

## Deep Learning-Based DDoS Attack Detection System with Attention Mechanism

M. Nosrati<sup>1</sup> , F. Bagheri<sup>2\*</sup> 

<sup>1</sup> Master's Student, Golestan University, Gorgan, Iran (\*Correspondence: [f.bagheri@gu.ac.ir](mailto:f.bagheri@gu.ac.ir))

<sup>2</sup> Assistant Professor, Golestan University, Gorgan, Iran. [sobazino@gmail.com](mailto:sobazino@gmail.com)

### ARTICLE INFO

#### Article history:

**Article Type:** Research paper

**Received:** 19 January 2026

**Revised:** 07 March 2026

**Accepted:** 13 April 2026

**Available online:** 21 April 2026

#### Keywords:

Intrusion Detection System  
Neural Network  
Attention Mechanism  
Distributed Denial of Service  
Attack

### ABSTRACT

With the rapid expansion of the internet and the increasing number of devices connected to the network, the level of cyberattacks has increased significantly. One of the serious threats in this field is Distributed Denial of Service (DDoS) attacks, which use a large number of infected systems to direct a massive volume of traffic towards specific targets. The distributed and scalable nature of these attacks makes detecting and defending against them considerably more difficult than other security threats. In recent years, various models have been developed to detect these types of attacks, but many of them face challenges in accurate detection or reducing the error rate. To address this issue, this paper proposes an intrusion detection system based on deep neural networks and an attention mechanism. The proposed method was implemented using the Python programming language and the PyTorch library and tested on the CICIDS2017, CICIDS2018, and CICDDoS2019 datasets. The results showed that the proposed model outperforms previous methods in detecting DDoS attacks and significantly reduces the false positive rate. These results indicate the potential of the proposed method in enhancing network security and providing an effective solution against cyber threats.

**Cite this article:** M.Nosrati, F.Bagheri.(2026). Deep Learning-Based DDoS Attack Detection System with Attention Mechanism. *Electronic and Cyber Defense*,14(1),91-105.

DOI: <https://dor.isc.ac/dor/20.1001.1.23224347.1405.14.1.6.8>



© Author(s) retain the copyright and full publishing rights

**Publisher:** Imam Hossein University.

## ارائه سیستم تشخیص حملات DDoS مبتنی بر یادگیری عمیق و مکانیزم توجه

مهران نصرتی<sup>۱</sup>، فاطمه باقری<sup>۲\*</sup>

<sup>۱</sup> دانشجوی کارشناسی ارشد، دانشگاه گلستان، گرگان، ایران. sobazino@gmail.com

<sup>۲</sup> استادیار، دانشگاه گلستان، گرگان، ایران (نویسنده مسئول): f.bagheri@gu.ac.ir

| چکیده                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | مشخصات مقاله                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>با گسترش سریع اینترنت و افزایش تعداد دستگاه‌های متصل به شبکه، سطح حملات سایبری به‌طور چشمگیری افزایش یافته است. یکی از تهدیدات جدی در این حوزه، حملات منع سرویس توزیع‌شده (DDoS) هستند که با بهره‌گیری از تعداد زیادی سیستم آلوده، حجم عظیمی از ترافیک را به سمت اهداف مشخص هدایت می‌کنند. ویژگی توزیع‌یافته و مقیاس‌پذیر این حملات، تشخیص و مقابله با آن‌ها را به‌مراتب دشوارتر از سایر تهدیدات امنیتی کرده است. در سال‌های اخیر، مدل‌های مختلفی برای شناسایی این نوع حملات توسعه یافته‌اند، اما بسیاری از آن‌ها در تشخیص دقیق یا کاهش نرخ خطا با چالش مواجه هستند. برای مقابله با این مسئله، در این مقاله یک سیستم تشخیص نفوذ مبتنی بر شبکه‌های عصبی عمیق و مکانیزم توجه پیشنهاد شده است. روش پیشنهادی با استفاده از زبان برنامه‌نویسی Python و کتابخانه PyTorch پیاده‌سازی و بر روی مجموعه داده‌های CICIDS2017، CICIDS2018 و CICDDoS2019 آزمایش شده است. نتایج نشان داد که مدل پیشنهادی در مقایسه با روش‌های پیشین، عملکرد بهتری در شناسایی حملات DDoS ارائه می‌دهد و نرخ خطای کاذب را به‌طور قابل توجهی کاهش می‌دهد. این نتایج بیانگر پتانسیل روش پیشنهادی در بهبود امنیت شبکه و ارائه یک راهکار مؤثر در برابر تهدیدات سایبری است.</p> | <p>تاریخچه مقاله:<br/>نوع مقاله: علمی پژوهشی</p> <p>دریافت: ۱۴۰۴/۱۰/۲۹<br/>بازنگری: ۱۴۰۵/۱۲/۱۶<br/>پذیرش: ۱۴۰۵/۰۱/۲۴<br/>ارائه آنلاین: ۱۴۰۵/۰۲/۰۱</p> <p>کلید واژه‌ها:<br/>سیستم تشخیص نفوذ<br/>شبکه عصبی<br/>مکانیزم توجه<br/>حمله منع سرویس توزیع شده</p> |

## ۱. مقدمه

توسعه سریع اینترنت و افزایش وابستگی به خدمات آنلاین، امنیت شبکه را به یکی از دغدغه‌های اصلی تبدیل کرده است. در میان انواع تهدیدات سایبری، حمله منع سرویس توزیع شده<sup>۱</sup> (DDoS) به دلیل ارسال حجم بسیار بالایی از ترافیک مخرب به سمت سامانه‌های هدف، موجب از دسترس خارج شدن آن‌ها برای کاربران قانونی می‌شوند. این حملات به تهدیدی جدی برای امنیت شبکه تبدیل شده و می‌توانند خدمات را مختل کرده و خسارات مالی قابل توجهی ایجاد کنند.

اقدامات امنیتی سنتی اغلب قادر به مقابله با ماهیت در حال رشد و پیچیده این حملات نیستند و معمولاً در شناسایی و مدیریت مقیاس و پیچیدگی حملات منع سرویس توزیع شده مدرن ناکارآمد عمل می‌کنند؛ بنابراین، توسعه رویکردهای پیشرفته برای شناسایی و طبقه‌بندی این حملات ضروری است.

حملات منع سرویس توزیع شده معمولاً از طریق شبکه‌ای از سیستم‌های آلوده شده به نرم‌افزارهای مخرب، معروف به بات‌نت<sup>۲</sup>، ترافیک انبوهی تولید می‌کنند. این حملات می‌توانند لایه‌های مختلف شبکه را هدف قرار دهند و با پیشرفت فن‌های مهاجمان، سازمان‌ها را در معرض خطرات جدی قرار می‌دهند که ممکن است منجر به از دست دادن مشتریان شود [۱].

معمولاً این حملات شامل تهدیدات هماهنگ شده متعددی هستند که به دلیل ناتوانی ابزارهای موجود در تشخیص دقیق نوع حمله، مقابله با آن‌ها را دشوار می‌سازد. پیامدهای مالی و عملیاتی حملات منع سرویس توزیع شده به‌ویژه زمانی که خدمات حیاتی مبتنی بر اینترنت هدف قرار گیرند، بسیار قابل توجه است [۲]. در این راستا، توسعه و به‌کارگیری سیستم‌های تشخیص نفوذ<sup>۳</sup> (IDS) برای شناسایی و کاهش این تهدیدات ضروری است.

سیستم‌های تشخیص نفوذ به‌منظور پایش یک سیستم رایانه‌ای یا شبکه برای فعالیت‌های مخرب، مانند دسترسی غیرمجاز، سوءاستفاده یا تغییر منابع سیستم طراحی شده‌اند. هدف شناسایی نفوذ، تشخیص این اقدامات در زمان واقعی یا نزدیک به آن و اتخاذ اقدامات مناسب برای محافظت در برابر از دست رفتن یا واگذاری داده‌ها است. سیستم‌های تشخیص نفوذ برای تحلیل فعالیت‌های سیستم و شبکه به‌منظور شناسایی الگوهای مشکوک که ممکن است نشان‌دهنده وقوع یک حمله باشد، طراحی شده‌اند. این سیستم‌ها می‌توانند به‌صورت مبتنی بر میزبان یا مبتنی بر شبکه باشند و از روش‌هایی مانند شناسایی مبتنی بر امضا، شناسایی مبتنی بر ناهنجاری یا

شناسایی مبتنی بر رفتار برای شناسایی خطرات احتمالی استفاده کنند. پس از شناسایی نفوذ، سیستم تشخیص نفوذ می‌تواند امنیت را از طریق اطلاع‌رسانی به کارکنان امنیتی یا فعال‌سازی مکانیسم‌های پاسخ‌دهی خودکار مانند دیوار آتش یا سیستم‌های امنیتی دیگر به اقدام مناسب برای مهار یا کاهش حمله هدایت کند. شناسایی نفوذ بخش ضروری از یک رویکرد امنیتی جامع است و به سازمان‌ها کمک می‌کند تا به طور مؤثر و سریع به حوادث امنیتی پاسخ دهند [۳، ۴].

یکپارچه‌سازی فناوری و اینترنت در تمام جنبه‌های زندگی، نحوه زندگی و کار مردم را دگرگون کرده است و فرصت‌های جدیدی برای کار از راه دور، یادگیری آنلاین و ارتباط بدون نقص ایجاد کرده است. با این حال، در کنار مزایای فناوری، خطرات امنیتی نیز وجود دارد، از جمله هک، حملات سایبری و نقض داده‌ها. محافظت از اطلاعات شخصی و حساس و ایمن ماندن در فضای آنلاین ضروری است. این موارد شامل احتیاط در برابر کلاهبرداری‌های فیشینگ، استفاده از گذرواژه‌های قوی و به‌روزرسانی نرم‌افزارها است. آموزش مداوم درباره خطرات امنیت سایبری و بهترین شیوه‌ها نیز ضروری است. شناسایی و تشخیص تهدیدات شبکه و حملات سایبری برای جلوگیری از آنها حیاتی است. این امر شامل آگاهی از آخرین خطرات امنیتی و هوشیاری در برابر علائم فعالیت‌های مشکوک است. برخی از نشانه‌های رایج یک حمله سایبری شامل پیام‌های خطا یا پاپ‌آپ‌های غیرمعمول، کاهش کارایی سیستم یا شبکه، ترافیک شبکه غیرعادی، تغییرات غیرمجاز در فایل‌ها یا تنظیمات و ایمیل‌ها یا پیوست‌های مشکوک است [۵، ۶]. ارزیابی‌ها و آزمایش‌های امنیتی منظم نیز می‌تواند به شناسایی آسیب‌پذیری‌های شبکه قبل از سوءاستفاده مهاجمان کمک کند.

