Electronic and Cyber Defens 2025/ Vol. 13/ No. 2/ 45-55

Electronic and Cyber Defens

ISSN: 2322-4347 , E-ISSN: 2980-8979

Anomaly Detection in Internet of Things Equipment Traffic with the Approach of Combining Deep Learning Models

V. Yadegari[1*], S. Sohrab[2], V. Mahmoudian[3]

[1] PhD Student of Information Technology Management at Allameh Tabatabai University

Email:(*Correspondence: v.yadegari58@yahoo.com)

[2] Researcher, Qom Higher Education Institute, Qom, Iran.Email: samad_sohrab@yahoo.com

[3]Ph.D. student, Faculty of Computer Science, Islamic Azad University, North Tehran Branch, Tehran, Iran

Email: mahmoudian.vahid@gmail.com

ARTICLE INFO

Article history:

Article Type: Research paper

Received: 23 April 2025

Revised: 25 May 2025

Accepted: 08 June 2025

Available online: 22 June 2025

Keywords:

Convolutional Neural Networks

Recurrent Neural Networks

Network Traffic Classification

Deep Learning

Internet of Things (IoT)

ABSTRACT

Network traffic classifiers play a critical role in network monitoring systems by detecting anomalies in network flows based on communication features. This is particularly significant for managing and monitoring Internet of Things (IoT) networks. In this study, a novel method for network traffic classification is proposed, leveraging a combination of deep learning models tailored for IoT traffic. Experimental results demonstrate that the hybrid CNN+RNN-2 model achieves an accuracy of 83.58%, outperforming standalone and other hybrid models. By combining local feature extraction through Convolutional Neural Networks (CNN) and temporal dependency analysis via Recurrent Neural Networks (RNN), the proposed model effectively identifies complex patterns and improves detection accuracy. Furthermore, the results indicate that the CNN+RNN-2 model surpasses traditional supervised, semi-supervised, and unsupervised methods without requiring manual feature engineering. The use of deep learning, with its capability for automatic feature extraction and learning complex patterns, provides a significant advantage over conventional artificial intelligence techniques.

Cite this article: Yadegari, V.©, Mahmoudian, V., Sohrab, S.© (2025). Anomaly Detection in Internet of Things Equipment Traffic with the Approach of Combining Deep Learning Models. Journal of Electronic and Cyber Defens. 2025; 13l(2):45-55.

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.2.5.2

Publisher: Imam Hossein University.

پدافند الکترونیک و سایبری/ سال ۱۴۰۴/ دوره ۱۳/ شماره ۲/ صفحه ۵۵-۴۵

پدافند الکترونیک و سایبری

شاپا الکترونیکی: ۴۳۴۷- ۲۳۲۲۲ شاپا چاپی: ۸۹۷۹-۲۹۸۰

تشخیص ناهنجاری در ترافیک تجهیزات اینترنت اشیا با رویکرد ترکیب مدل‌های یادگیری عمیق

وحید یادگاری[۱]*، صمد سهراب[۲]، وحید محمودیان[۳]

[۱] دانشجوی دکتری، دانشگاه علامه طباطبائی، تهران، ایران (نویسنده مسئول: v.yadegari58@yahoo.com)

[۲] پژوهشگر، مؤسسه آموزش عالی تعالی قم، قم، ایران (mahmoudian.vahid@gmail.com)

[۳] دانشجوی دکتری، دانشکده کامپیوتر، دانشگاه آزاد اسلامی واحد تهران شمال، تهران، ایران (samad_sohrab@yahoo.com)

چکیده (استایل عنوان چکیده)

طبقه‌بندی کننده‌های ترافیک شبکه نقش حیاتی در سیستم‌های نظارت بر شبکه‌ها ایفا می‌کنند و وظیفه آن‌ها تشخیص ناهنجاری‌ها در جریان‌های شبکه‌ای بر اساس ویژگی‌های ارتباطی است. این موضوع برای مدیریت و نظارت بر شبکه‌های اینترنت اشیا نیز اهمیت ویژه‌ای دارد. در این مقاله، یک روش نوین برای طبقه‌بندی ترافیک شبکه بر اساس ترکیبی از مدل‌های یادگیری عمیق ارائه‌شده است که می‌تواند برای طبقه‌بندی ترافیک اینترنت اشیا استفاده شود. نتایج تجربی نشان می‌دهد که مدل ترکیبی CNN+RNN-2 با دقت ۸۳،۵۸درصد، عملکرد بهتری نسبت به مدل‌های منفرد و ترکیبی دیگر ارائه می‌دهد. این مدل با ترکیب ویژگی‌های محلی استخراج‌شده توسط شبکه‌های عصبی کانولوشنال (CNN) و تحلیل وابستگی‌های زمانی توسط شبکه‌های عصبی بازگشتی (RNN)، قادر به شناسایی الگوهای پیچیده‌تری است و دقت تشخیص را بهبود می‌بخشد. همچنین، نتایج به‌دست‌آمده نشان می‌دهد که مدل ترکیبی CNN+RNN-2 بدون نیاز به مهندسی ویژگی دستی، نتایج بهتری نسبت به روش‌های کلاسیک نظارت‌شده، نیمه نظارت‌شده و بدون نظارت ارائه می‌دهد. استفاده از یادگیری عمیق به دلیل توانایی آن در استخراج خودکار ویژگی‌ها و یادگیری الگوهای پیچیده، برتری قابل‌توجهی نسبت به تکنیک‌های سنتی هوش مصنوعی دارد.

مشخصات مقاله

تاریخچه مقاله:

نوع مقاله: علمی پژوهشی

دریافت: ۱۴۰۴/۰۲/۰۳

بازنگری: ۱۴۰۴/۰۳/۰۴

پذیرش: ۱۴۰۴/۰۳/۱۸

ارائه آنلاین: ۱۴۰۴/۰۴/۰۱

کلید واژه‌ها:

شبکه‌های عصبی کانولوشنال

شبکه‌های عصبی بازگشتی

طبقه‌بندی ترافیک شبکه

یادگیری عمیق

اینترنت اشیا

استناد: یادگاری، وحید، محمودیان، وحید، سهراب، صمد. تشخیص ناهنجاری در ترافیک تجهیزات اینترنت اشیا با رویکرد ترکیب مدل‌های یادگیری عمیق. پدافند الکترونیک و سایبری. (۱۴۰۴)؛ ۱۳ (۲): ۵۵-۴۵.

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.2.5.2

ناشر: دانشگاه جامع امام حسین(ع).

۱- مقدمه

طبقه‌بندی ترافیک شبکه اولین گام برای تشخیص ناهنجاری یا سیستم تشخیص نفوذ مبتنی بر شبکه است و نقش مهمی در حوزه امنیت شبکه ایفا می‌کند. در حوزه امنیت شبکه، طبقه‌بندی ترافیک درواقع اولین قدم برای فعالیت‌هایی مانند تشخیص ناهنجاری برای شناسایی استفاده مخرب از منابع شبکه است[۱]. بدیهی است ترافیک اینترنت اشیاء به دلیل تعداد زیاد و ناهمگونی دستگاه‌های متصل، چالش‌های جدیدی را برای سیستم‌های مدیریت و نظارت شبکه فعلی ایجاد خواهد کرد. شناسایی دقیق ترافیک شبکه برای اجرای مدیریت مؤثر سیاست و منابع در شبکه‌های اینترنت اشیاء بسیار مهم است، زیرا شبکه باید بسته به اطلاعات ترافیک واکنش متفاوتی نشان دهد[۲].

