Journal of Information and Communication Technology

Volume 17, Issue 63-64, Spring and Summer 2025, pp. 269-282

Improving the Accuracy of Detection Botnet Attacks in Internet of Things Network by Using MLP Neural Network

Safieh Siadat[1], Amir Houshang Tajfar[2*]

[1] Department of Computer, University of Payam Noor, Tehran, Iran
[2*] Department of Computer, University of Payam Noor, Tehran, Iran

Received: 30 October 2024, Revised: 05 May 2025, Accepted: 07 May 2025
Paper type: Research

Abstract

Due to the increasing use of the Internet of Things around the world and the exponential increase in the number of devices connected to the network and the communication between them, the potential for security problems is increasing. Considering that many personal and public devices are connected to this network, any security problem can have unpredictable and significant consequences. Internet of Things applications include smart cities, smart transportation, responsive environments, and some other specific things that are directly controlled by users or digital devices, cyber-attacks through the Internet of Things and smart digital devices is the most important threat for these networks. So far, numerous researches have been conducted to detect Internet of Things attacks, in particular botnet attacks, as one of the most important attacks in this field. But the lack of a method that uses machine learning methods with high accuracy and low error to detect these attacks is strongly felt. In this research, by using the N-BaIoT dataset and Python simulator for modeling and also using deep learning methods and MLP neural network to evaluate and train the data (using the objective function and training), the neural system was used for detecting botnet attacks. This method obtained accuracy 90.35, precision 85.99, recall 90.53 and f1-score 87.50. Compared to other machine learning methods including random forest algorithm (RF), support vector machine algorithm (svm), K nearest neighbor algorithm (knn), XGBOOST algorithm, AdaBoost algorithm, the best result was obtained in all 4 evaluation parameters (accuracy, precision, recall and f1-score).

Keywords: Botnet, neural network, Internet of Things, Deep Learning

[*] Corresponding Author's email: amir.tajfar@pnu.ac.ir

دوفصلنامه
فناوری اطلاعات و ارتباطات ایران

سال هفدهم، شماره‌های ۶۳ و ۶۴ ، بهار و تابستان ۱۴۰۴، صفحه ۲۶۹ الی ۲۸۲

بهبود دقت تشخیص حملات بات‌نت در شبکه‌های اینترنت اشیا با استفاده از شبکه عصبی MLP

صفیه سیادت[۱]، امیرهوشنگ تاج‌فر [۲*]

[۱] گروه کامپیوتر و فناوری اطلاعات، دانشگاه پیام نور، ایران، تهران

[۲] گروه کامپیوتر و فناوری اطلاعات، دانشگاه پیام نور، ایران، تهران

تاریخ دریافت: ۱۴۰۳/۰۸/۰۹ تاریخ بازبینی: ۱۴۰۴/۰۲/۱۵ تاریخ پذیرش: ۱۴۰۴/۰۲/۱۷

نوع مقاله: پژوهشی

چکیده

گسترش فزاینده استفاده از اینترنت اشیا در سراسر جهان و افزایش تصاعدی تعداد دستگاه‌های متصل به شبکه و ارتباط بین آن‌ها، پتانسیل مشکلات امنیتی در حال افزایش است. با توجه به اتصال بسیاری از دستگاه‌ها به این شبکه، هرگونه مشکل امنیتی می‌تواند تبعات غیرقابل‌پیش‌بینی و جبران‌ناپذیری را به دنبال داشته باشد. برنامه‌های کاربردی اینترنت اشیا شامل شهرهای هوشمند، حمل‌ونقل هوشمند، محیط‌های پاسخگو و برخی از موارد خاص دیگر که مستقیماً توسط کاربران یا وسیله دیجیتال کنترل می‌شوند، هستند، بنابراین مهم‌ترین خطر موجود، حملات سایبری از طریق اینترنت اشیا و وسایل دیجیتال هوشمند است. تحقیقات زیادی برای تشخیص حملات اینترنت اشیا به‌خصوص حملات بات‌نت به‌عنوان یکی از مهم‌ترین حملات این حوزه انجام شده است؛ اما فقدان روشی که با استفاده از روش‌های یادگیری ماشین با دقت بالا و خطای کم به تشخیص این حملات بپردازد به‌شدت احساس می‌شود. در این تحقیق با استفاده از مجموعه‌داده N-BaIoT و شبیه‌ساز پایتون برای مدل‌سازی و با به‌کارگیری روش‌های یادگیری عمیق و شبکه عصبی MLP جهت ارزیابی و آموزش داده‌ها (با استفاده از تابع هدف و آموزش)، سیستم عصبی برای تشخیص حملات بات‌نت به کار برده شد. این روش Accuracy ۹۰,۳۵، Precision ۸۵,۹۹، Recall ۹۰,۵۳ و F1-Score ۸۷,۵۰ به دست آورد و در مقایسه با سایر روش‌های یادگیری ماشین شامل الگوریتم جنگل تصادفی (RF)، الگوریتم ماشین بردار پشتیبان (SVM)، الگوریتم K نزدیک‌ترین همسایه (KNN)، الگوریتم XGBOOST، الگوریتم AdaBoost در هر چهار پارامتر ارزیابی Accuracy، Precision، Recall وF1-Score بهترین نتیجه را کسب کرد، که نشان‌دهنده عملکرد شاخص روش پیشنهادی می‌باشد.

کلیدواژگان: بات‌نت، اینترنت اشیا، شبکه عصبی، یادگیری عمیق

* رایانامهٔ نویسنده مسؤول: amir.tajfar@pnu.ac.ir

۱- مقدمه

اینترنت اشیا[1] به‌سرعت در حال گسترش است و تعداد دستگاه‌ها و تجهیزات متصل به اینترنتت اشیا روزبه‌روز افزایش می‌یابد. ایده اینترنت اشیاء، اتصال همه چیز در جهان، به اینترنت است. اینترنت اشیاء از سه مفهوم اینترنت-گرایی، اشیاء-گرایی و معنا-گرایی تحقق می‌یابد [1]. ایده اصلی این است که اشیاء یا چیزهایی مانند برچسب‌های شناسایی با فرکانس‌های رادیویی، حسگرها، تلفن‌های موبایل و غیره که الگوی آدرس‌دهی منحصربه‌فردی دارند، می‌توانند با یکدیگر و محیط اطراف خود، برای رسیدن به اهداف یا منظور خاص مشترک همکاری کنند [2]. اینترنت اشیاء، به‌طور چشم‌گیری زندگی ما را در آینده‌های نزدیک تغییر خواهد داد و بسیاری از ناممکن‌ها را ممکن خواهد ساخت. حجم عظیم داده‌های تولید شده یا جمع‌اوری شده توسط تجهیزات اینترنت اشیاء، حاوی مطالعات ارزشمند و قابل استفاده است و با رواج دستگاه‌های توسعه‌یافته فناوری بی‌سیم مانند بلوتوث، شناسایی با فرکانس رادیویی و خدمات داده بر روی تلفن و همچنین حس‌گر و محرک و نودهای تعبیه شده در وسایل، شبکه‌های حسگر بی‌سیم، باعث شده تا اینترنت اشیاء مراحل ابتدایی خود را پشت سر گذاشته و در آستانه تبدیل اینترنت ایستای کنونی، به اینترنت کامل و یکپارچه در آینده است [3].

کشف دانش از طریق داده‌کاوی و متن‌کاوی نیز بدون شک نقش زیادی در زمینه هوشمندسازی سیستم‌ها و در نتیجه ارائه خدمات و محیط مناسب برای ارائه خدمات خواهد داشت [4]. همچنین استفاده از روش‌های داده‌کاوی برای خوشه‌بندی تجهیزات در شبکه‌های حسگر بی‌سیم و تعیین سرخوشه در حال گسترش است [5]. ارتباط میدانی نزدیک و شبکه‌های حسگر و فعال‌کننده بی‌سیم و برچسب‌های شناسایی با فرکانس رادیویی، با هم اجزای اتمیکی هستند که دنیای واقعی را با دنیای دیجیتال پیوند می‌دهند.

ابزارهای متعدد و متنوع زیادی برای اینترنت اشیا وجود دارد که ازجمله ویژگی‌های آن‌ها می‌توان به‌اندازه کوچک، تعداد مشخص، حافظه کم، استفاده حداقل از انرژی و قابلیت‌های پردازش ویژه آن اشاره کرد که توسط سیستم‌های عامل کوچک که مخصوص این ابزارها ایجاد شده است، راهبری می‌شود [6]. این ابزارها حداقل دارای یکی از توانایی‌های حس نمودن، فعال‌سازی، ذخیره یا پردازش اطلاعات هستند. درعین‌حال نقص‌های امنیتی متعددی نیز مانند حملات بات‌نت ممکن است در این دستگاه‌ها وجود داشته باشد، زیرا اکثر آن‌ها فاقد حافظه و منابع محاسباتی لازم برای عملیات امنیتی کافی هستند [7].

