JOURNAL OF SOUTHERN COMMUNICATION ENGINEERING
ISLAMIC AZAD UNIVERSITY BUSHEHR BRANCH
E-ISSN: 2980-9231
https://jce.bushehr.iau.ir
https://doi.org/10.30495/jce.2023.1984927.1201

Vol. 13/ No. 49/Autumn 2023

Research Article

Distributed Denial of Service Attacks Detection in Internet of Things Using the Majority Voting Approach

Habibollah Mazarei, MSc Student [1] | Marzieh Dadvar, Assistant Professor [2*] | MohammadHadi Atabakzadeh, Assistant Professor [3]

[1]Department of Computer Engineering, Bushehr Branch, Islamic Azad University, Bushehr, Iran
doktorhm@gmail.com

[2]Department of Computer Engineering, Bushehr Branch, Islamic Azad University, Bushehr, Iran
m.dadvar@srbiau.ac.ir

[3] Department of Mathematics, Bushehr Branch, Islamic Azad University, Bushehr, Iran
mh_atabak@yahoo.com

Correspondence
Marzieh Dadvar, Assistant Professor, Department of Computer Engineering, Bushehr Branch, Islamic Azad University, Bushehr, Iran
m.dadvar@srbiau.ac.ir

Received: 30 April 2023
Revised: 8 June 2023
Accepted: 15 June 2023

Abstract

With the ever-increasing number of Internet of Things devices, their security is becoming a very worrying issue. Weak security measures enable attackers to attack IoT devices. One of these attacks is the distributed denial of service(DDOS) attack. Therefore, the existence of intrusion detection systems in the Internet of Things is of special importance. In this research, the majority voting group approach, which is a subset of machine learning, has been used to detect and predict attacks. The motivation for using this method is to achieve better detection accuracy and a very low false positive rate by combining several machine learning classification algorithms in heterogeneous Internet of Things networks. In this research, the new and improved CICDDOS2019 dataset has been used to evaluate the proposed method. The simulation results show that by applying the majority voting Ensemble method on five attacks from this data set, this method respectively has achieved accuracy of detection 99.9669%, 99.9670%, 100%, 99.9686% and 99.9674% in identifying DNS, NETBIOS, LDAP, UDP and SNMP attacks which better and more stable performance in detecting and predicting attacks have achieved than the basic models.

Keywords: Internet of Things, Intrusion Detection System, Distributed Denial of Service Attack, Machine Learning, Majority Voting

Highlights

- Conducting experiments on five attacks from the new and improved CICDDOS2019 dataset.
- Using the Majority Voting Ensemble Model with the Combination of 5 Basic Algorithms.
- Combining Different Sampling Methods in the Training Set to Balance the Dataset.
- Achieving better and higher accuracy compared to basic algorithms and previous research.

Citation: H. Mazarei, M. Dadvar, and M. Atabakzadeh, "Distributed Denial of Service Attacks Detection in Internet of Things Using the Majority Voting Approach," Journal of Southern Communication Engineering, vol. 13, no. 49, pp. 23–48, 2023, doi: 10.30495/jce.2023.1984927.1201, (in Persian).

مقاله پژوهشی

تشخیص حملات منع سرویس توزیع‌شده در اینترنت اشیاء با استفاده از رویکرد رأی-گیری اکثریت

حبیب اله مزارعی[۱] | مرضیه دادور*[۲] | محمدهادی اتابک زاده[۳]

[۱] گروه مهندسی کامپیوتر، ،واحد بوشهر، دانشگاه آزاد اسلامی، بوشهر،ایران، doktorhm@gmail.com

[۲] گروه مهندسی کامپیوتر، واحد بوشهر، دانشگاه آزاد اسلامی، بوشهر،ایران، m.dadvar@srbiau.ac.ir

[۳]گروه ریاضی، واحد بوشهر، دانشگاه آزاد اسلامی، بوشهر،ایران، mh_atabak@yahoo.com

نویسنده مسئول
*مرضیه دادور، استادیار، گروه مهندسی کامپیوتر، واحد بوشهر، دانشگاه آزاد اسلامی، بوشهر، ایران،
m.dadvar@srbiau.ac.ir

چکیده:

با افزایش روزافزون دستگاه‌های اینترنت اشیاء، امنیت آن‌ها به موضوعی بسیار نگران‌کننده تبدیل‌شده است. اقدامات امنیتی ضعیف، مهاجمان را قادر می‌سازد تا دستگاه‌های اینترنت اشیاء را مورد حمله قرار دهند. یکی از این حملات، حمله منع سرویس توزیع‌شده است؛ بنابراین وجود سیستم-های تشخیص نفوذ در اینترنت اشیاء، از اهمیت ویژه‌ای برخوردار است. در این پژوهش، از رویکرد گروهی رأی‌گیری اکثریت که زیرمجموعه الگوریتم-های یادگیری ماشین است جهت تشخیص و پیش‌بینی حملات استفاده‌شده است. انگیزه استفاده از این روش، دستیابی به‌دقت تشخیص بهتر و نرخ مثبت کاذب بسیار پایین با ترکیب چند الگوریتم طبقه‌بندی یادگیری ماشین، در شبکه‌های ناهمگن اینترنت اشیاء است. در این پژوهش از مجموعه داده جدید و بهبودیافته CICDDOS2019 برای ارزیابی روش پیشنهادی استفاده‌شده است. نتایج شبیه‌سازی نشان می‌دهد که با اعمال روش گروهی رأی‌گیری اکثریت روی پنج حمله از این مجموعه داده، این روش به ترتیب به‌دقت تشخیص ۹۹/۹۶۶۹٪، ۹۹/۹۶۷۰٪، ۱۰۰٪، ۹۹/۹۶۸۶٪ و ۹۹/۹۶۷۴٪ در شناسایی حملات DNS، NETBIOS، LDAP، UDP و SNMP دست‌یافت که نسبت به مدل‌های پایه، عملکرد بهتر و پایدارتری در تشخیص و پیش‌بینی حملات، از خود نشان داده است.

کلید واژه‌ها: اینترنت اشیاء، سیستم تشخیص نفوذ، حمله منع سرویس توزیع‌شده، یادگیری ماشین، رأی‌گیری اکثریت

تاریخ دریافت: ۱۰ اردیبهشت ۱۴۰۲
تاریخ بازنگری: ۱۸ خرداد ۱۴۰۲
تاریخ پذیرش: ۲۵ خرداد ۱۴۰۲

https://doi.org/10.30495/jce.2023.1984927.1201

۱-مقدمه

اینترنت اشیاء[1] مجموعه‌ای از دستگاه‌های مرتبط با یکدیگر است که در آن دستگاه‌ها بدون نیاز به دخالت انسان توانایی اتصال به یکدیگر را دارند [۱]. محققان در [۲] پیش‌بینی کرده‌اند که تا سال ۲۰۳۰ تعداد دستگاه‌های اینترنت اشیاء مورد استفاده در سراسر جهان نزدیک به ۱۲۵ میلیارد دستگاه خواهد رسید که این رشد با افزایش انواع تهدیدات شبکه همراه خواهد بود. امروزه امنیت سیستم اینترنت اشیاء با توجه به افزایش تعداد دستگاه‌های هوشمند که اطلاعات خصوصی و ارزشمند افراد را حمل می‌کنند، به موضوعی بسیار نگران‌کننده تبدیل‌شده است [۳].

اقدامات امنیتی ضعیف، مهاجمان را قادر می‌سازد تا دستگاه‌های اینترنت اشیاء را مورد هدف قرار دهند [۴]. اینترنت اشیاء بر روی یک معماری چندلایه کار می‌کند و در برابر حملات مختلف امنیت سایبری آسیب‌پذیر است که یکی از این حملات، حمله

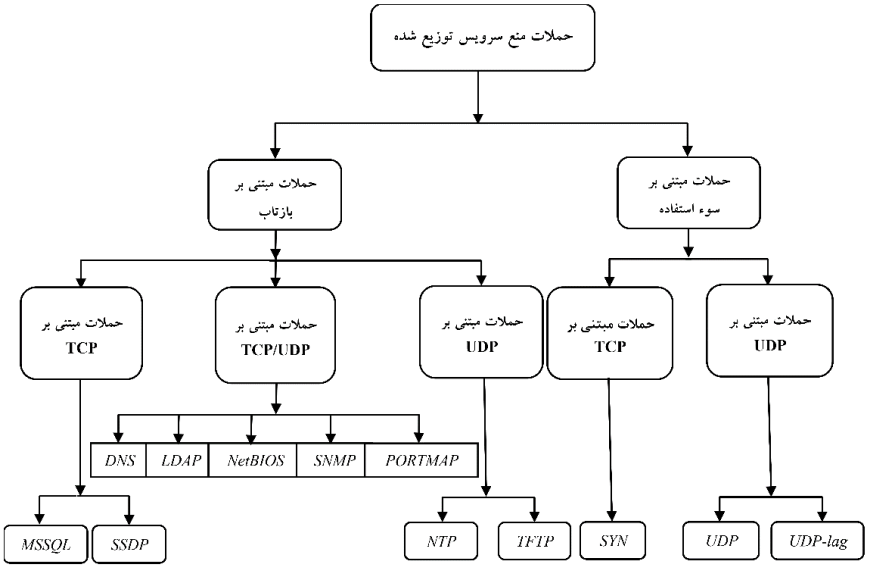
[1] Internet of Things

منع سرویس توزیع‌شده است [۵]. حمله منع سرویس توزیع‌شده به‌عنوان یکی از معروف‌ترین حملات در دهه گذشته، باعث می‌شود که یک سرویس آنلاین که کاربران قانونی به آن دسترسی دارند با غلبه بر ترافیک از منابع متعدد، غیرقابل‌دسترس شود. این منابع عموماً رایانه‌های آلوده‌شده‌ای هستند که به‌عنوان ربات در بات‌نت‌ها استفاده می‌شوند [۶].

در چند سال گذشته، جهان شاهد انقلابی چشم‌گیر در هوش مصنوعی و کاربردهای آن در بخش‌های مختلف بوده است [۴]. ازآنجایی‌که بیشتر دستگاه‌های اینترنت اشیاء محدود به منابعی چون باتری، پهنای باند، حافظه و محاسبات هستند، تکنیک‌های امنیتی مبتنی بر الگوریتم‌هایی با قابلیت پیکربندی بالا و پیچیده قابل اجرا نیستند؛ بنابراین به‌منظور ایمن‌سازی سیستم‌های اینترنت اشیاء، روش‌های مبتنی بر یادگیری ماشین[1]، یک جایگزین امیدبخش به حساب می‌آید [۷, ۳].

ازآنجاکه شبکه‌های اینترنت اشیاء از استانداردها و پروتکل‌های متنوع استفاده می‌کنند، تشکیل شبکه‌های ناهمگن، یادگیری الگوهای ترافیک مختلف را برای یک مدل پایه دشوار می‌سازد؛ بنابراین، با ترکیب خروجی‌های مدل‌ها در یک مدل یادگیری گروهی[2]، خطر انتخاب نادرست توسط یک الگوریتم طبقه‌بندی با عملکرد ضعیف کاهش می‌یابد [۷]. به‌طورکلی، استفاده از روش‌های گروهی به معنای ترکیب مدل‌ها در یک مجموعه است به‌طوری‌که این مدل ترکیبی به‌طور متوسط عملکرد بهتری نسبت به یک مدل یادگیری پایه داشته باشد، یعنی مدل‌ها برای داشتن نتایج بهتر باهم ترکیب می‌شوند [۸]. با این‌حال، گاهی اوقات عملکرد یک مدل پایه بر رویکرد گروهی غلبه می‌کند، اما تضمین می‌شود که رویکرد گروهی، خطر کل انتخاب نامعتبر را کاهش می‌دهد [۹].

در رویکرد رأی‌گیری اکثریت هر الگوریتم طبقه‌بند پایه، به یک کلاس رأی می‌دهد و کلاس خروجی هر یک از مدل‌ها در مدل گروهی، به‌عنوان یک رأی در نظر گرفته می‌شود و کلاسی که اکثریت آراء را کسب کند، خروجی مدل گروهی خواهد بود. به این روش انتخاب سخت یا رأی‌گیری اکثریت[3] گفته می‌شود. اکثریت به این معناست که باید بیش از نیمی از روش‌های طبقه‌بند پایه تصمیم یکسانی در مورد یک کلاس بگیرند [۷, ۹].



شکل ۱: روندنمای طبقه‌بندی حملات DDOS در مجموعه داده CICDDOS2019 [۱۰]

Figure 1. Flowchart of DDOS Classification in CICDDOS2019 Dataset [10]

در اکثر پژوهش‌ها از مجموعه داده‌های قدیمی مانند KDDCUP99، NSL-KDD، DARPA، UNSW-NB15 و... برای تشخیص حمله استفاده‌شده است. با توجه به آنچه در [۶] بیان‌شده است، مدل‌هایی که بر روی مجموعه داده‌های قدیمی فوق آموزش داده‌شده‌اند، دقت کمتری دارند؛ بنابراین در این پژوهش مجموعه داده جدید و بهبودیافته CICDDOS2019 برای پیش‌بینی حمله منع سرویس توزیع‌شده مورد استفاده قرار گرفته و از مهم‌ترین ویژگی‌های آن، برای شناسایی انواع مختلف حملات منع

[1] Machine Learning
[2] Ensemble Learning
[3] Hard Voting or Majority Voting

سرویس توزیع‌شده استفاده‌شده است. این مجموعه داده شامل ترافیک شبکه از دوازده حمله منع سرویس توزیع‌شده مختلف است. ازآنجاکه طبقه‌بندی حملات DDOS به‌طور گسترده مورد مطالعه قرارگرفته است، در این پژوهش به مطالعه شرافالدین و همکارانش [۱۰] اشاره شده است که در آن حملات جدید را همان‌طور که در شکل ۱ نشان داده‌شده، تجزیه‌وتحلیل می‌کنند. در شکل ۱ روندنمای طبقه‌بندی دقیق حملات منع سرویس توزیع‌شده ترسیم‌شده است که ساختار کلی این حملات را از نظر حملات مبتنی بر بازتاب و مبتنی بر سوءاستفاده توصیف می‌کند.

با توجه به این‌که حملات به دستگاه‌های اینترنت اشیاء، روزبه‌روز در حال افزایش هستند، هدف از انجام این پژوهش تشخیص حملات منع سرویس توزیع‌شده به این دستگاه‌ها است. انگیزه استفاده از رویکرد گروهی رأی‌گیری اکثریت در این پژوهش، کاهش خطر انتخاب نادرست توسط یک الگوریتم منفرد با عملکرد ضعیف در مدل گروهی است. ازاین‌رو برای دستیابی به نتایج بهتر، مدل‌ها باهم ترکیب می‌شوند تا ضعف مدل‌های پایه را کاهش داده و به‌دقت تشخیص بهتری دست یابند.

در این پژوهش ده الگوریتم بیز ساده، استنتاج قوانین، ماشین بردار پشتیبان، درخت تصمیم، جنگل تصادفی، شبکه عصبی، رگرسیون خطی، رگرسیون منطقی، یادگیری عمیق و مدل خطی تعمیم‌یافته از مجموعه الگوریتم‌های یادگیری ماشین برای دستیابی به‌دقت پیش‌بینی پنج حمله DNS، NetBIOS، LDAP، UDP و SNMP از مجموعه داده CICDDOS2019 مورد ارزیابی قرار می‌گیرند. از بین این ده الگوریتم، پنج الگوریتم که دارای دقت بالاتر، زمان اجرا و ریشه میانگین مربعات خطای کمتر هستند برای شرکت در رأی‌گیری اکثریت انتخاب می‌شوند. درنهایت نشان داده می‌شود که این رویکرد به عملکرد بهتری در تشخیص حملات دست می‌یابد.

این مقاله در چند بخش سازمان‌دهی شده است. کارهای مرتبط در بخش ۲ مورد بررسی قرارگرفته است. در بخش ۳ مفاهیم اولیه مرتبط تشریح شده‌اند. در بخش ۴ روش پیشنهادی به همراه تمام مراحل آن ارائه‌شده است. نتایج حاصل از این پژوهش در بخش ۵ و در نهایت، در بخش ۶ به نتیجه‌گیری پژوهش پرداخته‌شده است.

۲-کارهای مرتبط

در [۱۱]، از شبکه عصبی پس‌انتشار عمیق کالمن[1] برای تشخیص حمله منع سرویس توزیع‌شده در شبکه‌های اینترنت اشیاء دارای نسل پنج استفاده‌شده است. این روش مجموعه داده CICDDOS2019 را، برای پیاده‌سازی و ارزیابی مدل مورد استفاده قرار داده است که پس از ارزیابی مدل، به دقت تشخیص ۹۴٪ در شناسایی حملات دست پیدا کرد.

