلهٔ لایه‌های کانولوشنالی شناسایی و تفکیک شده‌اند؛ همچنین از دو لایهٔ MaxPool، یک لایهٔ Flatten و درنهایت یک لایهٔ Dense با ۳۲ نورون استفاده شده‌است. در این لایه، داده‌های شناسایی‌شده را به‌وسیلهٔ لایه‌های کانولوشنالی که شامل انواع مختلف حملات شناسایی شده‌است، دریافت و اقدام به مرتب‌سازی و تفکیک حملات شناسایی‌شده می‌کند تا یک بردار ستونی از این حملات تشکیل دهد و خروجی را در اختیار لایهٔ آخر قرار می‌دهد تا مطابق شکل (۵) این حملات در چهار دسته‌بندی DoS، U2R،R2L و Probe قرار گیرند. در لایهٔ خروجی این مدل نیز چهار نورون به‌منظور تشخیص طبقه‌های DoS، U2R، R2L و Probe وجود دارد. در این شبکه بین لایه‌های کانولوشن نخست و دوم یک لایهٔ Dropout قرار دارد. این لایه به‌منظور پیش‌گیری از بیش‌برازش[3] به‌کار گرفته شده‌است. بیش‌برازش زمانی اتفاق می‌افتد که مدل فقط نمونه‌داده‌های موجود در داده‌های آموزشی را یاد می‌گیرد و به درستی پیش‌بینی می‌کند و برای داده‌های جدید نمی‌تواند پاسخ مناسبی ارائه دهد.

۵-۴-خلاصهٔ کار روش پیشنهادی

در این پژوهش با استفاده از زبان پایتون و در محیط Anaconda Jupyter notebook مدل پیشنهادی پیاده‌سازی شده‌است؛ همان‌طور که پیش‌تر اشاره شد، دادگان مورد استفاده در این پژوهش NSL-KDD است که این مجموعه‌داده نسخهٔ بهبود داده شدهٔ مجموعه‌داده KDD99 است. همان‌طورکه توضیح داده شد، با استفاده از روش PCA به کاهش ابعاد در این دادگان می‌پردازیم. هدف از کاهش ابعاد در مجموعه‌داده‌ها کاهش حجم محاسبات اضافه و افزایش سرعت محاسبات به‌وسیلهٔ مدل‌های یادگیری عمیق است. روش PCA با استفاده از محاسبات جبر خطی و به‌دست‌آوردن واریانس و کواریانس به بررسی بردارهای وابسته و مستقل خطی می‌پردازد و با

[1] Conventional Neural Network
[2] Convolutional
[3] Overfitting

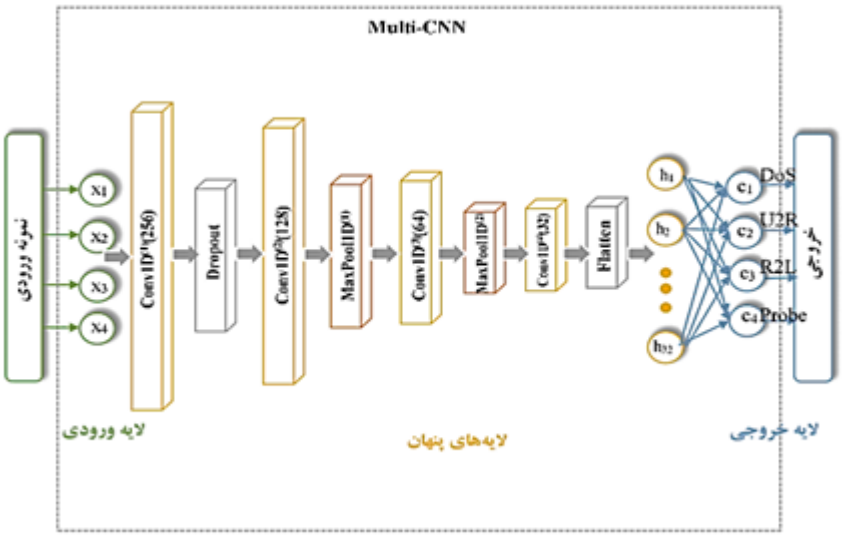
[DOI: 10.61186/jsdp.21.3.3]

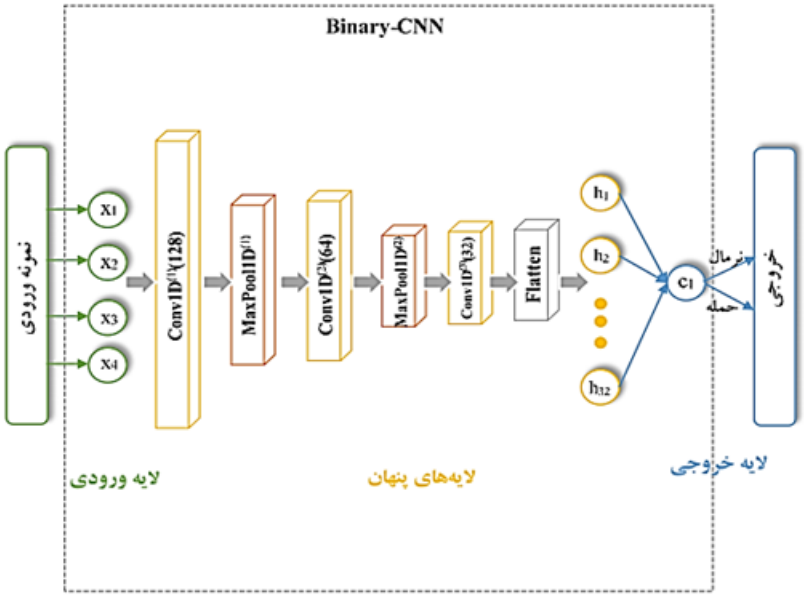
درنظرگرفتن این اصل، بردارهای وابستهٔ خطی را حذف و از بین این بردارها یک مؤلفه را به‌عنوان ویژگی حفظ می‌کند. دسته‌بندی در دو سطح انجام می‌شود؛ سطح نخست برای تشخیص حمله و سطح دوم برای تشخیص نوع حملهٔ طراحی شده‌است که هر دو سطح از نوع CNN هستند. ابتدا ابعاد به‌دست‌آمده از روش PCA به مدل CNN دودویی داده می‌شود. این مدل با توجه به پیکربندی گفته‌شده در بخش قبلی مدل خروجی را در دو دستهٔ حمله (نفوذ) یا ترافیک نرمال، دسته‌بندی می‌کند. بعد از این مرحله با استفاده از مدل CNN چندطبقه داده‌های خروجی نفوذ را به چهار طبقه DoS، U2R، R2L و Probe دسته‌بندی می‌کنیم.