امنیت سایبری از اطلاعات حساس در برابر سرقت، تغییر یا سوءاستفاده محافظت می‌کند. تهدیدات رایج شامل کلاهبرداری‌های فیشینگ، بدافزار، باج‌افزار و هک است. افراد و سازمان‌ها باید نرم‌افزارهای خود را به‌طور منظم به‌روزرسانی کنند، از گذرواژه‌های قوی استفاده کنند و خود را درباره آخرین خطرات امنیتی آموزش دهند تا در فضای آنلاین ایمن بمانند. پیاده‌سازی احراز هویت چندعاملی، دیوار آتش و پشتیبان‌گیری منظم از داده‌ها نیز می‌تواند به جلوگیری از حملات سایبری کمک کند [۷].

سیستم تشخیص نفوذ بخش مهمی از یک راه‌حل امنیتی جامع است؛ زیرا به شناسایی تهدیدات امنیتی در زمان واقعی و پاسخ سریع به آنها کمک می‌کند. این سیستم می‌تواند بسته به محل استقرار در شبکه، مبتنی بر شبکه یا میزبان باشد.

<sup>۱</sup>. Distributed Denial of Service.

<sup>۲</sup>. Botnet.

<sup>۳</sup>. Intrusion detection system.

این الگوریتم‌ها برای بهبود حریم خصوصی و کارایی سیستم‌های تشخیص نفوذ از طریق بهینه‌سازی انتخاب ویژگی‌هایی که برای پیش‌بینی استفاده می‌شوند، به کار گرفته شده‌اند [۱۸].

طراحی و پیاده‌سازی یک سیستم تشخیص نفوذ چالشی پیچیده و نیازمند تحلیل عمیق رفتارهای عادی و مخرب در محیط شبکه است. آزمایش‌های آزمایشگاهی مدل‌های سیستم‌های تشخیص نفوذ می‌توانند اطلاعات ارزشمندی درباره دقت و کارایی این سیستم‌ها ارائه دهند، اما ممکن است منجر به بیش‌برازش<sup>۱۵</sup> شوند؛ به این معنا که مدل بیش از حد به داده‌های آزمایشگاهی تطبیق یافته و در محیط‌های واقعی عملکرد مطلوبی نداشته باشد. از این‌رو، اعتبارسنجی مدل سیستم‌های تشخیص نفوذ در یک محیط واقعی برای اطمینان از اثربخشی آن امری حیاتی است. این فرایند می‌تواند با استقرار مدل در یک شبکه زنده و پایش مستمر عملکرد آن انجام شود که به ارائه نمایی دقیق‌تر از شرایط واقعی شبکه و شناسایی نقاط ضعف یا محدودیت‌های مدل کمک می‌کند. علاوه بر این، به‌روزرسانی مداوم و انجام آزمایش‌های مستمر برای انطباق با تهدیدات امنیتی جدید و رفتارهای در حال تحول شبکه ضروری است تا مدل همواره بتواند پاسخگوی چالش‌های جدید باشد.

یادگیری عمیق در حوزه‌های مختلفی مانند طبقه‌بندی تصاویر، تشخیص و تفکیک اشیا، شناسایی چهره، خودروهای خودران، پزشکی، بینایی ماشین، امور مالی، تبلیغات، پردازش زبان طبیعی، امنیت سایبری و سیستم‌های تشخیص نفوذ کاربردهای گسترده‌ای پیدا کرده است [۱۱].

در سال‌های اخیر، یادگیری ماشین نقش مهمی در سیستم‌های تشخیص نفوذ ایفا کرده‌اند. یادگیری ماشین به زیرمجموعه‌ای از هوش مصنوعی اشاره دارد که به رایانه‌ها امکان می‌دهد از داده‌ها بیاموزند و عملکرد خود را بهبود دهند. در زمینه شناسایی نفوذ، یادگیری ماشین می‌تواند برای توسعه الگوریتم‌هایی استفاده شود که به طور خودکار فعالیت‌های مخرب را شناسایی و نفوذهای شبکه را تشخیص دهند. فن‌های یادگیری ماشین با آموزش مدل‌ها بر روی حجم زیادی از داده‌های تاریخی کار کرده و از این مدل‌ها برای پیش‌بینی احتمال رخدادهای جدید به عنوان مخرب یا غیرمخرب استفاده می‌کنند. برای مثال، یک الگوریتم یادگیری ماشین ممکن است الگوهایی را که نشان‌دهنده تلاش مهاجم برای بهره‌برداری از یک آسیب‌پذیری در شبکه است، شناسایی کند. پس از آموزش، الگوریتم می‌تواند داده‌های جدید را طبقه‌بندی کرده و نفوذهای بالقوه را در زمان واقعی شناسایی کند.

سیستم‌های تشخیص نفوذ مبتنی بر شبکه<sup>۱</sup> ترافیک شبکه را برای علائم نفوذ بررسی می‌کند و در لایه شبکه عمل می‌کند، درحالی‌که سیستم‌های تشخیص نفوذ مبتنی بر میزبان<sup>۲</sup> بر روی میزبان‌های فردی نصب شده و رویدادهای خاص آن میزبان را برای نشانه‌های نفوذ پایش می‌کند. سیستم تشخیص نفوذ می‌تواند در دو حالت کار کند: شناسایی مبتنی بر امضا که از قوانین پیش تعریف شده برای شناسایی تهدیدات شناخته شده استفاده می‌کند، و شناسایی مبتنی بر ناهنجاری که از الگوریتم‌های یادگیری ماشین برای شناسایی انحرافات از رفتار عادی شبکه و شناسایی نفوذ استفاده می‌کند [۸].

در دهه‌های اخیر، مسائل مرتبط با حملات سایبری، به‌ویژه در حوزه سیستم‌های تشخیص نفوذ، مورد توجه گسترده‌ای قرار گرفته است. در این راستا، از طیف متنوعی از الگوریتم‌های یادگیری ماشین بهره‌برداری شده است، از جمله الگوریتم‌های درخت تصمیم [۷، ۹]، مدل‌های ماشین بردار پشتیبان<sup>۳</sup>، الگوریتم نزدیک‌ترین همسایه<sup>۴</sup>، و رویکردهای پیشرفته هوش مصنوعی. با این حال، در سال‌های اخیر روش‌های یادگیری عمیق<sup>۵</sup> محبوبیت زیادی در این حوزه پیدا کرده‌اند، الگوریتم‌هایی نظیر شبکه‌های عصبی کانولوشنال<sup>۶</sup>، شبکه‌های عصبی بازگشتی<sup>۷</sup>، ماشین بولتزمن محدود شده<sup>۸</sup>، و شبکه‌های عصبی پیام‌رسان<sup>۹</sup>. این مدل‌های پیشرفته یادگیری عمیق برای ارتقای دقت و کارایی سیستم‌های تشخیص نفوذ در محیط‌های مبتنی بر مه<sup>۱۰</sup>، ابر، و اینترنت اشیا به کار گرفته شده‌اند و نتایج قابل توجهی در بهبود عملکرد این سیستم‌ها به همراه داشته‌اند [۱۰-۱۴].

مدل‌سازی سیستم‌های تشخیص نفوذ به عنوان یک مسئله انتخاب ویژگی و استفاده از طبقه‌بندهای سنتی برای حل آن از جمله روش‌هایی است که در این زمینه به کار گرفته می‌شود. همچنین، الگوریتم‌های بهینه‌سازی متا هیوریستیک برای مقابله با مسائل پیچیده بهینه‌سازی در سیستم‌های تشخیص نفوذ مورد استفاده قرار می‌گیرند. این الگوریتم‌ها شامل الگوریتم بهینه‌سازی ازدحام ذرات<sup>۱۱</sup> [۱۵]، الگوریتم جستجوی کلاغ<sup>۱۲</sup> [۱۶]، الگوریتم ژنتیک<sup>۱۳</sup>، الگوریتم جستجوی تصادفی هارمونی و الگوریتم بهینه‌سازی گرگ خاکستری<sup>۱۴</sup> [۱۷] و غیره هستند.

<sup>1</sup>. Network-based Intrusion Detection System.

<sup>2</sup>. Host-based intrusion detection system.

<sup>3</sup>. Support vector machine.

<sup>4</sup>. k-nearest neighbors.

<sup>5</sup>. Deep learning.

<sup>6</sup>. Convolutional neural network.

<sup>7</sup>. Recurrent neural network.

<sup>8</sup>. Restricted Boltzmann machine.

<sup>9</sup>. Message passing neural network.

<sup>10</sup>. Fog-based environments.

<sup>11</sup>. Particle swarm optimization.

<sup>12</sup>. Crow Search Algorithm.

<sup>13</sup>. Genetic Algorithms.

<sup>14</sup>. Grey wolf optimizer.

<sup>15</sup>. Over fitting.

دستگاه‌های آلوده، برای ارسال حجم عظیمی از ترافیک یا درخواست‌های مخرب به سرور یا شبکه هدف استفاده می‌کند.

هدف اصلی این حمله، اشباع منابع سیستمی نظیر پهنای باند، پردازشگر یا حافظه است، به گونه‌ای که سیستم دیگر قادر به پاسخگویی به درخواست‌های کاربران عادی نباشد. ویژگی کلیدی حملات منع سرویس توزیع شده، توزیع شدگی منابع حمله است که شناسایی و جلوگیری از آن‌ها را به دلیل پراکندگی و ماهیت پیچیده ترافیک حمله، دشوارتر می‌سازد. این حملات تهدیدی جدی برای دسترس پذیری سرویس‌ها به شمار می‌روند و مقابله با آن‌ها نیازمند استفاده از راهکارهای پیشرفته‌ای مانند تحلیل ترافیک، استفاده از الگوریتم‌های یادگیری ماشین و سامانه‌های تشخیص نفوذ قدرتمند است.

## ۲-۲. یادگیری عمیق<sup>۴</sup>

یادگیری عمیق یکی از شاخه‌های پیشرفته یادگیری ماشین است که بر ساخت و آموزش شبکه‌های عصبی مصنوعی<sup>۵</sup> چندلایه تمرکز دارد. این شبکه‌ها به گونه‌ای طراحی شده‌اند که می‌توانند به صورت خودکار ویژگی‌های سطح بالا و معنادار را از داده‌های خام استخراج کنند. در این روش، هر لایه شبکه مسئولیت یادگیری و پردازش ویژگی‌های پیچیده‌تر را نسبت به لایه‌های قبلی بر عهده دارد. یادگیری عمیق با الهام از ساختار سلول‌های عصبی مغز و نحوه ارتباط آن‌ها، مدل‌هایی همچون شبکه‌های عصبی کانولوشنال<sup>۶</sup> و شبکه‌های بازگشتی<sup>۷</sup> را ارائه کرده است که برای تحلیل انواع داده‌ها، از جمله داده‌های ساختاریافته<sup>۸</sup> و غیرساختاریافته<sup>۹</sup>، کاربرد دارند [۱۹]. [۲۰] و می‌توانند تحت نظارت، نیمه نظارت یا بدون نظارت باشند [۲۱]. یکی از نقاط قوت این روش، توانایی آن در شناسایی الگوهای پیچیده و غیرخطی از مقادیر زیاد داده با استفاده از توان محاسباتی بالا است که آن را به ابزاری قدرتمند در کاربردهایی مانند تحلیل داده‌های جدولی، سیگنال‌ها و سری‌های زمانی تبدیل کرده است.