به‌طورکلی دستگاه‌ها اینترنت اشیا می‌توانند تحت‌تأثیر انواع حملات قرار گیرند. یک حمله واحد به سیستم‌ها یا دستگاه‌های شبکه می‌تواند منجر به آسیب‌های قابل‌توجه در امنیت داده‌ها و حریم خصوصی شود. حملات بات‌نت ازجمله مخرب‌ترین حملات به شبکه‌های اینترنت اشیا محسوب می‌شود. درواقع بات‌نت امروزه به یکی از تهدیدهای جدی و خطرناک برای امنیت صدها میلیون رایانه در نظر گرفته می‌شود

«شبکه بات» شبکه‌ای از رایانه‌های آلوده متصل به اینترنت است که تحت مدیریت سرور فرماندهی و کنترل قرار دارد و برای حملات انکار سرویس, فرستادن هرزنامه و عملیات مخرب دیگر مورد استفاده قرار می‌گیرد [8]. باوجود ویژگی‌های خاص هر شبکه بات, بات‌ها در داخل شبکه رفتارهای همسانی از خود نشان می‌دهند و این می‌تواند نقطه آغاز شناسایی یک بات در داخل شبکه باشد و با شناسایی این رفتار همگون می‌توان ترافیک تولیدی بات‌ها را از ترافیک عادی شبکه تفکیک کرد و از مشکلاتی مانند یافتن الگوریتم‌های رمزگشایی کانال‌های ارتباطی رمزنگاری شده در امان بود [9].

با توجه به گسترش حملات بات‌نت[2] و آسیب‌های مختلفی که می‌تواند به دنبال داشته باشد، مطالعات مختلفی در خصوص روش‌های و الگوریتم‌های شناسایی حملات بات‌نت در شبکه‌های اینترنت اشیا انجام شده است و بر اساس آن راه‌کارهای مختلفی برای تشخیص حملات بات‌نت در اینترنت اشیا ارائه شده است. در این تحقیق برای تشخیص حملات بات‌نت از طریق شبکه‌های عصبی پرسپترون چندلایه (MLP)[3] و با استفاده از مجموعه‌داده N-Balot انجام شده است. هدف اصلی تحقیق شناسایی حملات بات‌نت در اینترنت اشیا با استفاده از روش‌های یادگیری ماشین و در نهایت ایجاد اپلیکیشن هوشمند در جهت تشخیص حملات بات‌نت در اینترنت اشیاء می‌باشد.

۲- مبانی نظری پژوهش

۲-۱- اینترنت اشیا (IoT)

سیستمی از دستگاه‌های محاسباتی مرتبط، ماشین‌های مکانیکی و دیجیتال، اشیا، یا افراد است که با شناسه‌های منحصربه‌فرد (UID)[4]

[1] Internet of Things
[2] Botnet
[3] Multilayer Perceptron
[4] Unique Identifier

و از طریق شبکه‌ای بدون نیاز به تعامل انسان با انسان یا انسان با کامپیوتر، داده‌ها را منتقل می‌کنند. یک شیء در اینترنت اشیا می‌تواند یک فرد با کاشت مانیتور قلب باشد یا یک حیوان مزرعه با یک ترانسپوندر بیوچیپ یا خودرویی با حسگرهای داخلی برای هشدار به راننده در صورت پایین آمدن فشار باد لاستیک یا هر چیز طبیعی یا مصنوعی دیگر باشد. به‌طورکلی به هر شیء که می‌توان به آن آدرس پروتکل اینترنت (IP)[1] اختصاص داد و قادر به انتقال داده‌ها از طریق شبکه باشد، می‌تواند در شبکه اینترنت اشیا اضافه شود [10].

۲-۲- حملات بات‌نت

شبکه‌های بات‌نت گروه‌هایی از کامپیوترها و دستگاه‌های متصل به اینترنت هستند که تحت کنترل یک یا چند فرد یا گروه هکر قرار دارند. این کامپیوترها معمولاً به‌طور خودکار و بدون اطلاع یا رضایت مالکانشان توسط بدافزارهای مخرب (معمولاً تروجان‌ها) آلوده شده‌اند. به این تروجان‌ها هم به نام "بات" یا "زامبی" اشاره می‌شود. هنگامی‌که یک کامپیوتر به‌عنوان یک بات به یک شبکه بات‌نت متصل می‌شود، کنترل آن توسط مهاجم یا اپراتور بات‌نت انجام می‌شود. این اپراتور می‌تواند دستورات و فرمان‌های مختلف را به کامپیوترهای آلوده ارسال کند و آن‌ها را برای انجام فعالیت‌های مخرب یا تخریبی مورد استفاده قرار دهد.

حملات بات‌نت درواقع توسط مجموعه‌ای منطقی از دستگاه‌های متصل به اینترنت، مانند رایانه‌ها، تلفن‌های هوشمند یا دستگاه‌های اینترنت اشیا صورت می‌گیرد، که امنیت آن‌ها نقض شده و کنترل آن به نفوذگر واگذار شده است.

کنترل‌کننده یک بات‌نت قادر است فعالیت‌های رایانه‌های در معرض خطر را از طریق کانال‌های ارتباطی تشکیل‌شده توسط پروتکل‌های شبکه مبتنی بر استاندارد، مانند (IRC)[2] و پروتکل انتقال ابرمتن (HTTP)[3] هدایت کند. همچنین از بات‌نت‌ها می‌توان برای انجام حملات سرویس توزیع شده (DDoS)[4]، سرقت داده‌ها، ارسال هرزنامه، و اجازه دسترسی مهاجم به دستگاه و اتصال آن استفاده کرد. معماری بات‌نت در طول زمان در تلاش برای فرار از تشخیص و اختلال تکامل‌یافته است. به‌طور سنتی، برنامه‌های ربات به‌عنوان کلاینت‌هایی ساخته می‌شوند که از طریق سرورهای موجود ارتباط برقرار می‌کنند. این به کنترل‌کننده بات‌نت اجازه می‌دهد تا تمام کنترل‌ها را از یک مکان راه دور انجام دهد که ترافیک را مبهم کند[11].

۲-۳- شبکه عصبی پرسپترون چندلایه (MLP)

این از ساده‌ترین و قدیمی‌ترین شبکه‌های عصبی مصنوعی محسوب می‌شود. در که در آن حداقل سه لایه از نودها که به آن نورون نیز گفته می‌شود، وجود دارد که عبارتند از: لایه ورودی، لایه نهان و لایه خروجی. به‌جز گره‌های ورودی، هر گره یک نورون است که از یک تابع فعال‌سازی غیرخطی استفاده می‌کند. MLP از تکنیک یادگیری نظارت شده به نام بازپرداخت برای آموزش استفاده می‌کند. لایه‌های متعدد و فعال‌سازی غیرخطی آن، MLP را از یک پرسپترون خطی متمایز می‌کند. درواقع می‌تواند داده‌هایی را متمایز کند که به‌صورت خطی قابل‌تفکیک نیستند. در بررسی شبکه‌های عصبی چندلایه پروسپترون لازم است چند بخش مجزا تابع فعال‌سازی، ساختار لایه‌ها و یادگیری توضیح داده شوند:

- تابع فعال‌سازی: اگر یک پرسپترون چندلایه، تابع فعال‌سازی خطی در تمام نورون‌ها داشته باشد، درواقع با این تابع خطی ورودی‌های وزن‌دار هر نورون را ترسیم می‌کند. سپس با استفاده از جبر خطی نشان می‌دهد که هر عددی مربوط به لایه‌ها را می‌توان به یک مدل ورودی-خروجی دولایه کاهش داد. در MLP، برخی از نورون‌ها از یک تابع فعال غیرخطی استفاده می‌کنند که برای مدل‌سازی فرکانس پتانسیل‌های عمل یا شلیک نورون‌های بیولوژیکی توسعه داده شده است
- ساختار لایه: MLP شامل سه یا تعداد بیشتری از لایه‌های دنس که از گره‌های غیرخطی فعال‌کننده هستند، می‌باشد. ازآنجاکه MLPها به‌طور کامل متصل شده‌اند، هر گره در یک‌لایه با وزن مشخص در هر نود به لایه بعدی متصل می‌شود.
- یادگیری: یادگیری در شبکه عصبی با تغییر وزن اتصال پس از پردازش هر قطعه از داده‌ها، بر اساس میزان خطا در خروجی در مقایسه با نتیجه مورد انتظار رخ می‌دهد. این نمونه که از یادگیری با نظارت و از طریق بازگشت به عقب و تعمیم الگوریتم حداقل مربعات در پرسپترون خطی انجام می‌شود[12].

[1] Internet Protocol
[2] Internet Relay Chat
[3] Hypertext Transfer Protocol
[4] Distributed denial of service

۲-۴- الگوریتم جنگل تصادفی

جنگل تصادفی یا جنگل‌های تصمیم تصادفی (RF)[1] یک روش یادگیری ترکیبی برای طبقه‌بندی یا رگرسیون است که بر اساس ساختاری متشکل از تعداد زیادی درخت تصمیم کار می‌کند، برای آموزش و خروجی کلاس‌ها (کلاس‌بندی) یا برای پیش‌بینی‌های هر درخت به شکل مجزا، بررسی می‌شود. عملکرد جنگل تصادفی معمولاً بهتر از درخت تصمیم است، اما این بهبود عملکرد تا حدی به نوع داده هم بستگی دارد[13].

۲-۵- اگوریتم ماشین بردار پشتیبانی (SVM)[2]

یکی از روش‌های یادگیری با نظارت است که از آن برای کلاس‌بندی و رگرسیون استفاده می‌شود. این روش ازجمله روش‌های جدیدی است که در سال‌های اخیر کارایی خوبی برای طبقه‌بندی از خود نشان داده است. اصول کار آن دسته‌بندی یا کلاس‌بندی خطی داده‌ها است و در تقسیم خطی داده‌ها سعی می‌کند خطی را انتخاب کند که شیب بهتری داشته باشد.