۵- راه حل پیشنهادی

در این بخش به ارزیابی روش پیشنهادی و بیان نتایج آن می‌پردازیم. ابتدا مجموعه‌دادگان مورد استفاده برای پیاده‌سازی و پارامترهای ارزیابی روش پیشنهادی را شرح می‌دهیم؛ سپس به ارزیابی طبقه‌بندی دودویی خواهیم پرداخت که خود شامل مدل CNN است. در بخش بعد طبقه‌بندی چندطبقه مورد بررسی قرار گرفته و نتایج مدل CNN مربوط به این طبقه‌بند نیز شرح داده می‌شود. در بخش پایانی نیز روش پیشنهادی در این پژوهش با سایر روش‌های تشخیص نفوذ IOT مشابه و معتبر مقایسه خواهد شد.

(شکل-۴): معماری CNN در طبقه‌بند دودویی
(Figure-4): CNN architecture in the binary classifier





(شکل-۵): معماری شبکهٔ CNN در طبقه‌بند چندطبقه
(Figur-5): Architecture of CNN network in multi-class classification

[DOI: 10.61186/jsdp.21.3.3]

همان‌طور که پیش‌تر اشاره شد، در این پژوهش به منظور تحلیل و ارزیابی روش پیشنهادی از دادگان NSL-KDD استفاده شد. این دادگان نسخهٔ بهبودیافتهٔ دادگان KDD99 است. از جمله مزایای آن نسبت به دادگان KDD99، حذف رکوردهای تکراری و تنوع رکوردها برای بهبود طبقه‌بندی دادگان است؛ علاوه‌براین مشکل متعادل‌نبودن داده‌ها[1] در این دادگان برطرف شده‌است.

در پیاده‌سازی و ارزیابی روش پیشنهادی در این پژوهش، از زبان برنامه‌نویسی پایتون[2] و کتابخانه‌های تنسورفلو[3] و کراس[4] استفاده شد. همچنین کدنویسی با استفاده از یک رایانهٔ شخصی با پردازندهٔ core i5، چهار گیگابایت حافظهٔ داخلی و در ویندوز ۱۰ انجام شد.

همان‌طورکه در جدول (۲) نشان داده شده، این دادگان در مجموع شامل ۱۴۸۵۱۶ سطر است. از این تعداد، ۱۲۵۹۷۳ سطر به‌عنوان نمونه‌های آموزشی و ۲۲۵۴۳ سطر نیز به‌عنوان نمونه‌های آزمایش درنظر گرفته شده‌است؛ به عبارت دیگر از ۸۰ درصد دادگان به‌عنوان داده‌های آموزشی و بیست‌درصد به‌عنوان داده‌های آزمایش استفاده شده‌است؛ همچنین این دادگان شامل ۴۱ ستون است که چهل ستون ویژگی‌ها و یک ستون نیز نشان‌دهندهٔ طبقه هر نمونه است.

(جدول-۲): تعداد نمونه‌های دادگان آموزشی و آزمایش در پیاده‌سازی طبقه‌بند دودویی

(Table-2): The number of samples of training and test data in the implementation of binary classification

مجموعه	تعداد نمونه‌ها
دادگان آموزشی	۱۲۵۹۷۳
دادگان آزمایش	۲۲۵۴۳
کل دادگان	۱۴۸۵۱۶

۵-۱-پارامترهای ارزیابی

به‌منظور ارزیابی مدل‌های طبقه‌بندی از پارامترهای ارزیابی مختلف استفاده کرده‌ایم، که در این بخش هر یک از آن‌ها را بیان می‌کنیم:

صحت[5]:

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

در رابطهٔ (۴)، TP نمونه‌های مثبت صحیح[6] پیش‌بینی شده، TN نمونه‌های منفی صحیح[7] پیش‌بینی شده، FP نمونه‌های مثبت کاذب[8] پیش‌بینی شده و FN نمونه‌های منفی کاذب[9] پیش‌بینی شده‌است.

دقت[10]:

$$PR = \frac{TP}{TP+FP} \quad (۵)$$

نرخ تشخیص[11]:

$$DR = \frac{TP}{TP+FN} \quad (۶)$$

نام‌های دیگر این معیار، حساسیت[12] و یادآوری[13] است.

نرخ منفی صحیح[14]:

$$TNR = \frac{TN}{TN+FP} \quad (۷)$$

نام دیگر این معیار اختصاصی[15] است.

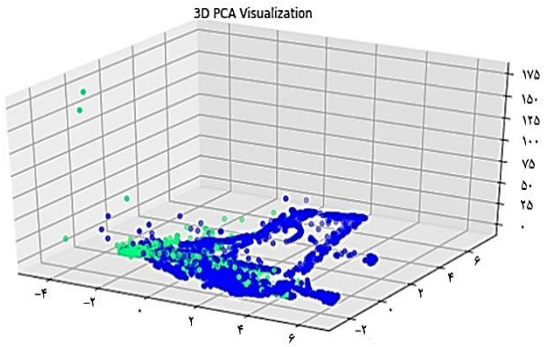
۵-۲-کاهش بُعد با PCA

همان‌طور که در بخش قبل بیان شد یکی از مراحل پیش‌پردازش دادگان در روش پیشنهادی، کاهش بُعد دادگان است. برای کاهش بعد از روش تحلیل مؤلفه‌های اصلی استفاده شد. در بخش قبل اشاره شد که هر سطر از دادگان NSL-KDD شامل ۴۱ ویژگی است. به طور طبیعی این تعداد ویژگی برای تحلیل و آنالیز از جنبه علوم داده و به خصوص استفاده از یادگیری عمیق مناسب نیست و موجب کاهش کارایی در مدل می‌شود؛ لذا در این پژوهش با استفاده از روش PCA دادگان را کاهش بُعد داده، به‌نحوی که بتوانیم از ۴۱ ویژگی درنهایت به چهار طبقه حمله برسیم. که این چهار نوع حمله DoS، R2L، U2R و Probe هستند. سایر انواع مختلف حملات، زیرمجموعهٔ این چهار نوع حمله دسته‌بندی می‌شوند. گفتنی است که در روش PCA با وجود کاهش ابعاد، اطلاعات حیاتی دادگان و مشخصات جداپذیری[16] نمونه‌ها حفظ می‌شود. در شکل‌های (۶ و ۷) به‌ترتیب نمودار پراکندگی داده‌ها و نرخ واریانس بعد از اجرای روش کاهش بُعد PCA نشان داده شده‌است.