## ۲-۳. شبکه عصبی کانولوشنال

شبکه عصبی کانولوشنال یکی از معماری‌های مهم در یادگیری عمیق است که به طور خاص برای استخراج الگوها و ویژگی‌های داده‌های ساختارمند طراحی شده است. این شبکه‌ها با بهره‌گیری از لایه‌های متوالی، توانایی شناسایی روابط محلی و ویژگی‌های پیچیده در داده‌ها را دارند. ساختار شبکه عصبی کانولوشنال به گونه‌ای است که با تمرکز

سیستم‌های تشخیص نفوذ ابزارهای ضروری برای شناسایی و جلوگیری از فعالیت‌های مخرب در شبکه‌های رایانه‌ای هستند. یادگیری ماشین [۱۲] تکنیکی محبوب هست که به طور گسترده در سیستم‌های تشخیص نفوذ برای بهبود دقت و کارایی آنها به کار گرفته می‌شود. الگوریتم‌های یادگیری ماشین می‌توانند حجم زیادی از داده‌ها را تحلیل کرده و الگوها و ناهنجاری‌ها را در ترافیک شبکه برای شناسایی حملات احتمالی شناسایی کنند.

در حوزه ایمن‌سازی شبکه‌های رایانه‌ای، تشخیص نفوذ نقشی حیاتی در حفاظت در برابر انواع حملات مخرب ایفا می‌کند. در این چشم‌انداز پویا و در حال تغییر امنیت شبکه، پیشرفت‌های اخیر در فناوری موجب شده‌اند مفاهیمی همچون یادگیری ماشین، یادگیری عمیق، یادگیری فدرال<sup>۱</sup> و هوش مصنوعی قابل توضیح<sup>۲</sup> به عنوان راهکارهای نویدبخش برای بهبود تشخیص نفوذ به کانون توجه تبدیل شوند. این تحولات، تغییرات چشمگیری در رویکردهای امنیتی شبکه ایجاد کرده و هم‌زمان فرصت‌های جدید و گسترده‌ای برای ارتقای این حوزه فراهم آورده‌اند.

در این پژوهش، تمرکز اصلی بر طراحی یک سیستم تشخیص نفوذ مؤثر و دقیق برای شناسایی حملات منع سرویس توزیع شده بوده است. به کارگیری معماری نوین TabM برای نخستین بار در حوزه تشخیص حملات DDoS یکی از نوآوری‌های کلیدی این مقاله محسوب می‌شود. این رویکرد، باهدف کاهش پیچیدگی محاسباتی و افزایش کارایی، ظرفیت بالایی برای به کارگیری در سامانه‌های امنیتی نوین فراهم می‌سازد.

ادامه این مقاله براین اساس سازماندهی شده است. در بخش ۲، به مفاهیم پایه پرداخته شده است. در بخش ۳، کارهای مرتبط بررسی شده است. سپس، در بخش ۴، روش پیشنهادی معرفی و توضیح داده شده و در بخش ۵، پیاده‌سازی مفصل روش پیشنهادی ارائه شده است. در بخش ۶ نتایج ارزیابی گردیده است. در نهایت، در بخش ۷، نتیجه‌گیری ارائه شده است.

## ۲. مفاهیم پایه

### ۲-۱. حمله منع سرویس توزیع شده

حمله منع سرویس توزیع شده<sup>۳</sup> یکی از تهدیدات رایج و مخرب در حوزه امنیت شبکه است که به منظور مختل کردن دسترسی به منابع یا خدمات یک سیستم هدف طراحی می‌شود. در این نوع حمله، مهاجم از چندین منبع توزیع شده، نظیر شبکه‌ای از

<sup>۴</sup>. Deep learning.

<sup>۵</sup>. Artificial neural network.

<sup>۶</sup>. Convolutional neural network.

<sup>۷</sup>. Recurrent neural network.

<sup>۸</sup>. Structured data.

<sup>۹</sup>. Unstructured data.

<sup>۱</sup>. Federated learning.

<sup>۲</sup>. Explainable artificial intelligence.

<sup>۳</sup>. Distributed Denial of Service.

در مقاله [۲۳]، مجتبی و همکاران سیستم تشخیص نفوذ به نام *Kitsune* را معرفی کردند که برای محیط‌های سخت‌افزاری محدود با استفاده از یادگیری بدون نظارت بهینه‌سازی شده است. این سیستم تشخیص نفوذ برای شناسایی ناهنجاری‌ها در داده‌های شبکه طراحی شده و از فن‌های یادگیری بدون نظارت برای افزایش کارایی خود استفاده می‌کند. هدف نویسندگان ارائه راه‌حلی است که بتواند تهدیدات امنیتی را به طور مؤثر شناسایی کرده و هم‌زمان برای استقرار در محیط‌های سخت‌افزاری محدود بهینه‌سازی شود. با استفاده از یادگیری بدون نظارت، سیستم تشخیص نفوذ قادر است از داده‌ها بیاموزد و خود را با تغییر رفتار شبکه وفق دهد بدون اینکه نیاز به داده‌های برچسب‌دار یا به‌روزرسانی‌های دستی داشته باشد. این مقاله *Kitsune* را به‌عنوان یک سیستم تشخیص نفوذ مبتنی بر شبکه با منابع کارآمد معرفی می‌کند، اما مقیاس‌پذیری آن در دنیای واقعی و تعمیم‌پذیری آن در محیط‌ها و حملات متنوع شبکه تأیید نشده است. علاوه بر این، میزان مداخله انسانی موردنیاز برای تنظیم و نگهداری آن مشخص نیست.

نویسندگان مقاله [۲۴] به بررسی کاربرد شبکه‌های عصبی مصنوعی<sup>۳</sup> و سایر روش‌های طبقه‌بندی برای شناسایی نفوذهای شبکه پرداختند. آن‌ها کارایی شبکه‌های عصبی مصنوعی را با سایر الگوریتم‌های طبقه‌بندی مقایسه کردند تا مؤثرترین روش برای مسئله خود را تعیین کنند. در نهایت مشخص شد که یک رویکرد تجمعی که چندین طبقه‌بند را ترکیب می‌کند، می‌تواند در مقایسه با استفاده از یک الگوریتم واحد کارایی بهتری ارائه دهد. این رویکرد تجمعی از نقاط قوت الگوریتم‌های مختلف بهره می‌برد و نقاط ضعف آن‌ها را کاهش می‌دهد و منجر به بهبود دقت و کارایی در شناسایی تهدیدات امنیتی در داده‌های شبکه می‌شود. در این کار، سیستم تشخیص نفوذ مبتنی بر ناهنجاری پیشنهادی با استفاده از الگوریتم ژنتیک و ماشین بردار پشتیبان با یک روش انتخاب ویژگی جدید، دقت بهتری ارائه می‌دهد و نرخ مثبت کاذب را کاهش می‌دهد. با این حال، این مطالعه فاقد ارزیابی جامع از عملکرد آن در محیط‌های شبکه متنوع و در برابر استراتژی‌های حمله در حال تحول است. مقیاس‌پذیری عملی مدل برای مدیریت ترافیک شبکه دنیای واقعی همچنان موردتوجه قرار نگرفته است.

نویسندگان مقاله [۲۵] یک مکانیزم امنیت شبکه جدید مبتنی بر استخراج ویژگی پیشنهاد دادند. این مدل از یک الگوریتم ژنتیک و ماشین بردار پشتیبان حداقل مربعات<sup>۴</sup> (*LS-SVM*) برای طبقه‌بندی ناهنجاری‌ها در مسائل امنیتی استفاده می‌کند. نتایج ارزیابی نشان داد که مدل دارای نرخ مثبت کاذب پایین و نرخ مثبت واقعی بالا است که آن را در شناسایی مسائل امنیتی

بر اطلاعات کلیدی، یادگیری مؤثر و کارآمدی را فراهم می‌کند. این مدل‌ها به دلیل انعطاف‌پذیری بالا، در طیف گسترده‌ای از مسائل، از جمله داده‌های غیرتصویری، کاربرد دارند و توانایی آن‌ها در پردازش و تحلیل داده‌های پیچیده، آن‌ها را به ابزاری قدرتمند در علوم داده تبدیل کرده است.

## ۴-۲. مکانیزم توجه<sup>۱</sup>

مکانیزم توجه یک چارچوب پیشرفته در یادگیری عمیق است که برای بهبود توانایی مدل‌ها در تمرکز بر بخش‌های مهم داده‌های ورودی طراحی شده است. ایده اصلی توجه این است که به جای پردازش یکنواخت کل داده‌ها، مدل بتواند وزن بیشتری به قسمت‌های مرتبط‌تر و مهم‌تر اختصاص دهد. این مکانیزم ابتدا در مدل‌های ترجمه ماشینی معرفی شد، اما به سرعت در حوزه‌های مختلف مانند پردازش زبان طبیعی، بینایی رایانه و داده‌های زمانی گسترش یافت. توجه، از طریق محاسبه وزن‌های تطبیقی برای هر بخش از ورودی، اطلاعات کلیدی را برجسته کرده و وابستگی‌های بلندمدت و پیچیده را به طور مؤثرتری مدل‌سازی می‌کند. این رویکرد نه تنها دقت مدل‌ها را بهبود می‌بخشد، بلکه باعث تفسیرپذیری بهتر خروجی‌ها نیز می‌شود.

## ۳. کارهای مرتبط

مطالعات اخیر نشان داده است که امنیت سایبری به یکی از نگرانی‌های حیاتی در سال‌های اخیر تبدیل شده است، زیرا فناوری اطلاعات به سرعت در حال گسترش است. به همین دلیل، سیستم‌های تشخیص نفوذ و بهبود آن‌ها از طریق یادگیری ماشین موردتوجه محققان قرار گرفته است. مطالعات متعددی در این زمینه برای توسعه مدل‌های جدید سیستم تشخیص نفوذ و افزایش کارایی آن‌ها در شناسایی تهدیدات امنیتی انجام شده است. هدف اصلی، ارائه راهکاری مؤثر و کارآمد برای محافظت از شبکه‌ها و سیستم‌ها در برابر حملات سایبری است.