در این پژوهش، یک روش نوین برای طبقه‌بندی ترافیک شبکه با استفاده از ترکیب شبکه‌های عصبی کانولوشنال (CNN) و شبکه‌های عصبی بازگشتی (RNN) ارائه‌شده است، طبقه‌بندی ارائه‌شده با استفاده از شبکه عصبی کانولوشن[۱] (CNN) داده‌های ترافیک را به به‌صورت تصاویر به‌عنوان ورودی مدل داده تزریق می‌گردد. در این روش نیازی به استخراج ویژگی به‌صورت دستی نداشته و ترافیک پس از تبدیل‌شدن به تصاویر سیاه‌وسفید، به‌عنوان داده‌های ورودی طبقه‌بندی کننده قرار گرفت. برای آموزش مدل از ۱۵۰،۰۰۰ تصویر که هرکدام یک جریان شبکه‌ای هستند، استفاده گردید. مدل با استفاده از داده‌های آموزشی آموزش داده می‌شود. از تابع فعال‌ساز ReLU و تابع ضرر آنتروپی متقاطع استفاده می‌شود[۳]. بهینه‌سازی مدل با استفاده از الگوریتم Adam انجام می‌شود. همان‌طور که اشاره شد روش پیشنهادی یک طبقه‌بندی بر اساس مدل یادگیری عمیق است که از یک شبکه عصبی کانولوشنال تشکیل‌شده است. در این پژوهش، مقایسه‌ای از نتایج عملکرد برای معماری‌های مختلف ارائه می‌گردد. به‌طور خاص، از شبکه‌های عصبی بازگشتی[۲] (RNN) منفرد، شبکه‌های عصبی کانولوشنال (CNN) منفرد و ترکیب‌های مختلف شبکه‌های عصبی کانولوشنال (CNN) و شبکه‌های عصبی بازگشتی (RNN) در نظر گرفته‌شده است.

چالش اصلی در تشخیص ناهنجاری‌های ترافیک اینترنت اشیا، پیچیدگی و ناهمگونی داده‌هاست. مدل CNN+RNN-2 با ترکیب ویژگی‌های محلی و زمانی، به‌طور مؤثری این چالش را حل کرده است. این مدل بدون نیاز به مهندسی ویژگی دستی، با استفاده از داده‌های ترافیک تبدیل‌شده به تصاویر سیاه‌وسفید، قادر به شناسایی دقیق ناهنجاری‌ها است. نتایج نشان می‌دهد که مدل پیشنهادی ارائه‌شده در این مقاله نسبت به روش‌های کلاسیک نظارت‌شده، نیمه نظارت‌شده و بدون نظارت عملکرد بهتری دارد و می‌تواند به‌عنوان یک ابزار کارآمد در سیستم‌های نظارت بر شبکه‌های اینترنت اشیا به کار گرفته شود.

در این پژوهش، علاوه بر مقایسه مدل ترکیبی با مدل‌های پایه، خروجی مدل ترکیبی با سایر مدل‌های موجود در ادبیات نیز مقایسه شده است تا کارایی و دقت مدل پیشنهادی به‌طور جامع‌تری ارزیابی شود.

در ادامه، روش تحقیق و جزئیات مدل پیشنهادی، شامل فرایند پیش‌پردازش داده‌ها و معماری مدل ترکیبی CNN+RNN، ارائه می‌شود. سپس، نتایج ارزیابی و مقایسه مدل پیشنهادی با سایر مدل‌های مشابه ارائه می‌گردد. درنهایت، نتیجه‌گیری و پیشنهادهایی برای تحقیقات آینده مطرح خواهد شد.

۲- روش تحقیق

۲-۱- تعاریف پایه

۲-۱-۱- تعریف اینترنت اشیا

اینترنت اشیا یک زیرساخت متصل متشکل از اشیا، افراد، سیستم ها، منابع اطلاعاتی و خدمات هوشمند است که به آن‌ها امکان می‌دهد اطلاعات حاصل از دنیای فیزیکی و مجازی را با یکدیگر ترکیب کرده و با استفاده از پردازش‌ها، واکنش‌های مناسب را ایجاد کند[۴].

۲-۱-۲- شبکه‌های عصبی مصنوعی[۳]

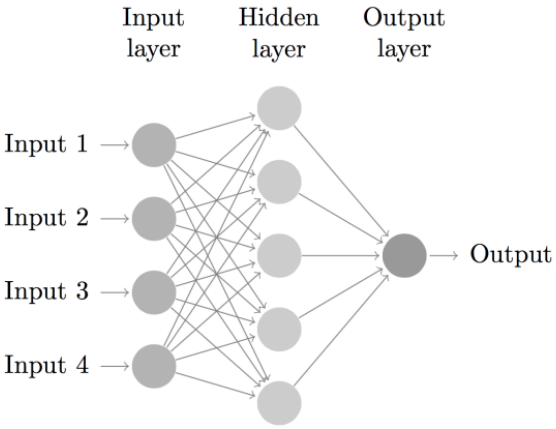
ساختار مغز انسان از شبکه‌های عصبی طبیعی متشکل از تعداد زیادی واحد ساده به نام نرون[۴] ساخته‌شده است. نرون‌ها سه نوع جز تشکیل‌دهنده دارند: دندریت‌ها[۵]، سوما[۶] و آکسون[۷]. هر نرون در داخل خودش با انجام فرایندهای شیمیایی، سیگنالی از خود تولید می‌کند که توسط آکسون نرون به دندریت نرونی دیگر منتقل می‌شود. بر اساس این سیگنال‌های ارسالی، مغز کار خاصی را انجام می‌دهد. شبکه‌های عصبی مصنوعی، یک شبیه‌سازی از ساختار مغز انسان است و بر پایه این فرضیات است:

- پردازش اطلاعات در ساختارهای ساده با تعداد زیاد، به نام نرون‌ها انجام می‌گیرد.
- سیگنال‌ها از طریق اتصالات بین نرون‌های شبکه منتقل می‌شوند.
- هر اتصال، وزن مربوط به خود را دارد که در یک شبکه عصبی این وزن‌ها در سیگنال انتقالی ضرب می‌شوند.
- هر نرون یک تابع فعال‌ساز بر روی جمع وزن‌دار سیگنال‌های ورودی اعمال می‌کند تا سیگنال خروجی را تولید نماید.

[1] Convolutional Neural Network
[2] Recurrent Neural Network
[3] Artificial Neural Networks
[4] Neuron
[5] Dendrites
[6] Soma
[7] Axon

با توجه به این فرضیات، الگوی اتصال بین نرون‌های مختلف شبکه را معماری شبکه و روش تعیین وزن‌ها بر اتصالات را الگوریتم آموزش شبکه گویند[۵]. یک شبکه عصبی از کنار هم قراردادن چندین نرون تشکیل یک‌لایه را می‌دهد.

