Electronic and Cyber Defens 2025/ Vol. 13/ No. 2/ 9-25

Electronic and Cyber Defens

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

An Attack Detection System in Internet of Things with Deep Learning Based on VGG16 Architecture and Siberian Tiger Optimization Algorithm (STO)

M. Eghbali[1], M.R. Mollhoseini Ardakani[2*], A. Heidary-Sharifabad[3]

[1] PhD Student, Computer Engineering, Department of Computer Engineering, Meybod Branch, Islamic Azad University, Meybod, Iran Email: m.eghbali@maybodiau.ac.ir(

[2] Associate Professor, Department of Computer Engineering, Maybod Branch, Islamic Azad University, Maybod, Iran Email:([*]Correspondence: Mr.mollahoseini@iau.ac.ir)

[3]Associate Professor, Department of Computer Engineering, Maybod Branch, Islamic Azad University, Maybod, Iran Email: ahmad.heidary@iau.ac.ir

ARTICLE INFO

Article history:

Article Type: Research paper

Received: 05 April 2025

Revised: 09 May 2025

Accepted: 16 June 2025

Available online: 22 June 2025

Keywords:

Internet of Things (IoT)

Intrusion Detection System (IDS)

Deep Learning

VGG16 Neural Network

Siberian Tiger Optimization (STO) Algorithm

ABSTRACT

One of the significant challenges in the Internet of Things is the presence of attacking nodes called botnets. Many nodes are infected with malware in these attacks and perform attacks against network services, such as distributed denial of service. In most cases, botnets target application services in the cloud computing layer. For this reason, it is essential to detect attacks in the Internet of Things as an intermediate layer. Providing a distributed intrusion detection system in the Internet of Things increases the ability to detect intrusion and has a high ability to analyze a large volume of network traffic. Deep learning methods such as convolutional neural networks have a high ability to recognize complex patterns in images. In this article, to use CNN network architecture in network intrusion detection, network traffic is coded in the form of images in a new way. Network traffic images are used to train the VGG16 model, a CNN technique. In the proposed method to focus the proposed penetration detection system, the Siberian tiger optimization algorithm is used to select features and reduce dimensions. The proposed intrusion detection system is trained on the NSL-KDD dataset. The evaluations showed that it has accuracy, sensitivity, and precision equal to 99.62%, 99.38%, and 98.74%, respectively. In the feature selection phase, the proposed method is more accurate than WOA, HHO, and AO algorithms. The proposed method is more accurate in detecting network attacks than CNN, VGG16, Muhti-CNN, and PSO-CNN methods.

Cite this article: Eghbali, M.©, Mollhoseini Ardakani, M. R.©, Heidary-Sharifabad, A.© (2025). An Attack Detection System in Internet of Things with Deep Learning Based on VGG16 Architecture and Siberian Tiger Optimization Algorithm (STO). Journal of Electronic and Cyber Defens. 2025; 13l(2):9-25.
DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.2.2.9

Publisher: Imam Hossein University.

پدافند الکترونیک و سایبری/ سال ۱۴۰۴/ دوره ۱۳/ شماره ۲/ صفحه ۲۵-۹

پدافند الکترونیک و سایبری

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

یک سیستم تشخیص حملات در اینترنت اشیا با یادگیری عمیق مبتنی بر معماری VGG16 و الگوریتم بهینه‌سازی ببر سیبری

محسن اقبالی[1*]، محمدرضا ملاحسینی اردکانی[2]، احمد حیدری شریف آباد[3]

[1] دانشجوی دکتری، گروه کامپیوتر، واحد میبد، دانشگاه آزاد اسلامی، میبد، ایران (m.eghbali@maybodiau.ac.ir)

[2] استادیار، گروه کامپیوتر، واحد میبد، دانشگاه آزاد اسلامی، میبد، ایران (نویسنده مسئول: Mr.mollahoseini@iau.ac.ir)

[3] استادیار، گروه کامپیوتر، واحد میبد، دانشگاه آزاد اسلامی، میبد، ایران (ahmad.heidary@iau.ac.ir)

چکیده (استایل عنوان چکیده)