در مقاله [۲۲]، یک سیستم تشخیص نفوذ برای دستگاه‌های اینترنت اشیا<sup>۲</sup> معرفی شده است که بر استقرار آن بر روی دستگاه‌های ارزان قیمت اینترنت اشیا تأکید دارد. با این حال، این مقاله به چالش‌های سازگاری با چشم‌انداز در حال تکامل سریع حملات اینترنت اشیا و نیاز به به‌روزرسانی‌های مداوم برای مقابله با تهدیدات جدید نمی‌پردازد. علاوه بر این، مسائل مربوط به مقیاس‌پذیری بالقوه برای استقرار چنین سامانه‌هایی در شبکه‌ای گسترده از دستگاه‌های اینترنت اشیا متنوع در حوزه‌های کاربردی مختلف مورد بررسی قرار نگرفته است.

<sup>۳</sup>. Artificial Neural Network.

<sup>۴</sup>. Least-squares support vector machine.

<sup>۱</sup>. Attention Mechanism.

<sup>۲</sup>. Internet of Things.

مدل برای سازگاری با استراتژی‌های حمله جدید یا در حال تحول ارزیابی نشده است. یافته‌های این مطالعه می‌تواند با انجام آزمایش‌های دنیای واقعی بیشتر و استفاده از مجموعه‌داده‌های متنوع، برای ارزیابی استحکام مدل اعتبارسنجی شود.

در مقاله [۲۸]، نویسندگان عملکرد یک سیستم تشخیص نفوذ مبتنی بر جنگل تصادفی را از نظر دقت و نرخ هشدار کاذب بررسی کردند. نویسندگان از مجموعه‌داده‌های *NSL-KDD*، *UNSW-NB15* و *GPRS* برای آموزش و آزمایش مدل استفاده کردند. سیستم تشخیص نفوذ پیشنهادی با استفاده از مجموعه‌هایی با اندازه‌های مختلف از درخت‌ها ارزیابی شد. تحلیل آماری مبتنی بر رتبه‌بندی فریدمن نشان داد که مجموعه‌ای متشکل از ۸۰۰ درخت بهترین نتایج را به دست آورده است، درحالی‌که مجموعه‌ای با ۲۰ درخت بدترین عملکرد را نشان داده است. علاوه بر این، نویسندگان نشان دادند که سیستم تشخیص نفوذ مبتنی بر جنگل تصادفی عملکرد بهتری نسبت به سایر طبقه‌بندها دارد. این مطالعه بر اثربخشی طبقه‌بند جنگل تصادفی در تشخیص نفوذ تأکید دارد؛ با این حال، تحلیل جامعی از سازگاری مدل با الگوهای حمله جدید و استحکام آن در برابر حملات خصمانه ارائه نشده است. ارزیابی انجام شده بر مجموعه‌داده‌های موجود متمرکز است و کاربرپذیری مدل در محیط‌های شبکه پویا و در حال تحول دنیای واقعی بررسی نشده است.

آوتوننده و همکاران [۲۹] سیستمی برای تشخیص نفوذ در شبکه ارائه کردند که در آن از شبکه عصبی پیش‌خور عمیق همراه با روش انتخاب ویژگی مبتنی بر قواعد استفاده شده است. در این پژوهش، مدل آموزش‌دیده برای تحلیل بسته‌های ورودی *TCP/IP* مورد استفاده قرار گرفته است.

نصیر و همکاران [۳۰] یک سیستم تشخیص نفوذ مبتنی بر ناهنجاری را توسعه دادند که از ساختارهای متنوع شبکه‌های عصبی عمیق بهره می‌برد. این مدل با استفاده از مجموعه‌داده *NSL-KDD* آموزش داده شده و مورد ارزیابی قرار گرفته است. نتایج به دست آمده نشان داده است که مدل‌های مبتنی بر یادگیری عمیق، در مقایسه با روش‌های سنتی یادگیری ماشین، در معیارهای کلیدی طبقه‌بندی عملکرد بهتری ارائه می‌دهند؛ امری که نشان‌دهنده قابلیت کاربردی آن‌ها در شناسایی ناهنجاری‌ها در شرایط واقعی است.

الزوغیبی و خدیری [۳۱] مدلی برای سیستم تشخیص نفوذ ارائه دادند که با بهره‌گیری از دو ساختار شبکه عصبی عمیق، عملکرد سیستم تشخیص نفوذ را در محیط‌های رایانش ابری بهبود می‌بخشد. در این مدل‌ها، از پرسپترون چندلایه و بهینه‌سازی ازدحام ذرات استفاده شده است. بر اساس ارزیابی

مؤثر می‌سازد درحالی‌که از هشدارهای کاذب جلوگیری می‌کند. استفاده از الگوریتم ژنتیک اختصاصی و *LS-SVM*، کارایی و دقت مدل را در مقایسه با فن‌های قبلی افزایش می‌دهد. در این کار، طبقه‌بند دومرحله‌ای با استفاده از الگوریتم *RepTree* و زیرمجموعه پروتکل، دقت تشخیص نفوذ را بهبود می‌بخشد، اما ممکن است در مواجهه با الگوهای حمله جدید یا در حال تحول که در داده‌های آموزشی وجود ندارند، مؤثر نباشد. مقاله فاقد تحلیل عمیق از استحکام مدل در برابر حملات خصمانه است و مقیاس‌پذیری آن برای مدیریت محیط‌های شبکه پیچیده دنیای واقعی با طیف وسیعی از پروتکل‌ها و انواع حملات مورد بررسی قرار نگرفته است.

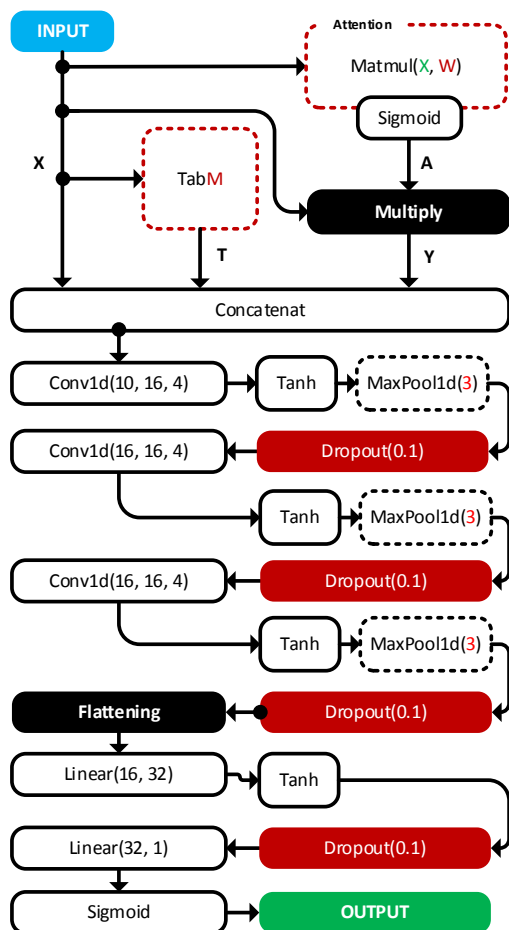
در مقاله [۲۶]، الگوریتم *REPTree* به عنوان روشی برای امنیت شبکه معرفی شد. مدل پیشنهادی دارای چهار مؤلفه کلیدی است: یک لایه انتخاب ویژگی و یک زیرلایه گروه‌بندی پروتکل. لایه انتخاب ویژگی به کاربران اجازه می‌دهد مرتبط‌ترین ویژگی‌ها را برای نیازهای امنیتی خود انتخاب کنند. زیرلایه گروه‌بندی پروتکل، جریان‌های شبکه را بر اساس پروتکل استفاده شده دسته‌بندی می‌کند. لایه شناسایی ناهنجاری از الگوریتم *REPTree* برای شناسایی رفتار غیرعادی شبکه استفاده می‌کند. در نهایت، لایه بازرسی، ناهنجاری‌های شناسایی شده را بررسی می‌کند تا مشخص کند که آیا آن‌ها یک تهدید امنیتی هستند یا خیر. هدف کلی مدل پیشنهادی، ارائه روشی جامع و کارآمد برای شناسایی تهدیدات امنیتی در داده‌های شبکه است. نویسندگان همچنین توضیح می‌دهند که شبکه عصبی مصنوعی مبتنی بر مجموعه آبخاری، برای تشخیص نفوذ چند کلاسه مؤثر است، اما ممکن است در برابر فن‌های حمله جدید و سریعاً در حال تحول دچار مشکل شود. مقیاس‌پذیری و عملکرد آن در محیط‌های پیچیده شبکه دنیای واقعی همچنان بررسی نشده باقی مانده است.

در مقاله [۲۷]، پژوهشگران یک سیستم تشخیص نفوذ جدید مبتنی بر ناهنجاری معرفی کردند که از ماشین‌های گرادیان بوستینگ<sup>۱</sup> به عنوان موتور اصلی تشخیص استفاده می‌کند. آن‌ها از روش جستجوی شبکه‌ای<sup>۲</sup> برای تعیین پارامترهای بهینه ماشین‌های گرادیان بوستینگ استفاده کردند. عملکرد سیستم تشخیص نفوذ پیشنهادی با استفاده از روش‌های اعتبارسنجی متقابل بر روی سه مجموعه‌داده *NSL-KDD*، *UNSW-NB15* و *GPRS* ارزیابی شد. نتایج تجربی نشان داد که سیستم تشخیص نفوذ پیشنهادی در مقایسه با چندین طبقه‌بند دیگر مانند طبقه‌بندهای فازی، جنگل *GAR*، در معیارهای مختلف عملکرد بهتری دارد. این مطالعه عملکرد برتر ماشین‌های گرادیان بوستینگ را در تشخیص ناهنجاری نشان می‌دهد، اما توانایی

<sup>۱</sup>. Gradient Boosting Machines.

<sup>۲</sup>. Grid Search.

ساختاری ترکیبی از لایه‌های کانولوشنال و لایه‌های کاملاً متصل، دقتی بالا در تشخیص حملات منع سرویس توزیع‌شده ارائه می‌دهد. شکل (۱) معماری مدل پیشنهادی را نمایش می‌دهد. این مدل با تمرکز ویژه بر استخراج ویژگی‌های کلیدی و تقویت نواحی برجسته ورودی، سعی در کاهش خطا دارد. معماری پیشنهادی با ۴۰۷,۲۹ پارامتر شامل چهار بخش اصلی است که باهدف ارائه سیستم تشخیص نفوذی قدرتمند برای شناسایی تهدیدات پیچیده در جریان‌های داده شبکه انجام شده است.



شکل (۱). معماری مدل پیشنهادی

#### ۴-۱. معماری TabM

در بخشی از مدل پیشنهادی، از معماری TabM استفاده شده است. در این معماری، یک پرسپترون چندلایه به‌گونه‌ای بهینه‌سازی شده است که با بهره‌گیری از فن تجمیع مدل به‌صورت بهینه از نظر پارامتر، چندین پیش‌بینی مستقل را به‌صورت هم‌زمان و با اشتراک حداکثری وزن‌ها تولید نماید. برای افزایش کارایی، از ساختار BatchEnsemble با اصلاحاتی در نحوه پارامترسازی و مقداردهی اولیه استفاده شده است. این طراحی موجب کاهش چشمگیر پیچیدگی محاسباتی در مقایسه با

صورت‌گرفته بر روی مجموعه‌داده CICIDS2018، دقت مدل در طبقه‌بندی دودویی به ۹۸ درصد گزارش شده است.