در حالت کلی، معماری یک شبکه عصبی از ۳ لایه تشکیل‌شده است که عبارت‌اند از: ورود، لایه پنهان و لایه خروج که در شکل (۱) آمده است.

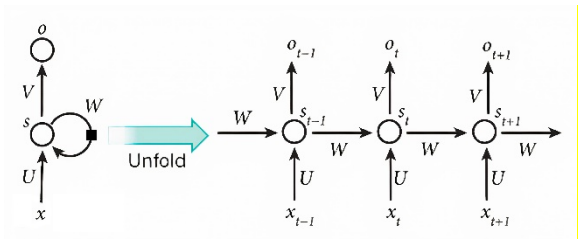


شکل (۱): مدل عمومی از یک شبکه عصبی[۶]

لایه ورودی، اطلاعات را دریافت کرده و یک یا چندلایه پنهان، عمل پردازش را انجام داده و لایه خروجی نتایج را نشان می‌دهد. با افزایش تعداد لایه‌های پنهان، شبکه به سمت عمیق‌شدن سوق پیداکرده که توانایی حل مسائل پیچیده‌تر را نسبت به همتایان کم‌عمق خود دارا است.

۲-۱-۳- شبکه عصبی بازگشتی (RNN)

شبکه‌های عصبی بازگشتی (RNN) به دلیل داشتن حافظه داخلی، برای پردازش داده‌های متوالی مانند سری‌های زمانی و ترافیک شبکه مناسب هستند. این شبکه‌ها قادر به یادگیری وابستگی‌های زمانی در داده‌ها هستند و می‌توانند الگوهای پیچیده‌تری را شناسایی کنند. در یک شبکه عصبی معمولی، ورودی‌ها و خروجی‌ها با یکدیگر ارتباطی ندارند، اما در بعضی کاربردها مثل پیش‌بینی کلمه بعدی در یک متن و یا ترجمه آن، نیاز به دانستن ارتباط بین کلمات است که در غیر این‌صورت، شبکه درست عمل نخواهد کرد. شبکه‌های عصبی بازگشتی، برای کار با داده‌های متوالی طراحی‌شده‌اند. داده‌ها در شبکه عصبی بازگشتی به‌صورت مجموعه‌ای متوالی از بردارها پردازش می‌شوند[۷] و در واحدهای پنهان خود دارای یک بردار حالت هستند، که به‌طور ضمنی حاوی اطلاعاتی در مورد تاریخچه تمامی عناصر متن هستند که به‌صورت دنباله‌ای از کلمات هستند[۸]، به‌طور خلاصه می‌توان گفت که این شبکه‌ها در ساختار درونی خود دارای نوعی حافظه بوده که اطلاعات مشاهده‌شده را در خود ضبط می‌کنند. معماری یک شبکه عصبی بازگشتی در شکل (۲) قابل‌مشاهده است.



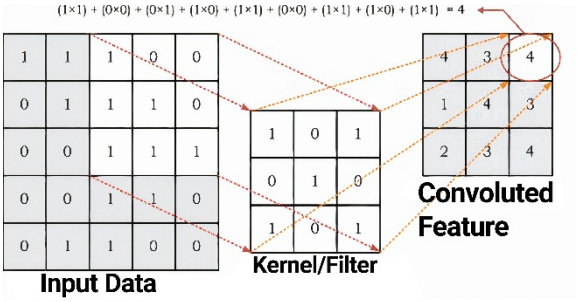
شکل (۲): معماری یک شبکه بازگشتی سه‌لایه[۹]

۲-۱-۴- شبکه‌های عصبی کانولوشنال (CNN)

شبکه‌های عصبی کانولوشنال که از آن‌ها با عنوان شبکه‌های عصبی پیچشی نیز یاد می‌شود، نوع خاصی از شبکه‌های عصبی برای پردازش داده‌هایی می‌باشند که دارای یک ساختار مکانی مشخصی هستند[۱۰]. شبکه‌های عصبی کانولوشنال (CNN) به دلیل توانایی بالای خود در استخراج ویژگی‌های محلی از داده‌های تصویری، برای پردازش داده‌های ساختاریافته مانند تصاویر و ترافیک شبکه بسیار مناسب هستند[۱۱]. این شبکه‌ها از لایه‌های کانولوشن برای استخراج ویژگی‌های تصویر استفاده کرده و برای شناسایی الگوها و اشیاء در تصویر به کار می‌روند. با استفاده از این شبکه‌ها، شبکه‌های عمیق این توانایی را خواهند داشت که داده‌های مکانی ساختاریافته همانند تصویر و متن را یاد بگیرند؛ این شبکه‌ها از لایه‌های کانولوشن برای استخراج ویژگی‌های تصویر استفاده کرده و برای شناسایی الگوها و اشیاء در تصویر به کار می‌روند[۱۲]. شبکه‌های پیچشی به بیانی ساده، شبکه‌های عصبی هستند که از پیچش[۱] به‌جای ضرب ماتریس عمومی، حداقل دریکی از لایه‌های خود استفاده می‌کنند. شبکه های پیچشی در پردازش تصویر کاربردهای زیادی دارند و در پردازش تصویر عملیات روی پیکسل‌ها انجام می‌گیرد[۱۳]. ساختار کلی یک شبکه پیچشی از سه‌لایه تشکیل‌شده که عبارت‌اند از: لایهٔ پیچش[۲]، لایه ادغام[۳] و لایه تماماً متصل[۴].

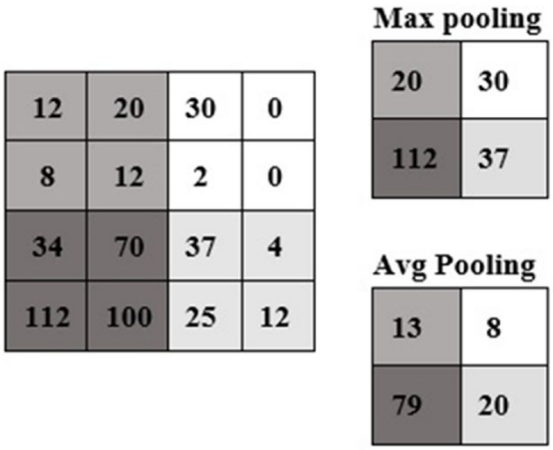
لایه پیچش: در این لایه از طریق عملگر ریاضی پیچش، با اعمال روی فیلترها و ماتریس ورودی، ویژگی‌ها یاد گرفته می‌شوند. شکل (۳) نمایشی از عملگر پیچش را در یک شبکه عصبی پیچشی نشان می‌دهد. همان‌طور که مشاهده می‌شود ماتریس نقشه ویژگی ۴×۳ با اعمال عملگر پیچش با ماتریس هسته‌ای[۵] در ابعاد ۲×۲ یک‌ضرب نقطه‌به‌نقطه انجام داده و در پایان خروجی با ابعاد ۳×۲ داشته است[۷].