یکی از چالش‌های عمده در اینترنت اشیا وجود گره‌های حمله‌کننده به نام بات نت است. در این حملات تعداد زیادی گره به بدافزار آلوده شده و بر علیه سرویس‌های شبکه حملاتی مانند رد سرویس خدمات توزیع شده را انجام می‌دهند. بات نت‌ها در بیشتر موارد سرویس‌های کاربردی در لایه ابر محاسباتی را هدف قرار می‌دهند و ازاین‌جهت تشخیص حملات در اینترنت اشیا به‌عنوان یک‌لایه میانی از اهمیت بالایی برخوردار است. ارائه یک سیستم تشخیص نفوذ توزیع شده در اینترنت اشیا توانایی تشخیص نفوذ را افزایش می‌دهد و توانایی بالایی برای تحلیل حجم زیاد ترافیک شبکه دارد. روش‌های یادگیری عمیق نظیر شبکه عصبی کانولوشن توانایی بالایی برای تشخیص الگوهای پیچیده در تصاویر دارند. در این مقاله برای استفاده از معماری شبکه CNN در تشخیص نفوذ به شبکه، ترافیک شبکه به‌صورت تصاویر به شیوه جدید کدگذاری می‌شود. تصاویر ترافیک شبکه برای آموزش مدل VGG16 که یک تکنیک CNN است استفاده می‌شود. در روش پیشنهادی برای تمرکز سیستم تشخیص نفوذ پیشنهادی، از الگوریتم بهینه‌سازی ببر سیبری برای انتخاب ویژگی و کاهش ابعاد استفاده می‌شود. سیستم تشخیص نفوذ پیشنهادی روی مجموعه‌داده NSL-KDD آموزش داده می‌شود و ارزیابی‌ها نشان داد دارای دقت، حساسیت و صحتی به ترتیب برابر ۹۹/۶۲٪، ۹۹/۳۸٪ و ۹۸/۷۴٪ است. روش پیشنهادی در فاز انتخاب ویژگی نسبت به الگوریتم بهینه‌سازی وال، بهینه‌سازی شاهین و بهینه‌سازی عقاب طلایی دقت بیشتری دارد. روش پیشنهادی در تشخیص حملات به شبکه از روش‌های CNN، VGG16، Multi-CNN و PSO-CNN دقت بیشتری دارد.

مشخصات مقاله

تاریخچه مقاله:

نوع مقاله: علمی پژوهشی

دریافت: ۱۴۰۴/۱/۱۶

بازنگری: ۱۴۰۴/۲/۱۹

پذیرش: ۱۴۰۴/۳/۲۶

ارائه آنلاین: ۱۴۰۴/۴/۰۱

کلید واژه‌ها:

اینترنت اشیا

سیستم تشخیص نفوذ

یادگیری عمیق

شبکه عصبی VGG16

الگوریتم بهینه‌سازی ببر سیبری

استناد: ملاحسینی اردکانی، محمدرضا©، اقبالی، محسن©، حیدری شریف آباد، احمد©. یک سیستم تشخیص حملات در اینترنت اشیا با یادگیری عمیق مبتنی بر معماری VGG16 و الگوریتم بهینه‌سازی ببر سیبری. پدافند الکترونیک و سایبری. (۱۴۰۴)؛ ۱۳ (۲): ۲۵-۹.

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.2.2.9

ناشر: دانشگاه جامع امام حسین(ع).