در [۱۲]، برای تشخیص حملات منع سرویس، از الگوریتم بیز ساده[2] در دستگاه‌های مبتنی بر اینترنت اشیاء با استفاده از مجموعه داده آموزشی[3] NSLKDD با فرمت KDD99 و مجموعه داده آزمایشی[4] تولیدشده از فرآیند ثبت حملات منع سرویس در دستگاه رزپری‌پای نسخه ۳[5] استفاده‌شده است. اعمال این الگوریتم روی مجموعه داده فوق، به دقت ۶۴/۰۲٪ در شناسایی حملات دست یافت.

در [۱۳]، از الگوریتم‌های K-نزدیکترین همسایه[6]، ماشین بردار پشتیبان[7]، درخت تصمیم[8]، بیز ساده، جنگل تصادفی[9]، شبکه عصبی مصنوعی[10] و رگرسیون منطقی[11] برای سیستم تشخیص نفوذ استفاده شد. بعد از اجرای این الگوریتم‌ها روی مجموعه داده Bot-IoT، در طبقه‌بندی دودویی[12]، دقت الگوریتم جنگل تصادفی در تشخیص حمله منع سرویس توزیع‌شده HTTP، برابر با ۹۹٪ به‌دست آمد. در طبقه‌بندی چندکلاسه[13] نیز، الگوریتم K- نزدیکترین همسایه با دقت ۹۹٪ بهتر از سایر الگوریتم‌ها عمل کرد.

---

[1] Deep Kalman Backpropagation Neural Network
[2] Naive Bayes
[3] Training Dataset
[4] Testing Dataset
[5] Raspberry Pi 3
[6] K-Nearest Neighbour (KNN)
[7] Support Vector Machine (SVM)
[8] Decision Tree (DT)
[9] Random Forest (RF)
[10] Artificial Neural Network (ANN)
[11] Logistic Regression (LR)
[12] Multi-Class Classification
[13] Binary Classification

در [۱۴]، الگوریتم رگرسیون منطقی روی مجموعه داده CICDDOS2019 برای پیش‌گیری از حملات امنیت سایبری[1] اینترنت اشیاء اعمال گردید. این روش به دقت پیش‌بینی ۹۹/۷٪ در تشخیص حملات دست یافت.

در [۱۵]، از الگوریتم جنگل تصادفی در شناسایی چهار نوع حمله DDOS و از مجموعه داده CICDDOS2019 و UNSW-NB15 برای مقایسه نتایج پیش‌بینی استفاده شد. در نتیجه این الگوریتم، به دقت تشخیص ۹۹/۹۲۶۶۷٪ در مجموعه داده CICDDOS2019 و به دقت تشخیص ۹۶/۲٪ در مجموعه داده UNSW-NB15 دست پیدا کرد.

در [۱۶]، برای پیش‌گیری از حملات منع سرویس توزیع‌شده یک سیستم تشخیص حمله چندلایه در اینترنت اشیاء پیشنهاد شد و با اجرای الگوریتم درخت تصمیم روی مجموعه داده Sensor data شاخص‌های دقت و امتیاز F1 به بیش از ۹۷٪ رسید.

در [۱۷]، با استفاده از شبکه رزنت[2] که یکی از مدل‌های یادگیری عمیق است، روشی برای تبدیل داده‌های ترافیک شبکه به شکل تصویر سه کانالی پیشنهاد شد. همچنین مجموعه داده CICDDOS2019 برای شناسایی حملات مورد استفاده قرار گرفت. سپس شبکه‌های عصبی پیچشی[3] یعنی شبکه رزنت را به دلیل عملکرد فوق‌العاده‌شان در زمینه پردازش تصویر، روی داده‌های تبدیل‌شده این مجموعه داده، آموزش داده شد. این روش توانست با استفاده از طبقه‌بندی دودویی به دقت ۹۹/۹۹٪ و با استفاده از طبقه‌بندی چندکلاسه به دقت ۸۷/۰۶٪، حملات را شناسایی کند.

در [۱۸]، تکنیک‌های سبک وزن[4] برای شناسایی حملات SYN در دستگاه‌هایی که به اینترنت متصل هستند، بررسی شد. به طور خاص، یک شبکه عصبی تصادفی[5] با یادگیری عمیق روی مجموعه داده مجازی ساخته‌شده با نام PCAP با استفاده از Wireshark برای این مدل پیش‌بینی پیاده‌سازی شد که با ترافیک عادی و یک شبکه عصبی با حافظه کوتاه مدت طولانی[6] آموزش دیده است. در نهایت نشان داده شد، شبکه عصبی تصادفی پیشنهادی با دقت ۸۰/۷٪، در مقایسه با شبکه عصبی با حافظه کوتاه مدت طولانی با دقت ۶۲/۷٪ به‌طور قابل‌توجهی تشخیص حمله بهتر و نرخ هشدار نادرست پایین‌تری ارائه کرده است.

در [۱۹]، مقایسه‌ای بین الگوریتم‌های مختلف یادگیری ماشین مورد استفاده در سیستم تشخیص نفوذ، برای محاسبات مه[7]، اینترنت اشیاء، داده‌های بزرگ[8]، شهر هوشمند[9] و شبکه 5G انجام شد. از مجموعه داده KDD-CUP برای طبقه‌بندی حملات استفاده شد. نتایج به‌دست آمده نشان داد که الگوریتم جنگل تصادفی با دقت ۹۹/۶۵٪ عملکرد بهتری نسبت به الگوریتم تجزیه و تحلیل تشخیص خطی با دقت ۹۸/۱٪ و الگوریتم طبقه‌بندی و درختان رگرسیون با دقت ۹۸٪ دارد.

در [۲۰]، یک سیستم تشخیص نفوذ مبتنی بر ترکیب یک روش بهینه‌سازی چندمنظوره سازگار با جهش ژنی[10] پیشنهاد شد. سپس برای طبقه‌بندی حملات از مدل‌های یادگیری عمیق شبکه عصبی پیچشی با حافظه کوتاه‌مدت طولانی، در آخرین مجموعه داده CICIDS2017 استفاده شد. در نتیجه این روش به دقت بالای ۹۹/۰۳٪ و میزان امتیاز Fl ، ۹۹/۳۶٪ دست یافت.

در [۲۱]، یک شبکه عصبی بازگشتی دوجهته[11] برای ایجاد یک راه‌حل امنیتی با دوام بالا برای امنیت شبکه اینترنت اشیاء و اجرای بهتر هر دو الگوریتم شبکه عصبی بازگشتی[12] و شبکه عصبی بازگشتی دروازه‌ای[13] پیشنهاد شد. همچنین از الگوریتم جنگل تصادفی در مجموعه داده KDDCup99 برای انتخاب ویژگی‌های مهم مرتبط با مدل استفاده شد. در نهایت الگوریتم شبکه عصبی بازگشتی دوجهته با دقت ۹۹/۰۴٪، نسبت به الگوریتم‌های شبکه عصبی بازگشتی و شبکه عصبی بازگشتی دروازه‌ای عملکرد بهتری را از خود نشان داد.

---

[1] Cybersecurity
[2] Residual Network (ResNet)
[3] Convolutional Neural Network (CNN)
[4] light-weight
[5] Random Neural Network
[6] Long-Short-Term-Memory (LSTM) Neural Network
[7] Fog Computing
[8] Big Data
[9] Smart City
[10] Jumping Gene
[11] Bi-directional Recurrent Neural Network (BRNN)
[12] Recurrent Neural Network (RNN)
[13] Gated Recurrent Neural Network (GRNN)

در [۲۲]، از یک مدل تشخیص حمله منع سرویس توزیع‌شده بر اساس محیط شبکه مبتنی بر نرم‌افزار با استفاده از الگوریتم ماشین بردار پشتیبان برای جمع‌آوری داده‌های جدول جریان، روی سوئیچ ترافیک شبکه پیشنهاد شد و نشان داده شد که میانگین میزان دقت با مقدار جریان ترافیک عادی ۹۶/۲۳٪ است. در نهایت یافته‌های پیش‌بینی شده، نرخ تشخیص حمله بهتر و نرخ هشدار نادرست پایین‌تری را در شبکه مبتنی بر نرم‌افزار ارائه داد.
در جدول ۱ نتایج کارهای مرتبط به همراه روش کار و مجموعه داده مورد استفاده و همچنین دقت تشخیص حملات مورد مقایسه قرار گرفته‌اند.

جدول ۱: مقایسه نتایج تحقیقات قبلی در زمینه تشخیص حمله DDOS
Table 1. Comparing the Results of Previous Researches in the field of DDOS Attack Detection

مرجع	سال	روش کار	مجموعه داده	دقت تشخیص
[۱۱]	۲۰۲۱	شبکه عصبی پس‌انتشار عمیق کالمن	CICDDoS2019	٪۹۴
[۱۲]	۲۰۲۱	الگوریتم بیز ساده	NSLKDD	٪۶۴/۰۲
[۱۳]	۲۰۲۱	الگوریتم جنگل تصادفی	Bot-IoT	٪۹۹
[۱۴]	۲۰۲۱	الگوریتم رگرسیون منطقی	CICDDoS2019	٪۹۹/۷
[۱۵]	۲۰۲۱	الگوریتم جنگل تصادفی	CICDDoS2019	٪۹۹/۹۲۶۶۷
[۱۶]	۲۰۲۰	الگوریتم درخت تصمیم	Sensor data	۹۷/٪۳۹
[۱۷]	۲۰۲۰	شبکه‌های عصبی پیچشی(ResNet)	CICDDOS2019	BC[1]=٪۹۹/۹۹ MC[2]=٪۸۷/۰۶
[۱۸]	۲۰۲۰	شبکه عصبی تصادفی با یادگیری عمیق	PCAP	٪۸۰/۷
[۱۹]	۲۰۲۰	الگوریتم جنگل تصادفی	KDD-CUP	٪۹۹/۶۵
[۲۰]	۲۰۲۰	شبکه عصبی پیچشی با حافظه کوتاه مدت طولانی	CICIDS2017	٪۹۹/۰۳
[۲۱]	۲۰۲۰	الگوریتم جنگل تصادفی	KDDCup99	٪۹۹/۰۴
[۲۲]	۲۰۱۹	الگوریتم ماشین بردار پشتیبان	یک مجموعه داده به‌دست آمده از ترافیک ورودی دستگاههای IOT	٪۹۶/۲۳

۳-مفاهیم اولیه

۱) اینترنت اشیاء[3]: اصطلاح اینترنت اشیاء که اولین بار توسط کِوین آشتون[4] در سال ۱۹۹۹ پیشنهاد شد، به ارتباط بین دستگاه‌های فیزیکی مختلف و اشیاء از طریق اینترنت، در سراسر دنیا اشاره دارد [۲۳]. اینترنت اشیاء، به افراد و اشیاء اجازه می‌دهد تا در هر زمان، هر مکان، با هر چیزی و هر کسی، در حالت ایده‌آل و با استفاده از هر مسیر یا هر شبکه‌ای و هر سرویسی به هم متصل شوند [۲۴]. هدف اصلی فناوری اینترنت اشیاء این است که زندگی انسان را با ادغام دستگاه‌های فیزیکی و هوش دیجیتالی، هوشمندتر و قابل مدیریت‌تر کند [۲۵].
۲) سیستم تشخیص نفوذ[5]: یک سیستم تشخیص نفوذ، که به آن سیستم پیش‌گیری از نفوذ[6] نیز گفته می‌شود، نوعی ابزار امنیتی شبکه در قالب نرم‌افزار یا سخت‌افزار است که روی فعالیت‌های مخرب ایجاد شده در شبکه‌ها یا سیستم‌هایی نظیر اینترنت اشیاء نظارت می‌کند. هدف آن شناسایی انواع مختلف ترافیک مخرب در شبکه و رایانه است که توسط یک فایروال سنتی، قابل

[1] Binary Classification
[2] Multi-Class Classification
[3] Internet of Things
[4] Kevin Ashton
[5] Intrusion Detection System (IDS)
[6] Intrusion Prevention System (IPS)

شناسایی نیستند [۲۶]. این سیستم‌ها، یک راه‌حل کارآمد و مؤثر در برابر حملات سایبری چندشکلی و صفر- روزه[1] در شبکه‌های اینترنت اشیاء هستند [۷].

۳) حمله منع سرویس توزیع‌شده[2]: یک نوع حمله عمدی است که معمولاً در یک محیط محاسباتی توزیع‌شده انجام می‌شود که در آن مهاجم با استفاده از چندین سیستم در یک شبکه، با ارسال درخواست‌های متعدد به سیستم یا سرور مورد نظر، به آن حمله می‌کند [۲۷]. این حمله باعث می‌شود که یک سرویس آنلاین که کاربران قانونی به آن دسترسی دارند با غلبه بر ترافیک از منابع متعدد، غیرقابل دسترس شود. این منابع عموماً رایانه‌های آلوده شده‌ای هستند که به عنوان ربات در بات‌نت‌ها استفاده می‌شوند [۶].

۴) یادگیری ماشین[3]: یکی از تکنیک‌های پیشرفته هوش مصنوعی است که ماشین‌ها را با استفاده از الگوریتم‌های مختلف آموزش می‌دهد و به آن‌ها کمک می‌کند تا به جای استفاده از برنامه‌نویسی، از تجربیات خود آموزش ببینند. همچنین در ساخت سیستم‌های تشخیص نفوذ برای شناسایی حملات، بسیار کارآمد است که در این زمینه، می‌توان حملات را در همان مراحل اولیه شناسایی و پیش‌بینی کرد [۷, ۳].

۳-۱-الگوریتم‌های یادگیری ماشین مورد استفاده

۱) بیز ساده[4]: طبقه‌بندی‌کننده بیز ساده را می‌توان به عنوان یک روش طبقه‌بندی مبتنی بر نظریه احتمال و قضیه بیزین با فرض مستقل بودن هر ویژگی یا پارامتر تصمیم‌گیری تعریف کرد، به طوری که وجود هر ویژگی، ربطی به وجود سایر ویژگی‌ها ندارد [۲۸].

۲) استنتاج قوانین[5]: این الگوریتم یک درخت تصمیم‌گیری و یا مجموعه‌ای از قوانین تصمیم‌گیری از مجموعه آموزشی که برای طبقه‌بندی آن‌ها تنظیم شده است را تولید می‌کند [۲۹].

۳) ماشین بردار پشتیبان[6]: یک مدل یادگیری ماشین نظارت‌شده است که از آن برای طبقه‌بندی و رگرسیون و تشخیص نقاط پرت استفاده می‌شود. این مدل، داده‌ها را بر اساس داده‌های آموزشی برچسب‌گذاری شده در کلاس‌های مختلف طبقه‌بندی می‌کند [۶].

۴) درخت تصمیم[7]: این طبقه‌بندی‌کننده دارای یک ساختار درختی است که از گره‌ها و برگ‌های تصمیم تشکیل شده است که در آن داده‌ها به گره‌های کوچک‌تر تقسیم می‌شوند. در این مدل هر گره برگ می‌تواند به عنوان یک قانون اگر/آنگاه[8] ارائه شود [۳۰ ,۵].

۵) جنگل تصادفی[9]: این یک الگوریتم گروهی است و از چندین درخت تصمیم‌گیری مستقل تشکیل شده است که به طور مستقل بر روی یک زیرمجموعه تصادفی از داده‌ها، از یک مجموعه داده برچسب‌دار آموزش داده می‌شوند. مشکل بیش‌برازش الگوریتم درخت تصمیم نیز، توسط این الگوریتم حل می‌شود [۶, ۳۰].

۶) شبکه عصبی[10]: این الگوریتم یک مدل محاسباتی انتزاعی از مغز انسان است و مانند مغز، از گره‌های پردازشی مشابه یاخته‌های عصبی و اتصالات مصنوعی تشکیل شده است. گره ورودی از طریق یک گره پنهان به گره خروجی متصل می‌شود تا یک ساختار شبکه چندلایه تشکیل شود. بزرگ‌ترین مزیت شبکه عصبی این است که می‌تواند به طور دقیق مسائل پیچیده را پیش‌بینی کند [۲۹ ,۳۱].

---

[1] Zero-Day
[2] Distributed Denial of Service (DDOS)
[3] Machine Learning
[4] Naïve Bayes (NB)
[5] Rule Induction (RI)
[6] Support Vector Machines (SVM)
[7] Decision Tree (DT)
[8] If/Then
[9] Random Forest (RF)
[10] Neural Network (NN)

۷) رگرسیون خطی[1]: یکی از رایج‌ترین و جامع‌ترین الگوریتم‌های آماری و یادگیری ماشین است که برای یافتن رابطه خطی بین یک یا چند پیش‌بینی‌کننده استفاده می‌شود. به بیانی دیگر این الگوریتم، برای پیش‌بینی یک یا چند متغیر از روی یک یا چند متغیر دیگر است که امکان پیش‌بینی متغیرهای پیوسته/واقعی یا ریاضی را فراهم می‌کند [۳۲].