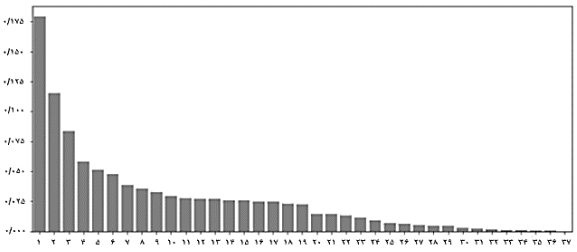
[1] Unbalamced Data
[2] Python
[3] Tensorflow
[4] Keras
[5] Accuracy

[6] True Positive
[7] True Negative
[8] False Positive
[9] False Negetive
[10] Precision
[11] Detection Rate
[12] Sensitivity
[13] Recall
[14] True Negative Rate
[15] Specificity
[16] Discriminative

[DOI: 10.61186/jsdp.21.3.3]



(شکل-۶): نمودار پراکندگی داده‌ها بعد از اجرای کاهش بعد PCA
(Figure-6): Scatter plot of data after PCA dimensionality reduction



(شکل-۷): نمودار نرخ واریانس بعد از اجرای کاهش بعد PCA
(Figure-7): Variance rate diagram after performing PCA dimension reduction

۳-۵-نتایج طبقه‌بندی دودویی

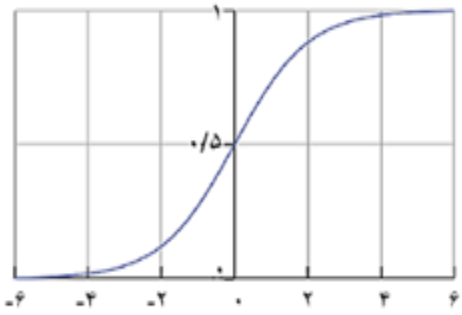
در روش پیشنهادی در این پژوهش ابتدا با استفاده از یک طبقه‌بند دودویی، حمله و یا نرمال‌بودن نمونهٔ ورودی تشخیص داده می‌شود. در این طبقه‌بند از مدل یادگیری عمیق CNN استفاده می‌شود. در بخش‌های بعد ابتدا پارامترهای پیاده‌سازی را بیان می‌کنیم.

۱-۳-۵-پارامترهای پیاده‌سازی طبقه‌بند دودویی

در این بخش پارامترهای پیاده‌سازی طبقه‌بند دودویی را به ترتیب بیان می‌کنیم. در شبکه‌های عصبی مصنوعی تابع فعال‌ساز وظیفهٔ تولید خروجی یک گره[1] از شبکه را برعهده دارد؛ به عبارت دیگر خروجی هر گره در شبکه با عبور از یک تابع فعال‌ساز تولید می‌شود. توابع فعال‌ساز متعددی وجود دارد که بسته به نوع شبکه و تعداد خروجی‌ها کاربردهای متفاوتی دارند؛ در اینجا از تابع سیگموئید (Sigmoid) که در شبکه‌های عصبی مصنوعی که طبقه‌بند دودویی انجام می‌دهند کاربرد فراوان دارد، استفاده شده‌است؛ این تابع طبق رابطهٔ (۸) محاسبه می‌شود. خروجی این تابع مقدار صفر و یک است. در شکل (۸) نمودار این تابع نشان داده شده‌است.

$$S(x) = \frac{1}{1+e^{-x}} \qquad (۸)$$

[1] Node



(شکل-۸): نمودار سیگموئید
(Figure-8): Sigmoid diagram

بهینه‌ساز Adam که نام دیگر آن گرادیان کاهشی تصادفی است[2]، روشی مبتنی بر تکرار برای بهینه‌سازی یک تابع هدف (تابع هزینه) است. این روش یک نسخهٔ بهبودیافته از روش گرادیان کاهشی است؛ به عبارت دیگر بهینه‌سازی Adam الگوریتمی است که طی چند حلقه تکرار، مقدار کمینهٔ یک تابع و مقادیری را که به‌ازای آن‌ها تابع کمینه می‌شود، به‌دست می‌آورد.

گام‌های بهینه‌ساز Adam مطابق رابطهٔ (۹) است که در این رابطه θ نشان‌دهندهٔ بردار پارامترهای تابع هزینه است. ابتدا θ را به‌صورت دلخواه و تصادفی مقداردهی، سپس بر اساس رابطهٔ (۸) و انتخاب یک عضو از مجموعه‌داده‌های آموزشی، آن را به‌روزرسانی می‌کنیم. در این رابطه، a نرخ یادگیری، $(x^{(i)}.y^{(i)})$ یک نمونه از داده‌های آموزشی که تصادفی انتخاب شده‌است، و τ_i تابع هزینه است.

$$\theta = \theta - a\nabla_\theta\, t_i(\theta; x^{(i)}y^{(i)}) \qquad (۹)$$

تابع هزینه[3] یکی از مهم‌ترین اجزای شبکه‌های عصبی مصنوعی و منظور از هزینه میزان خطای پیش‌بینی[4] در شبکه است و تابع هزینه وظیفهٔ محاسبهٔ این خطا را برعهده دارد؛ به عبارت دیگر تابع هزینه برای محاسبهٔ گرادیان‌ها مورد استفاده قرار می‌گیرد و گرادیان‌ها نیز برای به‌روزرسانی وزن‌های شبکهٔ عصبی کاربرد دارند. توابع هزینهٔ مختلفی وجود دارد که ما در این مدل از Binary Cross-Entropy استفاده کرده‌ایم.

تابع Binary Cross-Entropy برای طبقه‌بندی‌های دودویی مورد استفاده قرار می‌گیرد. این تابع طبق رابطهٔ (۱۰) محاسبه می‌شود. در این رابطه S(x) نشان‌دهندهٔ تابع سیگموئید است که پیش‌تر به آن اشاره شد.

$$CE = -t\log\big(S(x)\big) - (1-t)\log\,(1-S(x)) \qquad (۱۰)$$

[2] Stochastic Gradient Descent
[3] Loss Function
[4] Prediction Error

[DOI: 10.61186/jsdp.21.3.3]

۵-۳-۲-ارزیابی CNN دودویی

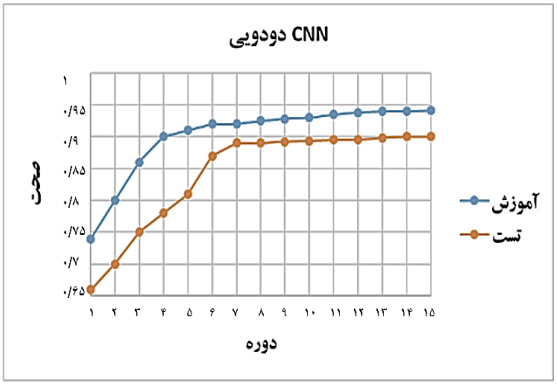
در این بخش CNN دودویی مورد بررسی قرار می‌گیرد. در جدول (۳) پارامترهای پیاده‌سازی این مدل نشان داده شده‌است. تعداد و اندازهٔ لایه‌های کانولوشن، لایهٔ Dense، تعداد نورون لایهٔ خروجی و نوع توابع فعال‌ساز و هزینهٔ این طبقه‌بند مشاهده می‌شود.