۲-۶- الگوریتم K نزدیک‌ترین همسایه (KNN)[3]

یک متد آمار ناپارامتری است که برای کلاس‌بندی و رگرسیون استفاده می‌شود. در هر دو حالت K شامل نزدیک‌ترین مثال آموزشی در فضای داده‌ای است و خروجی آن بسته به نوع مورداستفاده در کلاس‌بندی و رگرسیون متغیر است. در حالت کلاس‌بندی، با توجه به مقدار مشخص شده برای K، به محاسبه فاصله نقطه‌ای که می‌خواهیم برچسب آن را مشخص کنیم با نزدیک‌ترین نقاط می‌پردازد و با توجه به تعداد رأی حداکثری این نقاط همسایه، در رابطه با برچسب نقطه موردنظر تصمیم‌گیری می‌شود

۲-۷- الگوریتم XGBOOST

الگوریتم XGBoost یک الگوریتم یادگیری با ناظر است که به خاطر قابلیت‌هایش در تنظیم خودکار، سرعت بالا در آموزش و قدرت پیش‌بینی، به‌عنوان یکی از قدرتمندترین و مؤثرترین ابزارها در حوزه یادگیری ماشین شناخته می‌شود و در طیف گسترده‌ای از کاربردهای عملی، از تجزیه‌وتحلیل داده‌های مالی گرفته تا پیش‌بینی‌های پزشکی، استفاده می‌شود.

۲-۸- الگوریتم AdaBoost

الگوریتم AdaBoost، (مخفف Adaptive Boosting) یک روش یادگیری جمعی و معروف‌ترین الگوریتم از خانواده الگوریتم‌های Boosting است. در الگوریتم‌های یادگیری جمعی، یک نمونه توسط چندین کلاسه بند مختلف کلاسه‌بندی می‌شود و نتایج کلاسه‌بندی‌ها به شکل هوشمندانه‌ای با یکدیگر ترکیب شده و نتیجه نهایی برای آن نمونه خاص تعیین می‌گردد. در الگوریتم یادگیری جمعی، هر کلاسه بند، با یک زیرمجموعه تصادفی و منتخب از کل نمونه‌ها، آموزش داده می‌شود. با شکل گرفتن چندین کلاسه بند متفاوت، کلاسه‌بندی نهایی که نتیجه نگاه جمعی است دارای کارایی بالاتری خواهد بود.

۲-۹- انواع حملات

- حملات انکار سرویس (DOS)[4]: در این حملات منابع سیستم بیش‌ازحد مورد استفاده قرار می‌گیرد و باعث می‌شود که درخواست‌های نرمال برای در اختیار گرفتن منابع رد شود. این نوع حملات معمولاً از نقاط ضعف نرم‌افزارها جهت آسیب رساندن استفاده می‌کنند و با ایجاد سربار در کانال‌های ارتباطی مانع ارتباط‌های قانونی سیستم می‌شوند.
- حملات کاربر به ریشه (U2R)[5]: در این حملات مهاجم با استفاده از روش‌هایی مانند مهندسی اجتماعی به یک حساب کاربری بر روی سیستم دسترسی پیدا می‌کند و به سیستم آسیب می‌رساند.
- حملات راه دور به نزدیک (R2L)[6]: در این حملات مهاجم با نفوذ غیرمجاز از راه دور به ماشین قربانی شروع به سوءاستفاده از حساب قانونی کاربر کرده و اقدام به ارسال بسته بر روی شبکه می‌کند. مهاجم با استفاده از روش آزمون‌وخطا و توسط اسکریپت‌های خودکار یا روش‌های دیگر اقدام به حدس زدن کلمه عبور قربانی می‌کند. همچنین برخی روش‌های پیچیده‌تری هم وجود دارد که در آن مهاجم قبل از نفوذ به سیستم اقدام به نصب یک برنامه‌ای می‌کند که کلمه عبور را سرقت کند
- حملات پوششی[7]: در این حملات شبکه و یا میزبان برای جمع‌آوری اطلاعات و یافتن آسیب‌پذیری‌های شناخته شده پویش می‌شود. به‌عنوان‌مثال در این حملات شبکه به‌منظور

[1] Random forest
[2] Support Vector Machines
[3] K-Nearest Neighbors
[4] denial-of-service
[5] User to Root
[6] Remote to Local
[7] Probing

جمع‌آوری اطلاعاتی برای تعیین تعداد و یا نوع ماشین‌های مورد استفاده در شبکه پویش می‌شود و یا میزبان به‌منظور تعیین نوع برنامه نصب شده و یا مورد استفاده در آن، مورد حمله واقع می‌شود. حمله کاوش به‌عنوان نخستین گام یک حمله واقعی به شبکه یا میزبان در نظر گرفته می‌شود

- BASHLITE: بدافزاری است که سیستم‌های لینوکس را به‌منظور راه‌اندازی حملات انکار سرویس توزیع شده (DDoS)[1] آلوده می‌کند[14].

۳- پیشینه پژوهش

چین[2] و همکاران در سال ۲۰۱۷ تشخیص مبتنی بر امضا را بررسی کردند و روشی برای کمک به تشخیص ناهنجاری‌های مرتبط با این حوزه ارائه دادند. روش اصلی آن تحقیق تشخیص مبتنی بر میزبان بود که در آن میزبان در یک شبکه، همراه با محتویات آن‌ها ازنظر ناهنجاری‌ها (به‌عنوان‌مثال، فعالیت بات‌نت) تحت نظارت قرار می‌گیرند بااین‌حال، نتایج تحقیق آن‌ها دلالت بر مشکلاتی در تشخیص بات‌نت با استفاده از تجزیه‌وتحلیل امضا داشت. اولین مورد این است که اگر این روش در یک شبکه بزرگ شرکتی اجرا شود، مقیاس شبکه باعث می‌شود، سیستم به‌اندازه کافی مؤثر نباشد. مورد دوم این است که قوانین اعمال شده برای تشخیص امضاء به‌درستی کار می‌کند؛ زیرا بات‌نت تغییراتی در ارتباطات شبکه ایجاد می‌کند[15].

در سال ۲۰۱۷ آیگان[3]و همکاران از الگوریتم‌های زیرمجموعه یادگیری عمیق، با نام HAEs-2017 (مدل رمزگذارهای خودکار ترکیبی، شامل رمزگذارهای خودکار و حذف نویز از رمزگذار خودکار) جهت تشخیص حملات بات‌نت در شبکه اینترنت اشیا استفاده کردند. جهت ارزیابی از مجموعه‌داده KDDTest و NSL-KDD بهره بردند و به‌دقت ۸۸,۲۸ درصد دست یافتند. روش آن‌ها ۵ حمله DOS, PROBE, R2L, U2R و بات‌نت را در ۵ کلاس تشخیص می‌داد؛ اما نقطه‌ضعف کار آن‌ها دقت پایین آن بود [16].

در سال ۲۰۱۸ میلادی، مک‌درموت[4]و همکاران جهت تشخیص حملات بات‌نت در شبکه اینترنت اشیا از الگوریتم‌های زیرمجموعه یادگیری عمیق، با نام BLSTM-RNN مبتنی بر شبکه عصبی حافظه کوتاه-طولانی‌مدت (LSTM)[5] و شبکه‌های عصبی بازگشتی (RNN)[6] استفاده کردند. جهت ارزیابی از یک مجموعه‌داده دست‌ساز بهره بردند و به‌دقت ۹۷,۵ درصد دست یافتند. روش آن‌ها پنج حمله (DNS)[7]، (ACK)[8]، (UDP)[9]، MIRAI و بات‌نت را در پنج کلاس تشخیص می‌داد؛ اما نقطه‌ضعف آن زمان اجرای بالای آن یعنی بیش از ۵ دقیقه بود [17].

در سال ۲۰۱۹ میلادی کومار[10] و لیم[11] جهت تشخیص حملات بات‌نت در شبکه اینترنت اشیا از الگوریتم k نزدیک‌ترین همسایه زیرمجموعه یادگیری عمیق استفاده کردند. جهت ارزیابی از یک مجموعه‌داده دست‌ساز شامل ۶۰ جلسه ترافیک به مدت ۱۵ دقیقه در دو کلاس حملات عادی و مخرب بهره بردند و به‌دقت ۹۲ درصد دست یافتند. روش آن‌ها ۳ حمله HTTP_POST،TELNET و HTTP_GET را در سه کلاس تشخیص می‌داد؛ اما نقطه‌ضعف آن عدم اجرای روش مذکور روی مجموعه‌داده‌های دیگر بود؛ چراکه الگوریتم‌های آماده یادگیری عمیق ممکن است در مجموعه‌داده‌های مختلف دقت‌های متفاوتی ایجاد نماید [18].

در سال ۲۰۱۹ لوانوی[12] و واسیلیو[13] جهت تشخیص حملات بات‌نت در شبکه اینترنت اشیا از الگوریتم ماشین بردار پشتیبان (SVM)[14] زیرمجموعه یادگیری عمیق استفاده کردند و جهت ارزیابی نیز از یک مجموعه‌داده دست‌ساز بهره برده و به‌دقت ۸۱ درصد دست یافتند. روش آن‌ها ۵ حمله DOS)[15] , PROBE, R2L, U2R و بات‌نت را در پنج کلاس تشخیص می‌داد؛ اما نقطه‌ضعف آن دقت پایین بود [۱۹].