۸) رگرسیون منطقی[2]: یک الگوریتم طبقه‌بندی و گونه‌ای از رگرسیون خطی است که خروجی‌های دودویی را پیش‌بینی می‌کند. همچنین یک منحنی منطقی تولید می‌کند که به مقادیر بین ۰ و ۱ محدود می‌شود. برای طبقه‌بندی چندکلاسه و همچنین چندجمله‌ای نیز گسترش یافته است [۳۰].

۹) یادگیری عمیق[3]: یادگیری عمیق، به عنوان یکی از مهم‌ترین تکنیک‌های یادگیری ماشین در کاربردهایی از قبیل تحلیل تصویر، بازشناسی گفتار و درک متن به موفقیت‌های چشم‌گیری دست یافته است. در چند سال اخیر، یادگیری عمیق نقش مهمی در راه‌حل‌های تحلیلی داده‌های بزرگ ایفا کرده است [۳۳].

۱۰) مدل خطی تعمیم‌یافته[4]: تعمیمی انعطاف‌پذیر از رگرسیون خطی معمولی است. به عبارتی تعمیم رگرسیون خطی، برای داده‌های فاقد توزیع نرمال است؛ بنابراین مجموعه‌ای از روش‌ها موسوم به مدل‌های خطی تعمیم‌یافته، به تغییر شکل مدل‌هایی که آن‌ها را در پارامترها خطی می‌سازند، تکیه دارد [۳۴].

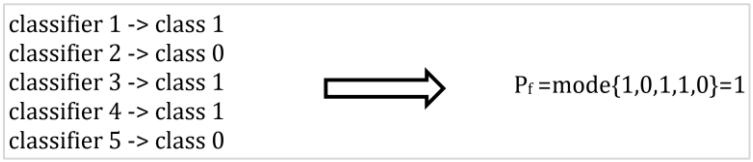
۳-۲-چارچوب رویکرد رأی‌گیری اکثریت

رویکرد رأی‌گیری اکثریت که با نام رأی‌گیری سخت نیز شناخته می‌شود، یک مدل طبقه‌بندی گروهی است که چندین مدل طبقه‌بندی‌کننده پایه را در یک مدل واحد ترکیب کرده، به طوری‌که عملکرد آن به تنهایی و در حالت ایده‌آل قویتر از هر یک از مدل‌های پایه باشد. در رأی‌گیری اکثریت، آراء هر کلاس بر روی طبقه‌بندی‌کننده‌های ورودی شمارش می‌شود و کلاسی که اکثریت آراء را کسب کند به عنوان خروجی مدل گروهی انتخاب می‌شود [۳۵]. در این پژوهش از مجموعه داده بهبودیافته CICDDOS2019، برای شناسایی حملات استفاده شد. برای بهبود عملکرد رویکرد رأی‌گیری اکثریت، ابتدا ده الگوریتم طبقه-بندی[5] به صورت تصادفی انتخاب شده و روی مجموعه داده متعادل‌شده CICDDOS2019 اعمال می‌شود. سپس مدل گروهی پیشنهادی با استفاده از انتخاب و ترکیب پنج الگوریتم طبقه‌بندی پایه از میان ده الگوریتم اعمال‌شده روی مجموعه داده، ایجاد می‌شود که به صورت موازی کار می‌کنند و هر کدام از آنها، مدل متفاوتی را مطابق با مجموعه داده آموزشی تولید می‌کنند؛ با این شرط که پنج الگوریتم منتخب، خطای طبقه‌بندی کمتر و دقت بالاتر و همچنین زمان پردازش کمتری نسبت به پنج الگوریتم دیگر داشته باشند.

با توجه به (۱)، برچسب کلاس P_f، از طریق اکثریت آراء مدل‌های طبقه‌بندی‌کننده C_j، پیش‌بینی می‌شود [۳۵]:

$$P_f = mode\{C1(\mathbf{x}), C2(\mathbf{x}), ..., Cm(\mathbf{x})\} \quad (۱)$$

در این پژوهش با ترکیب پنج طبقه‌بندی‌کننده، یک نمونه آموزشی فرضی با استفاده از رأی‌گیری اکثریت به صورت شکل ۲ طبقه‌بندی می‌شود:



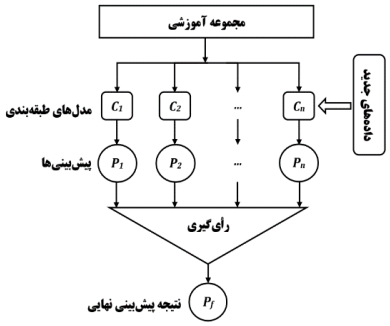
شکل ۲: طبقه‌بندی یک نمونه آموزشی فرضی با استفاده از رویکرد رأی‌گیری اکثریت

Figure 2. Classification of a Hypothetical Training Sample Using Majority Voting Approach

در نتیجه از طریق اکثریت آراء، نمونه با کلاس ۱ طبقه‌بندی خواهد شد. در شکل ۳ مفهوم رأی‌گیری اکثریت، به درستی به تصویر کشیده‌شده است. همان‌طور که در این شکل نشان داده شده است، یک مجموعه آموزشی و مجموعه‌ای از الگوریتم‌های

[1] Linear Regression (LR)
[2] Logistic Regression (LGR)
[3] Deep Learning (DL)
[4] Generalized Linear Model (GLM)
[5] Classifier Algorithm

طبقه‌بندی به عنوان C_1، C_2،...،C_n، وجود دارد که در آن هر یک از آنها روی مجموعه آموزشی، آموزش دیده است. پس از آموزش مدل، هر طبقه‌بندی‌کننده یک پیش‌بینی را تولید می‌کند؛ به این صورت که طبقه‌بندی‌کننده C_1 پیش‌بینی P_1، طبقه‌بندی‌کننده C_2، پیش‌بینی P_2 و... طبقه‌بندی‌کننده C_n، پیش‌بینی P_n را تولید می‌کنند. در نتیجه در رأی‌گیری اکثریت، با جمع‌آوری همه پیش‌بینی‌های هر کلاس، کلاسی که بیشترین رأی را به‌دست آورده به عنوان نتیجه نهایی برگردانده می‌شود.

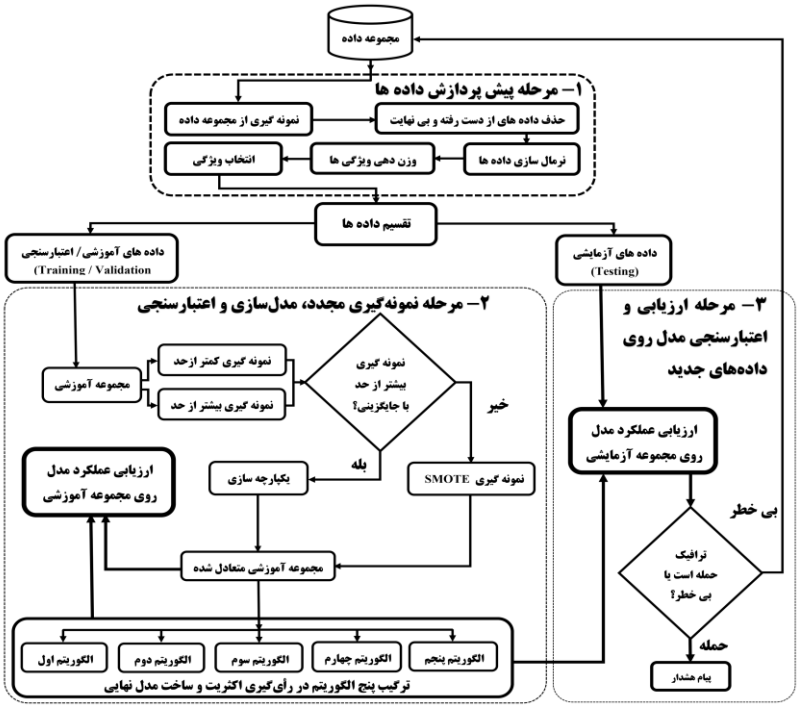


شکل ۳: نحوه پیش‌بینی نهایی در رویکرد گروهی رأی‌گیری اکثریت

Figure 3. The Way of Final Prediction in the Majority Voting Ensemble Approach

۴-روش پیشنهادی

در این پژوهش، یک چارچوب تشخیص حمله برای شناسایی حملات منع سرویس توزیع‌شده در اینترنت اشیاء پیشنهاد شد که بر اساس یادگیری گروهی است و با ترکیب مدل‌های پایه که به صورت موازی آموزش دیده‌اند، از رویکرد رأی‌گیری اکثریت استفاده کرده و به عنوان یک برنامه تشخیص حمله، پیاده‌سازی گردید. در ابتدا مراحل پیش‌پردازش داده‌ها برای بهبود کیفیت داده‌ها روی مجموعه داده انجام می‌شود. سپس برای توسعه مدل و تخمین عملکرد آن، داده‌ها به دو بخش آموزشی و آزمایشی تقسیم می‌شوند و در ادامه و در مرحله نمونه‌گیری، مدل‌سازی و اعتبارسنجی، دوباره از داده‌ها نمونه‌گیری شده و رویکرد پیشنهادی روی مجموعه داده آموزشی اعمال می‌شود. سپس در مرحله ارزیابی و اعتبارسنجی مدل روی داده‌های جدید، دقت پیش‌بینی واقعی مدل در شناسایی حملات به‌دست می‌آید. معماری رویکرد پیشنهادی در شکل ۴ آورده شده است.



شکل ۴: معماری روش پیشنهادی برای تشخیص حملات DDOS

Figure 4: The Architecture of the Proposed Method for DDOS Attacks Detection

۴-۱-پیش‌پردازش داده‌ها[1]

پیش‌پردازش داده‌ها، به عنوان اولین و مهم‌ترین گام در ایجاد یک مدل یادگیری ماشین، فرآیندی است که به دنبال بهبود کیفی و کمی داده‌های اولیه است و برای تمیزکردن داده‌ها و مناسب ساختن آن‌ها برای یک مدل یادگیری ماشین که باعث افزایش دقت و کارایی آن می‌شود، مورد استفاده قرار می‌گیرد [۳۶, ۳۷]. در ادامه به شرح مراحل پیش‌پردازش داده‌ها که در این پژوهش مورد استفاده قرار گرفته‌اند، پرداخته‌شده است.

۴-۱-۱-نمونه‌گیری از مجموعه داده[2]

در تجزیه و تحلیل داده‌ها، نمونه‌گیری داده‌ها تکنیکی است که برای تجزیه و تحلیل زیرمجموعه‌ای از داده‌ها به منظور کشف اطلاعات معنی‌دار در مجموعه داده‌های بزرگ مورد استفاده قرار می‌گیرد. همچنین برای این‌که بتوان مجموعه داده‌های نامتعادل را مدیریت کرد باید از روش‌های نمونه‌گیری استفاده شود [۳۸].

۴-۱-۲-حذف مقادیر از دست‌رفته و بی نهایت[3]

در علم داده، زمانی که یک مجموعه داده دارای یک یا چند نمونه با مقادیر ثبت نشده یا تهی در یک یا چند ویژگی از مجموعه داده است، گفته می‌شود که این مجموعه داده دارای داده‌هایی با مقادیر از دست‌رفته است. به طورکلی، از دست‌رفتن داده‌ها به صورت تصادفی مربوط به برخی از داده‌هایی است که قبلاً مشاهده شده است؛ بنابراین در این مورد، حذف داده‌های دارای مقادیر از دست‌رفته بسته به وقوع آنها، مشکلی ایجاد نمی‌کند [۳۹].

۴-۱-۳-نرمال‌سازی داده‌ها[4]

هنگام مدیریت مجموعه داده‌ها، غالباً تفاوت‌های زیادی بین بزرگترین و کوچکترین مقادیر ویژگی‌ها وجود دارد. نرمال‌سازی سازمان‌دهی داده‌هایی است که در تمامی نمونه‌ها و ویژگی‌ها، مشابه به نظر می‌رسند. [۳۸, ۳۹]. تکنیک‌های نرمال‌سازی متنوعی وجود دارد که در این پژوهش از تکنیک امتیاز z[5] استفاده‌شده است. این تکنیک، میانگین داده‌ها را از تمام مقادیر کم کرده و حاصل آنها را بر انحراف استاندارد تقسیم می‌کند. مقدار جدید و استاندارد شده ویژگی در این روش با استفاده از (۲) به‌دست می‌آید [۳۹]:

$$Z = \frac{x - Mean(x)}{Stdev(x)} \quad (۲)$$

۴-۱-۴-انتخاب ویژگی[6] و کاهش ابعاد داده

انتخاب ویژگی فرآیند انتخاب ویژگی‌های مجموعه داده است که بیشترین ارتباط را با مسئله مدل‌سازی پیش‌بینی‌کننده دارد که روی آن کار می‌شود. این تکنیک‌ها با انتخاب ویژگی‌هایی که منجر به دقت بهتر و پیچیدگی کمتر مدل می‌شوند به ایجاد یک مدل پیش‌بینی دقیق کمک می‌کنند [۳۸]. در این پژوهش از تکنیک وزن‌دهی ضریب بهره استفاده می‌شود که در آن می‌توان ویژگی‌های بهینه با وزن‌های بالا را در فرایند یادگیری انتخاب کرد. این تکنیک با استفاده از آنتروپی و بهره اطلاعات، ویژگی‌های مجموعه داده را وزن‌دهی می‌کند که در ذیل به تشریح آنها پرداخته‌شده است.

۱- آنتروپی[7]: ناخالصی اطلاعات یا عدم قطعیت در شناسایی کلاس، با استفاده از آنتروپی اندازه‌گیری می‌شود. اطلاعات مورد نیاز برای طبقه‌بندی نمونه‌ها در مجموعه داده آموزشی توسط (۳) به‌دست می‌آید که به عنوان آنتروپی داده‌ها در مجموعه داده آموزشی نیز شناخته می‌شود [۴۰, ۳۰]:

---

[1] Data Preprocessing
[2] Sampling of the Dataset
[3] Remove Missing and Infinite Values
[4] Data Normalization
[5] Z-Score
[6] Feature Selection
[7] Entropy

$$Entropy(D) = -\sum_{i=1}^{c} p_i \log_2(p_i) \quad (۳)$$

آنتروپی ویژگی A از مجموعه داده آموزشی، اطلاعات مورد نیاز برای طبقه‌بندی یک نمونه از مجموعه داده آموزشی بر اساس بخش‌بندی توسط ویژگی A است. این مقدار از (۴) به‌دست می‌آید [۴۰]:

$$Entropy_A(D) = -\sum_{j=1}^{v} \frac{|D_j|}{|D|} \times Entropy(D_j) \quad (۴)$$

۲- بهره اطلاعات[1]: بهره اطلاعات با مقایسه آنتروپی مجموعه داده‌ها قبل و بعد از تبدیل محاسبه می‌شود که از (۵) به‌دست می‌آید [۶]. بهره اطلاعات، کاهش مورد انتظار در آنتروپی ناشی از تقسیم‌بندی نمونه‌ها بر اساس یک ویژگی مشخص مانند A است.

$$InformationGain(A) = Entropy(D) - Entropy_A(D) \quad (۵)$$

۳- ضریب بهره[2]: نقطه ضعف بزرگ بهره اطلاعات این است که به سمت ویژگی‌های با مقادیر بزرگ‌تر متمایل می‌شود. اما ضریب بهره، بهره اطلاعات تغییر یافته است که نتیجه بهره اطلاعات را نرمال‌سازی می‌کند و از (۶) به‌دست می‌آید [۶].

$$GainRatio_A(D) = \frac{InformationGain(A)}{Entropy_A(D)} \quad (۶)$$

۴-۲-تقسیم داده‌ها[3]

برای توسعه مدل‌های یادگیری ماشین و تخمین عملکرد آنها، داده‌ها به دو یا سه بخش تقسیم می‌شوند. یکی از روش‌های جلوگیری از بیش‌برازش مدل‌های یادگیری ماشین روی مجموعه داده‌های بزرگ، نگه داشتن داده‌ها[4] است که در آن مجموعه داده‌ها به دو بخش آموزشی و اعتبارسنجی/ آزمایشی تقسیم می‌شوند. مجموعه آزمایشی شامل داده‌های دیده‌نشده‌ای است که برای آموزش مدل استفاده نشده‌اند [۴۱]. نحوه تقسیم مجموعه داده‌ها مشخص می‌کند که تا چقدر می‌توان به معیار ارزیابی مجموعه آزمایشی اعتماد کرد. در اینجا مشکلاتی که ممکن است در تحلیل داده‌ها به‌وجود آید و باید از آن جلوگیری کرد عبارتند از:

الف) بیش‌برازش یا آموزش بیشتر از حد[5]: به مدلی اطلاق می‌شود که داده‌های آموزشی را به خوبی مدل می‌کند و زمانی اتفاق می‌افتد که یک مدل داده‌های غیرضروری درون داده‌های آموزشی را تا حدی بیاموزد که تبدیل به یک مدل پیچیده شود [۴۲].