[1] Convolution
[2] Convolution Layer
[3] Pooling Layer
[4] Fully Connected Layer
[5] Kernel



شکل (۳): عملیات پیچش[۶]

لایه ادغام: این لایه وظیفه کاهش ابعاد و تعداد پارامترهای شبکه را انجام می‌دهد. ادغام حداکثری[۱] و ادغام میانگین[۲] دو عملگر اصلی این لایه هستند. ادغام حداکثری، بارزترین ویژگی‌ها (بیشترین مقادیر موجود در هر پنجره انتخاب‌شده) را از نقشه ویژگی استخراج می‌کند. برای مثال در یک تصویر، لبه‌ها را کشف می‌کند. ادغام میانگین مقادیر میانگین پنجره انتخاب‌شده را استخراج می‌کند. شکل (۴) تفاوت بین ادغام حداکثری و ادغام میانگین را نشان می‌دهد. در شکل برای هر نقشه ویژگی ۴×۴ یک پنجره ۲×۲ اعمال‌شده، مشاهده می‌گردد که در ادغام حداکثری بزرگ‌ترین مقادیر و در ادغام میانگین، مقادیر میانگین این پنجره‌های انتخاب‌شده محاسبه می‌شود.



شکل (۴): تفاوت ادغام حداکثری و میانگین[۶]

لایه متصل کامل: عملکرد این لایه همانند یک شبکه پرسپترون چندلایه[۳] است که در آن، نرون‌های یک‌لایه به نرون‌های لایه بعدی به‌طور کامل متصل بوده و مشخص می‌کند که کدام ویژگی، بیشترین ارتباط را با یک کلاس خاص دارد. این لایه همان‌جایی است که طبقه‌بندی در آن اتفاق می‌افتد.

۲-۲- مجموعه داده

برای ارزیابی مدل ترکیبی، از مجموعه داده‌های مختلفی استفاده‌شده است که شامل مجموعه داده CIC IoT 2022 [۱۳] و مجموعه داده‌های دیگر از پژوهش‌های مشابه، شامل ترافیک شبکه دستگاه‌های اینترنت اشیا که از طریق دروازه[۴] با استفاده از نرم‌افزارهای Wireshark و dumpcap در شش نوع آزمایش مختلف وارد می‌شوند، گردآوری‌شده است. این مجموعه داده از دسته‌های مختلف فعالیت دستگاه‌ها ازجمله قدرت[۵]، زمان بیکار[۶]، فعل‌وانفعال[۷]، سناریوها[۸]، فعال[۹] و حملات[۱۰] تشکیل‌شده است. بخش فعل‌وانفعال شامل ترافیک حالت عادی تجهیزات بوده و یکی از کلاس‌ها بوده که با عنوان کلاس Normal برچسب‌گذاری شده و بخش حملات نیز به‌عنوان ترافیک موردحمله از نوع سیل‌آسا[۱۱] و با عنوان کلاس Flood برچسب‌گذاری گردیده است. همان‌طور که در شکل (۵) قابل‌مشاهده است، ۸۰درصد از نمونه‌ها را به‌عنوان مجموعه آموزشی[۱۲]، ۱۰ درصد به‌عنوان آزمون[۱۳] و ۱۰درصد دیگر به‌عنوان ارزیابی[۱۴] مدل استفاده‌شده است.

در جدول (۱) تعداد نمونه‌ها با جزئیات بیشتر قابل‌مشاهده است.

شکل (۵): نمودار توزیع داده‌ها

جدول (۱): تعداد نمونه‌های مجموعه داده

عنوان	تعداد	درصد
تعداد کل نمونه‌های آموزشی	۱۲۰ هزار نمونه	٪۸۰
تعداد کل نمونه‌های آزمون	۱۵ هزار نمونه	٪۱۰
تعداد کل نمونه‌های ارزیابی	۱۵ هزار نمونه	٪۱۰

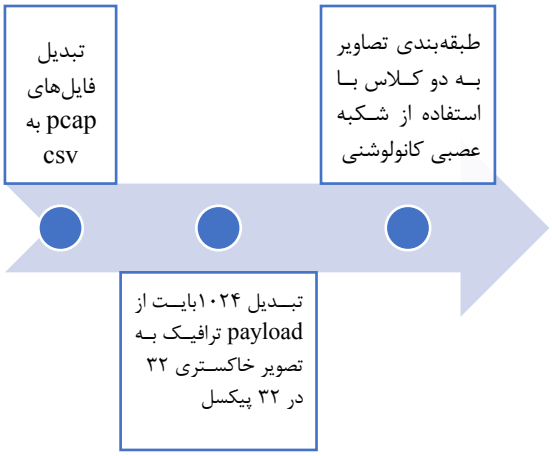
۲-۳- پیش‌پردازش[۱۵]

طبقه‌بندی ترافیک اولین گام برای تشخیص ناهنجاری شبکه یا سیستم تشخیص نفوذ مبتنی بر شبکه است و نقش مهمی در حوزه امنیت شبکه ایفا می‌کند. ترافیک مشاهده‌شده در یک سیستم شبکه را می‌توان به‌طور عمده به دو نوع تقسیم کرد:

[1] Max Pooling
[2] Average Pooling
[3] Multilayer Perceptron

[4] Gateway
[5] Power
[6] Idle
[7] Interactions
[8] Scenarios
[9] Active
[10] Attack
[11] Flood
[12] Train
[13] Test
[14] Validation
[15] Preprocess

ترافیک عادی[1] و ترافیک مخرب[2] ترافیک غیرضروری از منابع مخرب می‌تواند مشکلات زیادی مانند سیل پهنای باند شبکه[3]، حملات منع سرویس[4] و مسدود کردن گیرنده ایجاد کند، بنابراین تشخیص چنین ترافیک ناخواسته و طبقه‌بندی ترافیک موردنیاز بسیار مهم است. در شکل (۶) مراحل انجام پیش‌پردازش قابل‌مشاهده است.



شکل (۶): مراحل پیش‌پردازش

پیش‌پردازش مجموعه داده مورداستفاده[۱۴] شامل فرایند تبدیل ترافیک خام که از شبکه اینترنت اشیاء که با کمک نرم‌افزار وایرشارک[5] جمع‌آوری‌شده است. داده‌ها به سه دسته تقسیم‌شده‌اند: ۸۰٪ برای آموزش، ۱۰٪ برای آزمون، و ۱۰٪ برای ارزیابی مدل که به تصاویر سیاه‌وسفید تبدیل‌شده‌اند. از این تصاویر برای طبقه‌بندی ترافیک شبکه و ورودی مدل استفاده می شود[۱۵].

ازآنجایی‌که ترافیک خام شبکه‌ها معمولاً در قالب فایل‌های pcap. یا pcapng. ذخیره می‌شود، نمی‌توان آن را مستقیماً به شبکه عصبی وارد کرد و مدل شبکه عصبی مستلزم یکنواخت بودن طول داده‌های ورودی است، اما طول ترافیک خام شبکه یکنواخت نیست؛ بنابراین، برای تبدیل ترافیک خام شبکه به فرمت تصویر سیاه‌وسفید که به‌عنوان ورودی مدل استفاده می‌شود، نیاز به‌پیش پردازش داده‌ها است و سپس روش‌های مربوطه برای آموزش، آزمون و ارزیابی مدل برای دستیابی به هدف طبقه‌بندی ترافیک، فراخوانی می‌شود. فرایند پیش‌پردازش عمدتاً شامل تقسیم ترافیک، تمیز کردن ترافیک، ترکیب مجدد ترافیک و تبدیل ترافیک است.