در ادامه برخی دیگر از روش‌های مبتنی بر یادگیری ماشین و یادگیری عمیق [۳۲-۴۶] در جدول (۱) نشان‌داده شده است.

جدول (۱). روش‌های مبتنی بر یادگیری ماشین و یادگیری عمیق

| شماره ارجاع | مجموعه‌داده | روش                             | دقت   | سال  |
|-------------|-------------|---------------------------------|-------|------|
| [۳۲]        | KDD CUP 99  | ANN                             | ۴۰/۹۹ | ۲۰۲۰ |
| [۳۳]        | KDD CUP 99  | DT                              | ۸۹/۹۹ | ۲۰۲۱ |
| [۳۴]        | CICIDS2017  | KNN, SVM, RF                    | ۶۶/۹۶ | ۲۰۲۱ |
| [۳۵]        | NSL-KDD     | DL-IDS                          | ۰۰/۹۹ | ۲۰۲۲ |
| [۳۶]        | UNSW-NB15   | RF                              | ۱۰/۹۵ | ۲۰۲۲ |
| [۳۷]        | IDWSN       | SVR                             | ۰۰/۹۸ | ۲۰۲۲ |
| [۳۸]        | NSL KDD     | SVM                             | ۰۰/۹۸ | ۲۰۲۲ |
| [۳۹]        | BOUN DDoS   | KNN, NN                         | ۵۰/۹۹ | ۲۰۲۲ |
| [۴۰]        | NSL-KDD     | CNN-LSTM, GRU                   | ۸۹/۸۸ | ۲۰۲۳ |
| [۴۱]        | SDN-IoT     | LSTM                            | ۱۰/۹۷ | ۲۰۲۳ |
| [۴۲]        | CICIDS2017  | LSTM                            | ۰۰/۹۹ | ۲۰۲۳ |
| [۴۳]        | CICDDoS2019 | LightGBM, RF, Adaboost, XGBoost | ۱۰/۹۹ | ۲۰۲۳ |
| [۴۴]        | CICIDS2017  | MLP, DT, RF                     | ۸۱/۹۹ | ۲۰۲۳ |
| [۴۵]        | CICIDS2017  | CNN, GRU, MLP, ResNets          | ۸۵/۹۹ | ۲۰۲۴ |
| [۴۶]        | CICIDS2017  | SDAE, CNN                       | ۷۱/۹۳ | ۲۰۲۴ |

#### ۴. روش پیشنهادی

در این پژوهش، یک سیستم تشخیص نفوذ مبتنی بر شبکه‌های عصبی عمیق ارائه شده است که با بهره‌گیری از مکانیزم توجه و

لایه‌های کاملاً متصل در مدل پیشنهادی به عنوان مرحله نهایی پردازش داده‌ها عمل کرده و وظیفه تبدیل ویژگی‌های استخراج شده به خروجی نهایی را بر عهده دارند. این بخش شامل دولایه است، لایه اول با ۳۲ نورون، مسئول دریافت ورودی تخت شده از لایه‌های قبلی و مدل سازی روابط بین ویژگی‌هاست که این فرایند با استفاده از تابع فعال ساز  $Tanh$  انجام می‌شود. لایه دوم که به عنوان لایه خروجی طراحی شده، شامل یک واحد خطی است که با اعمال تابع فعال سازی سیگموئید، خروجی احتمالاتی در بازه  $[0, 1]$  تولید می‌کند.

این احتمال نمایانگر میزان تعلق نمونه ورودی به کلاس مثبت یا منفی است. به منظور بهبود تعمیم پذیری و کاهش خطر بیش برازش، از مکانیزم  $Dropout$  با نرخ  $1/10$  در بین لایه‌های کاملاً متصل استفاده شده است. این طراحی نه تنها قابلیت یادگیری روابط پیچیده میان ویژگی‌ها را تقویت می‌کند، بلکه پایداری و انعطاف پذیری مدل را در مواجهه با داده‌های جدید افزایش می‌دهد.

## ۵. پیاده سازی

روش پیشنهادی با استفاده از زبان برنامه نویسی *Python* نسخه  $10/10/3$  و *PyTorch* نسخه  $1/4/2$  پیاده سازی شده است.<sup>۲</sup> تمامی آزمایش‌ها بر روی سیستمی با پردازنده *Intel Core i9-9900K* با فرکانس  $6/3$  گیگاهرتز و  $16$  گیگابایت حافظه رم انجام شده است.

### ۵-۱. مجموعه داده

مجموعه داده *CICIDS2017* [۴۸] در اواخر سال ۲۰۱۷ توسط مؤسسه امنیت سایبری کانادا با کمک سیستم *B-Profile* [۴۹] جمع آوری و تهیه شده است. این مجموعه شامل  $473,830,2$  نمونه ترافیک شبکه است که شامل یک کلاس عادی و  $14$  دسته حمله مختلف است. ترافیک عادی  $30/80$  درصد و ترافیک حمله  $70/19$  درصد از کل داده‌ها را تشکیل می‌دهند. دسته‌های حمله شامل متداول ترین انواع حملات مانند *DDoS* (که در این پژوهش از ترافیک این نوع حملات استفاده شده است)، *DoS*، *Botnet*، *PortScan*، *Web Attacks* و... هستند. این مجموعه داده  $78$  ویژگی از ترافیک شبکه تولید شده استخراج کرده است که ستون آخر مربوط به برچسب چند کلاسه است [۵۰].

علاوه بر این، در مقایسه با مجموعه داده‌های عمومی در دسترس از سال  $1998$  تا  $2016$ ، این مجموعه داده کاملاً با  $11$  معیار ارزیابی عملکرد [۵۱] مطابقت دارد.

روش‌های گروهی<sup>۱</sup> سنتی شده و درعین حال، پایداری و دقت مدل را در مواجهه با داده‌های متنوع بهبود می‌بخشد [۴۷].

### ۴-۲. مکانیزم توجه

برای شناسایی و تمرکز بر ویژگی‌های کلیدی هر نمونه ورودی، از یک مکانیزم توجه مبتنی بر ضرب داخلی استفاده شده است. این مکانیزم با بهره‌گیری از وزن‌های توجه قابل آموزش  $W_{attn}$ ، به مدل اجازه می‌دهد که اطلاعات مهم‌تر را تقویت کرده و تأثیر داده‌های غیرمرتبط یا نویزی را کاهش دهد. بردار توجه با رابطه (۱) محاسبه می‌شود:

$$A = \sigma(X \times W_{attn}) \quad (1)$$

که در آن  $X$  ویژگی‌های ورودی است،  $W_{attn}$  بردار وزن توجه،  $\sigma$  تابع فعال سازی سیگموئید که مقادیر توجه را به بازه  $[0, 1]$  نگاشت می‌کند. تابع فعال ساز سیگموئید با رابطه (۲) محاسبه می‌شود:

$$Sigmoid(Z) = \frac{1}{1+e^{-z}} \quad (2)$$

پس از محاسبه بردار توجه  $A$ ، ضرب عنصری آن با  $X$  طبق رابطه (۳) انجام شده و نتیجه حاصل به لایه‌های بعدی مدل منتقل می‌شود:

$$Y = X \odot A \quad (3)$$

این عملیات به مدل امکان می‌دهد تا ویژگی‌های کلیدی را بهتر یاد بگیرد و دقت تشخیص را افزایش دهد.

### ۴-۳. لایه‌های کانولوشنال

لایه‌های کانولوشنال مدل پیشنهادی مسئول استخراج و پردازش اطلاعات از داده‌های ورودی در چندین مرحله متوالی است. این بخش شامل سه لایه کانولوشن یک بعدی است که به ترتیب  $16$  کانال را برای هر لایه فراهم می‌کند. هر لایه کانولوشنال، فیلترهایی با اندازه کرنل  $4$  را اعمال می‌کند تا ویژگی‌های متنوعی از داده‌های ورودی را استخراج کند. پس از هر لایه کانولوشن، یک تابع فعال ساز  $Tanh$  اعمال می‌شود. این تابع با رابطه (۴) محاسبه می‌شود:

$$\tanh(Z) = \frac{e^Z - e^{-Z}}{e^Z + e^{-Z}} \quad (4)$$

سپس به منظور جلوگیری از حفظ ویژگی‌های غیرمهم، از لایه  $MaxPooling$  با اندازه  $3$  استفاده شده است که نقش اساسی در تقویت ویژگی‌های غالب ایفا می‌کند. علاوه بر این، مکانیزم  $Dropout$  با نرخ  $1/10$  پس از هر مرحله به کار گرفته شده است تا از بیش برازش مدل جلوگیری کند. طراحی این بخش به مدل اجازه می‌دهد تا اطلاعات مهم را در مراحل مختلف تجزیه و تحلیل کرده و برای لایه‌های بعدی آماده سازی کند، به طوری که در نهایت، ویژگی‌های استخراج شده برای تصمیم گیری در لایه‌های کاملاً متصل قابل استفاده باشند.

### ۴-۴. لایه‌های کاملاً متصل

<sup>۲</sup>. <https://github.com/sobazino/IDS>.

<sup>۱</sup>. Ensemble.

تغییر باقی ماندند و در نهایت ویژگی‌های تقویت شده و سایر ویژگی‌ها با یکدیگر ترکیب شدند.

برای نرمال‌سازی داده‌ها، از *Min-Max Scaling* استفاده شد که با استفاده از رابطه (۵) تمام مقادیر را به بازه [۰، ۱] انتقال داد:

$$X_{scaled} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (5)$$

در اینجا  $X$  مقدار اصلی ویژگی،  $X_{min}$  حداقل مقدار آن ویژگی، و  $X_{max}$  حداکثر مقدار آن ویژگی است. این نرمال‌سازی کمک می‌کند تا تمامی ویژگی‌ها مقیاسی یکسان داشته باشند و مدل بتواند به طور یکنواخت تمامی ورودی‌ها را پردازش کند.

### ۳-۵. فرایند آموزش مدل

آموزش مدل پیشنهادی بر پایه طراحی دقیق و استفاده از روش‌های بهینه‌سازی پیشرفته انجام شده است تا عملکرد بهینه‌ای در شناسایی تهدیدات امنیتی ارائه دهد. در این پژوهش، تمامی ۷۸ ویژگی استخراج شده از مجموعه داده‌ها برای یادگیری مؤثر مدل به کار گرفته شده‌اند. فرایند آموزش با اندازه دسته ۲ برابر با ۶۴ و با استفاده از معیار *BCE Loss* که به طور خاص برای مسائل دسته‌بندی دوتایی مناسب است، به منظور محاسبه خطا و هدایت یادگیری مدل انجام شده است. همچنین برای بهینه‌سازی پارامترهای مدل، از الگوریتم *Adam* با نرخ یادگیری اولیه ۰.۰۱/۰ استفاده شده است. این الگوریتم به دلیل پایداری بالا و سرعت همگرایی سریع، یکی از محبوب‌ترین انتخاب‌ها برای بهینه‌سازی مدل‌های یادگیری عمیق به شمار می‌رود.