ب) کم‌برازش یا آموزش کمتر از حد[6]: به مدلی اطلاق می‌شود که نه می‌تواند داده‌های آموزشی را مدل کند و نه قابل تعمیم به داده‌های جدید است. زیرا به علت ساده شدن بیش از حد مدل نمی‌تواند نتایج خوبی به‌دست آورد [۴۲].

در این پژوهش از دو معیار ذیل در تعیین نسبت تقسیم داده‌ها برای هر مجموعه داده، در نظر گرفته شد:

۱) ضریب همبستگی[7]

ضریب همبستگی معمولاً همبستگی بین دو یا چند متغیر را ارزیابی می‌کند که مقدار آن در محدوده ۰ تا ۱ است. ضریب همبستگی لحظه‌ای پیرسون معیاری برای اندازه‌گیری قدرت ارتباط خطی بین متغیرها است [۴۳]. در این پژوهش ضریب همبستگی نشان‌دهنده همبستگی بین ویژگی‌های پیش‌بینی و متغیر هدف یا همان برچسب کلاس است. ضریب همبستگی پیرسون بین دو متغیر x و y از (۷) به‌دست می‌آید:

$$r_{xy} = \frac{n\sum x_i y_i - \sum x_i \sum y_i}{\sqrt{n\sum x_i^2 - (\sum x_i)^2}\sqrt{n\sum y_i^2 - (\sum y_i)^2}} \quad (۷)$$

[1] Information Gain
[2] Gain Ratio
[3] Split Data
[4] Hold out Data
[5] Overfitting
[6] Underfitting
[7] Correlation

۲) ریشه میانگین مربعات خطا[1]

ریشه میانگین مربعات خطا، مجموع مجذور خطا یا تفاوت بین مقادیر پیش‌بینی شده و مقادیر واقعی در مجموعه آزمایشی است و نشان می‌دهد که مدل واقعاً در هنگام پیش‌بینی متغیر هدف تا چه اندازه می‌تواند خوب عمل کند [۴۴]. با استفاده از ریشه میانگین مربعات خطا، می‌توان کارایی مدل را به راحتی اندازه‌گیری کرد. هر چقدر که این مقدار نزدیک به صفر باشد، یعنی هیچ تفاوتی در مقادیر پیش‌بینی شده و مشاهده شده وجود ندارد. مقدار ریشه میانگین مربعات خطای بین مقادیر پیش‌بینی شده و مقادیر واقعی توسط مدل، از (۸) به‌دست می‌آید [۴۵]:

$$RMSE = \sqrt{\frac{\sum_{i=1}^{N}(predicted_i - Actual_i)^2}{N}} \quad (۸)$$

نسبتی که معمولاً برای تقسیم داده‌ها استفاده می‌شود ۸۰:۲۰ است، به این معنی که ۸۰ درصد داده‌ها برای آموزش و اعتبارسنجی و ۲۰ درصد برای آزمایش مدل مورد استفاده قرار می‌گیرد. نسبت‌های دیگری مانند ۷۰:۳۰، ۶۰:۴۰ و حتی ۵۰:۵۰ و ۳۳: ۶۷ و ۹۰:۱۰ نیز در عمل استفاده می‌شوند. اما راهنمایی روشنی در مورد این که چه نسبتی از تقسیم داده‌ها، برای یک مجموعه داده معین بهینه است، وجود ندارد [۴۶, ۴۷].

۴-۳-نمونه‌گیری مجدد، مدل‌سازی و اعتبارسنجی

۴-۳-۱-طبقه‌بندی نامتعادل[2]

طبقه‌بندی نامتعادل شامل مجموعه داده‌ای است که در آن توزیع کلاس‌ها با یکدیگر برابر نیست. در مجموعه داده نامتعادل، وجود یک انحراف شدید در توزیع کلاس، که در آن نسبت تعداد نمونه‌ها در کلاس اقلیت به تعداد نمونه‌ها در کلاس اکثریت ۱:۱۰، ۱:۱۰۰ یا حتی ۱:۱۰۰۰ است، دور از انتظار نیست [۴۲]. در بسیاری از حوزه‌ها، هزینه طبقه‌بندی نادرست کلاس‌های اقلیت بیشتر از کلاس اکثریت در مجموعه داده‌های با توزیع کلاس نامتعادل است [۳۸]؛ بنابراین برای رفع این مشکل، در این پژوهش از تکنیک‌های ذیل برای نمونه‌گیری از داده‌ها برای متعادل کردن مجموعه داده نامتعادل استفاده‌شده است:

۱) نمونه‌گیری تصادفی کمتر از حد[3]: این تکنیک، شامل انتخاب تصادفی نمونه‌ها از کلاس اکثریت برای حذف از مجموعه داده اصلی و مجموعه داده آموزشی تا زمانی که تعداد مساوی از نمونه‌ها برای هر کلاس حاصل شود [۴۲].

۲) نمونه‌گیری تصادفی بیشتر از حد با جایگزینی[4]: این تکنیک، شامل تکرار تصادفی نمونه‌هایی از کلاس اقلیت و جایگزین کردن آنها در مجموعه داده آموزشی است [۴۲].

۳) نمونه‌گیری بیشتر از حد با استفاده از الگوریتم SMOTE[5]: الگوریتم SMOTE به عنوان مؤثرترین و موفق‌ترین روش نمونه‌گیری بیشتر از حد برای رفع مشکل نامتعادل بودن کلاس با تولید نمونه‌های مصنوعی در نظر گرفته می‌شود. ایده اصلی SMOTE این است که کلاس اقلیت را با تولید تصادفی نمونه‌های مصنوعی بین نمونه‌هایی از کلاس اقلیت و برخی از نزدیک‌ترین همسایگان خود که به شیوه‌ای تصادفی انتخاب شده‌اند، نمونه‌گیری می‌کند [۴۲, ۴۸, ۴۹].

۴) ترکیب روش‌های نمونه‌گیری: از آنجاکه استفاده از هر نوع نمونه‌گیری مجدد به تنهایی می‌تواند مؤثر باشد، اما ترکیب دو روش نمونه‌گیری، می‌تواند منجر به بهبود عملکرد کلی مدل در مقایسه با هر یک از روش‌ها به صورت جداگانه شود. به این معنی که می‌توان مقداری از کلاس اکثریت را حذف کرده و تعداد کمی به کلاس اقلیت اضافه کرد [۴۲]. جدول ۲ تعداد نمونه‌های پنج حمله از مجموعه داده CICDDOS2019 را بعد از مرحله اول نمونه‌گیری کمتر از حد تصادفی نشان می‌دهد:

[1] Root Mean Square Error (RMSE)
[2] Imbalanced Classification
[3] Random Under-sampling
[4] Random Oversampling
[5] Synthetic Minority Oversampling Technique

جدول ۲: تعداد نمونه‌های پنج حمله از مجموعه داده CICDDOS2019 بعد از نمونه‌گیری کمتر از حد
Table 2. Number of Samples of Five Attacks from CICDDOS2019 Dataset After Undersampling

مجموعه داده حمله	تعداد نمونه‌ها بعد از نمونه‌گیری کمتر از حد مرحله‌ی اول	ترافیک بی‌خطر	ترافیک حمله DDOS
DrDOS_DNS	۳۰,۱۶۷	۳,۴۰۲	۲۶,۷۶۵
DrDOS_NetBIOS	۳۰,۳۰۷	۱,۷۰۷	۲۸,۶۰۰
DrDOS_LDAP	۳۰,۹۸۸	۱,۶۱۲	۲۹,۳۷۶
DrDOS_UDP	۳۱,۸۰۷	۲,۱۵۷	۲۹,۶۵۰
DrDOS_SNMP	۳۰,۶۷۵	۱,۵۰۷	۲۹,۱۵۰

پس از ایجاد مجموعه داده آموزشی متعادل‌شده، با اجرای رویکرد رأی‌گیری اکثریت با ترکیب پنج الگوریتم انتخابی روی آن، مدل ایجاد خواهد شد. سپس برای بررسی دقت و کیفیت مدل و اعتبارسنجی داده‌های آموزشی با استفاده از تکنیک اعتبارسنجی درون نمونه[1]، مدل روی مجموعه داده آموزشی که برای ساخت مدل استفاده می‌شود، مورد آزمایش قرار می‌گیرد.

۴-۴-ارزیابی و اعتبارسنجی مدل روی داده‌های جدید

اعتبارسنجی خارج از نمونه[2] یک مدل [۵۰]، فرآیندی است که پس از آموزش مدل انجام می‌شود که در آن مدل آموزش دیده با مجموعه داده‌های آزمایشی ارزیابی می‌شود. به عبارت دیگر در این تکنیک، آزمایش داده‌ها از مجموعه داده جدیدی که برای ساخت مدل استفاده نمی‌شود، صورت می‌گیرد. هدف نهایی مدل، نیز همین است که نمونه‌ها را به‌گونه‌ای یاد بگیرد که مدل بتواند یادگیری را به نمونه‌های جدیدی تعمیم دهد که هنوز ندیده است؛ بنابراین در این مرحله، مدل به یک ارزیابی واقعی روی داده‌های جدید دست پیدا خواهد کرد. در مقایسه‌ای که بین عملکرد مجموعه آموزشی و آزمایشی هر یک از الگوریتم‌های طبقه‌بندی انجام شد می‌توان دریافت، هنگامی که دقت مجموعه آموزشی بسیار بالاتر از دقت مجموعه آزمایشی باشد مشکل بیش‌برازش رخ می‌دهد و برعکس هنگامی که دقت داده‌های مجموعه آموزشی بسیار کمتر از دقت مجموعه آزمایشی باشد مشکل کم‌برازش رخ خواهد داد. در این پژوهش از الگوریتم‌هایی برای شرکت در رأی‌گیری استفاده شد، که با مشکل بیش‌برازش و کم‌برازش روبرو نشده‌اند.

۵-نتایج

این بخش بر آزمایش و ارزیابی الگوریتم‌های یادگیری ماشین و همچنین مدل پیشنهادی روی مجموعه داده CICDDOS2019 تمرکز دارد. همچنین از ابزار RapidMiner [۵۱, ۵۲, ۵۳, ۵۴, ۵۵]، برای تجزیه و تحلیل داده‌ها استفاده‌شده است.

۵-۱-مجموعه داده CICDDOS2019

در این پژوهش برای تشخیص حملات منع سرویس توزیع‌شده از مجموعه داده بهبودیافته CICDDOS2019 که از مؤسسه امنیت سایبری کانادا در دانشگاه نیوبرانزویک دریافت‌شده، استفاده‌شده است. این مؤسسه، یک مجموعه داده حمله منع سرویس توزیع‌شده کامل را برای اهداف تحقیقاتی ارائه داده است. این مجموعه داده شامل ۱۲ نوع حمله منع سرویس توزیع‌شده است که ترافیک‌های مربوط به هر کدام از حملات، در یک فایل با پسوند CSV جداگانه ذخیره شده و دارای ۸۷ ویژگی است که به جریان ترافیک شبکه مربوط می‌شود و شامل ۵۵,۶۰۴,۰۴۴ نمونه است که از این تعداد، ۷۴,۴۶۱ نمونه ترافیک بی‌خطر و ۵۵,۵۲۹,۵۸۳ نمونه ترافیک حمله است. این مجموعه داده در وب‌سایت مؤسسه کانادایی امنیت سایبری[3] برای عموم در دسترس قرار گرفته است[۱۰]. نویسندگان در مقالات [۱۱] ، [۱۴] ، [۱۵] ، [۱۷] نیز از این مجموعه داده برای تشخیص حملات بهره برده‌اند. جدول ۳ تعداد ترافیک‌های حمله و بی‌خطر را بر اساس نوع حمله در این مجموعه داده نشان می‌دهد.

[1] In of Sample Validation
[2] Out of Sample Validation
[3] https://www.unb.ca/cic/datasets/ddos-2019.html

جدول ۳: تعداد نمونه‌ها در مجموعه داده CICDDOS2019 [۱۰]
Table 3. Number of Samples in CICDDOS2019 Dataset [10]

ویژگی (برچسب کلاس)	تعداد نمونه‌ها	تعداد نمونه‌های حمله	تعداد نمونه‌های بی‌خطر
DNS	۵,۰۷۴,۴۱۳	۵,۰۷۱,۰۱۱	۳,۴۰۲
LDAP	۲,۱۸۱,۵۴۲	۲,۱۷۹,۹۳۰	۱,۶۱۲
MSSQL	۴,۵۲۴,۴۹۸	۴,۵۲۲,۴۹۲	۲,۰۰۶
NetBIOS	۴,۰۹۴,۹۸۶	۴,۰۹۳,۲۷۹	۱,۷۰۷
NTP	۱,۲۱۷,۰۰۷	۱,۲۰۲,۶۴۲	۱۴,۳۶۵
SNMP	۵,۱۶۱,۳۷۷	۵,۱۵۹,۸۷۰	۱,۵۰۷
SSDP	۲,۶۱۱,۳۷۴	۲,۶۱۰,۶۱۱	۷۶۳
SYN	۴,۳۲۰,۵۴۱	۴,۲۸۴,۷۵۱	۳۵,۷۹۰
TFTP	۲۰,۱۰۷,۸۲۸	۲۰,۱۰۵,۵۰۷	۲,۳۲۱
UDP	۳,۱۳۶,۸۰۲	۳,۱۳۴,۶۴۵	۲,۱۵۷
UDP-LAG	۳۷۰,۶۰۵	۳۶۶,۹۰۰	۳,۷۰۵
PORTMAP	۱۹۱,۶۹۴	۱۸۶,۹۶۰	۴,۷۳۴

۵-۲-محیط آزمایش

تمامی آزمایش‌ها بر روی یک رایانه با مشخصاتی که در جدول ۴ آورده‌شده است، انجام شد.

جدول ۴: پیکربندی سخت‌افزاری و نرم‌افزاری محیط آزمایش
Table 4. Hardware and Software Configuration of the Testing Environment

مشخصات سیستم	توضیح
نوع سیستم	سیستم عامل ویندوز ۱۱ نسخه تجاری و ۶۴ بیتی
نوع پردازنده	AMD FX-8370E Eight-Core Processor x64
سرعت پردازنده	۳/۳ گیگاهرتز
مقدار RAM و HDD و VGA	۱۲ گیگابایت RAM و ۳ ترابایت HDD و ۱ گیگابایت VGA
ابزار تجزیه و تحلیل	RapidMiner 9.10

۵-۳-معیارهای ارزیابی الگوریتم‌ها

بر اساس تشخیص‌های صورت‌گرفته، عملکرد الگوریتم‌های استفاده‌شده در روش پیشنهادی، بر اساس ماتریس درهم‌ریختگی محاسبه و ارزیابی می‌شود. در طبقه‌بندی داده‌ها، ماتریس درهم‌ریختگی جدولی است که عملکرد یک مدل طبقه‌بندی یادگیری ماشین را اندازه‌گیری می‌کند و شبیه یک ساختار جدول مانند است که نمایشی بصری از مقادیر واقعی در مقابل مقادیر پیش‌بینی شده را ارائه می‌دهد که به عنوان ماتریس خطا نیز شناخته می‌شود [۴۴].

جدول ۵: ماتریس درهم‌ریختگی
Table 5. Confusion matrix

		مقادیر واقعی		
		مثبت (P)	منفی (N)	P+N = تعداد کل
مقادیر پیش‌بینی	منفی کاذب (FN)	منفی واقعی (TN)	منفی (N)	
	مثبت واقعی (TP)	مثبت کاذب (FP)	مثبت (P)	

پارامترهای این ماتریس، به شرح ذیل است [۵۶]:

TN[1]: منفی واقعی مواردی که منفی بوده و در واقع به درستی پیش‌بینی شده‌اند.

[1] True Negative (TN)

TP[1]: مثبت واقعی مواردی که مثبت بوده و در واقع به درستی پیش‌بینی شده‌اند.
FN[2]: منفی کاذب مواردی که منفی بوده و در واقع اشتباه پیش‌بینی شده‌اند.
FP[3]: مثبت کاذب مواردی که مثبت بوده و در واقع اشتباه پیش‌بینی شده‌اند.
معیارهای ارزیابی مرتبط با پارامترهای ماتریس درهم‌ریختگی که برای محاسبه پیش‌بینی‌ها استفاده می‌شوند، عبارتند از:
۱) دقت[4]: میزان دقت پیش‌بینی را محاسبه می‌کند [۱۳, ۵۷].