حال نتایج مدل CNN دودویی را بیان می‌کنیم. در شکل (۹)، مقادیر پارامتر صحت به ازای دوره‌های مختلف آموزش و آزمایش CNN دودویی مشاهده می‌شود. در اینجا تعداد پانزده دوره را در نظر گرفتیم. همان‌طورکه از نمودار مربوط به آموزش مشخص است، مقادیر صحت در دوره‌های پایانی به مقدار ۰/۹۴ رسیده و صحت آزمایش نیز در آخرین دوره‌های اجرا به مقدار ۰/۹ نزدیک شده‌است.

(جدول-۳): پارامترهای پیاده‌سازی CNN دودویی
(Table-3): Binary CNN implementation parameters

پارامتر	مقدار
اندازهٔ لایه‌های کانولوشن	۳۲، ۶۴، ۱۲۸
اندازهٔ لایه Dense	۱۲۸
تعداد نورون لایهٔ خروجی	۱
تابع فعال‌ساز	Sigmoid
بهینه‌ساز	Adam (Stochastic Gradient Descent)

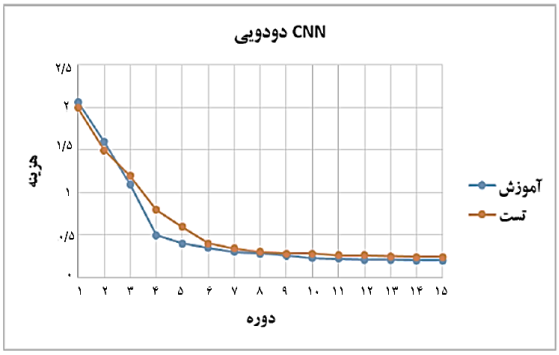
در شکل (۱۰) نمودارهای مقادیر هزینهٔ به‌دست‌آمده در آموزش و آزمایش CNN دودویی نشان داده شده‌است. همان‌طور که از نمودارها مشخص است، مقادیر هزینه در دوره‌های پایانی آموزش و آزمایش به‌ترتیب ۰/۲ و ۰/۲۴ حاصل شده‌است.



(شکل-۹): مقادیر صحت در آموزش و آزمایش CNN دودویی
(Figure-9): Accuracy values in binary CNN training and testing

۵-۳-۳-ماتریس درهم‌ریختگی CNN دودویی

ماتریس درهم‌ریختگی CNN دودویی در جدول (۴) نشان داده شده‌است. درکل از ۲۲۵۴۳ نمونه‌دادهٔ آزمایش، ۲۰۲۸۹ نمونه به‌درستی و ۲۲۵۴ نمونه نیز به‌اشتباه به‌وسیلهٔ CNN دودویی پیش‌بینی شده‌است.



(شکل-۱۰): مقادیر هزینه در آموزش و آزمایش CNN دودویی
(Figure-10): Cost values in binary CNN training and testing

(جدول-۴): ماتریس درهم‌ریختگی CNN دودویی
(Table-4): Binary CNN confusion matrix

تعداد کل داده‌های آزمایش = ۲۲۵۴۳	پیش‌بینی شده: نرمال	پیش‌بینی شده: حمله
واقعی: نرمال	۸۷۹۰	۹۲۰
واقعی: حمله	۱۳۳۴	۱۱۴۹۹

۵-۴-نتایج طبقه‌بندی چندطبقه

همان‌طور که در بخش قبل بیان شد، در روش پیشنهادی در این پژوهش، ابتدا با استفاده از یک طبقه‌بند دودویی، نرمال و یا حمله‌بودن نمونهٔ ورودی تشخیص داده می‌شود. درصورتی‌که نوع نمونهٔ ورودی به‌وسیلهٔ طبقه‌بند دودویی حمله تشخیص داده شود، از یک طبقه‌بند چندطبقه برای تشخیص نوع حمله استفاده می‌شود. مشابه طبقه‌بند دودویی، در طبقه‌بند چندطبقه نیز از مدل CNN استفاده شده‌است. در بخش‌های بعد ابتدا پارامترهای پیاده‌سازی آن‌ها را بیان، سپس مدل را بررسی و نتایج آن‌ها را بیان می‌کنیم.

۵-۴-۱-پارامترهای پیاده‌سازی طبقه‌بند چندطبقه

در این بخش هر یک از پارامترهای پیاده‌سازی طبقه‌بند چندطبقه را شرح می‌دهیم. در اینجا تابع فعال‌ساز Softmax استفاده شده‌است. این تابع فعال‌ساز، خروجی یک شبکهٔ عصبی را به‌صورت توزیع احتمال از طبقه‌ها تولید می‌کند. ورودی تابع SoftMax بردار z از K عدد حقیقی است و خروجی آن بردار K بعدی $\sigma(z)$ از مقادیر [۰،۱] به‌صورت توزیع احتمال نرمال شده‌است. این تابع در رابطهٔ (۱۰) نشان داده شده‌است. تابع Softmax به طور معمول در شبکه‌های عصبی مصنوعی که طبقه‌بند چندطبقه انجام می‌دهند کاربرد دارد؛ لذا در این پژوهش نیز در طبقه‌بندی چندطبقه از این تابع به‌عنوان تابع فعال‌ساز لایهٔ خروجی استفاده کرده‌ایم.

[DOI: 10.61186/jsdp.21.3.3]

$$\sigma(z_i) = \frac{e^{z_i}}{\sum_{j=1}^{k} e^{z_j}} for i = 1 \dots k \; and \; z \qquad (۱۰)$$

تابع هزینهٔ رسته‌ای پراکنده[1] Cross-Entropy: این تابع که در شبکه‌های عصبی مصنوعی چندطبقه کاربرد فراوان دارد، مقدار هزینهٔ $Cross-Entropy$ بین برچسب طبقه‌ها و پیش‌بینی‌ها را محاسبه می‌کند. این تابع مطابق رابطهٔ (۱۱) محاسبه می‌شود. در این رابطه w وزن‌های شبکهٔ عصبی، y_i برچسب صحیح شمارهٔ i و $\hat{y}_i$ برچسب پیش‌بینی‌شده به‌وسیلهٔ شبکه است.

$$j(w) = \frac{1}{n}\sum_{i=1}^{n}[y_i \log(\hat{y}_i) + (1-y_i)log(1-\hat{y}_i)] \qquad (۱۱)$$

مشابه طبقه‌بندی دودویی در این طبقه‌بندی نیز از بهینه‌ساز Adam (گرادیان نزولی تصادفی) استفاده شده‌است.