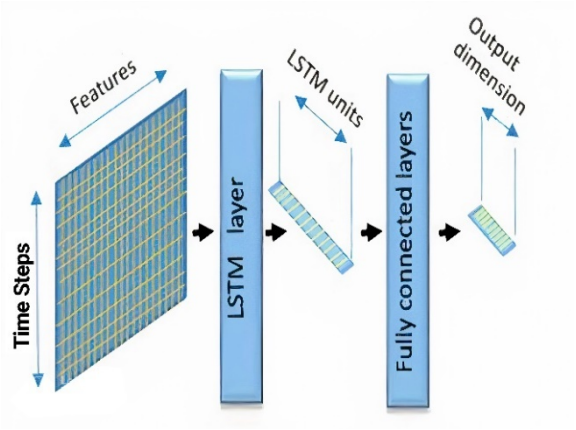
همان‌طور که اشاره شد فایل‌های ترافیک از نوع pcap هستند که ابتدا باید به CSV[6] تبدیل‌شده و فیلدهای مؤثر آن استخراج گردد. برای انکار از نرم‌افزار nPrint [۱۴] استفاده‌شده که وظیفه تبدیل فایل‌های ترافیک به CSV را دارد، درواقع nPrint یک بازنمایی استاندارد از داده‌های ترافیک شبکه است که به‌طور مستقیم با الگوریتم‌های یادگیری ماشین قابل‌استفاده بوده و جایگزین مهندسی ویژگی[7] برای طیف گسترده‌ای از مشکلات تحلیل ترافیک است. مطابق تصاویر قابل‌مشاهده در شکل (۷)، رکوردهای موجود در فایل‌های CSV به تصاویر سیاه‌وسفید در ابعاد ۳۲ در ۳۲ پیکسل تبدیل می‌شوند تا به‌عنوان ورودی به مدل طبقه‌بندی کانولوشن واردشده و طبقه‌بندی روی تصاویر انجام شود.

شکل (۷): نمونه تصاویر ۳۲ در ۳۲ پیکسل

۲-۴- مدل پیشنهادی

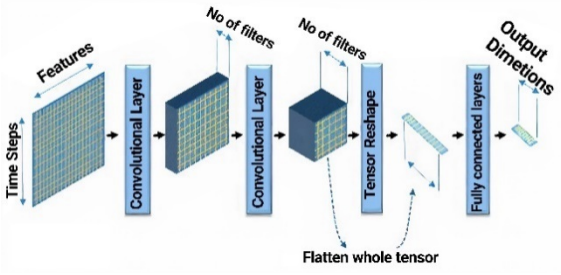
برای مقایسه مدل ترکیبی، از مدل‌های مختلفی که در پژوهش‌های مشابه استفاده‌شده‌اند، بهره‌برداری شده است. این مدل‌ها شامل شبکه‌های عصبی کانولوشنال منفرد (CNN)، شبکه‌های عصبی بازگشتی منفرد (RNN)، و مدل‌های ترکیبی دیگر مانند CNN+LSTM و CNN+GRU هستند. مدلی که بهترین عملکرد و دقت تشخیص را داشت ترکیبی از شبکه عصبی کانولوشنال (CNN)[۱۶] و شبکه عصبی بازگشتی (RNN)[۱۷] بوده است. ترکیب شبکه‌های عصبی کانولوشنال (CNN) و شبکه‌های عصبی بازگشتی (RNN) این امکان را می‌دهد که از مزایای هر دو نوع شبکه بهره‌مند شد. شبکه‌های عصبی کانولوشنال ویژگی‌های محلی را استخراج می‌کنند و سپس این ویژگی‌ها به شبکه‌های عصبی بازگشتی ارسال می‌شوند تا ارتباطات زمانی بین ویژگی‌ها تحلیل شوند. این ترکیب باعث می‌شود که مدل ما بتواند الگوهای پیچیده‌تری را شناسایی کند و دقت تشخیص را افزایش دهد. در این قسمت تمامی مدل‌هایی که موردبررسی قرارگرفته‌اند، بررسی خواهد شد. اولین مدل، یک RNN ساده است. به‌طور خاص، از یک نوع RNN به نام LSTM[8] [۱۷] استفاده‌شده که آموزش آن آسان‌تر بوده و مشکل محوشدگی گرادیان نیز حل‌شده است، یک LSTM با ماتریسی از مقادیر با دو بعد، آموزش داده می‌شود: بُعد زمانی و بردار ویژگی‌ها. LSTM یک شبکه عصبی (سلول) را با بردارهای ویژگی متوالی زمانی و دو بردار اضافی مرتبط باحالت‌های پنهان داخلی و سلولی آن تکرار می‌کند. حالت پنهان نهایی سلول با مقدار خروجی مطابقت دارد؛ بنابراین، بعد از خروجی یک‌لایه LSTM با اندازه حالت پنهان داخلی آن (واحدهای LSTM) برابر است. در مدل شکل (۸) در انتها چندین لایه کاملاً متصل اضافه می‌گردد.

[1] Normal
[2] Malign
[3] Flood
[4] Denial of Service
[5] Wireshark
[6] Comma-Separated Values
[7] Feature Engineering
[8] Long Short Term Memory(LSTM)



شکل (۸): مدل یادگیری عمیق RNN [۱۸]

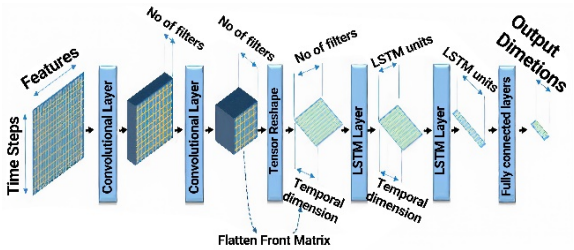
در شکل (۹) یک شبکه CNN قابل‌مشاهده است. CNNها ابتدا برای پردازش تصویر به‌عنوان یک مدل الهام گرفته‌شده از بیولوژیک برای انجام طبقه‌بندی تصویر استفاده می‌شدند، جایی که مهندسی ویژگی به‌طور خودکار توسط شبکه به لطف عملکرد هسته (فیلتر) انجام می‌شد که الگوهای ثابت مکان را از تصویر استخراج می‌کند. متصل کردن چندین لایه کانولوشن امکان استخراج خودکار ویژگی‌های پیچیده را فراهم می‌کند. از این روش پردازش تصویر برای اعمال تکنیک در مجموعه داده‌های بسیار متفاوت استفاده‌شده است. برای انجام این کار، ماتریس تشکیل‌شده توسط سری‌های زمانی، بردارهای ویژگی را به‌عنوان یک تصویر در نظر می‌گیرد. پیکسل‌های تصویر به‌صورت محلی در ارتباط هستند. به‌طور مشابه، بردارهای ویژگی مرتبط با شکاف‌های زمانی متوالی، یک رفتار محلی همبسته را نشان می‌دهند که اجازهٔ این قیاس را اتخاذ می‌کند. هر لایه کانولوشن یک آرایه چندبعدی[1] تولید می‌کند که در آن ابعاد تصویر کاهش می‌یابد، اما در همان زمان، یک بعد جدید تولید می‌شود که اندازه این بعد برابر با تعداد فیلترهای اعمال‌شده بر روی تصویر است. لایه‌های متوالی کانولوشن باعث کاهش بیشتر ابعاد تصویر و افزایش اندازه ابعاد جدید تولیدشده می‌شود. برای تکمیل مدل، لازم است تنسور را به بردار تبدیل کرد که می‌تواند ورودی لایه‌های کاملاً متصل نهایی باشد. برای انجام این تبدیل می‌توان یکدست تانسور ساده انجام داد.