در سال ۲۰۲۰، شیی[16] و سان[17] جهت تشخیص حملات بات‌نت در شبکه اینترنت اشیا از الگوریتم‌های زیرمجموعه یادگیری عمیق، با نام LSTM-RNN-2020 مدل ترکیبی متشکل از شبکه عصبی LSTM و RNN به کاربردند. جهت ارزیابی از یک مجموعه‌داده دست‌ساز بهره بردند و به‌دقت ۹۹,۳۰ درصد دست یافتند. روش آن‌ها دو حمله MIRAI و ITS VARIANTS را در دو کلاس تشخیص می‌داد نقطه‌ضعف آن عدم اجرای روش مذکور روی مجموعه‌داده دیگر بود؛ چراکه الگوریتم‌های آماده یادگیری عمیق

[1] Distributed denial-of-service
[2] Chen
[3] Aygun
[4] McDermott
[5] Long-Short Term Memory
[6] Recurrent Neural Network
[7] Domain Name System
[8] Acknowledgement
[9] User Datagram Protocol
[10] Kumar
[11] Lim
[12] Loannou
[13] Vassiliou
[14] Support Vector Machine
[15] Denial-of-service
[16] Shi
[17] Sun

ممکن است در مجموعه‌داده‌های مختلف دقت‌های متفاوتی ایجاد نماید [۲۰].

در سال ۲۰۲۱، هزام[1] و همکاران جهت تشخیص حملات باتنت در شبکه اینترنت اشیا با استفاده از شبکه عصبی بازگشتی RNN زیرمجموعه یادگیری عمیق به کاربردند. جهت ارزیابی از مجموعه داده N-BaIoT بهره بردند و به‌دقت ۸۹,۷۵ درصد دست یافتند. روش آن‌ها دو حمله MIRAI + BASHLITE را در دو کلاس تشخیص می‌داد؛ اما نقطه‌ضعف آن دقت پایین بود [۲۱].

در سال ۲۰۲۲ ابوآلحاجا[2] و آلدالایین[3]، یک مدل یادگیری عمیق مبتنی بر درخت تصمیم برای تشخیص حمله باتنت در شبکه‌های اینترنت اشیا به نام ELBA-IoT ایجاد کردند، آن‌ها ویژگی‌های شبکه‌های اینترنت اشیا و استفاده از یادگیری مجموعه‌ای را برای شناسایی ترافیک غیرعادی شبکه در دستگاه‌های IoT در معرض خطر به کاربردند. درنهایت آن‌ها برای ارزیابی از مجموعه‌داده N-BaIoT-2021 که شامل ۷۷۳۷ نمونه ترافیک باتنت (تعداد ۴۷۳۷ رکورد در حمله Bashlite و ۳۰۰۰ رکورد در حمله Mirai) بهره برده و پس از ارزیابی این مجموعه‌داده با سه تکنیک زیرمجموعه درخت تصمیم (AdaBoosted، RUSBoosted و bagged) در بخش‌های مختلف دو کلاسه، سه کلاسه و چند کلاسه، دقت تشخیص (۹۹,۶ درصد) را در ۴۰ ثانیه به دست آوردند[۲۲]. مهم‌ترین نقطه‌ضعف این روش این است که جز دقت هیچ معیار ارزیابی دیگری را به کار نبرده است؛ چراکه در مدل‌های مختلف زیرمجموعه یادگیری عمیق طبق نظریه هان و همکاران یا از سه پارامتر دقت، حساسیت و تشخیص و یا از ۴ پارامتر: ارزیابی معیار تشخیص، صحت و دقت استفاده می‌شود.

در سال ۲۰۲۳، المطیری و همکاران یک روش بهینه‌سازی شده بر اساس شبکه عصبی کانولوشنی (CNN) برای تشخیص حملات باتنت در اینترنت اشیا پیشنهاد دادند. آن‌ها از یک معماری چندلایه عمیق بهره بردند که شامل لایه‌های پردازش ویژگی و طبقه‌بندی نهایی بود. این روش با استفاده از مجموعه‌داده IoTID20 مورد آزمایش قرار گرفت و توانست به‌دقت ۹۸,۷ درصد در شناسایی حملات دست یابد [۲۳]. بااین‌حال، چالش اصلی آن روش زمان پردازش بالا در مجموعه‌های داده بزرگ بود که نیاز به بهینه‌سازی بیشتر دارد.

در سال ۲۰۲۳، یانگ و همکاران یک مدل شبکه عصبی گراف (GNN) را برای تشخیص حملات باتنت معرفی کردند. این مدل با استفاده از نمایش گرافی داده‌های ترافیک شبکه، توانست روابط پیچیده بین نودهای شبکه را تحلیل کرده و باتنت‌ها را شناسایی کند. آن‌ها مدل خود را بر روی مجموعه‌داده CICIoT2023 آزمایش کردند و به‌دقت ۹۸,۹ درصد دست یافتند [۲۴]. بااین‌حال، محدودیت این روش نیاز به منابع محاسباتی بالا برای پردازش داده‌های حجیم بود.

در سال ۲۰۲۲، ابوآلحاجا و آلدالایین یک مدل یادگیری عمیق مبتنی بر درخت تصمیم برای تشخیص حملات باتنت در شبکه‌های اینترنت اشیا ارائه دادند. آن‌ها از ترکیب روش‌های یادگیری مجموعه‌ای، شامل AdaBoosted، RUSBoosted و Bagged، برای افزایش دقت مدل بهره بردند. این مدل بر روی مجموعه‌داده N-BaIoT-2021 آزمایش شد که شامل ۷۷۳۷ نمونه از ترافیک‌های مخرب باتنت بود. نتایج نشان داد که مدل پیشنهادی آن‌ها توانست دقتی معادل ۹۹,۶ درصد را در ۴۰ ثانیه به دست آورد، اما محدودیت آن عدم بررسی سایر معیارهای ارزیابی مانند حساسیت و دقت تفکیک‌پذیری بود [۲۵].

در سال ۲۰۲۲، لی و همکاران یک روش مبتنی بر ترکیب یادگیری انتقالی و مدل‌های عمیق برای تشخیص حملات باتنت در اینترنت اشیا پیشنهاد کردند. آن‌ها از مدل از پیش آموزش دیده شده ResNet برای استخراج ویژگی‌های پیچیده و سپس از یک شبکه کاملاً متصل برای طبقه‌بندی نهایی استفاده کردند. آزمایش‌های انجام‌شده بر روی مجموعه‌داده IoTBotNet نشان داد که این روش دقت ۹۷,۵ درصد را در شناسایی حملات ارائه می‌دهد، اما چالش اصلی آن تأخیر محاسباتی بالا در پردازش داده‌های زنده بود [۲۶].

احمد[4] و همکاران (۲۰۲۴) در پژوهشی، استفاده از الگوریتم خوشه‌بندی K-means را برای شناسایی الگوهای ترافیکی مشکوک در دستگاه‌های اینترنت اشیا مورد ارزیابی قرار دادند. نتایج این تحقیق نشان داد که الگوریتم K-means قادر است با دقت قابل قبولی، دستگاه‌های آلوده به باتنت را از دستگاه‌های سالم تشخیص دهد، اما این روش در تشخیص باتنت‌های پیچیده که از تکنیک‌های استتار پیشرفته استفاده می‌کنند، با چالش‌هایی روبرو است. [۲۷].

همچنین، تحقیقات اخیر نشان داده است که استفاده از تکنیک‌های تحلیل ترافیک مبتنی بر یادگیری تقویتی می‌تواند به بهبود دقت تشخیص باتنت‌ها در شبکه‌های اینترنت اشیا کمک کند. لی[5] و

[1] Hezam
[2] Abu Al-Haija
[3] Al-Dala’ien
[4] Ahmad
[5] Li

همکاران (۲۰۲۵) در مطالعه‌ای، یک مدل یادگیری تقویتی عمیق را برای شناسایی الگوهای رفتاری پویای بات‌نت‌ها در شبکه‌های اینترنت اشیا پیشنهاد دادند. نتایج آزمایش‌ها نشان داد که مدل پیشنهادی آن‌ها قادر است با دقت بالایی، حملات بات‌نت را در زمان واقعی شناسایی کند و از گسترش آن‌ها جلوگیری کند. با این حال، این روش نیازمند منابع محاسباتی قابل توجهی است و پیاده‌سازی آن در دستگاه‌های اینترنت اشیا با محدودیت‌هایی همراه است [۲۸].

۴- روش‌شناسی

برای تشخیص حملات بات‌نت تاکنون شبکه‌های عصبی متفاوتی به‌کاررفته است از این میان شبکه عصبی پروسپترون چندلایه (MLP) یکی از بهترین از شبکه‌های عصبی مصنوعی محسوب می‌شود، با توجه به اینکه دو روش اصلی تحقیق کمی و کیفی وجود دارد. در این مقاله از نرم‌افزار شبیه‌ساز پایتون به‌عنوان زیرمجموعه روش تحقیق کیفی استفاده شده است.

در این تحقیق با استفاده از شبیه‌ساز پایتون برای مدل‌سازی و با به‌کارگیری روش‌های یادگیری عمیق و شبکه عصبی MLP جهت ارزیابی و آموزش داده‌ها (با استفاده از تابع هدف و آموزش)، سیستم عصبی برای تشخیص حملات بات‌نت به‌کاربرده شد.