علاوه بر این، مکانیزم *Cosine Annealing* برای کاهش تدریجی نرخ یادگیری به منظور بهبود فرایند همگرایی و دستیابی به یک نقطه بهینه دقیق‌تر به کار گرفته شده است. این روش ابتدا امکان آموزش سریع‌تر مدل را با نرخ یادگیری بالا فراهم می‌کند و سپس با کاهش تدریجی نرخ یادگیری، مدل را به سمت یک بهینه‌سازی دقیق‌تر هدایت می‌کند.

### ۶. آزمایش و ارزیابی

در این بخش، عملکرد روش پیشنهادی با سایر روش‌های موجود مقایسه و ارزیابی می‌شود تا کارایی و مزایای آن به طور دقیق تحلیل گردد. برای این منظور، نتایج به دست آمده از روش پیشنهادی با روش‌های مطرح شده در پژوهش‌های قبلی از جمله [۳۴]، [۴۴] و [۵۳] مقایسه شده است.

#### ۶-۱. روش اندازه‌گیری عملکرد

ارزیابی مدل پیشنهادی یکی از مراحل کلیدی این پژوهش است که به منظور سنجش عملکرد مدل در شناسایی تهدیدات امنیتی

مجموعه داده *CICIDS2018* در ادامه نسخه ۲۰۱۷، توسط مؤسسه امنیت سایبری کانادا تولید شده است و شامل ترافیک شبکه ترکیبی از فعالیت‌های عادی و انواع مختلف حملات است.

مجموعه داده *CICDDoS2019* با تمرکز ویژه بر حملات *DDoS* در مقیاس وسیع، طراحی شده است و شامل انواع مختلف حملات *DDoS* در بسترهای متنوع شبکه است [۵۲].

### ۵-۲. پیش‌پردازش مجموعه داده

در این پژوهش، آماده‌سازی داده‌ها باهدف بهبود کیفیت ورودی‌های مدل انجام شد. مجموعه داده‌ی اولیه شامل مقادیر گمشده، مقادیر بی‌نهایت بود. ابتدا، تمامی مقادیر گمشده و مقادیر بی‌نهایت ( $\pm \infty$ ) از مجموعه داده حذف شدند تا از بروز خطا در فرایند محاسبات جلوگیری شود. همچنین برچسب‌های خروجی که به صورت مقادیر متنی ذخیره شده بودند، با استفاده از روش *Label Encoding* به مقادیر عددی صفر برای دسته غیرتهاجمی و یک برای دسته تهاجمی تبدیل شدند.

به منظور ارزیابی دقیق روش پیشنهادی نسبت به سایر مقالات، سه ارزیابی انجام شد و مجموعه داده‌ها به سه بخش مجزا تقسیم شد: ۷۰ درصد برای آموزش مدل، ۱۵ درصد برای اعتبارسنجی طی فرایند آموزش، و ۱۵ درصد برای ارزیابی نهایی عملکرد. این تقسیم‌بندی با بهره‌گیری از روش *Train-Test Split* کتابخانه *scikit-learn* جهت حفظ ماهیت تصادفی نمونه‌گیری انجام شد تا از یادگیری جهت‌دار مدل نسبت به داده‌های خاص جلوگیری شود و توانایی تعمیم آن به داده‌های جدید تضمین گردد.

در ارزیابی اول جهت مقایسه با مقاله آمیر و همکاران [۳۴] و مقاله خرم و همکاران [۴۴]، از یک زیرمجموعه ۱۰، ۰۰۰ نمونه‌ای از مجموع ۲۲۵،۷۴۵ نمونه داده استفاده شد که با استفاده از روش برهم‌زدن و تصادفی‌سازی<sup>۱</sup> استخراج گردید. این زیرمجموعه دارای توزیع مشابهی از ترافیک نرمال و ترافیک *DDoS* نسبت به مجموعه داده اصلی است. به این ترتیب، ۴۳۲۵ نمونه از ترافیک نرمال و ۵۶۷۵ نمونه از ترافیک *DDoS* به طور تصادفی انتخاب شدند.

در مرحله بعد، پس از انجام بررسی‌های اولیه از وبگاه مرجع مجموعه داده‌ها، مشخص شد که سازندگان این مجموعه داده ویژگی‌ها را بر اساس میزان تأثیر آن‌ها در شناسایی ترافیک مرتب کرده‌اند. بر این اساس، در این پژوهش، چهار ویژگی کلیدی شامل *Bwd Packet Length*، *Flow IAT*، *Flow Duration*، *Average Packet Size*، *Std* با ضریب ۰/۲ تقویت شدند تا تأثیر آن‌ها در شناسایی دقیق‌تر ترافیک *DDoS* افزایش یابد. سایر ویژگی‌ها بدون

<sup>۲</sup>. Batch size.

<sup>۱</sup>. Shuffling and randomization.

می دهد. این معیار نشان دهنده توانایی مدل در پیش بینی دقیق نمونه های منفی و اجتناب از پیش بینی های اشتباهی است. در شرایطی که مدل باید از پیش بینی تهدیدات کاذب اجتناب کند، *Specificity* اهمیت زیادی دارد.

در نهایت، نرخ هشدار کاذب (*FAR*) به نسبت پیش بینی های منفی اشتباه *FP* به مجموع *FP+TN* اشاره دارد و برای اندازه گیری میزان اشتباهات منفی مدل استفاده می شود. این معیار با استفاده از رابطه (۱۰) محاسبه می شود:

$$FAR = \frac{FP}{FP+TN} \quad (10)$$

## ۲-۶. تنظیمات آزمایش

انتخاب ابرپارامترهای مناسب نقش کلیدی در عملکرد مدل های یادگیری عمیق ایفا می کند. جدول (۲) مقادیر انتخاب شده برای ابرپارامترهای کلیدی را نمایش می دهد.

جدول (۲). ابرپارامترهای مدل

| مقدار                    | ابرپارامترها          |
|--------------------------|-----------------------|
| ۲۰۰                      | تعداد دوره ها         |
| ۰۰۱/۰                    | حداکثر نرخ یادگیری    |
| ۰۰۰۰۱/۰                  | حداقل نرخ یادگیری     |
| ۶۴                       | اندازه دسته           |
| <i>CosineAnnealingLR</i> | شیوه کاهش نرخ یادگیری |
| <i>Early Stopping</i>    | رویکرد توقف           |
| ۱۲۳۴                     | بذر تصادفی اولیه      |

## ۳-۶. ارزیابی اول بر روی مجموعه داده CICIDS2017

در این بخش، نتایج آزمایش روش پیشنهادی با مقاله آمیر و همکاران [۳۴] و مقاله خرم و همکاران [۴۴] بررسی شده است. در پژوهش آمیر و همکاران آن ها، رویکردی مبتنی بر خوشه بندی برای شناسایی داده های ترافیک شبکه، شامل ترافیک عادی و حملات *DDoS*، پیشنهاد شده است. در این روش از الگوریتم های خوشه بندی مانند خوشه بندی تجمیعی و *K-means* همراه با تحلیل مؤلفه های اصلی برای استخراج ویژگی استفاده شده است. پس از برچسب گذاری داده ها به کمک روش رأی گیری، الگوریتم های یادگیری ماشین نظارت شده نظیر *kNN*، *SVM* و *RF* مورد استفاده قرار گرفته اند.

با استفاده از مجموعه داده های آزمایشی انجام شده است. در این بخش، از معیارهای گوناگون ارزیابی استفاده شده است تا عملکرد مدل به صورت جامع و دقیق بررسی شود.

*Accuracy* یکی از معیارهای رایج است که نشان دهنده توانایی کلی مدل در پیش بینی درست نمونه ها است. این معیار به وسیله رابطه (۶) محاسبه می شود و از مجموع نمونه های درست شناسایی شده *TP+TN* نسبت به تمامی نمونه ها *TP+TN+FP+FN* به دست می آید.

$$AC = \frac{TP+TN}{TP+TN+FP+FN} \quad (6)$$

*Precision* به نسبت پیش بینی های مثبت درست *TP* به مجموع *TP+FP* اشاره دارد و نشان دهنده توانایی مدل در شناسایی حملات صحیح است. این معیار با استفاده از رابطه (۷) محاسبه می شود:

$$PR = \frac{TP}{TP+FP} \quad (7)$$

*Recall* به نسبت پیش بینی های مثبت درست *TP* به مجموع *TP+FN* است و نشان دهنده توانایی مدل در شناسایی تمامی نمونه های مثبت موجود است. این معیار با رابطه (۸) محاسبه می شود:

$$RE = \frac{TP}{TP+FN} \quad (8)$$

*F1-Score* معیار دیگری است که به طور هماهنگ عملکرد *Precision* و *Recall* را با هم ارزیابی می کند و معمولاً زمانی که آن ها در تضاد هستند، به کار می رود. این معیار با استفاده از رابطه (۹) به دست می آید:

$$F1 = \frac{2*Precision*Recall}{Precision+Recall} \quad (9)$$

*ROC AUC* یک معیار کلیدی دیگری است که برای ارزیابی عملکرد مدل های طبقه بندی استفاده می شود که نشان دهنده توانایی مدل در تفکیک صحیح بین کلاس های مثبت و منفی است. منحنی *ROC* یک نمایش گرافیکی از رابطه بین *TPR* و *FPR* است. مساحت زیر این منحنی (*AUC*) مقدار ۱ نشان دهنده عملکرد عالی مدل در شناسایی تمایز میان دسته ها است. هرچه *AUC* نزدیک به ۱ باشد، مدل در تفکیک صحیح بین نمونه های مثبت و منفی بهتر عمل کرده است.

*AUPR* یک معیار دیگر است که به ویژه در مواقعی که داده ها نامتوازن هستند، اهمیت پیدا می کند. این معیار به تحلیل دقیق عملکرد مدل در شناسایی کلاس های مثبت اختصاص دارد. منحنی *PR* به بررسی *Precision* و *Recall* در مواجهه با نمونه های مثبت می پردازد. *AUPR*، مساحت زیر این منحنی را محاسبه می کند که هرچه این مقدار بالاتر باشد، مدل در شناسایی نمونه های مثبت به طور دقیق تری عمل کرده است.

*Specificity* که به آن نرخ منفی درست نیز گفته می شود، میزان شناسایی صحیح نمونه های منفی توسط مدل را نشان

سایبری مطرح می‌شود. این قابلیت‌ها، مدل را به یک استاندارد جدید در حوزه امنیت سایبری تبدیل کرده و امکان پیاده‌سازی مؤثر آن را در محیط‌های واقعی و مقیاس‌پذیر فراهم می‌سازد.