شکل (۹): مدل یادگیری عمیق (CNN) [۱۶]

[1] Tensor

درنهایت، مدل معرفی‌شده در شکل (۱۰) مدلی از ترکیب یک CNN و دو LSTM ایجاد شد. هنگامی‌که چندین لایه LSTM به هم متصل می‌شوند. علاوه بر این، برای انواع مختلف لایه‌هایی که قبلاً ارائه شد، از چندلایه اضافی استفاده می‌شود: نرمال‌سازی دسته‌ای، حداکثر ادغام و لایه‌های حذف تصادفی یک‌لایه با حذف (تنظیم روی صفر) درصدی از خروجی‌ها از لایه قبلی، منظم سازی[2] (تعمیم نتایج برای داده‌های دیده نشده) را فراهم می‌کند[۱۲]. این اقدام ظاهراً بی‌معنی، شبکه را وادار کرده که بیش‌ازحد بر هیچ ورودی خاصی تکیه نکند، با بیش برازش[3] مقابله کند و تعمیم سازی را بهبود بخشد. ادغام حداکثری[4][۱۹] نوعی لایه کانولوشن بوده که تفاوت در فیلتر استفاده‌شده است. در ادغام حداکثری از فیلتر انتخاب مقادیر حداکثر استفاده گردیده که بیشترین مقدار ناحیه تصویری را که فیلتر روی آن اعمال می‌شود را انتخاب می‌کند. اندازه فضایی خروجی و تعداد ویژگی‌ها و پیچیدگی محاسباتی شبکه را کاهش می‌دهد. مشابه لایهٔ حذف تصادفی، یک‌لایهٔ ادغام حداکثری منظم سازی را فراهم می‌کند. نرمال‌سازی دسته‌ای همگرایی آموزش را سریع‌تر کرده و می‌تواند نتایج عملکرد را بهبود بخشد[۲۰]. این کار با نرمال‌سازی در زمان آموزش، هر ویژگی در سطح دسته‌ای و مقیاس بندی مجدد بعدی، با درنظرگرفتن کل مجموعه داده آموزشی انجام می‌شود. میانگین و واریانس آموزش داده‌شده، جایگزین آن‌هایی می‌شود که در سطح دسته‌ای احصاء گردیده‌اند.



شکل (۱۰): مدل یادگیری عمیق (CNN) و دولایه LSTM [۱۸]

۳- ارزیابی

روش پیشنهادی، ترکیبی از شبکه‌های عصبی کانولوشنال (CNN) و دو شبکه عصبی بازگشتی (RNN) است که به‌طور خاص برای تشخیص ناهنجاری‌های ترافیک اینترنت اشیا طراحی‌شده است. شبکه‌های عصبی کانولوشنال به دلیل توانایی بالای خود در استخراج ویژگی‌های محلی از داده‌های تصویری، برای پردازش داده‌های ساختاریافته مانند تصاویر و ترافیک شبکه بسیار مناسب هستند. از سوی دیگر، شبکه‌های عصبی بازگشتی به دلیل داشتن حافظه داخلی، برای پردازش داده‌های متوالی مانند سری‌های زمانی و ترافیک شبکه مناسب هستند؛ بنابراین

[2] Regularization
[3] Overfitting
[4] Max Pooling

لایه‌های کانولوشنال ویژگی‌های محلی را استخراج می‌کنند و سپس این ویژگی‌ها به لایه‌های بازگشتی ارسال می‌شوند تا ارتباطات زمانی بین ویژگی‌ها تحلیل شوند. با بررسی نتایج به‌دست‌آمده از RNN-1 منفرد، CNN-1 منفرد و مدل CNN+RNN-2، مدل CNN+RNN-2 بهترین نتایج را برای معیارهای ارزیابی ارائه می‌دهد که در معادله‌های (۱ تا ۴) نحوه محاسبه معیارهای ارزیابی قابل‌مشاهده است. در تمامی مراحل آموزش مدل، آموزش با تعداد دوره[1] بین ۶۰ تا ۹۰ انجام گردید که ۱۰ دوره آخر تابع ضرر[2] را بهبود بخشیده که با توقف زودهنگام انجام شد. برای تابع فعال‌ساز[3] از تابع یک‌سوساز خطی[4] (ReLU) استفاده گردیده است و در آخرین لایه از تابع فعال‌ساز Softmax با تابع ضرر آنتروپی متقاطع[5] و بهینه‌ساز با گرادیان کاهشی نزولی[6] (SGD) و آدام[7] (Adam) انجام شد. جدول (۲) جزئیات معماری مدل شبکه‌های عصبی را نشان داده‌شده است.

$$Accuracy = \frac{TP+TN}{TP+FN+TN+FP} \quad (۱)$$

$$Precision = \frac{TP}{TP+FP} \quad (۲)$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \quad (۳)$$

$$F1 - Score = \frac{2\times Precision\times recall}{Precision\times recall} \quad (۴)$$

مدل با استفاده از داده‌های آزمون و ارزیابی می‌شود. جدول (۳) معیارهای ارزیابی مدل‌ها که شامل دقت[8]، امتیاز F1[9]، صحت[10] و فراخوان[11] را نشان می‌دهد.

۴- مقایسه با تحقیقات مشابه

در پژوهش حاضر، مدل ترکیبی CNN+RNN-2 با سایر مدل‌های ارائه شده در ادبیات مقایسه گردیده است. برای مثال، در مقاله لی و وانگ[۲۲]، تشخیص بی‌درنگ ترافیک شبکه بر اساس شبکه‌های عصبی کانولوشنال (CNN) منفرد بررسی‌شده است. این مدل‌ها به دلیل توانایی در استخراج ویژگی‌های مکانی، در تشخیص ناهنجاری‌ها موفق بوده‌اند، اما به دلیل عدم تحلیل وابستگی‌های زمانی، در مقایسه با مدل پیشنهادی ما، دقت کمتری داشته‌اند. در مقابل، پژوهش دوان و همکاران[۲۳] از طبقه‌بندی کننده‌های باقیمانده چند مقیاسی استفاده کرده‌اند که بر پایه شبکه‌های عصبی بازگشتی (RNN) منفرد طراحی‌شده است. اگرچه این مدل‌ها قادر به تشخیص وابستگی‌های زمانی هستند، اما در استخراج ویژگی‌های محلی به‌اندازه مدل ترکیبی ما کارآمد نبوده‌اند بنابراین هرکدام از این مدل‌ها به‌تنهایی قادر به تشخیص ناهنجاری‌ها هستند، اما دقت تشخیص آن‌ها نسبت به مدل ترکیبی ارائه شده در این مقاله کمتر است؛ زیرا نتایج ارزیابی همانند جدول شماره ۴ است.