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (۹)$$

۲) صحت[5]: مکمل معیار دقت است و میزان درستی طبقه‌بندی داده‌ها را سنجش می‌کند [۱۳, ۵۷].

$$Precision = \frac{TP}{TP + FP} \quad (۱۰)$$

۳) فراخوانی[6]: مکمل معیار صحت است و در هنگام برخورد با داده‌های نامتعادل شدید، بسیار کارآمد است. [۱۳, ۵۷].

$$Recall = \frac{TP}{TP + FN} \quad (۱۱)$$

۴) خطای طبقه‌بندی[7]: میزان خطای طبقه‌بندی الگوریتم‌های طبقه‌بندی را مشخص می‌کند.

$$CE = \frac{FP + FN}{TP + TN + FP + FN} \quad (۱۲)$$

۵) معیار-F[8]: برای مقایسه مدل‌هایی که دارای میزان صحت کم و فراخوانی بالا یا برعکس هستند و همچنین یک معیار مهم برای ارزیابی الگوریتم‌ها روی مجموعه داده‌های نامتعادل است [۱۳, ۵۶].

$$F - measure = \frac{2 \times Precision \times Recall}{Precision + Recall} \quad (۱۳)$$

۶) منحنی ROC-AUC: AUC به مساحت زیر منحنی[9] ROC یعنی مشخصه‌های عملیاتی گیرنده[10] معروف است. در این منحنی، AUC عملکرد یادگیرنده را در تمام آستانه‌های طبقه‌بندی‌کننده نشان می‌دهد و معیاری بسیار مفید در مجموعه داده‌های نامتعادل است [۴۶]. این منحنی از نرخ مثبت واقعی[11] در محور عمودی و نرخ مثبت کاذب[12] در محور افقی استفاده می‌کند و عمدتاً برای مسائل طبقه‌بندی دودویی برای ارزیابی عملکرد آنها استفاده می‌شود [۱۳]. در این منحنی، مقدار AUC از ۰ تا ۱ متغیر است، که هر چقد AUC به ۱ نزدیکتر باشد عملکرد مدل در تشخیص کلاس‌های مثبت و منفی بهتر خواهد بود [۴۲, ۴۹, ۵۸].

$$TPR = \frac{TP}{TP + FN} \quad (۱۴)$$

$$FPR = \frac{FP}{FP + TN} \quad (۱۵)$$

$$AUC = \int_0^1 \frac{TP}{TP + FN} d \frac{FP}{FP + TN} \quad (۱۶)$$

[1] True Positive (TP)
[2] False Negative (FN)
[3] False Positive (FP)
[4] Accuracy
[5] Precision
[6] Recall
[7] Classification Error
[8] F-measure
[9] Area Under the Curve (AUC)
[10] Receiver Operating Characteristics (ROC)
[11] True Positive Rate (TPR)
[12] False Positive Rate (FPR)

۵-۴-معرفی ویژگی‌های منتخب مجموعه داده CICDDOS2019

فهرست ویژگی‌های منتخب مجموعه داده حملات منع سرویس توزیع‌شده که در این پژوهش مورد تجزیه و تحلیل قرار گرفته‌اند، در جدول ۶ نشان داده‌شده است:

جدول ۶: فهرست ویژگی‌های منتخب مجموعه داده CICDDOS2019

Table 6. List of Selected Features of CICDDOS2019 Dataset

برچسب کلاس	تعداد ویژگی‌ها	ویژگی‌های مورد استفاده
DrDOS_DNS	۱۶	Flow Bytes/s , Min Packet Length , Fwd Packet Length Min , Inbound , Source Port , Total Backward Packets , Subflow Bwd Packets , Bwd Packets/s , Fwd Packet Length Mean , Avg Fwd Segment Size , Average Packet Size , Flow IAT Std , Bwd IAT Min , Flow Packets/s , Flow IAT Mean , Protocol.
DrDOS_NetBIOS	۷	Min Packet Length , Fwd Packet Length Min , Fwd Packet Length Mean , Avg Fwd Segment Size , Average Packet Size , Flow Bytes/s , Packet Length Mean.
DrDOS_LDAP	۱۱	Min Packet Length , Fwd Packet Length Min , Fwd Packet Length Mean , Avg Fwd Segment Size , Average Packet Size , Packet Length Mean , Fwd Packet Length Max , Flow Bytes/s , Total Length of Fwd Packets , Subflow Fwd Bytes , Max Packet Length.
DrDOS_UDP	۱۷	Fwd Packet Length Min , Min Packet Length , Fwd Packet Length Mean , Avg Fwd Segment Size , Packet Length Mean , Average Packet Size , Fwd Packet Length Max , Total Length of Fwd Packets , Subflow Fwd Bytes , Max Packet Length , Inbound , Destination Port , Total Backward Packets , Bwd Packets/s , Subflow Bwd Packets , Bwd IAT Mean , Bwd IAT Min.
DrDOS_SNMP	۲۶	Min Packet Length , Fwd Packet Length Min , Fwd Packet Length Mean , Avg Fwd Segment Size , Flow Bytes/s , Average Packet Size , Packet Length Mean , Fwd Packet Length Max , Total Length of Fwd Packets , Subflow Fwd Bytes , Inbound , Max Packet Length , Source Port , Flow IAT Max , Flow Duration , Flow Packets/s , Flow IAT Std ,Protocol , Total Backward Packets , Bwd Packets/s , Subflow Bwd Packets , Flow IAT Mean , Bwd IAT Mean , Packet Length Std , Packet Length Variance , Bwd IAT Min.

۵-۵- ارزیابی الگوریتم‌های یادگیری ماشین

در این بخش عملکرد ده الگوریتم یادگیری ماشین مورد بحث در بخش ۳-۱ و رویکرد پیشنهادی، روی پنج حمله از مجموعه داده CICDDOS2019، مورد تجزیه و تحلیل قرار گرفت. مراحل اجرای الگوریتم‌ها و سپس انتخاب پنج الگوریتم طبقه‌بندی روی پنج حمله از مجموعه داده CICDDOS2019، برای شرکت در رأی‌گیری به شرح ذیل است:

مرحله ۱: ابتدا مرحله پیش‌پردازش داده‌ها که شامل نمونه‌گیری اولیه از مجموعه داده، حذف داده‌های از دست رفته و بی‌نهایت، نرمال‌سازی داده‌ها و انتخاب ویژگی است روی مجموعه داده اعمال شد. سپس برای تقسیم داده‌ها به دو بخش، ضریب تقسیم داده‌ها به مجموعه داده آموزشی و آزمایشی در مجموعه داده حمله DNS ، LDAP و SNMP، ۸۰:۲۰ انتخاب شد که در آن از ۸۰٪ داده‌ها برای آموزش مدل و اعتبارسنجی آن و ۲۰٪ باقیمانده برای آزمایش مدل استفاده شد. همچنین در مجموعه داده حمله NetBIOS و UDP ضریب تقسیم داده‌ها ۷۰:۳۰ انتخاب گردید که در آن ۷۰٪ داده‌ها برای آموزش مدل و اعتبارسنجی آن و ۳۰٪ درصد باقیمانده برای آزمایش مدل مورد استفاده قرار گرفت. برای متعادل‌سازی کلاس‌ها در مجموعه داده آموزشی حملات NETBIOS و LDAP، از ترکیب دو روش نمونه‌گیری کمتر از حد و بیشتر از حد با ایجاد نمونه‌های تصادفی توسط الگوریتم SMOTE و در مجموعه داده آموزشی حملات DNS ، UDP و SNMP از ترکیب دو روش نمونه‌گیری کمتر از حد و بیشتر از حد با جایگزینی نمونه‌های اقلیت در مجموعه آموزشی استفاده شد تا مانع از ارائه عملکرد خوش‌بینانه و گمراه‌کننده مدل شود. سپس با استفاده از نرم افزار RapidMiner، تعداد ده الگوریتم طبقه‌بندی‌کننده به‌طور تصادفی انتخاب شده و روی هر مجموعه داده حمله، آزمایش شدند و میزان دقت، خطای طبقه‌بندی، صحت، فراخوانی، معیار-F و زمان اجرای الگوریتم‌ها مورد بررسی قرار گرفت. نتایج عملکرد تک‌تک الگوریتم‌های یادگیری ماشین ذکر شده در بخش ۳-۱، روی پنج مجموعه داده حمله، در جدول ۷ نشان داده‌شده است.

جدول ۷: عملکرد ده الگوریتم یادگیری ماشین روی پنج حمله مجموعه داده CICDDOS2019

Table 7. Performance of Ten Machine Learning Algorithms on Five Attacks of the CICDDOS2019 Dataset

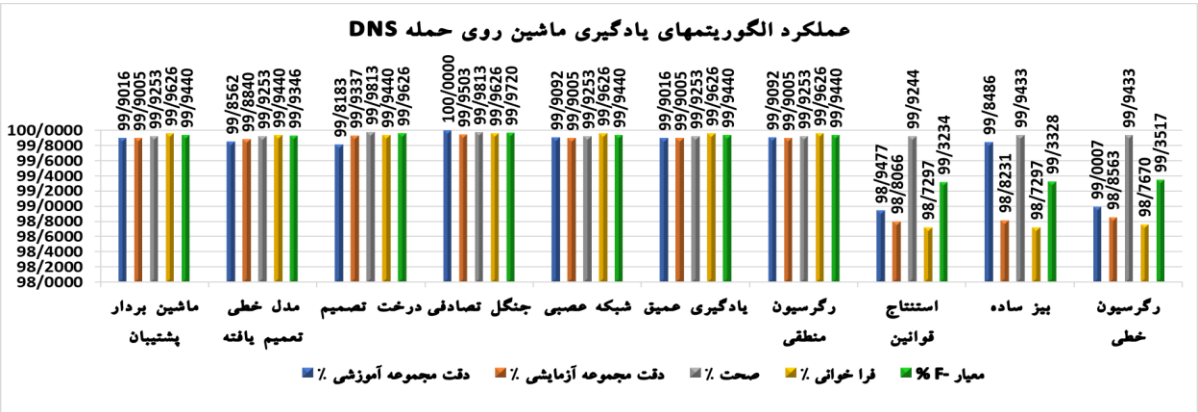
حمله	الگوریتم	دقت مجموعه آموزشی ٪	دقت مجموعه آزمایشی ٪	صحت ٪	فرا خوانی ٪	معیار -F ٪	خطای طبقه بندی ٪	زمان اجرا (ثانیه)	همبستگی	ریشه میانگین مربعات خطا
DNS	SVM	۹۹/۹۰۱۶	۹۹/۹۰۰۵	۹۹/۹۲۵۳	۹۹/۹۶۲۶	۹۹/۹۴۴۰	۰/۰۹۹۵	۴	۰/۹۹۵	۰/۱۱۹
	GLM	**۹۹/۸۵۶۲**	**۹۹/۸۸۴۰**	**۹۹/۹۲۵۳**	**۹۹/۹۴۴۰**	**۹۹/۹۳۴۶**	**۰/۱۱۶۰**	**۳**	**۰/۹۹۴**	**۰/۰۳۷**
	DT	**۹۹/۸۱۸۳**	**۹۹/۹۳۳۷**	**۹۹/۹۸۱۳**	**۹۹/۹۴۴۰**	**۹۹/۹۶۲۶**	**۰/۰۶۶۳**	**۲**	**۰/۹۹۷**	**۰/۰۲۷**
	RF	**۱۰۰/۰۰۰۰**	**۹۹/۹۵۰۳**	**۹۹/۹۸۱۳**	**۹۹/۹۶۲۶**	**۹۹/۹۷۲۰**	**۰/۰۴۹۷**	**۴**	**۰/۹۹۸**	**۰/۰۲۰**
	NN	۹۹/۹۰۹۲	۹۹/۹۰۰۵	۹۹/۹۲۵۳	۹۹/۹۶۲۶	۹۹/۹۴۴۰	۰/۰۹۹۵	۱۵	۰/۹۹۵	۰/۰۳۱
	DL	۹۹/۹۰۱۶	۹۹/۹۰۰۵	۹۹/۹۲۵۳	۹۹/۹۶۲۶	۹۹/۹۴۴۰	۰/۰۹۹۵	۷	۰/۹۹۵	۰/۰۳۲
	LGR	**۹۹/۹۰۹۲**	**۹۹/۹۰۰۵**	**۹۹/۹۲۵۳**	**۹۹/۹۶۲۶**	**۹۹/۹۴۴۰**	**۰/۰۹۹۵**	**۴**	**۰/۹۹۵**	**۰/۰۳۲**
	RI	۹۸/۹۴۷۷	۹۸/۸۰۶۶	۹۹/۹۲۴۴	۹۸/۷۲۹۷	۹۹/۳۲۳۴	۱/۱۹۳۴	۳	۰/۹۴۴	۰/۱۰۸
	NB	۹۹/۸۴۸۶	۹۸/۸۲۳۱	۹۹/۹۴۳۳	۹۸/۷۲۹۷	۹۹/۳۳۲۸	۱/۱۷۶۹	۲	۰/۹۴۵	۰/۱۰۸
	LR	**۹۹/۰۰۰۷**	**۹۸/۸۵۶۳**	**۹۹/۹۴۳۳**	**۹۸/۷۶۷۰**	**۹۹/۳۵۱۷**	**۱/۱۴۳۷**	**۸**	**۰/۹۴۶**	**۰/۳۸۵**
NetBIOS	SVM	۹۹/۷۸۳۵	۹۹/۹۲۳۰	۹۹/۹۶۵۰	۹۹/۹۵۳۴	۹۹/۹۵۹۲	۰/۰۷۷۰	۱۷	۰/۹۹۳	۰/۱۳۰
	GLM	۵۰/۰۰۰۰	۵/۶۳۱۳	unknown	۰/۰۰۰۰	unknown	۹۴/۳۶۸۷	۱۹	0	۰/۵۰۰
	DT	**۹۹/۹۴۴۵**	**۹۹/۹۴۵۰**	**۱۰۰/۰۰۰۰**	**۹۹/۹۴۱۷**	**۹۹/۹۷۰۹**	**۰/۰۵۵۰**	**۱۵**	**۰/۹۹۵**	**۰/۰۲۴**
	RF	**۹۹/۹۹۴۴**	**۹۹/۹۲۳۰**	**۱۰۰/۰۰۰۰**	**۹۹/۹۱۸۴**	**۹۹/۹۵۹۲**	**۰/۰۷۷۰**	**۱۶**	**۰/۹۹۳**	**۰/۰۲۷**
	NN	**۹۹/۷۸۹۱**	**۹۹/۹۰۱۰**	**۹۹/۹۶۵۰**	**۹۹/۹۳۰۱**	**۹۹/۹۴۷۵**	**۰/۰۹۹۰**	**۲۰**	**۰/۹۹۱**	**۰/۰۲۸**
	DL	**۹۹/۸۱۶۸**	**۹۹/۹۱۲۰**	**۹۹/۹۶۵۰**	**۹۹/۹۴۱۷**	**۹۹/۹۵۳۴**	**۰/۰۸۸۰**	**۱۹**	**۰/۹۹۲**	**۰/۰۴۵**
	LGR	۹۹/۷۹۴۶	۹۹/۹۴۵۰	۹۹/۹۶۵۰	۹۹/۹۷۶۷	۹۹/۹۷۰۹	۰/۰۵۵۰	۱۶	۰/۹۹۵	۰/۰۲۵
	RI	**۹۹/۸۰۵۷**	**۹۹/۸۹۰۰**	**۹۹/۹۶۵۰**	**۹۹/۹۱۸۴**	**۹۹/۹۴۱۷**	**۰/۱۱۰**	**۱۵**	**۰/۹۹۰**	**۰/۰۳۳**
	NB	۹۹/۵۹۴۸	۹۹/۹۴۵۰	۹۹/۹۴۱۸	۱۰۰/۰۰۰۰	۹۹/۹۷۰۹	۰/۰۵۵	۱۴	۰/۹۹۵	۰/۰۲۳
	LR	۹۹/۷۶۱۳	۹۹/۹۲۳۰	۹۹/۹۶۵۰	۹۹/۹۵۳۴	۹۹/۹۵۹۲	۰/۰۷۷	۱۵	۰/۹۹۳	۰/۳۹۳
LDAP	**SVM**	**۹۹/۹۸۱۱**	**۹۹/۹۵۱۶**	**۱۰۰/۰۰۰۰**	**۹۹/۹۴۸۷**	**۹۹/۹۷۴۴**	**۰/۰۴۸۴**	**۲۹**	**۰/۹۹۵**	**۰/۰۴۴**
	GLM	۵۰/۰۰۰۰	۵/۵۸۲۴	unknown	۰/۰۰۰۰	unknown	۹۴/۴۱۷۶	۲۸	۰/۰۰۰	۰/۵۰۰
	DT	**۹۹/۹۸۱۱**	**۹۹/۹۸۳۹**	**۱۰۰/۰۰۰۰**	**۹۹/۹۸۲۹**	**۹۹/۹۹۱۵**	**۰/۰۱۶۱**	**۲۶**	**۰/۹۹۸**	**۰/۰۱۳**
	RF	۹۹/۹۸۱۱	۹۹/۹۸۳۹	۱۰۰/۰۰۰۰	۹۹/۹۸۲۹	۹۹/۹۹۱۵	۰/۰۱۶۱	۲۹	۰/۹۹۸	۰/۰۱۳
	NN	۹۹/۹۸۱۱	۹۹/۹۸۳۹	۱۰۰/۰۰۰۰	۹۹/۹۸۲۹	۹۹/۹۹۱۵	۰/۰۱۶۱	۳۶	۰/۹۹۸	۰/۰۱۴
	DL	**۹۹/۹۷۶۴**	**۹۹/۹۶۷۷**	**۱۰۰/۰۰۰۰**	**۹۹/۹۶۵۸**	**۹۹/۹۸۲۹**	**۰/۰۳۲۳**	**۳۴**	**۰/۹۹۷**	**۰/۰۱۵**
	LGR	۹۹/۹۷۶۴	۹۹/۹۵۱۶	۱۰۰/۰۰۰۰	۹۹/۹۴۸۷	۹۹/۹۷۴۴	۰/۰۴۸۴	۲۸	۰/۹۹۵	۰/۰۲۰
	RI	۹۹/۹۸۱۱	۹۹/۹۸۳۹	۱۰۰/۰۰۰۰	۹۹/۹۸۲۹	۹۹/۹۹۱۵	۰/۰۱۶۱	۳۰	۰/۹۹۸	۰/۰۱۳
	NB	**۹۹/۹۶۲۲**	**۹۹/۸۳۸۷**	**۱۰۰/۰۰۰۰**	**۹۹/۸۲۹۱**	**۹۹/۹۱۴۵**	**۰/۱۶۱۳**	**۲۶**	**۰/۹۸۵**	**۰/۰۴۰**
	LR	**۹۹/۴۷۱۰**	**۹۹/۷۹۰۳**	**۹۹/۸۹۷۵**	**۹۹/۸۸۰۴**	**۹۹/۸۸۸۹**	**۰/۲۰۹۷**	**۲۹**	**۰/۹۸**	**۰/۳۸۴**