#### ۴-۶. ارزیابی دوم بر روی مجموعه داده CICIDS2018

در این بخش، نتایج آزمایش روش پیشنهادی با مقاله آبراماسونداری و همکاران [۵۳] بررسی شده است. جدول (۶) مقایسه روش پیشنهادی با مقاله آبراماسونداری و همکاران را نشان می‌دهد.

جدول (۶). مقایسه روش پیشنهادی با مقاله آبراماسونداری و همکاران

| شماره ارجاع                        | AC   | F1   | RE   | PR   |
|------------------------------------|------|------|------|------|
| روش پیشنهادی                       | ۱۰۰  | ۱۰۰  | ۱۰۰  | ۱۰۰  |
| [۵۳]                               | ۹۷/۰ | ۹۷/۰ | ۹۵/۰ | ۹۹/۰ |
| زمان آموزش روش پیشنهادی: ۱۲۵ ثانیه |      |      |      |      |

جدول (۷). ماتریس درهم‌ریختگی

|        | Benign | Attack |
|--------|--------|--------|
| Benign | ۴۳۰۵   | ۰      |
| Attack | ۰      | ۳۱۹۵   |

#### ۴-۵. ارزیابی سوم بر روی مجموعه داده CICDDoS2019

در این بخش، نتایج آزمایش روش پیشنهادی با مقاله آبراماسونداری و همکاران [۵۳] بررسی شده است. جدول (۸) مقایسه روش پیشنهادی با مقاله آبراماسونداری و همکاران را نشان می‌دهد.

جدول (۸). مقایسه روش پیشنهادی با مقاله آبراماسونداری و همکاران

| شماره ارجاع                        | AC   | F1   | RE   | PR   |
|------------------------------------|------|------|------|------|
| روش پیشنهادی                       | ۱۰۰  | ۹۹/۰ | ۱۰۰  | ۹۹/۰ |
| [۵۳]                               | ۹۸/۰ | ۹۸/۰ | ۹۸/۰ | ۹۸/۰ |
| زمان آموزش روش پیشنهادی: ۲۹۵ ثانیه |      |      |      |      |

نتایج نشان داد که مدل‌های  $kNN$ ،  $SVM$  و  $RF$  در پژوهش آن‌ها به ترتیب دقت‌هایی برابر با ۹۵٪، ۹۲٪ و ۶۶/۹۶٪ داشته‌اند. با این حال، مدل پیشنهادی ما با بهره‌گیری از شبکه عصبی عمیق، موفق به دستیابی به دقت ۱۰۰٪ شده است که این امر، توانمندی مدل در یادگیری ویژگی‌های پیچیده و شناسایی حملات  $DDoS$  با دقت بسیار بالا را نشان می‌دهد. جدول (۳) مقایسه روش پیشنهادی با مقاله آمیر و همکاران و مقاله خرم و همکاران را نشان می‌دهد.

جدول (۳). مقایسه روش پیشنهادی با مقاله آمیر و همکاران و خرم و همکاران

| شماره ارجاع                       | AC    | PR    | FAR |
|-----------------------------------|-------|-------|-----|
| روش پیشنهادی                      | ۱۰۰   | ۱۰۰   | ۰   |
| [۳۴]                              | ۶۶/۹۶ | ۱۰/۸۲ | -   |
| [۴۴]                              | ۸۱/۹۹ | -     | -   |
| زمان آموزش روش پیشنهادی: ۸۱ ثانیه |       |       |     |

جدول (۴). نتایج ارزیابی مدل پیشنهادی با بذرهای تصادفی مختلف بر اساس متریک‌های  $F1$ -Score،  $Recall$ ،  $Precision$ ،  $Accuracy$ ،  $FAR$ ،  $FPR$ ،  $FNR$

| Seed | AC  | PR  | RE  | F1  | FAR | FPR | FNR |
|------|-----|-----|-----|-----|-----|-----|-----|
| ۲۸   | ۱۰۰ | ۱۰۰ | ۱۰۰ | ۱۰۰ | ۰   | ۰   | ۰   |
| ۷    | ۱۰۰ | ۱۰۰ | ۱۰۰ | ۱۰۰ | ۰   | ۰   | ۰   |
| ۱۲۳۴ | ۱۰۰ | ۱۰۰ | ۱۰۰ | ۱۰۰ | ۰   | ۰   | ۰   |
| ۲۰۲۵ | ۱۰۰ | ۱۰۰ | ۱۰۰ | ۱۰۰ | ۰   | ۰   | ۰   |

جدول (۵). مقایسه مصرف حافظه در زمان تست و عملکرد مدل در معیارهای

$ROC$ ،  $AUC$ ،  $Specificity$  و  $AUPR$

| Seed | ROC AUC | PR AUC | Specificity | Memory Usage (MB) |
|------|---------|--------|-------------|-------------------|
| ۲۸   | ۱۰۰     | ۱۰۰    | ۱۰۰         | ۲۹/۶۰۸            |
| ۷    | ۱۰۰     | ۱۰۰    | ۱۰۰         | ۴۵/۶۱۱            |
| ۱۲۳۴ | ۱۰۰     | ۱۰۰    | ۱۰۰         | ۴۴/۵۱۳            |
| ۲۰۲۵ | ۱۰۰     | ۱۰۰    | ۱۰۰         | ۹۰/۴۲۸            |

به‌طور کلی، مدل پیشنهادی نه تنها از نظر معیارهای عددی عملکردی برتر نسبت به پژوهش‌های پیشین دارد، بلکه با سرعت یادگیری بالا، پایداری در تشخیص و کاهش نرخ خطا کاذب به صفر، به‌عنوان یک راهکار قدرتمند و عملیاتی در برابر تهدیدات

industry,” in Security Engineering for Embedded and Cyber-Physical Systems, CRC Press, pp. 51-70, 2022. doi:10.1201/9781003278207-6.

- [4] Z.A. Chughtai, S. Chughtai, R. Malik, H. Raza, and M. Saleem, “Towards a blockchain enabled integrated library management system using Hyperledger Fabric,” Int. J. Comput. Innov. Sci., vol. 1, no. 3, pp. 17-24, 2022.
- [5] J. Wei, C. Long, J. Li, and J. Zhao, “An intrusion detection algorithm based on bag representation with ensemble support vector machine in cloud computing,” Concurrency and Computation, vol. 32, no. 24, p. e5922, 2020. doi:10.1002/cpe.5922.
- [6] P. Mishra, E.S. Pilli, V. Varadharajan, and U. Tupakula, “Intrusion detection techniques in cloud environment: a survey,” Journal of Network and Computer Applications, vol. 77, pp. 18-47, 2017. doi:10.1016/j.jnca.2016.10.015.
- [7] K. Peng, V.C.M. Leung, L. Zheng, S. Wang, C. Huang, and T. Lin, “Intrusion detection system based on decision tree over big data in fog environment,” Wireless Communications and Mobile Computing, vol. 2018, no. 1, p. 4680867, 2018. doi:10.1155/2018/4680867.
- [8] Q. Schueller, K. Basu, M. Younas, M. Patel, and F. Ball, “A hierarchical intrusion detection system using support vector machine for SDN network in cloud data center,” in 2018 International Telecommunication Networks and Applications Conference (ITNAC), pp. 1-6, 2018. doi:10.1109/ATNAC.2018.8615255.
- [9] C. Modi, D. Patel, B. Borisanya, A. Patel, and M. Rajarajan, “A novel framework for intrusion detection in cloud,” in Proceedings of the Fifth International Conference on Security of Information and Networks, pp. 67-74, 2012. doi:10.1145/2388576.2388585.
- [10] V.R. Pathmudi, N. Khatrri, S. Kumar, A.S.H. Abdul-Qawy, and A.K. Vyas, “A systematic review of IoT technologies and their constituents for smart and sustainable agriculture applications,” Scientific African, vol. 19, p. e01577, 2023. doi:10.1016/j.sciaf.2023.e01577.
- [11] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K. R. Choo, “A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks,” IEEE Internet Things J., vol. 8, no. 12, pp. 9463–9472, 2021. doi:10.1109/JIOT.2020.2996590.
- [12] R. Zhao, Y. Yin, Y. Shi, and Z. Xue, “Intelligent intrusion detection based on federated learning aided long short-term memory,” Physical Communication, vol. 42, p. 101157, 2020. doi:10.1016/j.phycom.2020.101157.
- [13] A. Dawoud, S. Shahristani, and C. Raun, “Deep learning and software-defined networks: towards secure IoT architecture,” Internet of Things, vol. 3-4, pp. 82-89, 2018. doi:10.1016/j.iot.2018.09.003.
- [14] M. Almiani, A. 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, p. 102031, 2020. doi:10.1016/j.simpat.2019.102031.
- [15] P. Ghosh, A. Karmakar, J. Sharma, and S. Phadikar, “CS-PSO based intrusion detection system in cloud environment,” Emerging Technologies in Data Mining

جدول (۹). ماتریس درهمیختگی

|        | Benign | Attack |
|--------|--------|--------|
| Benign | ۵۸۱۳   | ۲۱     |
| Attack | ۱      | ۱۶۶۵   |

## ۷. نتیجه‌گیری

در این پژوهش، یک سیستم تشخیص نفوذ مبتنی بر شبکه‌های عصبی عمیق و مکانیزم توجه برای شناسایی حملات منع سرویس توزیع شده ارائه شد. نتایج آزمایش‌ها نشان داد که روش پیشنهادی، با استخراج ویژگی‌های کلیدی و تمرکز بر بخش‌های مهم داده‌ها، توانسته است دقت بی‌نظیر نزدیکی به ۱۰۰ درصدی را در شناسایی این حملات به دست آورد. این عملکرد بی‌نقص، برتری سیستم پیشنهادی را در مقایسه با روش‌های مشابه به اثبات رسانده و گامی مؤثر در بهبود امنیت سایبری و مقابله با تهدیدات پیچیده‌ای همچون حملات منع سرویس توزیع شده محسوب می‌شود. همچنین، این روش می‌تواند به عنوان زیربنایی برای توسعه سیستم‌های پیشرفته‌تر در حوزه تشخیص نفوذ مورد استفاده قرار گیرد.

باتوجه به رشد مداوم تهدیدات و چالش‌های امنیت سایبری، نیاز به تحقیقات و پیشرفت‌های بیشتر در این حوزه به وضوح احساس می‌شود. در این راستا، به عنوان کار آینده، قصد داریم روش پیشنهادی خود را در محیط‌های واقعی و عملیاتی آزمایش کنیم تا ارزیابی‌های بیشتری از قابلیت‌های آن به دست آوریم و به تکمیل آن در شرایط پیچیده‌تر بپردازیم.