۲-۴-۵-ارزیابی CNN چندطبقه

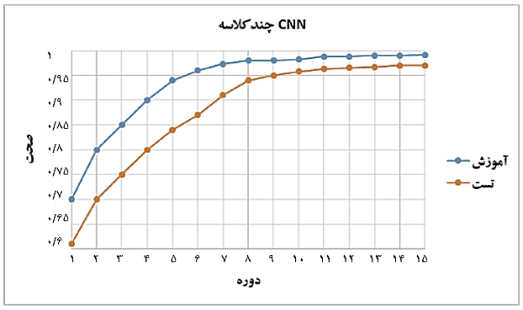
در این بخش نتایج طبقه‌بندی CNN چندطبقه بیان می‌شود. در جدول (۵) پارامترهای پیاده‌سازی این مدل بیان شده‌است. پارامترهایی از قبیل اندازهٔ لایه‌های کانولوشن، اندازهٔ لایهٔ Dense، تعداد نورون لایهٔ خروجی، تعداد دوره‌ها، توابع فعال‌ساز، بهینه‌ساز و هزینه که در پیاده‌سازی CNN چندطبقه مورد استفاده قرار گرفته‌است، در جدول مشاهده می‌شود.

در شکل (۱۱) نمودار مقادیر صحت به‌ازای دوره‌های مختلف آموزش و آزمایش CNN چندطبقه نشان داده شده‌است. تعداد دوره‌ها را همان‌طور که در جدول (۵) بیان شد، پانزده درنظر گرفته‌ایم. همان‌طورکه در نمودارها مشاهده می‌شود، مقدار نهایی صحت در طبقه‌بندی داده‌های آموزشی ۰/۹۹ و در طبقه‌بندی داده‌های آزمایش ۰/۹۷ به‌دست آمده‌است.

(جدول-۵): پارامترهای پیاده‌سازی CNN چندطبقه
(Table-5): Multi-class CNN implementation parameters

پارامتر	مقدار
اندازهٔ لایه‌های کانولوشن	۳۲،۶۴،۱۲۸،۲۵۶
اندازهٔ لایهٔ Dense	۳۲
تعداد نورون لایهٔ خروجی	۴
تعداد دوره‌ها	۱۵
تابع فعال‌ساز	Softmax
بهینه‌ساز	Adam (Stochastic Gradient Descent)
تابع هزینه	Sparse Categoricaly Cross-Entropy

[1] Spare Categorical Cross-Entropy



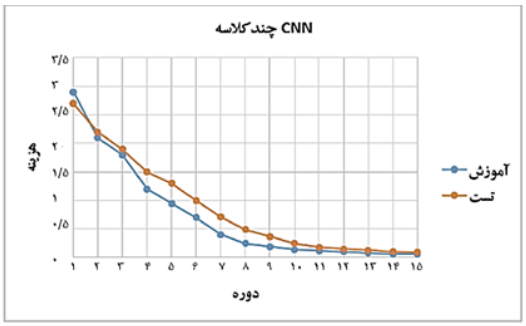
(شکل-۱۱): مقادیر صحت در آموزش و آزمایش CNN چندطبقه
(Figure-11): Accuracy values in multi-class CNN training and testing

در شکل (۱۲) نمودارهای هزینه برای دوره‌های آموزش و آزمایش CNN چندطبقه نشان داده شده‌است.

مقدار هزینهٔ آموزش و آزمایش در دوره‌های پایانی به‌ترتیب ۰/۰۶ و ۰/۰۹ حاصل شده‌است.

۳-۴-۵-ماتریس درهم ریختگی CNN چندطبقه

در جدول (۶) ماتریس درهم‌ریختگی مربوط به CNN چندطبقه نشان داده شده‌است. در اینجا نیز تعداد نمونه‌های درست و اشتباه پیش‌بینی‌شده برای هر طبقه مشخص شده‌است. CNN چندطبقه از ۱۳۵۴۵ نمونه‌دادهٔ آزمایش، ۱۳۱۳۹ نمونه را به‌درستی و تنها ۴۰۶ نمونه را اشتباه پیش‌بینی کرده‌است.



(شکل-۱۲): مقادیر هزینه در آموزش و آزمایش CNN چندکلاسه
(Figure-12): Cost values in multi-class CNN training and testing

(جدول-۶): ماتریس درهم ریختگی CNN چندطبقه
(Table-6): Confusion matrix of multi-class CNN

تعداد کل= 13545	DoS:	U2R:	R2L:	Probe:
واقعی: Dos	۶۹۹۷	۳۵	۴۴	۹۳
واقعی: U2R	۳۳	۱۰۴۵	۱۴	۲۱
واقعی: R2L	۳۶	۲۱	۲۰۰۳	۳۱
واقعی: Probe	۴۱	۹	۲۸	۳۰۴۸

[DOI: 10.61186/jsdp.21.3.3]

۵-۵-مقایسهٔ روش پیشنهادی با سایر روش‌ها

در این بخش نتایج روش پیشنهادی با سایر روش‌های مشابه مقایسه می‌شود؛ به این منظور تعدادی از روش‌های تشخیص نفوذ ارائه‌شده را انتخاب کرده‌ایم. کلیات مربوط به این روش‌ها در جدول (۷) فهرست شده‌اند. همان‌طور که در جدول مشاهده می‌شود مرجع، روش پیشنهادی و دادگان هر یک از آن‌ها در این جدول آمده‌است. مراجع انتخاب‌شده، مقالات معتبر در حوزهٔ تشخیص نفوذ در اینترنت اشیا هستند.

(جدول-۷): روش‌های تشخیص نفوذ IOT انتخاب‌شده جهت مقایسه
(Table-7): IOT intrusion detection methods selected for

مرجع	روش	دادگان
(Hode, et al., 2016, pp. 1-6)	شبکهٔ پرسپترون چندلایه	شبیه‌سازی
(Kumari, et al., 2017, pp. 481-485)	ماشین بردار پشتیبان + خوشه‌بندی	NSL-KDD
(Pajouh, et al., 2016)	بیز ساده و K نزدیک‌ترین همسایه	NSL-KDD
(Lopez-Martin, et al., 2017, p. 1967)	شبکهٔ خودرمزنگار	NSL-KDD
(Diro et al., 2018, pp. 761-768)	یادگیری عمیق چندلایه	NSL-KDD
(Hosseinpour et al., 2016)	سامانهٔ ایمنی مصنوعی	KDD99 و SSH Brute Force
(Almiani, et al., 2020, p. 102031)	شبکه‌های عصبی مصنوعی بازگشتی	NSL-KDD

(جدول-۸): مقایسهٔ روش پیشنهادی با سایر روش‌ها
(Table-8): Comparison of the proposed method with other methods