ادامه جدول ۷: عملکرد ده الگوریتم یادگیری ماشین روی پنج حمله مجموعه داده CICDDOS2019

Table Continues7. Performance of Ten Machine Learning Algorithms on Five Attacks of the CICDDOS2019 Dataset

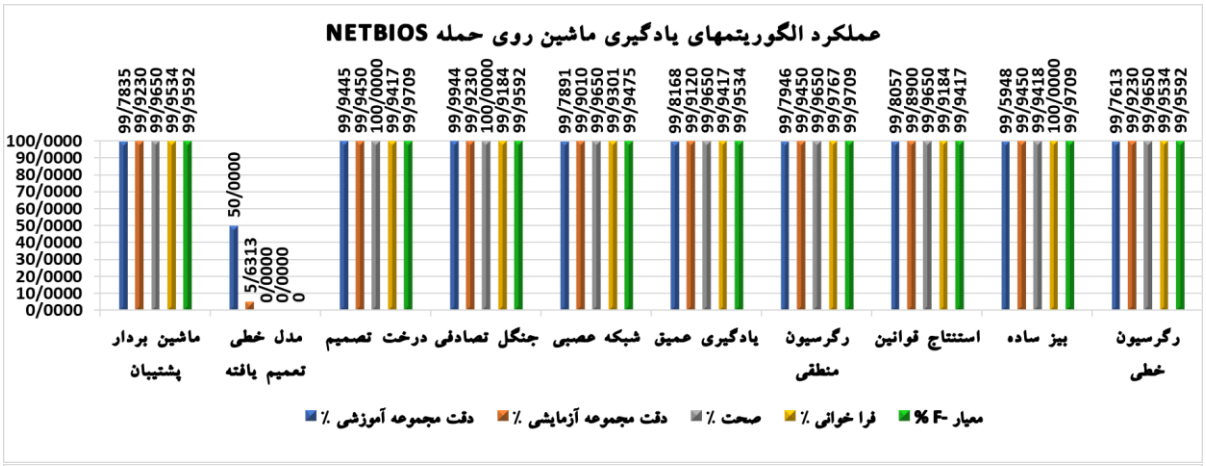
حمله	الگوریتم	دقت مجموعه آموزشی ٪	دقت مجموعه آزمایشی ٪	صحت ٪	فرا خوانی ٪	معیار F- ٪	خطای طبقه بندی ٪	زمان اجرا (ثانیه)	همبستگی	ریشه میانگین مربعات خطا
UDP	**SVM**	**۹۹/۹۴۸۶**	**۹۹/۹۱۶۲**	**۹۹/۹۸۸۸**	**۹۹/۹۲۱۳**	**۹۹/۹۵۵۰**	**۰/۰۸۳۸**	**۴**	**۰/۹۹۳**	**۰/۲۱۸**
	GLM	۸۹/۱۵۶۳	۹۸/۳۳۳۷	۹۸/۲۵۴۵	۹۹/۹۸۸۸	۹۹/۱۱۴۱	۱/۶۶۶۳	۳	۰/۸۶۱	۰/۱۹۹
	DT	**۹۹/۹۶۰۰**	**۹۹/۹۰۵۷**	**۱۰۰/۰۰۰۰**	**۹۹/۸۹۸۸**	**۹۹/۹۴۹۴**	**۰/۰۹۴۳**	**۳**	**۰/۹۹۳**	**۰/۰۳۱**
	RF	**۹۹/۹۹۴۳**	**۹۹/۸۸۴۷**	**۹۹/۹۸۸۷**	**۹۹/۸۸۷۶**	**۹۹/۹۳۸۱**	**۰/۱۱۵۳**	**۵**	**۰/۹۹۱**	**۰/۰۲۷**
	NN	۹۹/۹۴۸۶	۹۹/۹۳۷۱	۱۰۰/۰۰۰۰	۹۹/۹۳۲۵	۹۹/۹۶۶۳	۰/۰۶۲۹	۱۸	۰/۹۹۵	۰/۰۲۶
	DL	**۹۹/۹۵۴۳**	**۹۹/۹۳۷۱**	**۱۰۰/۰۰۰۰**	**۹۹/۹۳۲۵**	**۹۹/۹۶۶۳**	**۰/۰۶۲۹**	**۸**	**۰/۹۹۵**	**۰/۰۲۶**
	LGR	**۹۹/۹۴۸۶**	**۹۹/۹۲۶۶**	**۹۹/۹۸۸۸**	**۹۹/۹۳۲۵**	**۹۹/۹۶۰۶**	**۰/۰۷۳۴**	**۵**	**۰/۹۹۴**	**۰/۰۲۶**
	RI	۹۹/۷۰۲۸	۹۹/۳۹۲۲	۱۰۰/۰۰۰۰	۹۹/۳۴۷۹	۹۹/۶۷۲۹	۰/۶۰۷۸	۳	۰/۹۵۵	۰/۰۷۷
	NB	۹۹/۹۲۵۷	۹۹/۹۰۵۷	۹۹/۹۸۸۷	۹۹/۹۱۰۱	۹۹/۹۴۹۴	۰/۰۹۴۳	۳	۰/۹۹۳	۰/۰۳۱
	LR	۹۹/۶۶۲۷	۹۹/۸۷۴۲	۹۹/۹۳۲۵	۹۹/۹۳۲۵	۹۹/۹۳۲۵	۰/۱۲۵۸	۶	۰/۹۹۰	۰/۳۸۲
SNMP	**SVM**	**۹۹/۷۲۹۴**	**۹۹/۹۵۱۱**	**۹۹/۹۸۲۹**	**۹۹/۹۶۵۷**	**۹۹/۹۷۴۳**	**۰/۰۴۸۹**	**۷**	**۰/۹۹۵**	**۰/۰۷۱**
	GLM	۹۲/۷۹۸۸	۹۹/۰۸۶۶	۹۹/۱۴۹۷	۹۹/۸۹۷۲	۹۹/۵۲۲۰	۰/۹۱۳۴	۳	۰/۸۹۶	۰/۱۵۲
	DT	۹۹/۷۱۹۰	۹۹/۹۱۸۴	۹۹/۹۶۵۷	۹۹/۹۴۸۶	۹۹/۹۵۷۲	۰/۰۸۱۶	۲	۰/۹۹۱	۰/۰۲۸
	RF	**۹۹/۹۹۴۸**	**۹۹/۹۱۸۴**	**۹۹/۹۸۲۹**	**۹۹/۹۳۱۵**	**۹۹/۹۵۷۲**	**۰/۰۸۱۶**	**۵**	**۰/۹۹۱**	**۰/۰۲۱**
	NN	۹۹/۷۸۱۵	۹۹/۴۱۲۸	۱۰۰/۰۰۰۰	۹۹/۳۸۳۱	۹۹/۶۹۰۶	۰/۵۸۷۲	۳۶	۰/۹۴۱	۰/۰۶۵
	DL	**۹۹/۷۸۱۵**	**۹۹/۹۳۴۸**	**۹۹/۹۸۲۹**	**۹۹/۹۴۸۶**	**۹۹/۹۶۵۷**	**۰/۰۶۵۲**	**۹**	**۰/۹۹۳**	**۰/۰۲۴**
	LGR	۹۹/۷۶۵۹	۹۹/۹۱۸۴	۹۹/۹۸۲۹	۹/۹۳۱۵	۹۹/۹۵۷۲	۰/۰۸۱۶	۶	۰/۹۹۱	۰/۰۲۷
	RI	**۹۹/۷۱۹۰**	**۹۹/۸۶۹۵**	**۹۹/۹۶۵۷**	**۹۹/۸۹۷۲**	**۹۹/۹۳۱۴**	**۰/۱۳۰۵**	**۴**	**۰/۹۸۶**	**۰/۰۳۶**
	NB	**۹۹/۷۹۱۹**	**۹۹/۹۰۲۱**	**۱۰۰/۰۰۰۰**	**۹۹/۸۹۷۲**	**۹۹/۹۴۸۶**	**۰/۰۹۷۹**	**۳**	**۰/۹۸۹**	**۰/۰۳۱**
	LR	۹۹/۰۸۹۴	۹۸/۶۲۹۹	۹۹/۹۸۲۶	۹۸/۵۷۷۸	۹۹/۲۷۵۲	۱/۳۷۰۱	۲۲	۰/۸۷۵	۰/۳۸۳

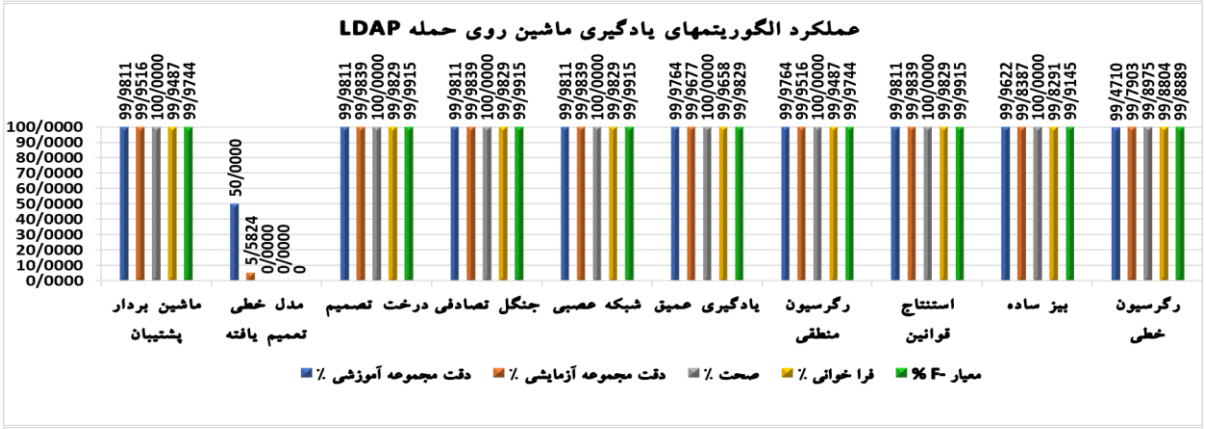
مرحله ۲: برای آزمایش مدل گروهی رأی‌گیری اکثریت از بین ده الگوریتم اجرا شده روی پنج حمله از مجموعه داده CICDDOS2019، پنج الگوریتم طبقه‌بندی بر اساس بالاترین دقت مجموعه آموزشی و آزمایشی، صحت، فراخوانی، معیار-F و کمترین زمان پردازش انتخاب شدند. ضمناً اگر چند الگوریتم دقت یکسانی روی یک مجموعه داده حمله داشتند، الگوریتمی که زمان کمتری را برای اجرا صرف کرده بود، انتخاب شد. در غیر این‌صورت الگوریتمی که دارای ریشه میانگین مربعات خطای کمتری بود برای شرکت در رأی‌گیری انتخاب گردید. شکل ۵ نتیجه تحلیل معیارهای ارزیابی طبقه‌بندی‌کننده‌ها روی پنج حمله را به‌صورت گرافیکی نشان می‌دهد.

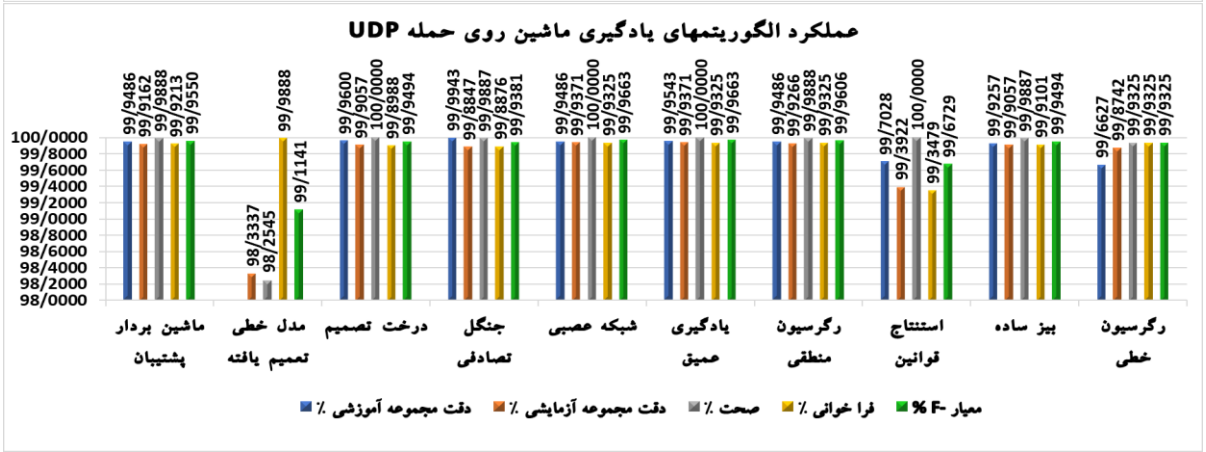


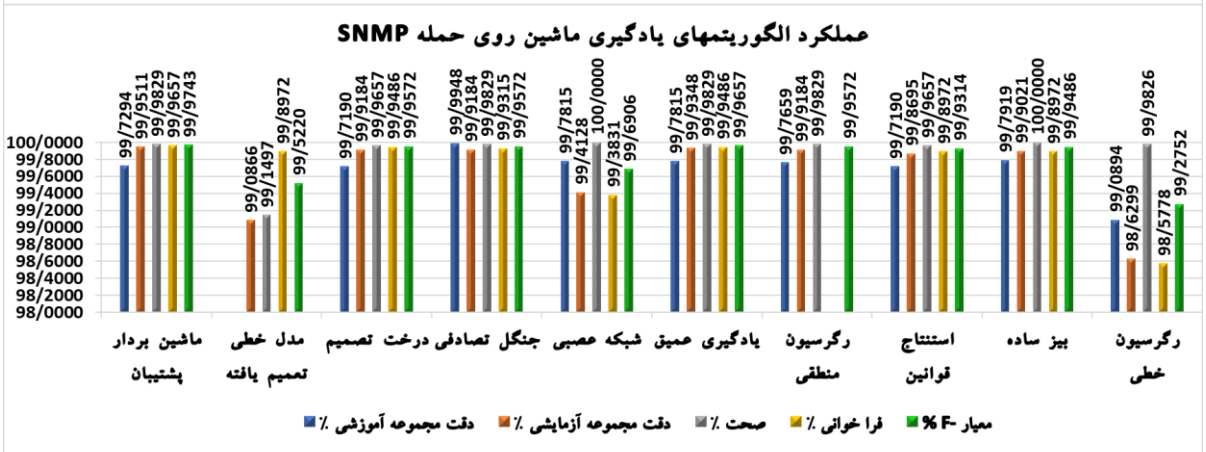
شکل ۵: نمودار مقایسه عملکرد الگوریتم‌های یادگیری ماشین روی حملات مجموعه داده CICDDOS2019

Figure 5. Performance Comparison Chart of Machine Learning Algorithms on CICDDOS2019 Dataset Attacks









ادامه شکل ۵: نمودار مقایسه عملکرد الگوریتم‌های یادگیری ماشین روی حملات مجموعه داده CICDDOS2019

Figure Continues 5. Performance Comparison Chart of Machine Learning Algorithms on CICDDOS2019 Dataset Attacks

مرحله ۳: با توجه به جدول ۷ و شکل ۵، در مجموعه داده حمله DNS، پنج الگوریتم انتخابی با بالاترین دقت به ترتیب جنگل تصادفی، درخت تصمیم، رگرسیون منطقی، مدل خطی تعمیم‌یافته و رگرسیون خطی بود. در مجموعه داده NetBIOS نیز به ترتیب درخت تصمیم، جنگل تصادفی، یادگیری عمیق، شبکه عصبی، استنتاج قوانین به عنوان بهترین الگوریتم‌ها انتخاب شدند. همچنین در مجموعه داده LDAP به ترتیب درخت تصمیم، یادگیری عمیق، ماشین بردار پشتیبان، بیز ساده، و رگرسیون خطی الگوریتم‌های انتخابی برای شرکت در رأی‌گیری بودند. در مجموعه داده UDP نیز الگوریتم‌های انتخابی به ترتیب یادگیری عمیق، رگرسیون منطقی، ماشین بردار پشتیبان، درخت تصمیم و جنگل تصادفی بود. در مجموعه داده SNMP نیز ماشین بردار پشتیبان، یادگیری عمیق، جنگل تصادفی، بیز ساده و استنتاج قوانین پنج الگوریتم انتخابی برای شرکت در رأی‌گیری بودند. در نهایت، مدل گروهی رأی‌گیری اکثریت با استفاده از الگوریتم‌های انتخابی، روی تک‌تک حملات مورد آزمایش قرار گرفت.