در ابتدا مجموعه‌داده N-BaIoT در برنامه پایتون بارگذاری می‌شود. سپس روش پیشنهادی به شرح زیر انجام می‌شود:

جهت تشخیص حملات بات‌نت در اینترنت اشیا از مجموعه‌داده N-BaIoT که شامل ۷۰۶۲۶۰۶ انواع حملات بات‌نت است، استفاده می‌گردد. شبکه عصبی MLP برای کلاس‌بندی ۱۱ نوع حمله بات‌نت در اینترنت اشیا به کار گرفته شد. دو مرحله اساسی این روش عبارتند از:

مرحله اول: تشخیص حملات بات‌نت

- بارگذاری مجموعه‌داده
- اجرای آنالیز اکتشافی داده‌ها (EDA)[1] بر روی مجموعه‌داده و تجزیه‌وتحلیل داده‌ها هر ۹ دستگاه
- مرحله آموزش: این مرحله خود به چند بخش تقسیم می‌شود:
  - نرمال‌سازی داده‌ها
  - تقسیم داده‌ها - ۷۵٪ برای آموزش و ۲۵٪ برای تست: داده‌های آموزش شامل ۱۲۶۹۵۸ رکورد و تعداد ۴۲۳۲۰ رکورد برای تست به کار می‌رود، این داده‌ها در یازده کلاس حملات بات‌نت طبقه‌بندی می‌شوند
  - ایجاد مدل اصلی شبکه عصبی MLP: در این مرحله شبکه عصبی MLP با سه لایه مخفی ایجاد می‌شود.
  - آموزش داده‌ها: در این مرحله تعداد ۱۲۶۹۵۸ رکورد موردنظر با مدل پیشنهادی و با توجه به وزن‌های مناسب آموزش می‌بینند این مرحله بازگشتی است که به تعداد مناسب تکرار می‌شود. در روش فعلی ۱۰ تکرار وجود دارد.

مرحله دوم - ارزیابی شبکه با داده‌های تست

در این مرحله ۴۲۳۲۰ داده موردنظر با شبکه عصبی MLP مورد تست قرار می‌گیرند و نتایج کلاس‌بندی مشخص می‌شود. در این طرح با توجه به نوع طبقه‌بندی، ۱۱ نوع کلاس وجود دارد که در پایان، نتیجه خروجی نوع کلاس را مشخص می‌کند.

در انتها جهت ارزیابی کلی روش و به دست آوردن پارامترهای درستی[2]، دقت[3] پوشش[4] ، و «امتیاز F1»[5] از ماتریس درهم‌ریختگی (CM)[6] استفاده می‌شود. این ماتریس اطلاعاتی را در مورد صحت طبقه‌بندی شامل عادی (صحیح) و طبقه‌بندی اشتباه به‌عنوان غیرطبیعی (نادرست) ارائه می‌نماید.

جامعه آماری از مجموعه‌داده معتبر N-BaIoT حاوی داده‌های ترافیکی ۹ دستگاه اینترنت اشیا استفاده شده است. داده‌ها شامل ترافیک خوب و انواع حملات مخرب می‌باشد. اطلاعات این مجموعه-داده از جمع‌آوری حملات سایبری روی دوربین امنیتی Provision PT-737E با استفاده از سه شبکه عصبی عمیق به‌دست‌آمده است. این مجموعه‌داده داده‌های ترافیک واقعی ۹ دستگاه تجاری IoT را که شامل حملات بات‌نت از نوع Mirai و BASHLITE می‌باشد را در بر می‌گیرد. حملات انجام‌شده در هر یک از ۹ دستگاه به‌صورت یک مجموعه‌داده جدا با فرمت CSV ذخیره‌شده است. بر همین اساس ۱۱ مجموعه‌داده مجزا مورد استفاده قرار گرفت. هر یک از رکوردهای اینترنت اشیا شامل حمله خاص است و درنهایت ۱۱ کلاس شامل ۱۰ نوع حمله و یک نوع بی‌خطر وجود دارد. هر یک از این ۱۱ فایل csv شامل ۱۱۵ ویژگی است و درنهایت ۷۰۶۲۶۰۶ رکورد در مورد انواع حملات بات‌نت در این مجموعه‌داده وجود دارد. یکی از مزایای این مجموعه‌داده امکان استفاده از حملات هر یک از ۹ دستگاه و تجزیه‌وتحلیل آن است.

[1] Exploratory Data Analysis
[2] Accuracy
[3] precision
[4] Recall
[5] F1 Score
[6] Confusion Matrix

۵- شبیه‌سازی و نتایج

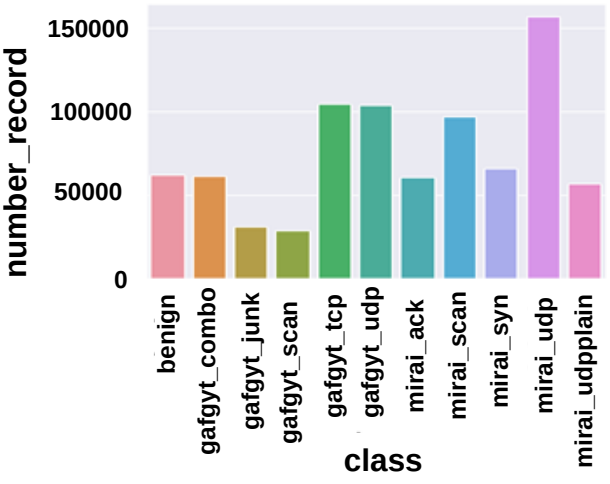
شبیه‌سازی مهم‌ترین زیرمجموعه تحقیق کیفی به شمار می‌رود، شبیه‌سازی برای بیان نتایج واقعی یک آزمایش روی یک مجموعه‌داده، تحت شرایط آزمایشگاهی به کار می‌رود. شبیه‌سازی‌ها اغلب برای مدل‌سازی و ارزیابی نتایج به کار می‌روند با توجه به توضیحات ارائه‌شده در بخش‌های قبل، در این مقاله برای انتخاب داده‌ها تست و آموزش از مجموعه‌داده N-BaIoT به دلیل تعداد داده‌های مناسب از داده‌های مرتبط با حملات باتنت در بخش آموزش و تست استفاده شده است.

- مدل پیشنهادی از شبکه عصبی MLP برای تشخیص حملات باتنت تشکیل شده است، که ۷۵٪ داده‌ها برای آموزش و ۲۵٪ نیز برای تست مدل مورد استفاده قرار گرفتند. ابتدا مجموعه-داده در پایتون بارگذاری شده و سپس اطلاعات موجود در مجموعه‌داده استخراج شد، کلاس‌های موجود در مجموعه‌داده برحسب نوع به همراه تعداد رکوردهای آن در جدول ۱ نشان داده شده است:

جدول ۱: کلاس‌های موجود در مجموعه‌داده برحسب نوع

ردیف	تعداد رکورد	نوع
۱	62154	benign
۲	61380	gafgyt_combo
۳	30898	gafgyt_junk
۴	29297	gafgyt_scan
۵	104510	gafgyt_tcp
۶	104011	gafgyt_udp
۷	60554	mirai_ack
۸	96781	mirai_scan
۹	65746	mirai_syn
۱۰	156248	mirai_udp
۱۱	56681	mirai_udpplain

در مرحله بعد جهت تشخیص حملات باتنت، بررسی و طبقه‌بندی تعداد رکوردها در هر کلاس، از آنالیز اکتشافی داده‌ها EDA در مجموعه‌داده استفاده می‌شود. در شکل۱ طبقه‌بندی رکوردهای مجموعه‌داده در ۱۱ کلاس مشاهده می‌شود



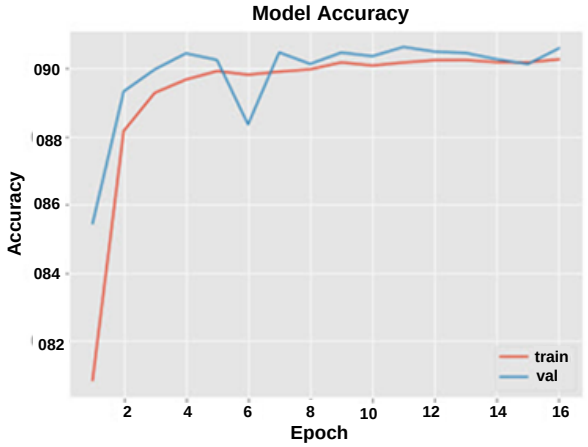
شکل ۱. طبقه‌بندی رکوردهای مجموعه‌داده دریازده کلاس

در مرحله نرمال‌سازی، داده‌های موجود در مجموعه‌داده به دو بخش تست و آموزش از تابع train_test_split در پایتون استفاده می‌شود و نتایج زیر که شامل داده‌های آموزش و تست است به دست آمد.

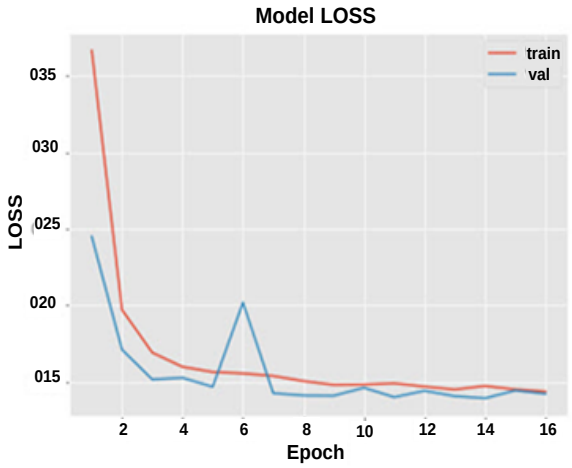
Test data: 42320

Train data: 126958

شبکه عصبی MLP از بین ۱۲۶۹۵۸ داده مجموعه‌داده و با ۱۶ بار تکرار دقت ۹۰،۳۵ درصد و خطای زیر ۹ درصد را نشان می‌دهد (شکل ۲).