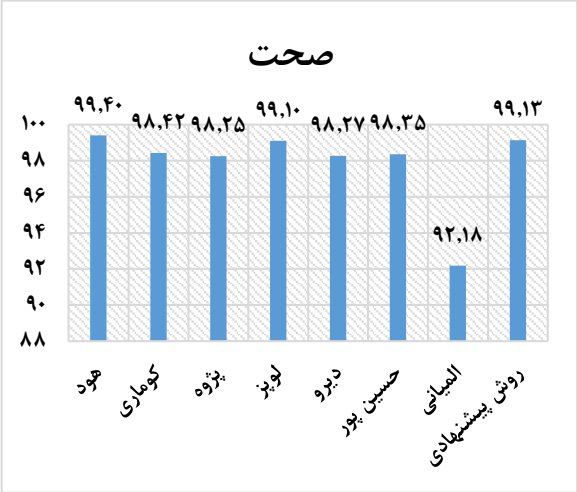
روش	صحت	دقت	نرخ تشخیص	نرخ مثبت کاذب
(Hode, et al., 2016, pp. 1-6)	۹۹/۴	۹۸/۳	۱۰۰	۰/۹
(Kumari , et al., 2017, pp. 481-485)	۹۸/۴۲	۹۱/۳۷	۹۹/۶	۵/۸۶
(Pajouh, et al., 2016)	۹۸/۲۵	۹۲/۲۶	۸۴/۸۶	۴/۸۶
(Lopez-Martin, et al., 2017, p. 1967)	۹۹/۱	۸۱/۵۹	۸۰/۱	۴/۲۵
(Diro et al., 2018, pp. 761-768)	۹۸/۲۷	۹۲/۳۹	۹۶/۵	۲/۵۷
(Hosseinpour et al., 2016)	۹۸/۳۵	۹۷/۸۳	۹۰/۵۴	۴/۴۱
(Almiani, et al., 2020, p. 102031)	۹۲/۱۸	۹۰/۲۳	۹۴/۲۷	۹/۸
روش پیشنهادی	۹۹/۱۳	۹۲/۸۴	۹۳/۹۴	۴/۳۱

در جدول (۸) نتایج روش پیشنهادی ارائه‌شده در این پژوهش با روش‌های ذکرشده در بالا مقایسه شده‌است. همان‌طورکه در جدول مشخص است، مقدار پارامتر صحت به‌دست‌آمده در روش پیشنهادی ما به غیر از روش هودو و همکاران از دیگر روش‌های ذکرشده بیشتر است.

مقدار دقت به‌دست‌آمده نیز از روش‌های لوپزمارتین و همکاران و المیانی و همکاران بیشتر و از روش‌های هودو و همکاران و حسین‌پور و همکاران کمتر است؛ همچنین نرخ تشخیص روش پیشنهادی از بیشتر روش‌های ذکرشده به غیر از هودو و همکاران و کوماری و همکاران بالاتر است.

در ستون پایانی جدول نیز مقدار پارامتر نرخ مثبت کاذب ذکر شده‌است. درکل به غیر از روش هودو و همکاران، روش پیشنهادی در این پژوهش در مقایسه با بیش‌تر روش‌ها عملکرد بهتری را از خود نشان داده‌است.

در شکل (۱۳) نمودار مقایسهٔ نرخ صحت روش پیشنهادی با سایر روش‌های دیگر نشان داده شده‌است. در این معیار روش پیشنهادی ما نسبت به باقی روش‌ها نتیجهٔ بهتری کسب کرده و تنها روش هود نتیجهٔ بهتری داشت به این دلیل که در روش هود به جای مجموعه‌دادگان از شبیه‌سازی استفاده شده‌است. در روش پیشنهادی ما در مقایسه با آزمایش‌های مشابهی که از روش‌های یادگیری سنتی بهره برده بودند، استفاده از الگوریتم‌های یادگیری عمیق به نزدیک‌شدن مقادیر به مقدار واقعی در قالب معیار صحت کمک زیادی کرد.

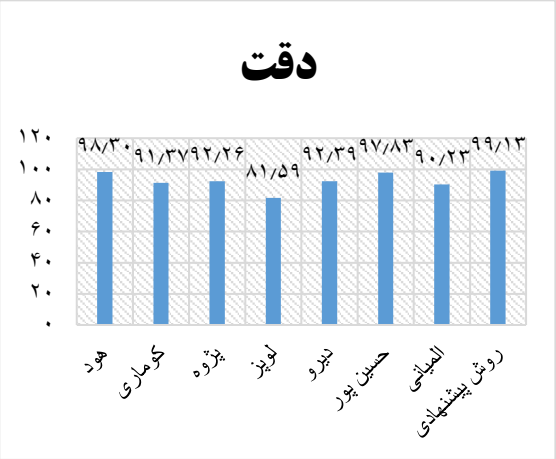


(شکل-۱۳): نمودار مقایسهٔ نرخ صحت روش پیشنهادی با سایر روش‌های دیگر
(Figure-13): Comparison graph of the accuracy rate of the proposed method with other methods

در شکل (۱۴) نمودار مقایسهٔ نرخ دقت روش پیشنهادی با سایر روش‌های دیگر نشان داده شده‌است. در معیار دقت با بررسی‌های صورت‌گرفته روش پیشنهادی ما نسبت به تمام روش‌های دیگر نتیجهٔ بهتری کسب کرده‌است؛ در واقع استفاده از الگوریتم CNN به صورت دو وجهی به این صورت که ابتدا حملات از مجموعه‌دادگان

[DOI: 10.61186/jsdp.21.3.3]

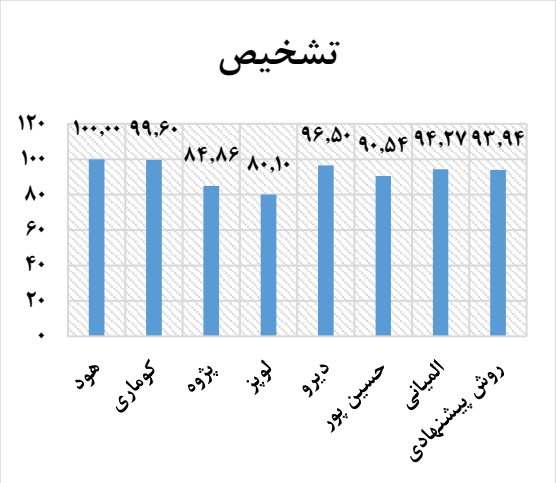
جداسازی شدند و سپس طبقه‌بند چندطبقه بر روی مجموعه‌دادگان جدید اقدامات شناسایی نوع حملات را انجام داد موجب افزایش دقت در شناسایی حملات شد و نسبت به روش‌های مشابه شاهد رشد نرخ این معیار بودیم.