۵-۶- ارزیابی مدل گروهی رأی‌گیری اکثریت

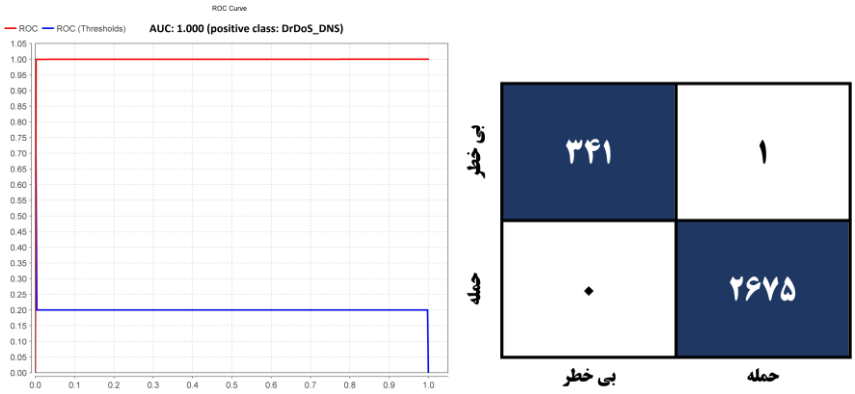
برای اعمال رویکرد رأی‌گیری اکثریت نیز قبل از اجرای مدل روی مجموعه داده، پیش‌پردازش داده‌ها انجام شد. سپس ضریب تقسیم داده‌ها به داده‌های آموزشی و آزمایشی برای پیاده‌سازی رویکرد رأی‌گیری اکثریت در مجموعه داده حمله DNS ، LDAP و SNMP، ۹۰:۱۰ و در مجموعه داده حمله NetBIOS و UDP، ۸۰:۲۰ انتخاب شد. همچنین با توجه به بخش ۵-۵ از ترکیب نمونه‌گیری کمتر از حد و بیشتر از حد با جایگزینی و نمونه‌گیری بیشتر از حد با الگوریتم SMOTE برای متعادل‌سازی کلاس‌ها استفاده گردید. در نهایت پس از انتخاب الگوریتم‌ها برای شرکت در رأی‌گیری، مدل گروهی رأی‌گیری اکثریت با ترکیب الگوریتم‌های انتخابی، روی تک‌تک حملات مورد آزمایش قرار گرفت. نتایج عملکرد مدل گروهی رأی‌گیری اکثریت روی پنج حمله از مجموعه داده CICDDOS2019 در جدول ۸ نشان داده‌شده است.

جدول ۸: عملکرد رویکرد رأی‌گیری اکثریت روی پنج حمله مجموعه داده CICDDOS2019

Table 8. Performance of the majority voting approach on the five attacks of the CICDDOS2019 Dataset

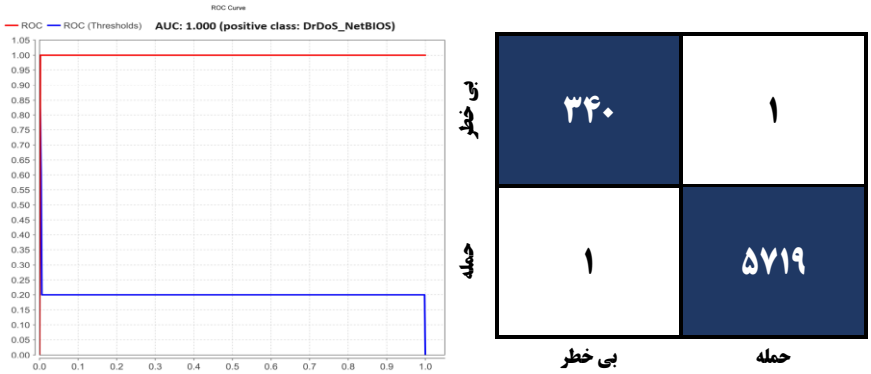
حمله	دقت مجموعه آموزشی ٪	دقت مجموعه آزمایشی ٪	صحت ٪	فرا خوانی ٪	معیار -F ٪	خطای طبقه بندی ٪	زمان اجرا (ثانیه)	همبستگی	ریشه میانگین مربعات خطا	مقدار AUC
DNS	۹۹/۹۳۷۲	**۹۹/۹۶۶۹**	۱۰۰/۰۰۰۰	۹۹/۹۶۲۶	۹۹/۹۸۱۳	۰/۰۳۳۲	۱۲	۰/۹۹۸	۰/۰۲۸	۱
NetBIOS	۹۹/۸۷۸۶	**۹۹/۹۶۷۰**	۹۹/۹۸۲۵	۹۹/۹۸۲۵	۹۹/۹۸۲۵	۰/۰۳۳۰	۳۶	۰/۹۹۷	۰/۰۱۹	۱
LDAP	۹۹/۹۷۹۰	**۱۰۰/۰۰۰۰**	۱۰۰/۰۰۰۰	۱۰۰/۰۰۰۰	۱۰۰/۰۰۰۰	۰/۰۰۰۰	۴۲	۱/۰۰۰	۰/۰۱۰	۱
UDP	۹۹/۹۶۰۰	**۹۹/۹۶۸۶**	۱۰۰/۰۰۰۰	۹۹/۹۶۶۳	۹۹/۹۸۳۱	۰/۰۳۱۴	۱۶	۰/۹۹۸	۰/۰۱۸	۱
SNMP	۹۹/۹۳۹۶	**۹۹/۹۶۷۴**	۱۰۰/۰۰۰۰	۹۹/۹۶۵۶	۹۹/۹۸۲۸	۰/۰۳۲۶	۱۹	۰/۹۹۷	۰/۰۲۰	۱

همان‌طور که در جدول ۸ نشان داده‌شده است، میزان دقت تشخیص حملات DNS، NetBIOS، LDAP، UDP و SNMP به ترتیب ۹۹/۹۶۶۹٪، ۹۹/۹۶۷۰٪، ۱۰۰٪، ۹۹/۹۶۸۶٪ و ۹۹/۹۶۷۴٪ به‌دست آمد. مقدار AUC به‌دست آمده توسط رویکرد پیشنهادی نیز، در تمامی حملات برابر با یک شد که با توجه به مطالب ذکرشده در بخش ۵-۳، نشان‌دهنده عملکرد خوب مدل روی مجموعه داده است. با توجه به نتایج به‌دست آمده حاصل از اجرای رویکرد رأی‌گیری اکثریت روی این پنج حمله، می‌توان دریافت که مدل پیشنهادی عملکرد خیلی خوبی در شناسایی حملات از خود نشان داده است. ماتریس درهم‌ریختگی و منحنی ROC-AUC بعد از اجرای مدل گروهی رأی‌گیری اکثریت روی حملات فوق، در شکل‌های ۶ تا ۱۰ نشان داده‌شده است.



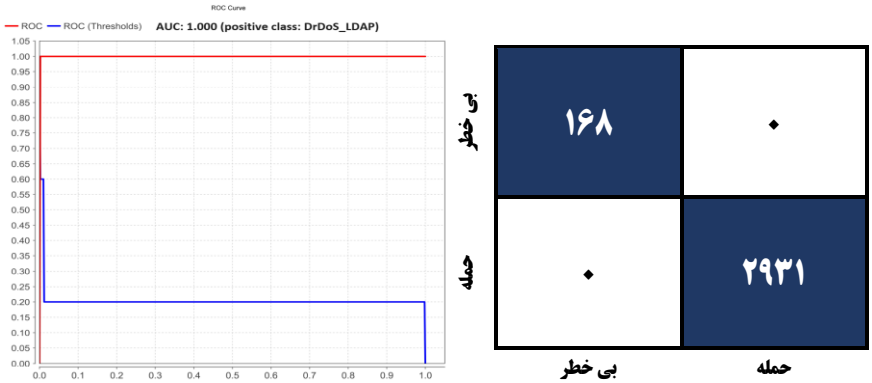
شکل ۶: منحنی ROC-AUC و ماتریس درهم‌ریختگی رویکرد رأی‌گیری اکثریت روی حمله NetBIOS

Figure6: ROC-AUC Curve and Confusion Matrix of Majority Voting Approach on DNS Attack :



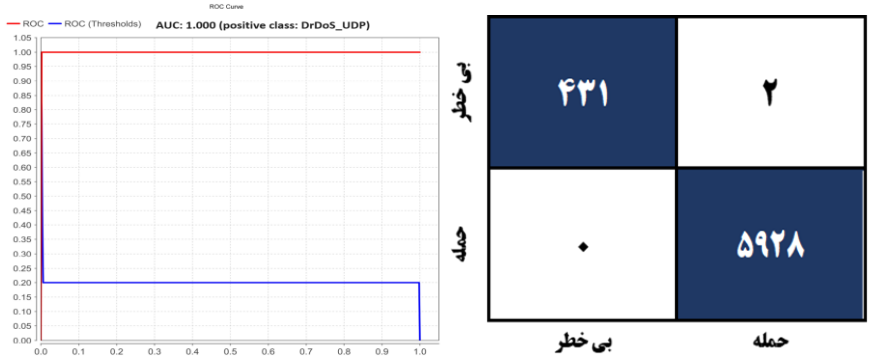
شکل ۷: منحنی ROC-AUC و ماتریس درهم‌ریختگی رویکرد رأی‌گیری اکثریت روی حمله NetBIOS

Figure 7: ROC-AUC Curve and Confusion Matrix of Majority Voting Approach on NetBIOS Attack



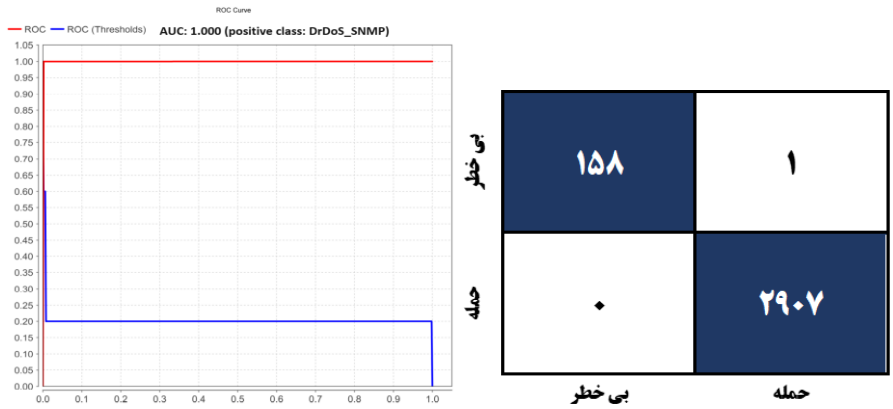
شکل ۸: منحنی ROC-AUC و ماتریس درهم‌ریختگی رویکرد رأی‌گیری اکثریت روی حمله LDAP

Figure 8: ROC-AUC Curve and Confusion Matrix of Majority Voting Approach on LDAP Attack



شکل ۹: منحنی ROC-AUC و ماتریس درهم‌ریختگی رویکرد رأی‌گیری اکثریت روی حمله UDP

Figure 9: ROC-AUC Curve and Confusion Matrix of Majority Voting Approach on UDP Attack



شکل ۱۰: منحنی ROC-AUC و ماتریس درهم‌ریختگی رویکرد رأی‌گیری اکثریت روی حمله SNMP

Figure 10: ROC-AUC Curve and Confusion Matrix of Majority Voting Approach on SNMP Attack

جدول ۹ نتایج نهایی پژوهش فعلی را با کارهای دیگران مورد مقایسه قرار داده است. همان‌طور که در این جدول مشاهده می‌شود با مقایسه این پژوهش با پژوهش‌های دیگران، می‌توان دریافت که روش پیشنهادی توانسته است در تشخیص حملات، به دقت تشخیص بالاتری نسبت به سایر پژوهش‌ها، دست پیدا کند.

جدول ۹: مقایسه نتایج نهایی پژوهش فعلی با پژوهش‌های دیگران

Table 9. Comparison of the Final Results of the Current Research With Others' Research

مرجع	سال	روش کار	مجموعه داده	دقت تشخیص
[۱۱]	۲۰۲۱	شبکه عصبی پس‌انتشار عمیق کالمن	CICDDoS2019	٪۹۴
[۱۴]	۲۰۲۱	الگوریتم رگرسیون منطقی	CICDDoS2019	٪۹۹/۷
[۱۵]	۲۰۲۱	الگوریتم جنگل تصادفی	CICDDoS2019	٪۹۹/۹۲۶۶۷
[۱۷]	۲۰۲۰	شبکه‌های عصبی پیچشی(ResNet)	CICDDOS2019	BC=٪۹۹/۹۹ MC= ٪۸۷/۰۶ DNS =٪۹۹/۹۶۶۹ NetBIOS =٪۹۹/۹۶۷۰
پژوهش فعلی	۲۰۲۳	اجرای رویکرد رأی‌گیری اکثریت روی ۵ حمله	CICDDOS2019	LDAP =٪۱۰۰ UDP =٪۹۹/۹۶۸۶ SNMP =٪۹۹/۹۶۷۴

۶- نتیجه گیری

در این پژوهش برای مدیریت رفتارهای غیرعادی و شناسایی حملات متنوع یک سیستم تشخیص نفوذ پیشنهاد شد. پیاده‌سازی این سیستم بر پایه یادگیری ماشین بود و در آن، رویکرد گروهی رأی‌گیری اکثریت برای دستیابی به نتایج بهتر در شناسایی حملات، مورد استفاده قرار گرفت. برای تشخیص حملات نیز، مجموعه داده CICDDoS2019 به‌کارگرفته شد. در بخش دوم این پژوهش کارهای مرتبط در زمینه شناسایی حملات مورد بررسی قرار گرفت. در بخش سوم به مراحل پیش‌پردازش داده‌ها و همچنین تشریح روش پیشنهادی پرداخته شد. در بخش چهارم مدل‌های پایه یادگیری ماشین و رویکرد گروهی پیشنهادی از طریق ابزار RapidMiner مورد آزمایش قرار گرفتند. به منظور ارزیابی روش پیشنهادی، از معیارهای دقت، صحت، فراخوانی، معیار-F و میزان AUC استفاده شد. نتایج شبیه‌سازی نشان می‌دهد که با اعمال روش گروهی رأی‌گیری اکثریت روی پنج حمله از مجموعه داده CICDDOS2019، این روش به ترتیب به دقت تشخیص واقعی ٪۹۹/۹۶۶۹، ٪۹۹/۹۶۷۰، ٪۱۰۰، ٪۹۹/۹۶۸۶ و ٪۹۹/۹۶۷۴ در حملات DrDOS_DNS، DrDOS_NETBIOS، DrDOS_LDAP، UDP، DrDOS_SNMP دست پیدا کرد. میزان درستی تشخیص این حملات نیز به ترتیب برابر با ٪۱۰۰، ٪۹۹/۹۸۲۵، ٪۱۰۰، ٪۱۰۰، ٪۱۰۰، میزان فراخوانی برابر با ٪۹۹/۹۶۲۶، ٪۹۹/۹۸۲۵، ٪۱۰۰، ٪۹۹/۹۹۶۳، ٪۹۹/۹۶۵۶، و معیار-F برابر با ٪۹۹/۹۸۱۳، ٪۹۹/۹۸۲۵، ٪۱۰۰، ٪۹۹/۹۸۳۱،

۹۹/۹۸۲۸٪ و در زمان اجرای ۱۲ ثانیه، ۳۶ ثانیه، ۴۲ ثانیه، ۱۶ ثانیه و ۱۹ ثانیه به‌دست آمد. همچنین در روش پیشنهادی مقدار AUC در ارزیابی تمامی این حملات، برابر با یک شد؛ بنابراین می‌توان نتیجه گرفت که مدل پیشنهادی، عملکرد خوبی در تشخیص کلاس‌های حمله و بی‌خطر از خود نشان داده است. همچنین با مقایسه این پژوهش با پژوهش‌های ذکر شده در بخش ۲ می‌توان دریافت که روش پیشنهادی برای تشخیص حملات با استفاده از تکنیک‌های نمونه‌گیری مختلف و کاهش ابعاد داده، همچنین نرمال‌سازی داده‌ها با بیش از ۳۰۰۰۰ نمونه و تنها با تحلیل پنج حمله، توانست به دقت تشخیص بالاتری نسبت به پژوهش‌های ذکر شده، دست پیدا کند. البته ذکر این نکته ضروری به نظر می‌رسد که مدل گروهی رأی‌گیری اکثریت اعمال‌شده روی این پنج حمله، تنها توانست در تشخیص حمله LDAP ، به دقت ۱۰۰٪ دست یابد که نسبت به روش به‌کاررفته در پژوهش حسین و همکارانش عملکرد بهتری را به‌دست آورد. به‌طورکلی با توجه به نتایج شبیه‌سازی می‌توان فهمید که مدل پیشنهادی همان‌طور که انتظار می‌رفت عمل کرد و با تنها بخشی از ویژگی‌های مجموعه داده حمله، توانست به دقت بهتری برای شناسایی حمله DDOS نسبت به روش‌های سایر محققان دست یابد. ضمناً این پژوهش تنها به مجموعه داده جدید CICDDOS2019، محدود شده و حملات قدیمی را پوشش نمی‌دهد.