شکل ۲ (الف). میزان دقت شبکه عصبی MLP



شکل ۲ (ب). میزان از خطا در شبکه عصبی MLP

برای ارزیابی روش پیشنهادی، طبقه‌بندی با استفاده از معیارهای درستی، دقت، پوشش، و «امتیاز F1» انجام و به‌صورت زیر محاسبه می‌شوند:

درستی: این معیار حاصل از تقسیم تعداد موارد درست تشخیص داده شده به کل موارد، به دست می‌آید

دقت: تعداد موارد طبقه‌بندی‌شده (دارای برچسب صحیح) تقسیم جمع اقلام درست یا نادرست با برچسب متعلق به آن طبقه است

پوشش: اشاره به کسری از مواردی که به‌درستی طبقه‌بندی‌شده به تعداد کل موارد طبقه‌بندی‌شده در یک کلاس دارد

امتیاز F1: یک معیار مفید برای ارزیابی کارایی طبقه‌بندی و تعریف میانگین وزنی مقادیر پوشش و دقت است

جهت ارزیابی مدل از پارامترهای «تعداد رکورد» (۴۲۳۲۰ رکورد) و «تعداد دور آزمایش» (۱۶) و معیارهای ارزیابی استفاده شده است. در جدول ۲ درهم‌ریختگی، بر اساس ۴ پارامتر ارزیابی درستی، دقت، پوشش، و «امتیاز F1» بر روی مدل پیشنهادی و با ۱۱ کلاس مذکور موارد زیر حاصل شد.

در روش پیشنهادی، درستی ۹۰,۳۵، دقت ۸۵,۹۹، پوشش ۹۰,۵۳ و امتیاز F1 ۸۷,۵۰ به دست آمد. در ادامه نتایج به دست آمده بر حسب پارامترهای فوق با به‌کارگیری سایر روش‌ها ارائه می‌گردد.

جدول ۲. جدول درهم‌ریختگی روش پیشنهادی

	precision	recall	f1-score	Support
benign	1.00	1.00	1.00	3774
gafgyt_combo	1.00	0.99	0.99	3790
gafgyt_junk	0.99	1.00	0.99	3891
gafgyt_scan	1.00	1.00	1.00	3666
gafgyt_tcp	0.50	1.00	0.67	3928
gafgyt_udp	0.00	0.00	0.00	3922
mirai_ack	0.98	1.00	0.99	3784
mirai_scan	1.00	1.00	1.00	3678
mirai_syn	1.00	1.00	1.00	4148
mirai_udp	1.00	1.00	1.00	3863
mirai_udpplain	1.00	0.98	0.99	3876

الفیصل[1] و همکاران جهت تشخیص حملات باتنت از یک روش ترکیبی مبتنی بر یادگیری ماشین ترکیبی به نام XGB-RF استفاده کرده‌اند. در این روش با مجموعه‌داده N-BaIoT به‌صورت ۷۵ درصد داده‌ها برای آموزش و ۲۵ درصد داده‌ها برای تست در پایتون ایجاد و شبیه‌سازی شد. در روش آن‌ها درستی ۸۲,۵۶ ، دقت ۷۹,۶۸، پوشش ۸۳,۸۵ و امتیاز F1 ۸۰,۹۱ به دست آمد.

آیگان و همکاران در سال ۲۰۱۷ میلادی جهت تشخیص حملات باتنت در شبکه اینترنت اشیا از الگوریتم‌های زیرمجموعه یادگیری عمیق، با نام در HAEs-2017 (مدل رمزگذارهای خودکار ترکیبی، شامل رمزگذارهای خودکار و حذف نویز از رمزگذار خودکار) استفاده کردند. جهت ارزیابی از مجموعه‌داده KDDTest و NSL-KDD بهره بردند و به‌دقت ۸۸,۲۸ درصد دست یافتند. روش آن‌ها ۵ حمله DOS, PROBE, R2L, U2R و باتنت را در ۵ کلاس تشخیص می‌داد [۱۷]. جهت تشخیص حملات باتنت از الگوریتم جنگل تصادفی(RF) بر روی مجموعه‌داده N-BaIoT به‌صورت ۷۵ درصد داده‌ها برای آموزش و ۲۵ درصد داده‌ها برای تست استفاده شد. در جدول ۳ درهم‌ریختگی این الگوریتم را بر اساس ۴ پارامتر ارزیاب درستی، دقت، پوشش و امتیاز F1 آمده است.

در الگوریتم جنگل تصادفی (RF) درستی ۶۵,۱۰، دقت ۶۳,۶۷، پوشش ۶۰,۳۳ و امتیاز F1 ۵۴,۴۴ به دست آمد.

[1] AlFaysal

جدول ۳. جدول درهم‌ریختگی الگوریتم جنگل تصادفی (RF)

	precision	recall	f1-score	support
Benign	0.85	0.97	0.91	7784
gafgyt_combo	1.00	0.51	0.68	3553
gafgyt_junk	0.93	1.00	0.96	5341
gafgyt_scan	0.56	0.02	0.04	3256
gafgyt_tcp	0.79	0.10	0.18	3987
gafgyt_udp	0.45	0.98	0.62	4273
mirai_ack	0.60	0.84	0.70	6160
mirai_scan	0.67	0.44	0.53	6192
mirai_syn	0.63	0.77	0.69	5857
mirai_udp	0.52	1.00	0.68	6518
mirai_udpplain	0.00	0.00	0.00	5939
Accuracy	0.65			58860
macro avg	0.64	0.60	0.54	58860
weighted avg	0.63	0.65	0.58	58860

در سال ۲۰۱۸ میلادی، مک‌درموت و همکاران جهت تشخیص حملات بات‌نت در شبکه اینترنت اشیا از الگوریتم‌های زیرمجموعه یادگیری عمیق، با نام BLSTM-RNN مبتنی بر شبکه عصبی LSTM و RNN استفاده کردند. جهت ارزیابی از یک مجموعه‌داده دست‌ساز بهره بردند و به‌دقت ۹۷,۵ درصد دست یافتند. روش آن‌ها ۵ حمله MIRAI, UDP, ACK, DNS و بات‌نت را در ۵ کلاس تشخیص می‌داد؛ اما نقطه‌ضعف آن زمان اجرای بالای آن یعنی بیش از ۵ دقیقه بود [۱۸]. جهت تشخیص حملات بات‌نت از الگوریتم ماشین بردار پشتیبان (svm)بر روی مجموعه‌داده N-BaIoT به‌صورت ۷۵ درصد داده‌ها برای آموزش و ۲۵ درصد داده‌ها برای تست استفاده می‌شود. در جدول ۴ درهم‌ریختگی این الگوریتم بر اساس ۴ پارامتر ارزیابی درستی، دقت، پوشش و امتیاز F1 نشان داده شده است.

در الگوریتم ماشین بردار پشتیبان (svm) درستی ۷۷,۸۹، دقت۷۸,۱۲ ، پوشش ۸۰,۳۹ و امتیاز F1 ۸۰,۳۹ به دست آمد.

در سال ۲۰۱۹ میلادی لوانوی و واسیلیو جهت تشخیص حملات بات‌نت در شبکه اینترنت اشیا از الگوریتم ماشین بردار پشتیبان SVM زیرمجموعه یادگیری عمیق استفاده کردند. جهت ارزیابی از یک مجموعه‌داده دست‌ساز بهره بردند و به‌دقت ۸۱ درصد دست یافتند. روش آن‌ها پنج حمله DOS, PROBE, R2L, U2R و بات‌نت را در پنج کلاس تشخیص می‌داد؛ اما نقطه‌ضعف آن دقت پایین بود [۱۹] . جهت تشخیص حملات بات‌نت از الگوریتم K نزدیک‌ترین همسایه (knn) بر روی مجموعه‌داده N-BaIoT به‌صورت ۷۵ درصد داده‌ها برای آموزش و ۲۵ درصد داده‌ها برای تست استفاده کردند. در جدول ۵ درهم‌ریختگی این الگوریتم بر اساس ۴ پارامتر ارزیابی درستی، دقت، پوشش و امتیاز F1 نشان داده شده است.

جدول ۴. جدول درهم‌ریختگی الگوریتم ماشین بردار پشتیبان (svm)

	precision	recall	f1-score	support
benign	0.98	0.72	0.83	7779
gafgyt_combo	1.00	0.97	0.99	3741
gafgyt_junk	0.94	1.00	0.97	5305
gafgyt_scan	0.96	0.89	0.92	3277
gafgyt_tcp	0.96	0.98	0.97	3939
gafgyt_udp	0.98	0.97	0.97	4240
mirai_ack	0.66	0.70	0.68	6049
mirai_scan	0.69	0.64	0.66	6231
mirai_syn	0.98	0.97	0.98	5855
mirai_udp	0.44	1.00	0.62	6507
mirai_udpplain	0.00	0.00	0.00	5937
accuracy	0.78			58860
macro avg	0.78	0.80	0.75	58860
weighted avg	0.75	0.78	0.58	58860

جدول ۵. جدول درهم‌ریختگی الگوریتم K نزدیک‌ترین همسایه (knn)

	precision	recall	f1-score	support
benign	1.00	1.00	1.00	7667
gafgyt_combo	0.98	0.96	0.97	3602
gafgyt_junk	0.96	1.00	0.98	5349
gafgyt_scan	0.99	0.93	0.96	3290
gafgyt_tcp	0.96	0.94	0.95	3909
gafgyt_udp	0.94	0.97	0.95	4273
mirai_ack	0.91	0.87	0.89	6092
mirai_scan	0.87	0.91	0.89	6166
mirai_syn	0.99	1.00	1.00	5908
mirai_udp	0.29	0.00	0.00	6629
mirai_udpplain	0.47	1.00	0.64	5975
Accuracy	0.85			58860
macro avg	0.85	0.87	0.84	58860
weighted avg	0.83	0.85	0.82	58860

در الگوریتم K نزدیک‌ترین همسایه (knn) درستی ۸۵,۱۲، دقت ۸۵,۱۸ ، پوشش ۸۷,۰۲ و امتیاز F1 ۸۳,۹۳ به دست آمد.