جدول (۲): جزئیات مدل‌های شبکه عصبی برای طبقه‌بندی ترافیک

مدل	جزئیات معماری	نام
مدل ترکیبی از شبکه عصبی کانولوشنال (CNN) و شبکه عصبی بازگشتی (RNN)	Conv(32,4,2,1,V)-BN-Conv(64,4,2,1,V)-BN-LSTM(100)-DR(0.2)-FC(100)-DR(0.4)-FC(108)	CNN+RNN-2
شبکه عصبی کانولوشنال (CNN)	Conv(32,4,2,1,V)-MaxPool(3,2,1,V)-BN-Conv(64,4,2,1,V)-MaxPool(3,2,1,V)-BN-FC(200)-FC(108)	CNN-1
شبکه عصبی بازگشتی (RNN)	LSTM(100)-FC(100)-FC(108)	RNN-1
مدل ترکیبی از شبکه عصبی کانولوشنال (CNN) و شبکه عصبی بازگشتی (LSTM)	Conv(32,4,2,1,V)-BN-Conv(64,4,2,1,V)-BN-LSTM(100)-DR(0.2)-FC(100)-DR(0.4)-FC(108)	CNN+LSTM
مدل ترکیبی از شبکه عصبی کانولوشنال (CNN) و شبکه عصبی بازگشتی [۲۱]	Conv(32,4,2,1,V)-BN-Conv(64,4,2,1,V)-BN-GRU(100)-DR(0.2)-FC(100)-DR(0.4)-FC(108)	CNN+GRU

جدول (۳): معیارهای ارزیابی مدل‌ها

مدل	دقت	امتیاز F1	صحت	فراخوان
CNN+RNN-2	۰,۸۳۵۸	۰,۸۱۷۰	۰,۸۲۷۹	۰,۸۳۸۸
CNN-1	۰,۸۱۰۲	۰,۷۸۰۹	۰,۷۸۴۳	۰,۸۱۰۲
RNN-1	۰,۷۸۵۵	۰,۷۴۳۳	۰,۷۵۰۰	۰,۷۸۵۵
CNN+LSTM	۰,۸۲۵۰	۰,۸۰۵۰	۰,۸۱۵۰	۰,۸۳۰۰
CNN+GRU	۰,۸۲۰۰	۰,۸۰۰۰	۰,۸۱۰۰	۰,۸۲۵۰

[1] Epoch
[2] Loss Function
[3] Activation Function
[4] Rectified Linear Unit (ReLU)
[5] Cross Entropy Loss
[6] Stochastic Gradient Descent
[7] Adam
[8] Accuracy
[9] F1-Score
[10] Precision
[11] Recall

جدول (۴): نتایج ارزیابی مدل‌های مقاله‌های نمونه

فراخوان	صحت	امتیاز F1	دقت	مدل	ارجاع
—	۰.۹۸۵	۰.۹۸۴	۰.۹۸۵	*Flow Transformer*	[۲۴]
۰.۹۹۹۳	۰.۹۹۹۳	۰.۹۹۹۳	۰.۹۹۹۳	*FFNN*	[۲۵]
۰.۹۹۸۹	۰.۹۹۸۹	۰.۹۹۸۹	۰.۹۹۸۹	*LSTM*	
۰.۹۶۴۲	۰.۹۶۴۲	۰.۹۶۴۲	۰.۹۶۴۲	*RandNN*	
۰.۸۳۸۸	۰.۸۱۷۰	۰.۸۲۷۹	۰.۸۳۵۸	*CNN+RNN-2*	پیشنهادی
۰.۸۱۰۲	۰.۷۸۴۳	۰.۷۸۰۹	۰.۸۱۰۲	*CNN-1*	تست مدل
۰.۷۸۵۵	۰.۷۵۰۰	۰.۷۴۳۳	۰.۷۸۵۵	*RNN-1*	تست مدل
۰.۸۳۰۰	۰.۸۱۵۰	۰.۸۰۵۰	۰.۸۲۵۰	*CNN+LSTM*	تست مدل
۰.۸۲۵۰	۰.۸۱۰۰	۰.۸۰۰۰	۰.۸۲۰۰	*CNN+GRU*	تست مدل

مزیت اصلی مدل CNN+RNN-2 در توانایی ترکیب ویژگی‌های محلی و زمانی است که از طریق شبکه‌های کانولوشنال و بازگشتی به دست می‌آید. این مدل به‌طور مؤثری الگوهای پیچیده‌تری را شناسایی می‌کند و در تمامی معیارهای ارزیابی مانند دقت، صحت، فراخوان و امتیاز F1 عملکرد بهتری نسبت به مدل‌های منفرد دارد. به‌طور خاص، مدل پیشنهادی، دقت ۸۳٫۵۸٪ و امتیاز F1 81.70% را به دست آورده است که به‌طور معناداری بالاتر از مدل‌های منفرد ذکرشده در پژوهش‌های مشابه است.

تحلیل‌های آماری انجام‌شده نشان می‌دهد که بهبودهای حاصل‌شده در مدل پیشنهادی به‌صورت آماری معنادار هستند. آزمون‌های آماری مختلف تأیید می‌کنند که تفاوت‌های مشاهده‌شده در عملکرد مدل‌ها به دلیل ویژگی‌های ذاتی مدل ترکیبی ما است و نه به دلیل تغییرات تصادفی در داده‌ها. این تحلیل‌ها نشان می‌دهند که مدل CNN+RNN-2 ازنظر تئوری و عملی برتری قابل‌توجهی نسبت به مدل‌های موجود دارد و می‌تواند به‌عنوان یک روش مؤثر برای طبقه‌بندی ترافیک اینترنت اشیا مورداستفاده قرار گیرد.

۵- نتیجه‌گیری

ترکیب شبکه عصب کانولوشنال (RNN) و شبکه‌های عصبی بازگشتی (RNN) در مدل CNN+RNN-2، توانسته است به‌طور مؤثری ناهنجاری‌های ترافیک اینترنت اشیاء را با دقت بالا تشخیص دهد. این مدل با ترکیب ویژگی‌های محلی استخراج‌شده توسط CNN و تحلیل وابستگی‌های زمانی توسط RNN، قادر به شناسایی الگوهای پیچیده‌تری است و باعث بهبود عملکرد در معیارهای ارزیابی مانند دقت، صحت، فراخوان و امتیاز F1 شده است. به‌طور خاص، این مدل توانست در مجموعه داده‌های مختلف ازجمله CIC IoT 2022، عملکرد برتری نسبت به مدل‌های منفرد مانند CNN-1 و RNN-1 و همچنین مدل‌های ترکیبی دیگر مانند CNN+LSTM و CNN+GRU نشان دهد. [۲۶] و [۲۷]. تحلیل‌های آماری انجام‌شده بر روی نتایج نشان‌دهنده‌ی بهبودهای معنادار آماری در عملکرد مدل پیشنهادی در مقایسه با سایر مدل‌های موجود است. آزمون‌های آماری مختلف تأیید کرده‌اند که این بهبودها ناشی از ویژگی‌های ذاتی مدل ترکیبیِ ارائه شده در این پژوهش است. این نتایج نشان می‌دهند که روش پیشنهادی می‌تواند به‌عنوان یک ابزار کارآمد و مؤثر برای طبقه‌بندی ترافیک شبکه‌های اینترنت اشیاء به کار گرفته شود، به‌ویژه در شرایطی که داده‌ها به‌صورت متوالی و با پیچیدگی بالا هستند.