مراجع

[1] J. Alsamiri and K. Alsubhi, "Internet of Things Cyber Attacks Detection using Machine Learning," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 12, pp. 627-634, 2019, doi: 10.14569/IJACSA.2019.0101280.

[2] Z. Shah, I. Ullah, H. Li, A. Levula and K. Khurshid, "Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey," *Multidisciplinary Digital Publishing Institute Sensors*, vol. 22, no. 3, 2022, doi: 10.3390/s22031094.

[3] S. M. Tahsien, H. Karimipour and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *Journal of Network and Computer Applications*, vol. 161, 2020, doi: 10.1016/j.jnca.2020.102630 .

[4] M. Shurman, R. Khrais and A. Yateem, "DoS and DDoS Attack Detection Using Deep Learning and IDS," *The International Arab Journal of Information Technology*, vol. 17, no. 4A, pp. 655-661, 2020, doi: 10.34028/iajit/17/4A/10.

[5] D. K. Sharma, T. Dhankhar, G. Agrawal, S. K. Singh, D. Gupta, J. Nebhen and I. Razzak, "Anomaly detection framework to prevent DDoS attack in fog empowered IoT networks," *Ad Hoc Networks*, vol. 121, 2021, doi: 10.1016/j.adhoc.2021.102603 .

[6] A. K. Jain, H. Dhawan and B. Sowmiya, "DDoS Detection Using Machine Learning Ensemble," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 12, pp. 1647-1655, 2021.

[7] A. Alhowaide, I. Alsmadi and J. Tang, "Ensemble Detection Model for IoT IDS," *Internet of Things*, vol. 16, p. 100435, 2021, doi: 10.1016/j.iot.2021.100435.

[8] S. Raschka, "Ensemble Methods," in Machine Learning, Department of Statistics University of Wisconsin-Madison, 2019.

[9] R. Alghamdi and M. Bellaiche, "Evaluation and Selection Models for Ensemble Intrusion Detection Systems in IoT," *IoT*, vol. 3, no. 2, pp. 285-314, 2022, doi: 10.3390/iot3020017.

[10] I. Sharafaldin, A. H. Lashkari, S. Hakak and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," *International Carnahan Conference on Security Technology (ICCST)*, 2019, pp. 1-8, doi: 10.1109/CCST.2019.8888419.

[11] M. Almiani, A. AbuGhazleh, Y. Jararweh and A. Razaque, "DDoS detection in 5G enabled IoT networks using deep Kalman backpropagation neural network," *International Journal of Machine Learning and Cybernetics*, vol. 12, no. 11, pp. 3337-3349, 2021, doi: 10.1007/s13042-021-01323-7 .

[12] F. F. Setiadi, M. W. A. Kesiman and K. Y. E. Aryanto, "Detection of dos attacks using naive bayes method based on internet of things (iot)," in *Journal of Physics: Conference Series*, vol. 1810, p. 012013, 2021, doi: 10.1088/1742-6596/1810/1/012013

.

[13] A. Churcher, R. Ullah, J. Ahmad, S. u. Rehman, F. Masood, M. Gogate, F. Alqahtani, B. Nour and W. J. Buchanan, "An Experimental Analysis of Attack Classification Using Machine Learning in IoT Networks," *Multidisciplinary Digital Publishing Institute Sensors*, vol. 21, no. 2, p. 446, 2021, doi: 10.3390/s21020446.

[14] S. Chesney, K. Roy and S. Khorsandroo, "Machine Learning Algorithms for Preventing IoT Cybersecurity Attacks," in *Proceedings of SAI Intelligent Systems Conference*, 2020, pp. 679-686.

[15] P. S. Samom and A. Taggu, "Distributed Denial of Service (DDoS) Attacks Detection: A Machine Learning Approach," *Applied Soft Computing and Communication Networks*, 2021, pp. 75-87.

[16] Y. W. Chen, J. P. Sheu, Y. C. Kuo and N. V. Cuong, "Design and Implementation of IoT DDoS Attacks Detection System based on Machine Learning," *European Conference on Networks and Communications (EuCNC)*, Dubrovnik, Croatia, 2020, pp. 122-127, doi: 10.1109/EuCNC48522.2020.9200909.

[17] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad and G. A. Shah, "IoT DoS and DDoS Attack Detection using ResNet," *IEEE 23rd International Multitopic Conference (INMIC)*, Bahawalpur, Pakistan, 2020, pp. 1-6, doi: 10.1109/INMIC50486.2020.9318216.

[18] S. Evmorfos, G. Vlachodimitropoulos, N. Bakalos and E. Gelenbe, "Neural Network Architectures for the detection of SYN flood attacks in IoT systems," in *Proceedings of the 13th ACM International Conference on PErvasive Technologies Related to Assistive Environments*, 2020, pp. 1-4, doi: 10.1145/3389189.3398000.

[19] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung and M. A. Khan, "Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review," *Procedia Computer Science*, vol. 171, pp. 1251-1260, 2020, doi: 10.1016/j.procs.2020.04.133.

[20] M. Roopak, G. Y. Tian and J. Chambers, "An Intrusion Detection System Against DDoS Attacks in loT Networks," *10th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2020, pp. 0562-0567, doi: 10.1109/CCWC47524.2020.9031206.

[21] A. Dushimimana, T. Tao, R. Kindong and A. Nishyirimbere, "Bi-directional Recurrent Neural network for Intrusion Detection System (IDS) in the internet of things (IoT)," I*nternational Journal of Advanced Engineering Research and Science (IJAERS)*, vol. 7, no. 3, pp. 524-539, 2020, doi: 10.22161/ijaers.73.68.

[22] A. Mubarakali, K. Srinivasan, R. Mukhalid, S. C. Jaganathan and N. Marina, "Security challenges in internet of things: Distributed denial of service attack detection using support vector machine-based expert systems," *Computational Intelligence*, vol. 36, no. 4, pp. 1580-1592, 2020, doi: 10.1111/coin.12293.

[23] P. Gokhale, O. Bhat and S. Bhat, "Introduction to IOT," *International Advanced Research Journal in Science, Engineering and Technology*, vol. 5, no. 1, pp. 41-44, 2018, doi: 10.17148/IARJSET.2018.517.

[24] J. S. Kumar and D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues," *International Journal of Computer Applications*, vol. 90, no. 11, 2014, doi: 10.5120/15764-4454.

[25] A. Seifousadati, S. Ghasemshirazi and M. Fathian, "A Machine Learning Approach for DDoS Detection on IoT Devices," *Computer Science*, 2021, doi: 10.48550/arXiv.2110.14911.

[26] A. Khraisat, I. Gondal, P. Vamplew and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1-22, 2019, doi: 10.1186/s42400-019-0038-7.

[27] S. Sambangi and L. Gondi, "A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression," *Multidisciplinary Digital Publishing Institute Proceedings*, vol. 63, no. 1, p. 51, 2020, doi: 10.3390/proceedings2020063051.

[28] I. Romli, T. Pardamean, S. Butsianto and T. N. Wiyatno, "Naive Bayes Algorithm Implementation Based on Particle Swarm Optimization in Analyzing the Defect Product," *Journal of Physics: Conference Series*, vol. 1845, no. 1, p. 012020, 2021, doi: 10.1088/1742-6596/1845/1/012020.

[29] T. Xiuyi and G. Yuxia, "Research on Application of Machine Learning in Data Mining," 2018.

[30] A. Abbas, M. A. Khan, S. Latif, M. Ajaz, A. A. Shah and J. Ahmad, "A New Ensemble-Based Intrusion Detection System for Internet of Things," *Arabian Journal for Science and Engineering*, vol. 47, no. 2, pp. 1805-1819, 2022, doi: 10.1007/s13369-021-06086-5.

[31] M. Hofmann and R. Klinkenberg, RapidMiner: Data mining use cases and business analytics applications, CRC Press, 2016.

[32] D. H. Maulud and A. M. Abdulazeez, "A Review on Linear Regression Comprehensive in Machine Learning," Journal of Applied Science and Technology Trends, vol. 1, no. 4, pp. 140-147, 2020, doi: 10.38094/jastt1457.

[33] Q. Zhang, L. T. Yang, Z. Chen and P. Li, "A survey on deep learning for big data," *Information Fusion*, vol. 42, pp. 146-157, 2018, doi: 10.1016/j.inffus.2017.10.006.

[34] S. Pardo, Statistical Analysis of Empirical Data, Springer International Publishing, 2020.

[35] M. Aslam, D. Ye, A. Tariq, M. Asad, M. Hanif, D. Ndzi, S. A. Chelloug, M. A. Elaziz, M. A. A. Al-Qaness and S. F. Jilani, "Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT," *sensors*, vol. 22, no. 7, p. 2697, 2022, doi: 10.3390/s22072697.

[36] P. Golchin, R. Kundel, T. Steuer, R. Hark and R. Steinmetz, "Improving DDoS Attack Detection Leveraging a Multi-aspect Ensemble Feature Selection," *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, pp. 1-5, 2022, doi: 10.1109/NOMS54207.2022.9789763.

[37] D. Kshirsagar and S. Kumar, "A feature reduction based reflected and exploited DDoS attacks detection system," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 1, pp. 393-405, 2022, doi: 10.1007/s12652-021-02907-5.

[38] A. Mahfouz, A. Abuhussein, D. Venugopal and S. Shiva, "Ensemble Classifiers for Network Intrusion Detection Using a Novel Network Attack Dataset," *Future Internet*, vol. 12, no. 11, p. 180, 2020, doi: 10.3390/fi12110180.

[39] S.-A. N. ALEXANDROPOULOS, S. B. KOTSIANTIS and M. N. VRAHATIS, "Data preprocessing in predictive data mining," *The Knowledge Engineering Review*, p. 34, 2019, doi: 10.1017/S026988891800036X.

[40] J. Han, M. Kamber and J. Pei, Data mining concepts and techniques, ELSEVIER, 2016.

[41] S. Yadav and S. Shukla, "Analysis of k-fold cross-validation over hold-out validation on colossal datasets for quality classification," *IEEE 6th International conference on advanced computing (IACC)*, 2016, pp. 78-83, doi: 10.1109/IACC.2016.25..

[42] J. Brownlee, Imbalanced classification with Python: better metrics, balance skewed classes, cost-sensitive learning, Machine Learning Mastery, 2020.

[43] S. Senthilnathan, "USEFULNESS OF CORRELATION ANALYSIS," Available at SSRN 3416918, 2019.

[44] K. N. Mallikarjunan, A. Bhuvaneshwaran, K. Sundarakantham and S. M. Shalinie, "DDAM: Detecting DDoS Attacks Using Machine Learning Approach," *Computational Intelligence: Theories, Applications and Future Directions*,vol. 1, pp. 261-273, 2019, doi: 10.1007/978-981-13-1132-1_21.

[45] D. Chicco, M. . J. Warrens and G. Jurman, "The coefficient of determination R-squared is more informative than SMAPE, MAE, MAPE, MSE and RMSE in regression analysis evaluation," *PeerJ Computer Science*, vol. 7, p. e623, 2021, doi: 10.7717/peerj-cs.623.

[46] B. K. Chae, "The evolution of the Internet of Things (IoT): A computational text analysis," *Telecommunications Policy*, vol. 43, no. 10, p. 101848, 2019, doi: 10.1016/j.telpol.2019.101848.

[47] V. R. Joseph, "Optimal ratio for data splitting," Statistical Analysis and Data Mining: The ASA Data Science Journal, 2022.

[48] F. Rodríguez-Torres, J. F. Martínez-Trinidad and J. A. Carrasco-Ochoa, "An Oversampling Method for Class Imbalance Problems on Large Datasets," *Applied Sciences*, vol. 12, no. 2, p. 3424, 2022, doi: 10.3390/app12073424.

[49] T. Hasanin, T. M. Khoshgoftaar, J. L. Leevy and R. A. Bauder, "Severely imbalanced Big Data challenges: investigating data sampling approaches," *Journal of Big Data*, vol. 6, no. 1, pp. 1-25, 2019, doi: 10.1186/s40537-019-0274-4.

[50] M. Á. Canela, I. Alegre and A. Ibarra, "Out-of-Sample Validation," in *Quantitative Methods for Management, Springer*, 2019, pp. 83-89, doi: 10.1007/978-3-030-17554-2_9.

[51] H. Roohi and Q. Usman, "An Approach to Detect Spam Emails by Using Majority Voting," in *Proceedings of the International Conference on Data Mining, Internet Computing and Big Data (BigData2014)*, 2014.

[52] A. Sifaunajah and R. D. Wahyuningtyas, "The Classification of Prospective Students with Rapid Miner," *NEWTON: Networking and Information Technology*, vol. 2, no. 2, pp. 72-78, 2022.

[53] S. Bashir, I. U. Khattak, A. Khan, F. H. Khan, A. Gani and M. Shiraz, "A Novel Feature Selection Method for Classification of Medical Data Using Filters, Wrappers, and Embedded Approaches," *Complexity*, vol. 2022, 2022, doi: 10.1155/2022/8190814.

[54] R. Rizal, M. Martanto and Y. A. Wijaya, "ANALISA DATASET SOFTWARE DEFINED NETWORK INTRUSION MENGGUNAKAN ALGORITMA DEEP LEARNING H2O," *JATI (Jurnal Mahasiswa Teknik Informatika*, vol. 6, no. 2, pp. 747-757, 2022, doi: 10.36040/jati.v6i2.5724.

[55] D. J. Arunadevi, S. Ramya and M. R. Raja, "A study of classification algorithms using RapidMiner," *International Journal of Pure and Applied Mathematics*, vol. 119, no. 12, pp. 15977-15988, 2018.

[56] Y. B. Lasotte, E. J. Garba, Y. M. Malgwi and M. A. Buhari, "An Ensemble Machine Learning Approach for Fake News Detection and Classification Using a Soft Voting Classifier," *European Journal of Electrical Engineering and Computer Science*, vol. 6, no. 2, pp. 1-7, 2022, doi: 10.24018/ejece.2022.6.2.409.

[57] O. Thorat, N. Parekh and R. Mangrulkar, "TaxoDaCML: Taxonomy based Divide and Conquer using machine learning approach for DDoS attack classification," *International Journal of Information Management Data Insights*, vol. 1, no. 2, p. 100048, 2021, doi: 10.1016/j.jjimei.2021.100048.

[58] A. Verma and V. Ranga, "Machine Learning Based Intrusion Detection Systems for IoT Applications," *Wireless Personal Communications*, vol. 111, pp. 2287-2310, 2019, doi: 10.1007/s11277-019-06986-8.