علاوه بر این، ما قصد داریم در پروژه‌های آینده به سمت تشخیص حملات در سیستم‌های SCADA و UAV حرکت کنیم. این حوزه‌ها به دلیل ویژگی‌های خاص خود و چالش‌های امنیتی که دارند، نیازمند روش‌های خاص و کارآمد برای شناسایی تهدیدات و محافظت در برابر آن‌ها هستند؛ لذا، ما در حال توسعه روش خود برای مقابله با تهدیدات این سیستم‌ها و افزایش کارایی آن در محیط‌های پیچیده‌تری هستیم.

## ۸. مراجع

- [1] K. Nikolskaia and A. Minbaleev, “Legal regulation of incidents related to DDoS attacks,” in 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), pp. 53-55, 2020. doi:10.1109/ITQMIS51053.2020.9322874.
- [2] M. Sachdeva, G. Singh, K. Kumar, and K. Singh, “DDoS Incidents and their Impact: A Review,” Int. Arab J. Inf. Technol., vol. 7, no. 1, pp. 14-20, 2010.
- [3] J.A. Malik and M. Saleem, “Blockchain and cyber-physical system for security engineering in the smart

- [28] R. Primartha and B.A. Tama, "Anomaly detection using random forest: A performance revisited," in 2017 International Conference on Data and Software Engineering (ICoDSE), pp. 1-6, 2017. doi:10.1109/ICoDSE.2017.8285847.
- [29] J.B. Awotunde, C. Chakraborty, and A.E. Adeniyi, "Intrusion detection in industrial Internet of Things network-based on deep learning model with rule-based feature selection," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, p. 7154587, 2021. doi:10.1155/2021/7154587.
- [30] S. Naseer et al., "Enhanced network anomaly detection based on deep neural networks," *IEEE Access*, vol. 6, pp. 48231-48246, 2018. doi:10.1109/ACCESS.2018.2863036.
- [31] S. Alzughaibi and S. El Khediri, "A cloud intrusion detection systems based on DNN using backpropagation and PSO on the CSE-CIC-IDS2018 dataset," *Applied Sciences*, vol. 13, no. 4, p. 2276, 2023. doi:10.3390/app13042276.
- [32] A. Maroosi, E. Zabbah, and H. Ataei Khabbaz, "Network Intrusion Detection using a combination of artificial neural networks in a hierarchical manner," *Electronic and Cyber Defense*, vol. 8, no. 1, pp. 89-99, 2020. (In Persian). <https://dor.isc.ac/dor/20.1001.1.23224347.1399.8.1.8.8>.
- [33] A. Tajari Siahmarzkooh, "Intrusion Detection in Computer Networks Using Decision Tree and Feature Reduction," *Electronic and Cyber Defense*, vol. 9, no. 3, pp. 99-108, 2021. (In Persian). <https://dor.isc.ac/dor/20.1001.1.23224347.1400.9.3.8.9>.
- [34] M. Aamir and S.M. Ali Zaidi, "Clustering based semi-supervised machine learning for DDoS attack classification," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 4, pp. 436-446, 2021. doi:10.1016/j.jksuci.2019.02.003.
- [35] Y. Otoum, D. Liu, and A. Nayak, "DL-IDS: a deep learning-based intrusion detection framework for securing IoT," *Trans Emerging Tel Tech*, vol. 33, no. 3, p. e3803, 2022. doi:10.1002/ett.3803.
- [36] H.A. Ahmed, A. Hameed, and N.Z. Bawany, "Network intrusion detection using oversampling technique and machine learning algorithms," *PeerJ Computer Science*, vol. 8, p. e820, 2022. doi:10.7717/peerj-cs.820.
- [37] A. Singh, J. Amutha, J. Nagar, S. Sharma, and C.-C. Lee, "LT-FS-ID: log-transformed feature learning and feature-scaling-based machine learning algorithms to predict the k-barriers for intrusion detection using wireless sensor network," *Sensors*, vol. 22, no. 3, p. 1070, 2022. doi:10.3390/s22031070.
- [38] A. Raghuvanshi et al., "Intrusion detection using machine learning for risk mitigation in IoT-enabled smart irrigation in smart farming," *Journal of Food Quality*, vol. 2022, pp. 1-8, 2022. doi:10.1155/2022/3955514.
- [39] A. Jaszcz and D. Polap, "AIMM: artificial intelligence merged methods for flood DDoS attacks detection," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 8090-8101, 2022. doi:10.1016/j.jksuci.2022.07.021.
- and *Information Security*, vol. 755, pp. 261-269, 2019. doi:10.1007/978-981-13-1951-8\_24.
- [16] R. SaiSindhuTheja and G.K. Shyam, "An efficient metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment," *Applied Soft Computing*, vol. 100, p. 106997, 2021. doi:10.1016/j.asoc.2020.106997.
- [17] M.R. Gauthama Raman, N. Somu, K. Kirthivasan, R. Liscano, and V.S. Shankar Sriram, "An efficient intrusion detection system based on hypergraph - genetic algorithm for parameter optimization and feature selection in support vector machine," *Knowledge-Based Systems*, vol. 134, pp. 1-12, 2017. doi:10.1016/j.knsys.2017.07.005.
- [18] S.P. RM et al., "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Computer Communications*, vol. 160, pp. 139-149, 2020. doi:10.1016/j.comcom.2020.05.048.
- [19] D. Ciregan, U. Meier, and J. Schmidhuber, "Multi-column deep neural networks for image classification," in 2012 IEEE Conference on Computer Vision and Pattern Recognition, pp. 3642-3649, 2012. doi:10.1109/CVPR.2012.6248110.
- [20] A. Krizhevsky, I. Sutskever, and G.E. Hinton, "ImageNet classification with deep convolutional neural networks," *Commun. ACM*, vol. 60, no. 6, pp. 84-90, 2017. doi:10.1145/3065386.
- [21] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436-444, 2015. doi:10.1038/nature14539.
- [22] M. Eskandari, Z.H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6882-6897, 2020. doi:10.1109/JIOT.2020.2970501.
- [23] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for online network intrusion detection," *arXiv preprint arXiv:1802.09089*, 2018.
- [24] H. Gharraee and H. Hosseinvand, "A new feature selection IDS based on genetic algorithm and SVM," in 2016 8th International Symposium on Telecommunications (IST), pp. 139-144, 2016. doi:10.1109/ISTEL.2016.7881798.
- [25] M. Belouch, S.E. Hadaj, and M. Idhammad, "A two-stage classifier approach using RepTree algorithm for network intrusion detection," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, no. 6, pp. 30-44, 2017. doi:10.14569/IJACSA.2017.080651.
- [26] M.M. Baig, M.M. Awais, and E.-S.M. El-Alfy, "A multiclass cascade of artificial neural network for network intrusion detection," *Journal of Intelligent & Fuzzy Systems*, vol. 32, no. 4, pp. 2875-2883, 2017. doi:10.3233/JIFS-169230.
- [27] B.A. Tama and K.-H. Rhee, "An in-depth experimental study of anomaly detection using gradient boosted machine," *Neural Comput & Applic*, vol. 31, no. 4, pp. 955-965, 2019. doi:10.1007/s00521-017-3128-z.

- [48] I. Sharafaldin, A. Habibi Lashkari, and A.A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in Proceedings of the 4th International Conference on Information Systems Security and Privacy, Funchal, Madeira, Portugal: SCITEPRESS - Science and Technology Publications, pp. 108-116, 2018. doi:10.5220/0006639801080116.
- [49] I. Sharafaldin, A. Gharib, A.H. Lashkari, A.A. Ghorbani, "Towards a reliable intrusion detection benchmark dataset," JSN, vol. 2017, no. 1, pp. 177-200, 2017. doi:10.13052/jsn2445-9739.2017.009.
- [50] R. Abdulhammed, H. Musafar, A. Alessa, M. Faezipour, and A. Abuzneid, "Features dimensionality reduction approaches for machine learning based network intrusion detection," Electronics, vol. 8, no. 3, p. 322, 2019. doi:10.3390/electronics8030322.
- [51] A. Gharib, I. Sharafaldin, A.H. Lashkari, and A.A. Ghorbani, "An evaluation framework for intrusion detection dataset," in 2016 International Conference on Information Science and Security (ICISS), pp. 1-6, 2016. doi:10.1109/ICISSEC.2016.7885840.
- [52] I. Sharafaldin, A.H. Lashkari, S. Hakak, and A.A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," in 2019 International Carnahan Conference on Security Technology (ICCST), pp. 1-8, 2019. doi:10.1109/CCST.2019.8888419.
- [53] S. Abiramasundari and V. Ramaswamy, "Distributed Denial-of-Service (DDoS) Attack Detection Using Supervised Machine Learning Algorithms," Sci Rep, vol. 15, no. 1, p. 13098, 2025. doi:10.1038/s41598-024-84879-y.
- [40] J. Mazloun and H. Bigdeli, "An Optimized Compound Deep Neural Network Integrating With Feature Selection for Intrusion Detection System in Cyber Attacks," Electronic and Cyber Defense, vol. 10, no. 4, pp. 41-51, 2023. (In Persian). <https://dor.isc.ac/dor/20.1001.1.23224347.1401.10.4.5.5>.
- [41] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, "Deep learning approach for SDN-enabled intrusion detection system in IoT networks," Information, vol. 14, no. 1, p. 41, 2023. doi:10.3390/info14010041.
- [42] J. Figueiredo, C. Serrão, and A.M. De Almeida, "Deep learning model transposition for network intrusion detection systems," Electronics, vol. 12, no. 2, p. 293, 2023. doi:10.3390/electronics12020293.
- [43] S.V.J. Rani et al., "Detection of DDoS attacks in D2D communications using machine learning approach," Computer Communications, vol. 198, pp. 32-51, 2023. doi:10.1016/j.comcom.2022.11.013.
- [44] M. Khorram and M. Rahmanimanesh, "DDoS Attack Detection System Using Ensemble Method Classification and Active Learning Approach," Electronic and Cyber Defense, vol. 11, no. 3, pp. 101-118, 2023. (In Persian). <https://dor.isc.ac/dor/20.1001.1.23224347.1402.11.3.10.5>
- [45] A. Alfatemi et al., "Identifying distributed denial of service attacks through multi-model deep learning fusion and combinatorial analysis," J Netw Syst Manage, vol. 33, no. 1, p. 8, 2025. doi:10.1007/s10922-024-09882-0.
- [46] H. Lu, J. Liu, J. Peng, and J. Lu, "Adversarial attacks based on time-series features for traffic detection," Computers & Security, vol. 148, p. 104175, 2025. doi:10.1016/j.cose.2024.104175.
- [47] Y. Gorishniy, A. Kotelnikov, and A. Babenko, "TabM: Advancing tabular deep learning with parameter-efficient ensembling," arXiv preprint arXiv:2410.24210, 2024.