۱- مقدمه

عملکرد سیستم‌های فناوری اطلاعات و ارتباطات[1] در تمام جنبه های صنعت و زندگی انسان حیاتی است. در دهه های اخیر، سازمان‌های متعددی در برابر حملات سایبری[2] پیچیده آسیب‌پذیر شده‌اند که منجر به شکل‌گیری سیستم‌های تشخیص نفوذ[3] شده است. سیستم‌های تشخیص نفوذ یک روش امنیتی شبکه استفاده نشده برای شناسایی اشکال مختلف نفوذهای مخرب است] [جان اندرسون[4] اولین کسی بود که در سال ۱۹۸۰ کار قابل‌توجهی در زمینه شناسایی نفوذ به شبکه انجام داد. هر حمله سایبری مستلزم هزینه‌های اقتصادی، آسیب به شهرت و عواقب قانونی است. ازاین‌رو، توسعه سیستم‌های تشخیص نفوذ تأثیری جهانی بر جامعه دانشگاهی و بخش تجاری و از جمله امنیت شبکه دارد] ۲] مهم است که شبکه‌ها در برابر دسترسی ناخواسته محافظت شوند و از تعامل کاربر و داده‌های کاربر محافظت شود. علاوه بر آشکارکردن آسیب‌پذیری‌های امنیتی جدید این سیستم‌ها باید بتوانند حملات جدید و روز صفر[5] را تشخیص دهند [۳] سیستم تشخیص نفوذ یک تکنیک مؤثر برای افزایش امنیت برای شناسایی و جلوگیری از حملات سایبری شبکه‌ها یا سیستم‌های ارتباطی است. سیستم‌های تشخیص نفوذ مسئول شناسایی فعالیت‌های مشکوک و امنیت کلی یک زیرساخت شبکه در برابر حملات سایبری و کاهش خسارات مالی و عملیاتی هستند. باتوجه‌به مطالعات انجام شده برای سیستم‌های تشخیص نفوذ چند معماری وجود دارد [۴] سیستم‌های تشخیص نفوذ مبتنی بر شبکه[6] که اجزای بسته‌های منحصربه‌فرد را برای شناسایی الگوهای رفتار ترافیک شبکه مضر بررسی می‌کنند] ۵]سیستم‌های تشخیص نفوذ مبتنی بر امضا[7] که گزارش‌های سیستم فعالیت هر میزبان را تجزیه‌وتحلیل می کند و حملات مخرب و سیستم‌های شناسایی ترکیبی را شناسایی می‌کند] ۶]سیستم‌هایی که از سیستم‌های تشخیص نفوذ غیرعادی و مبتنی بر امضا استفاده می کنند، کیفیت بالاتر و اقدامات امنیتی قوی‌تری دارند. روش تشخیص امضا از الگوها و طبقه‌بندی‌کننده‌های ازپیش‌تعیین‌شده برای ارزیابی بهتر حملات مخرب استفاده می کند. از اطلاعات موجود برای شناسایی تهدیدات مضر استفاده می‌کند. ازاین‌رو، از آن به‌عنوان یک استراتژی مبتنی بر دانش نام برده می‌شود. این رویکرد به یک مثبت کاذب کم همراه بادقت بالاتر دست می‌یابد، اما در تشخیص حملات جدید شبکه ناتوان است. برای کشف تهدیدات خصمانه ناشناخته، رویکرد تشخیص ناهنجاری از روش‌های اکتشافی استفاده می کند. در نتیجه، اثربخشی این رویکرد تشخیص ناهنجاری برای تشخیص ناهنجاری‌ها باوجود نرخ مثبت کاذب بالا خوب است] ۷] .در برخی از پژوهش‌ها سیستم‌های تشخیص نفوذ بر اساس تجزیه‌وتحلیل پروتکل تلاش دارند تا حملات را تشخیص دهند. در برخی از مطالعات برای تشخیص حملات از ترکیبی از سیستم‌های تشخیص حملات بر پایه تشخیص ناهنجاری و مبتنی بر امضا استفاده می‌کند تا از این مشکل را حل کنند. باتوجه‌به الگوی استقرار، سیستم‌های تشخیص نفوذ به دو نوع اصلی تقسیم می‌شوند که عبارت‌اند از سیستم‌های تشخیص نفوذ توزیع شده و غیر توزیع شده هستند. سیستم تشخیص نفوذ توزیع‌شده شامل چندین زیرسیستم تشخیص نفوذ در یک معماری توزیع شده است که روی یک شبکه گسترده متصل شده‌اند، درحالی‌که یک ساختار غیر توزیع‌شده، نشان‌دهنده یک سیستم تشخیص نفوذ متمرکز است. مزیت سیستم‌های تشخیص نفوذ توزیع شده آن است که توانایی تحلیل حجم زیادی از ترافیک شبکه را دارند و از این دسته می‌توان سیستم‌های تشخیص نفوذ در لایه مه را نام برد] ۸] سیستم‌های تشخیص نفوذ غیر توزیع شده به‌صورت متمرکز ترافیک شبکه را تحلیل نموده؛ اما توانایی پردازش حجم زیادی از ترافیک شبکه را ندارند[۹].

سیستم‌های تشخیص نفوذ مبتنی بر امضا بر آزمایش‌های آماری بر محدودیت‌های ترافیکی متعددی، مانند طول بسته، زمان رسیدن بسته، و حجم جریان ترافیک، بسته به ترافیک شبکه مدل در مدت‌زمان ازپیش‌تعیین‌شده، متکی است. باتوجه‌به پیچیدگی حملات مخرب مدرن امروزی، این امکان وجود دارد که این استراتژی‌ها مؤثر واقع نشوند] ۱۰] برای جایگزینی این تکنیک‌های مبتنی بر آمار، راه‌حلی موردنیاز است که بهینه‌ترین و کارآمدترین باشد. رویکردهای مبتنی بر یادگیری ماشین[8] به طور گسترده برای کمک به مدیران شبکه برای مقابله با طیف گسترده‌ای از حملات مضر در جلوگیری از این حملات استفاده شده است] ۱۱] سیستم‌های تشخیص نفوذ بر پایه یادگیری عمیق نوع پیشرفته‌تری از یادگیری ماشین هستند و توانایی تشخیص حملات پیچیده را دارند. از جمله روش‌های یادگیری عمیق برای تشخیص نفوذ می‌توان به شبکه عصبی کانولوشن [۱۲]شبکه عصبی [۱۳LSTM] و شبکه عصبی بازگشتی [۱۴] اشاره نمود. برای تشخیص نفوذ به شبکه خلاءهای زیادی وجود دارد و این خلاءها در روش‌های مبتنی بر امضا، روش‌های اکتشافی و یادگیری ماشین و عمیق وجود دارد. روش‌های مبتنی بر امضا یا لیست سیاه به حافظه زیادی نیاز دارند و زمان جستجوی لیست در برخی موارد قابل‌تحمل نیست و مانند روش‌های اکتشافی