درنهایت، مزیت دیگر مدل پیشنهادی این است که بدون نیاز به مهندسی ویژگی دستی، و تنها با تعداد کمی از ویژگی‌ها، به نتایج مطلوب دست‌یافته است. ویژگی‌های مؤثر به‌صورت خودکار توسط لایه‌های کانولوشنال استخراج می‌شوند و نیازی به تکیه‌بر آدرس‌های IP یا داده‌های اصلی نیست که احتمالاً محرمانه یا رمزگذاری شده هستند. این امر باعث می‌شود که مدل پیشنهادی در مواجهه با ترافیک ناشناخته و داده‌های جدید، قابلیت تعمیم بهتری داشته باشد و بتواند به‌عنوان یک راهکار مؤثر در سیستم‌های نظارت بر شبکه‌های اینترنت اشیا استفاده شود.

۶- پیشنهادها برای تحقیقات آینده

۱. بهبود مدل: تحقیقات آینده می‌تواند بر روی بهبود مدل CNN+RNN-2 با استفاده از تکنیک‌های پیشرفته‌تر یادگیری عمیق و بهینه‌سازی تمرکز کند.

۲. گسترش به مجموعه داده‌های جدید: بررسی عملکرد مدل بر روی مجموعه داده‌های جدید و متنوع‌تر می‌تواند به تعمیم‌پذیری و کارایی بیشتر مدل کمک کند.

۳. کاربردهای عملی: توسعه کاربردهای عملی مدل در سیستم‌های نظارت بر شبکه‌های اینترنت اشیا و بررسی تأثیر آن بر بهبود امنیت و مدیریت شبکه.

۷- مراجع

- [1] B. Kaur and V. Dhir, "Internet of things: Vision, challenges and future scope," International Journal of Advanced Research in Computer Science, vol. 8, no. 4, pp. 40-43, 2017.

[2] T. Fougeroux, A. Douyere, P. O. L. de Peslouan, N. M. 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] M. Lee, "Mathematical analysis and performance evaluation of the gelu activation function in deep learning," Journal of Mathematics, vol. 2023, no. 1, p. 4229924, 2023.

[4] F. Masoodi and B. A. Pandow, "Internet of things: Financial perspective and its associated security concerns," International Journal of Electronic Finance, vol. 10, no. 3, pp. 145-158, 2021.

[5] A. Sivanathan, "IoT behavioral monitoring via network traffic analysis," arXiv preprint arXiv:2001.10632, 2020.

[6] X. Zhao, L. Wang, Y. Zhang, X. Han, M. Deveci, and M. Parmar, "A review of convolutional neural networks in computer vision," Artificial Intelligence Review, vol. 57, no. 4, p. 99, 2024.

[7] A. Kumar and T. J. Lim, "Early detection of Mirai-like IoT bots in large-scale networks through sub-sampled packet traffic analysis," in Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC), Volume 2, 2020: Springer, pp. 847-867.

[8] 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: IEEE, pp. 1-7.

[9] E. Nichani, A. Damian, and J. D. Lee, "Provable guarantees for nonlinear feature learning in three-layer neural networks," Advances in Neural Information Processing Systems, vol. 36, 2024.

[10] A. E. Omolara, A. Alabdulatif, O. I. Abiodun, M. Alawida, A. Alabdulatif, and H. Arshad, "The internet of things security: A survey encompassing unexplored areas and new insights," Computers & Security, vol. 112, p. 102494, 2022.

[11] N. Mahmoodi, H. Shirazi, M. Fakhredanesh, and K. Dadashtabar Ahmadi, "Improving the performance of the convolutional neural network using incremental weight loss function to deal with class imbalanced data," Electronic and Cyber Defense, vol. 11, no. 4, pp.-34-17, 2024.(persian)https://dor.isc.ac/dor/20.1001.1.23224347.1402.11.4.2.9

[12] 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," Biocybernetics and Biomedical Engineering, vol. 40, no. 1, pp. 23-39, 2020.

[13] M. Hassani and E. Sarmadi, "A recommender system using a support vector machine and the TOPSIS model in the Internet of Things," Electronic and Cyber Defense, vol. 11, no. 4, pp.-61-73, 2024.(persian).https://dor.isc.ac/dor/20.1001.1.23224347.1402.11.4.5.2

[14] P. Pietrzak, P. Pietrzak, and M. Wolkiewicz, "Microcontroller-Based Embedded System for the Diagnosis of Stator Winding Faults and Unbalanced Supply Voltage of the Induction Motors," Energies, vol. 17, no. 2, p. 387, 2024.

[15] H. Tanha and M. Abbasi, "Identify malicious traffic on IoT infrastructure using neural networks and deep learning," Electronic and Cyber Defense, vol. 11, no. 2, pp. 1-13, 2023.(persian).https://dor.isc.ac/dor/20.1001.1.23224347.1402.11.2.1.4

[16] I. AlMohimeed, "Epilepsy Seizure Identification Using the One Dimensional Convolutional Neural Network from Electroencephalogram Signals," in 2024 2nd International Conference on Networking and Communications (ICNWC), 2024: IEEE, pp. 1-6.

[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: The Steering Committee of The World Congress in Computer Science, Computer …, p. 61.

[18] Y. Zhang, Q. Huang, W. Sun, F. Chen, D. Lin, and F. Chen, "Research on lung sound classification model based on dual-channel CNN-LSTM algorithm," Biomedical Signal Processing and Contr

[19] ol, vol. 94, p. 106257, 2024.

[20] 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.

[21] M. Mohammadrezaei, "Detecting Fake Accounts in Social Networks Using Principal Components Analysis and Kernel Density Estimation Algorithm (A Case Study on the Twitter Social Network)," Electronic and Cyber Defense, vol. 9, no. 3, pp. 109-123,

2021.(persian).https://dor.isc.ac/dor/20.1001.1.23224347.1400.9.3.9.0

[22] G. N. Arzhantseva, C. H. Cashen, D. Gruber, and D. Hume, "Characterizations of Morse quasi-geodesics via superlinear divergence and sublinear contraction," Documenta Mathematica, vol. 22, pp. 1193-1224, 2017.

[23] H. Liu and H. Wang, "Real-Time Anomaly Detection of Network Traffic Based on CNN," Symmetry, vol. 15, no. 6, p. 1205, 2023.

[24] X. Duan, Y. Fu, and K. Wang, "Network traffic anomaly detection method based on multi-scale residual classifier," Computer Communications, vol. 198, pp. 206-216, 2023.

[25] R. Zhao et al., "A novel traffic classifier with attention mechanism for industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 19, no. 11, pp. 10799-10810, 2023.

[26] S. A. Bakhsh, M. A. Khan, F. Ahmed, M. S. Alshehri, H. Ali, and J. Ahmad, "Enhancing IoT network security through deep learning-powered Intrusion Detection System," Internet of Things, vol. 24, p. 100936, 2023.

[27] 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," Electronic and Cyber Defense, vol. 9, no. 2, pp. 9-16, 2021.(persian).

[28] 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: IEEE, pp. 382-388.