(شکل-۱۴): نمودار مقایسهٔ دقت روش پیشنهادی با سایر روش‌ها

(Figure-14): Comparison graph of the accuracy of the proposed method with other methods

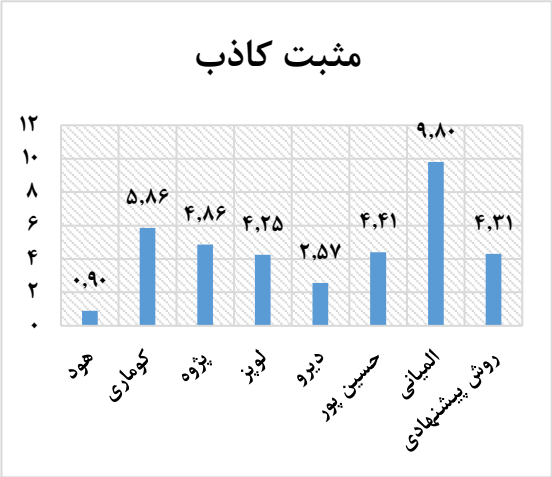
در شکل (۱۵) نمودار مقایسهٔ نرخ تشخیص روش پیشنهادی با سایر روش‌ها نشان داده شده‌است. در این معیار نتایج روش پیشنهادی ما پس از روش‌های هود، کوماری، دیرو و المیانی از میان هشت روش، رتبهٔ پنجم را به خود اختصاص داده‌است. در روش پیشنهادی ما استفاده از الگوریتم PCA برای کاهش ابعاد دادگان موجب ساده‌سازی و کاهش حجم مجموعه‌دادگان ورودی به الگوریتم شد و همین امر به رشد معیار تشخیص الگوریتم کمک کرد.



(شکل-۱۵): نمودار مقایسهٔ نرخ تشخیص روش پیشنهادی با سایر روش‌ها

(Figure-15): Comparison chart of the detection rate of the proposed method with other methods

شکل (۱۶) نمودار مقایسهٔ نرخ مثبت کاذب روش پیشنهادی با سایر روش‌ها را نشان می‌دهد. در این معیار روش پیشنهادی ما پس از روش‌های هود، دیرو و لوپز نسبت به باقی روش‌ها نتیجهٔ بهتری کسب کرده و از بین هشت روش، رتبهٔ چهارم را به خود اختصاص داده‌است؛ در واقع این معیار نشان می‌دهد که حملاتی وجود داشته‌اند که به‌وسیلهٔ الگوریتم به اشتباه به‌عنوان دادهٔ نرمال شناسایی شده‌اند که استفاده از طبقه‌بند به صورت دووجهی به این امر کمک کرد تا نرخ این معیار نسبت به برخی روش‌های دیگر کاهش پیدا کند.



(شکل-۱۶): نمودار مقایسهٔ نرخ مثبت کاذب روش پیشنهادی با سایر روش‌ها

(Figure-16): Comparing the false positive rate of the proposed method with other methods

درمجموع، اشکال بالا برتری نسبی روش پیشنهادی در مقابل بیشتر روش‌های ارائه‌شدهٔ قبلی را نشان می‌دهند. این برتری به خاطر استفاده از ساختار مناسب یادگیری عمیق و پارامترهای مناسب به‌کاررفته در این ساختار است؛ همچنین استفاده از دو سطح از دسته‌بندی که در سطح نخست حمله‌بودن یک نمونه و در سطح دوم نوع حمله را مشخص می‌کنند، تأثیر زیادی در کارایی روش پیشنهادی دارد. در بیشتر معیارها روش هود نتیجهٔ بهتری نسبت به روش پیشنهادی ما داشت که دلیل این نتایج را می‌توان در استفاده از شبیه‌سازی به‌جای مجموعه‌دادگان دانست که بر این اساس نتایج به‌دست‌آمده نیز جای بحث دارد.

۶- نتیجه‌گیری و کارهای آینده

از آنجا که دادگان مورد استفاده در این پژوهش یک بعدی بود، روش پیشنهادی با مشکل زمان اجرا مواجه نبود؛ لذا

[DOI: 10.61186/jsdp.21.3.3]

لزومی بر پیاده‌سازی موازی و توزیع‌شدهٔ روش پیشنهادی وجود نداشت. همان‌طور که در بخش‌های پیش اشاره شد، در روش پیشنهادی ارائه‌شده در این پژوهش، از دو مدل یادگیری عمیق استفاده شد. در زمان ارزیابی روش پیشنهادی، معماری‌های مختلف یادگیری عمیق با تعداد لایه‌های مختلف مورد بررسی قرار گرفت. یک معماری به‌کار گرفته‌شده شبکهٔ یادگیری عمیق بازگشتی بود که نتوانست عملکرد خوبی از خود نشان دهد. همچنین از پارامترهای پیاده‌سازی مختلفی برای آزمایش روش پیشنهادی استفاده شد. معماری و پارامترهای به‌کار رفته در روش پیشنهادی نتیجهٔ ارزیابی‌ها متعدد بود که منجر به گرفتن مناسب‌ترین نتیجه شد.

الگوریتم CNN به‌طور معمول جهت شناسایی تصاویر و در روش‌های مربوط به آن مورد استفاده قرار می‌گیرد، اما ما از این الگوریتم برای شناسایی حملات استفاده کردیم و شاهد نتایج خوبی نیز بودیم. روش‌های متفاوتی با استفاده از الگوریتم‌های یادگیری سنتی بر روی همین مجموعه‌دادگان مورد آزمایش و ارزیابی قرار گرفته‌اند، اما ما در این روش شاهد این بودیم که استفاده از روش‌های یادگیری عمیق کمک زیادی به بهبود نتایج کسب‌شده و همچنین افزایش دقت در شناسایی و صحت موارد استخراج‌شده کرد و با مقایسهٔ نتایج مربوطه به این نتیجه می‌رسیم که استفاده از الگوریتم‌های یادگیری عمیق به بهبود نتایج کمک کرده‌اند؛ همچنین استفاده از الگوریتم PCA جهت کاهش ابعاد دادگان ورودی، به افزایش دقت شناسایی و همچنین افزایش سرعت عملکرد الگوریتم کمک زیادی کرد؛ درواقع ما قبل از اینکه داده‌های ورودی را در اختیار الگوریتم قرار دهیم، با استفاده از این الگوریتم اقدام به کاهش ابعاد دادگان کرده و خروجی این الگوریتم را در اختیار CNN قرار دادیم؛ زیرا موضوع شناسایی حملات در شبکه اهمیت بالایی داشته و ممکن است لحظات تعیین‌کننده باشند و در این حالت سرعت شناسایی از اهمیت بالایی برخوردار است.