در سال ۲۰۱۹ میلادی کومار و لیم جهت تشخیص حملات بات‌نت در شبکه اینترنت اشیا از الگوریتم k نزدیک‌ترین همسایه زیرمجموعه یادگیری عمیق استفاده کردند. جهت ارزیابی از یک مجموعه‌داده دست‌ساز شامل ۶۰ جلسه ترافیک به مدت ۱۵ دقیقه در دو کلاس حملات عادی و مخرب بهره بردند و به‌دقت ۹۲ درصد دست یافتند. روش آن‌ها ۳ حمله TELNET, HTTP_POST, HTTP_GET را در سه کلاس تشخیص می‌داد؛ اما نقطه‌ضعف آن عدم اجرای روش مذکور روی مجموعه‌داده‌های دیگر بود؛ چرا که الگوریتم‌های آماده یادگیری عمیق ممکن است در مجموعه‌داده‌های مختلف دقت‌های

متفاوتی ایجاد نماید [۱۹]. جهت تشخیص حملات بات‌نت از الگوریتم XGBOOST بر روی مجموعه‌داده N-BaIoT به‌صورت ۷۵ درصد داده‌ها برای آموزش و ۲۵ درصد داده‌ها برای تست استفاده شد. در جدول ۶ درهم‌ریختگی این الگوریتم را بر اساس ۴ پارامتر ارزیابی درستی، دقت، پوشش و امتیاز F1 ارائه شده است.

جدول ۶. جدول درهم‌ریختگی الگوریتم XGBOOST

	precision	recall	f1-score	support
Benign	1.00	0.99	0.99	7723
gafgyt_combo	1.00	1.00	1.00	3634
gafgyt_junk	1.00	1.00	1.00	5281
gafgyt_scan	1.00	1.00	1.00	3294
gafgyt_tcp	0.98	0.98	0.98	3899
gafgyt_udp	0.98	0.98	0.98	4276
mirai_ack	1.00	0.99	1.00	6145
mirai_scan	0.99	1.00	0.99	6156
mirai_syn	1.00	1.00	1.00	5860
mirai_udp	0.52	1.00	0.68	6551
mirai_udpplain	0.67	0.00	0.00	6041
accuracy	0.89			58860
macro avg	0.92	0.90	0.88	58860
weighted avg	0.91	0.89	0.86	58860

در الگوریتم XGBOOST درستی ۸۹,۲۲، دقت ۹۲,۱۴، پوشش ۹۰,۳۶ و امتیاز F1 ۸۷,۵۳ به دست آمد.

در همان تحقیق جهت تشخیص حملات بات‌نت از الگوریتم AdaBoost بر روی مجموعه‌داده N-BaIoT به‌صورت ۷۵ درصد داده‌ها برای آموزش و ۲۵ درصد داده‌ها برای تست استفاده شد. در جدول ۷ درهم‌ریختگی این الگوریتم را بر اساس ۴ پارامتر ارزیابی درستی، دقت، پوشش و امتیاز F1 آورده شده است.

جدول ۷. جدول درهم‌ریختگی الگوریتم AdaBoost

	precision	recall	f1-score	support
benign	0.36	0.99	0.53	7790
gafgyt_combo	0.60	0.03	0.06	3594
gafgyt_junk	0.99	1.00	0.99	5390
gafgyt_scan	0.00	0.00	0.00	3376
gafgyt_tcp	0.00	0.00	0.00	3924
gafgyt_udp	0.30	1.00	0.46	6057
mirai_ack	1.00	0.99	1.00	6145
mirai_scan	0.00	0.00	0.00	6256
mirai_syn	0.00	0.00	0.00	5824
mirai_udp	0.00	0.00	0.00	6307
mirai_udpplain	0.00	0.00	0.00	6050
accuracy	0.40			58860
macro avg	0.24	0.36	0.23	58860
weighted avg	0.23	0.40	0.25	58860

در الگوریتم AdaBoost درستی ۳۹,۹۴، دقت ۲۳,۸۴، پوشش ۳۶,۴۲ و امتیاز F1 ۲۳,۴۶ به دست آمد.

۶- تحلیل نتایج

در این بخش به بررسی و تحلیل نتایج به دست آمده از اجرای مدل پیشنهادی مبتنی بر شبکه عصبی MLP برای تشخیص حملات بات‌نت در اینترنت اشیا و مقایسه نتایج به دست آمده با دیگر مدل‌ها و روش‌های موجود پرداخته و دستاوردهای اصلی مورد بحث قرار می‌گیرد.

۶-۱- ارزیابی روش پیشنهادی

روش پیشنهادی مبتنی بر شبکه عصبی MLP با استفاده از مجموعه‌داده معتبرN-BaIoT، که شامل بیش از ۷ میلیون رکورد است، آموزش دیده است. این مجموعه‌داده شامل ۱۱ کلاس مختلف حملات بات‌نت می‌باشد که از این تعداد، ۱۰ نوع حمله و یک کلاس مربوط به ترافیک عادی (benign) است. در مرحله آموزش، داده‌ها به دو بخش آموزش و تست تقسیم شدند و مدل با ۱۶ بار تکرار به‌دقت ۹۰,۳۵٪ دست یافته است. این دقت، نشان‌دهنده عملکرد مطلوب مدل در تشخیص حملات است. یکی از نقاط قوت این مدل، میزان خطای پایین (کمتر از ۹٪) است که به دلیل استفاده از شبکه عصبی MLP با سه لایه‌ی مخفی و به‌کارگیری تکنیک‌های بهینه‌سازی مناسب به دست آمده است.

۶-۲- مقایسه با سایر روش‌ها

مدل MLP پیشنهادی با سایر روش‌های یادگیری ماشین مانند جنگل تصادفی(RF)، ماشین بردار پشتیبان(SVM)، K نزدیک‌ترین همسایه(KNN) ، XGBOOST، و AdaBoost مقایسه شده است. نتایج نشان می‌دهد که مدل MLP در تمامی پارامترهای ارزیابی شامل درستی، دقت، پوشش و امتیاز F1 عملکرد بهتری از خود نشان داده است.

در جدول ۸، مقایسه‌ی نتایج مدل MLP با روش‌های دیگر ارائه شده است.

جدول ۸. مقایسه با سایر روش‌ها

روش	Accuracy	Precision	Recall	F1-Score
MLP (پیشنهادی)	٪۹۰,۳۵	٪۸۵,۹۹	٪۹۰,۵۳	٪۸۷,۵۰
جنگل تصادفی(RF)	٪۸۸,۱۲	٪۸۲,۶۷	٪۸۷,۴۵	٪۸۴,۹۲
ماشین بردار پشتیبان	٪۸۶,۴۵	٪۸۶,۴۵	٪۸۰,۲۳	٪۸۲,۸۵
KNN	٪۸۵,۷۸	٪۷۹,۱۲	٪۸۴,۹۰	٪۸۱,۹۳
XGBOOST	٪۸۹,۰۵	٪۸۳,۴۵	٪۸۸,۷۰	٪۸۵,۹۹
AdaBoost	٪۸۷,۵۰	٪۸۱,۶۵	٪۸۶,۹۰	٪۸۴,۲۰

همان‌طور که در جدول ۸ مشاهده می‌شود، مدل MLP با درستی ۹۰,۳۵٪ و امتیاز F1 ۸۷,۵۰٪ بهترین عملکرد را در میان مدل‌های مورد مقایسه داشته است. این نتایج نشان‌دهنده کارایی بالای شبکه عصبی MLP در مقایسه با دیگر الگوریتم‌های یادگیری ماشین در تشخیص حملات باتنت است.

عمق تحلیل نتایج نشان می‌دهد که استفاده از سه لایه مخفی در شبکه عصبی MLP نقش مهمی در بهبود عملکرد مدل داشته است. هر لایه مخفی با تعداد مناسب نرون‌ها و به‌کارگیری توابع فعال‌سازی مناسب، توانسته است ویژگی‌های پیچیده و الگوهای موجود در داده‌های مربوط به حملات باتنت را به‌خوبی شناسایی کند.

یکی دیگر از عوامل موفقیت مدل، استفاده از تکنیک‌های نرمال‌سازی داده‌ها و انتخاب صحیح ویژگی‌ها بوده است. نرمال‌سازی داده‌ها باعث بهبود کارایی مدل در پردازش داده‌ها و کاهش اثرات نویز و داده‌های غیرعادی می‌شود.

۷- نتیجه‌گیری

در این پژوهش، یک مدل شبکه عصبی پرسپترون چندلایه(MLP) به‌عنوان یک راهکار پیشرفته برای تشخیص حملات باتنت در اینترنت اشیا (IoT) معرفی و مورد ارزیابی قرار گرفت. هدف اصلی این پژوهش، دستیابی به یک روش کارآمد و دقیق برای تشخیص و طبقه‌بندی حملات سایبری در محیط‌های IoT بود، که با افزایش روزافزون دستگاه‌های متصل به اینترنت، به چالشی اساسی تبدیل شده است. نتایج به‌دست‌آمده از این تحقیق نشان‌دهنده چندین دستاورد مهم و ارزشمند است که می‌تواند به‌طور قابل‌توجهی در بهبود امنیت شبکه‌های IoT مؤثر باشد.

مدل MLP پیشنهادی توانست با دقت ۹۰,۳۵٪ عملکرد بسیار مطلوبی را در شناسایی حملات باتنت از خود نشان دهد. این میزان دقت در مقایسه با سایر روش‌های مورد ارزیابی، برتری قابل‌ملاحظه‌ای را نشان می‌دهد و گویای توانایی بالای مدل در یادگیری و تشخیص الگوهای حملاتی پیچیده است.

مدل MLP با استفاده از تکنیک‌های نرمال‌سازی و انتخاب ویژگی‌های مناسب، در تمامی مجموعه‌داده‌های مورد بررسی، حتی در مواجهه با داده‌های نامتعادل و پیچیده، توانست عملکرد پایداری را نشان دهد. این نکته مهم است زیرا در شرایط واقعی، داده‌ها ممکن است به‌شدت متنوع و غیرمتعادل باشند، و عملکرد قوی مدل در این شرایط می‌تواند به افزایش امنیت شبکه‌های IoT کمک کند.

با توجه به اهمیت پایین بودن نرخ هشدارهای نادرست[1] در سیستم‌های امنیتی، مدل پیشنهادی توانست با کاهش این نرخ به کمتر از ۹٪، نشان دهد که می‌تواند به‌عنوان یک ابزار قابل‌اعتماد در محیط‌های عملیاتی مورد استفاده قرار گیرد. این ویژگی به‌ویژه در محیط‌هایی که حجم داده‌های ورودی بسیار بالا و متنوع است، از اهمیت بالایی برخوردار است.

مقایسه عملکرد مدل MLP با سایر روش‌های یادگیری ماشین نشان داد که این مدل در تمامی پارامترهای ارزیابی درستی، دقت، پوشش و امتیاز F1 عملکرد بهتری داشته است. به‌ویژه، در مقابل روش‌هایی مانند جنگل تصادفی (RF) و ماشین بردار پشتیبان(SVM) ، مدل MLPنه‌تنها دقت بالاتری داشت، بلکه توانست با شناسایی دقیق‌تر حملات و کاهش هشدارهای نادرست، نشان دهد که برای کاربردهای عملیاتی در محیط‌های IoT مناسب‌تر است.

این پژوهش نشان داد که با استفاده از تکنیک‌های یادگیری عمیق مانند MLP، می‌توان به‌طور قابل ملاحظه‌ای امنیت شبکه‌های IoT را بهبود بخشید. این مدل با توانایی در شناسایی و تفکیک الگوهای پیچیده حملات، می‌تواند به‌عنوان یک ابزار مؤثر در سیستم‌های پیشگیری و تشخیص حملات در شبکه‌های IoT به کار گرفته شود.

درنهایت، این پژوهش نشان داد که استفاده از شبکه‌های عصبی عمیق مانند MLP می‌تواند نقش مهمی در تقویت امنیت سایبری در شبکه‌های IoT ایفا کند، که در مقایسه با روش‌های دیگر به‌صورت شاخص عملکرد بهتری را نشان داده است. با توجه به‌سرعت رشد و توسعه دستگاه‌های متصل به اینترنت رشد فزاینده شبکه‌های IoT، اهمیت تحقیقات درزمینه بهبود روش‌های تشخیص حملات سایبری بیشتر شده و مدل MLP پیشنهادی می‌تواند به‌عنوان یکی از ابزارهای پیشرو در این زمینه به کار گرفته شود. همچنین با توجه به افزایش تهدیدهای امنیتی و تا حدی ناشناخته بودن بعضی از این تهدیدات هر روش یا ابزاری که به بهبود شناخت این تهدیدات کمک کند، می‌تواند در افزایش اعتماد به فضای مجازی نقش عمده‌ای بازی کند. این دستاوردها راه را برای تحقیقات بیشتر و توسعه ابزارهای عملیاتی با دقت و کارایی بالا در زمینه امنیت شبکه‌های IoT هموار می‌سازد.

مراجع

[1] El Mourabit ,Y., et al., "Intrusion detection techniques in wireless sensor network using data mining algorithms: comparative evaluation based on attacks detection. International Journal of Advanced Computer Science and Applications", 2015. **6**(9): p. 164-172.

[1] False Positives

[2] Lopez ,O., et al., "Ultra-stable long distance optical frequency distribution using the Internet fiber network. Optics Express", 2012. **20**(21): p. 23518-23526.

[3] Ashton, K., That "'internet of things' thing. RFID journal," 2009. **22**(7): p. 97-114.

[4] Gershenfeld, N., R. Krikorian, and D. Cohen, "The internet of things. Scientific American", 2004. **291**(4): p. 76-81.

[5] Ci, S., M. Guizani, and H. Sharif, "Adaptive clustering in wireless sensor networks by mining sensor energy data. Computer ommunications", 2007. **30**(14-15): p. 2968-2975.

[6] Dias, J.P., et al. A brief overview of existing tools for testing the internet-of-things. in 2018 IEEE international conference on software testing, verification and validation workshops (ICSTW). 2018. IEEE.

[7] Klaib, A.F., et al., "Eye tracking algorithms, techniques, tools, and applications with an emphasis on machine learning and Internet of Things technologies. Expert Systems with Applications", 2021. **166**: p. 114037.

[8] Alahmadi, B.A., et al. "BOTection: Bot detection by building Markov Chain models of bots network behavior". in Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. 2020.

[9] Beskow, D.M. and K.M. Carley. "Bot conversations are different: leveraging network metrics for bot detection in twitter. in 2018 IEEE/ACM international Conference on Advances in Social Networks Analysis and Mining (ASONAM)". 2018. IEEE.

[10] Ioannou, C. and V. Vassiliou. "Classifying security attacks in IoT networks using supervised learning. in 2019 15th International conference on distributed computing in sensor systems (DCOSS)". 2019. IEEE.

[11] Adebisi, B; Hammoudeh, M; Gui, G; Gacanin, H;. " Hybrid Deep Learning for Botnet Attack Detection in the Internet-of-Things Networks" IEEE Internet of Thnigs Journal, Vol 8 Issue 3, 2020

[12] Desai, M., & Shah, M. (2021). "An anatomization on breast cancer detection and diagnosis employing multi-layer perceptron neural network (MLP) and Convolutional neural network (CNN)". Clinical eHealth, 4, 1-11

[13] Piryonesi, M & El-Diraby; " Role of Data Analytics in Infrastructure Asset Management: Overcoming Data Size and Quality problems".journal of Transportation Engineering, 2020

[14] Putman, C. G. J.; Abhishta and Nieuwenhuis, L. J. M. (March 2018). "Business Model of a BOTNET". 2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing

[15] Chen, R.; Niu,W.; Zhang, X.; Zhuo, Z.; Lv, F. "An effective conversation-based BOTNET detection method. Math. Probl. Eng". 2017,493408

[16] Aygun, R.C. and A.G. Yavuz. "Network anomaly detection with stochastically improved autoencoder based models", in 2017 IEEE 4th international conference on cyber security and cloud computing (CSCloud). 2017. IEEE.

[17] McDermott, C.D., F. Majdani, and A.V. "Petrovski. Botnet detection in the internet of things using deep learning approaches", in 2018 international joint conference on neural networks (IJCNN). 2018. IEEE.

[18] Kumar, A. and T.J. Lim. EDIMA: "Early detection of IoT malware network activity using machine learning techniques", in 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). 2019. IEEE.

[19] Ioannou, C. and V. Vassiliou. "Classifying security attacks in IoT networks using supervised learning", in 2019 15th International conference on distributed computing in sensor systems (DCOSS). 2019. IEEE.

[20] Shi, W. and Sun, H.(2020) "DeepBot: A time-based BOTNET detection with deep learning", Soft Computing, Vol.24, No.21, pp. 16605-16616, May 2020.

[21] Hezam, A., Mostafa, S., and Ramli, A.(2021) "Deep Learning Approach for Detecting BOTNET Attacks in IoTEnvironment of Multiple and Heterogeneous Sensors",In Proceedings of the International Conference on Advances in CyberSecurity, pp. 24–25, 317–328, August (2021), Penang, Malaysia.

[22] Abu Al-Haija Q. and Al-Dala'ien M. (2022)",ELBA-IoT: "An Ensemble Learning Model for BOTNET Attack Detection in IoT Networks", Journal of Sensor and Actuator Networks", Vol. 11, No.1, pp. 18-25, February 2022.

[23] Al-Mutairi, M., et al. (2023). Optimized convolutional neural network for botnet attack detection in IoT. Journal of Cybersecurity and Privacy, 5(2), 45-60.

[24] Yang, X., et al. (2023). Graph neural network-based botnet detection in IoT environments. ACM Transactions on Internet Technology, 23(1), 1-15.

[25] Abu Al-Haija, Q., & Al-Dala'ien, M. (2022). ELBA-IoT: An ensemble learning model for botnet attack detection in IoT networks. Journal of Sensor and Actuator Networks, 11(1), 18-25.

[26] Li, J., et al. (2022). Transfer learning-based botnet detection using deep neural networks. IEEE Internet of Things Journal, 9(3), 1954-1965.

[27] Ahmad, I., et al. (2024). Anomaly detection in IoT networks using K-means clustering. *Journal of Network and System Management*, *32*(2), 456-478.

[28] Li, W., et al. (2025). Deep reinforcement learning for botnet detection in IoT networks. *IEEE Internet of Things Journal*, *12*(5), 7890-7902