روش پیشنهادی در این مقاله با استفاده از یک دادگان معتبر پیاده‌سازی و ارزیابی شد. با وجود این‌که این دادگان در مقالات معتبر متعددی مورد استفاده قرار گرفته است، اما شاید بتوان گفت روش‌های تشخیص نفوذ در IoT به‌منظور ارزیابی نهایی باید در دنیای واقعی مورد استفاده قرار گیرند؛ لذا روش پیشنهادی در این پژوهش نیز می‌تواند در دنیای واقعی اینترنت اشیا مورد استفاده و ارزیابی قرار گیرد. بیشتر روش‌های تشخیص نفوذ در IoT تنها توانایی تشخیص حملات شناخته‌شده را دارند. درنتیجه اگر شبکهٔ IoT، مورد نفوذ یک حملهٔ ناشناخته قرار گیرد، این روش‌ها توانایی تشخیص آن حمله را نخواهند داشت؛ ازاین‌رو ارائه یک روش تشخیص نفوذ در IoT که علاوه بر تشخیص حملات شناخته‌شده، توانایی تشخیص حملات ناشناخته را نیز داشته باشد از اهمیت بالایی برخوردار است. می‌توان با ترکیب روش پیشنهادی در این پژوهش با یک روش تشخیص حملات ناشناخته به نتایج قابل توجهی دست یافت.

۷-مراجع 7-Reference

[1] S. Prabavathy, K. Sundarakantham, and S. M. Shalinie. "Design of cognitive fog computing for intrusion detection in internet of things,", vol. 20, no. 3, pp. 291-298, 2018.

[2] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits. "Denial-of-Service detection in 6LoWPAN based Internet of Things,", pp. 600-607, 2013

[3] G. Appice, A. Paolo Caforio, F. Andresini, & D. Malerba, "Improving cyber-threat detection by moving the boundary around the normal samples. In Machine Intelligence and Big Data Analytics for Cybersecurity Applications," pp. 105-127, 2021.

[4] S. Hajj, R. El Sibai, J. Bou Abdo, J. Demerjian, A. Makhoul, & C. Guyeux, "Anomaly-based intrusion detection systems: The requirements, methods, measurements, and datasets. Transactions on Emerging Telecommunications Technologies", 32(4), e4240, 2021.

[5] M. Nobakht, V. Sivaraman, and R. Boreli, "A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow," 11th International conference on availability, reliability and security (ARES), pp. 147-156, 2016.

[6] H. Bostani and M. Sheikhan, "Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach," Computer Communications, vol. 98, pp. 52-71, 2017.

[7] M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas, and J. Lloret. "Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in iot," Sensors, vol. 17, no. 9, p. 1967, 2017.

[8] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for IoT," Applied Soft Computing, vol. 72, pp. 79-89, 2018.

[9] Diro and N. Chilamkurti. "Distributed attack detection scheme using deep learning approach for Internet of Things," Future Generation Computer Systems, vol. 82, pp. 761-768, 2018.

[10] V. Kumari and P. R. K. Varma. "A semi-supervised intrusion detection system using active learning SVM and fuzzy c-means clustering," in

[DOI: 10.61186/jsdp.21.3.3]

maximize diversity using evolutionary optimization algorithms", Signal and Data Processing, 19 (4), pp. 95-120, 2023.

احمد تیموری تحصیلات کارشناسی و کارشناسی ارشد خود را در رشتهٔ مهندسی کامپیوتر گرایش نرم‌افزار به ترتیب در سال‌های ۱۳۹۶ و ۱۴۰۲ در دانشگاه آزاد اسلامی واحد تهران جنوب گذرانده‌است. زمینه‌های پژوهشی مورد علاقهٔ ایشان امنیت شبکه، یادگیری عمیق و بلاک‌چین است.
نشانی رایانامهٔ ایشان عبارت‌است از:
Trmahmad@gmail.com

محمود دی پیر مدرک دکترای خود را در رشتهٔ مهندسی کامپیوتر- سامانه‌های نرم‌افزاری و مدرک کارشناسی‌ارشد خود را در رشتهٔ مهندسی کامپیوتر-نرم‌افزار هر دو از دانشگاه شیراز دریافت کرده‌است. زمینه‌های پژوهشی ایشان شامل داده‌کاوی، امنیت داده و شبکه است. ایشان دارای مقالات متعددی در مجلات و همایش های ملی و بین‌المللی است؛ همچنین در پروژه‌های پژوهشی و صنعتی متعدد به عنوان مجری و همکار مشارکت داشته‌است.
نشانی رایانامهٔ ایشان عبارت‌است از:
mdeypir@ssau.ac.ir

2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pp. 481-485, 2017.
[11] Z. K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh. "IoT security: ongoing challenges and research opportunities," in 2014 IEEE 7th international conference on service-oriented computing and applications, pp. 230-234, 2014.
[12] M. Cheema, H. K. Qureshi, C. Chrysostomou, & M. Lestas, "Utilizing blockchain for distributed machine learning based intrusion detection in internet of things." In 2020 16th International Conference on Distributed Computing in Sensor Systems pp. 429-435, 2020.
[13] T. Hagemann, & Katsarou, K. A systematic "review on anomaly detection for cloud computing environments. In 2020 3rd Artificial Intelligence and Cloud Computing Conference." pp. 83-96, 2020.
[14] AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque. "Deep recurrent neural network for IoT intrusion detection system," Simulation Modelling Practice and Theory, vol. 101, pp. 10203, 2020.
[15] Dhanabsl, S.P. Shantharajah, "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms." PP. 2319-5940, 2015.
[16] Mackiewicz, and W. ratajczak, "Principal components analysis(PCA)" pp. 0098-3004, 1993.
[17] S. Indolia, A. K. Goswami, S. P. Mishra, and P. Asopa, "Conceptual Understanding of Convolutional Neural Network- A Deep Learning Approach" pp. 10-1016, 2018.
[18] S. Raza, L. Wallgren, and T. Voigt. "SVELTE: Real-time intrusion detection in the Internet of Things," Ad hoc networks, vol. 11, no. 8, pp. 2661-2674, 2013.
[19] Jun and C. Chi. "Design of complex event-processing IDS in internet of things," in 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation, pp. 226-229, 2014.
[20] T. S. Naseri, and F. S. Gharehchopogh, "A Feature Selection Based on the Farmland Fertility Algorithm for Improved Intrusion Detection Systems". Journal of Network and Systems Management, 30(3), pp. 1-27, 2022.
[21] S. K. Amalapuram, A.Tadwai, , R.Vinta, , S. S.Channappayya, and B. R. Tamma, "Continual Learning for Anomaly based Network Intrusion Detection". In 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS), pp. 497-505, 2022.
[22] D.Teixeira, , S. Malta, , and P.Pinto, "A Vote-Based Architecture to Generate Classified Datasets and Improve Performance of Intrusion Detection Systems Based on Supervised Learning". Future Internet, 14(3), 72, 2022.
[23] E. Gharavi, H. Veisi, "Using RST-based deep neural networks to improve text representation", Signal and Data Processing, 20 (1), pp. 181-197, 2023.
[24] S. Abbasi, S. Nejatian, H. Parvin, K. Bagherifard, V. Rezaie, "The ensemble clustering with

[DOI: 10.61186/jsdp.21.3.3]