[1] Information and Communication Technology (ICT)
[2] Cyber-Attacks
[3] Intrusion Detection System (IDS)
[4] John Anderson
[5] Zero Day Attacks
[6] Intrusion Detection Systems Based On The Network
[7] Signature-Based Intrusion Detection Systems
[8] Machine Learning (ML)-Based Approaches

توانایی تشخیص حملات جدید را ندارد. روش‌های یادگیری عمیق باوجودآنکه دارای توانایی تشخیص حملات روز صفر هستند؛ اما چالش‌های نیز دارند. این روش‌ها برای‌آنکه بتوانند دقت بیشتری داشته باشند باید آموزش زیادی ببینند که در حالت عادی زمان‌بر است و یا داده‌های زیادی برای آموزش آن وجود ندارد. از طرفی بیشتر روش‌های یادگیری عمیق مانند شبکه‌های CNN برای کار بر روی تصاویر طراحی شده‌اند و نمی‌توان در حالت عادی از آنها برای تشخیص نفوذ استفاده نمود. عدم انتخاب ورودی بهینه در روش‌های یادگیری عمیق نیز یک چالش مهم است که می‌توان آن را با روش‌های فراابتکاری هوشمند حل نمود. شبکه‌های عصبی کانولوشن مانند معماری VGG16[1] در تشخیص انواع بیماری‌ها و پردازش تصویر موفق بوده است. هدف از این مقاله آن است که ترافیک شبکه به فرمت تصاویر رنگی تبدیل شود و این تصاویر دودسته حمله و عادی در نظر گرفته شود و برای آموزش VGG16 استفاده شود. در روش پیشنهادی برای‌آنکه روش ویژگی‌های مهم ترافیک شبکه مدل VGG16 را آموزش داد می‌توان از انتخاب ویژگی استفاده نمود. در روش پیشنهادی برای بهینه‌سازی ویژگی‌ها و کاهش ابعاد مجموعه‌داده از الگوریتم بهینه‌سازی ببر سیبری [۱۵] استفاده می‌شود. در روش پیشنهادی برای‌آنکه بتوان حجم زیادی از ترافیک شبکه را مورد تحلیل قرارداد. سیستم تشخیص نفوذ در لایه مه استقرار پیدا می‌کند. در لایه مه گره اصلی مه که منابع بیشتری دارد از الگوریتم STO برای انتخاب ویژگی استفاده نموده و بردار ویژگی بهینه را برای گره‌های مه ارسال می‌کند. هر گره فرعی مه شبکه VGG16 را بر اساس ترافیک کاهش ابعاد یافته آموزش داده تا ترافیک حمله از عادی تشخیص داده شود. سهم نویسندگان از این مقاله به شرح ذیل است:

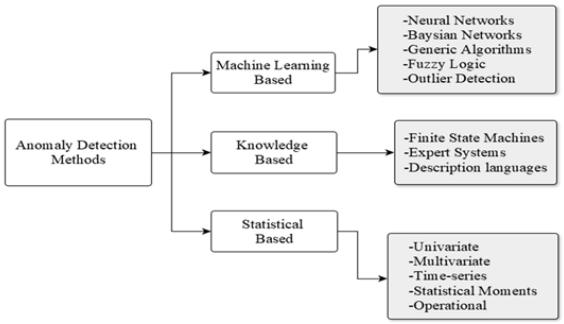
- ارائه یک نسخه باینری از الگوریتم STO برای انتخاب ویژگی
- کاهش ابعاد ترافیک شبکه در گره‌های که با بردار ویژگی بهینه و تبدیل ترافیک کاهش ابعاد یافته به تصاویر RGB
- ارائه یک سیستم تشخیص نفوذ بر اساس معماری VGG16
- ارائه یک سیستم تشخیص نفوذ توزیع شده در اینترنت اشیا
- بهینه‌سازی ورودی‌های VGG6 با الگوریتم STO در تشخیص حملات

این مقاله یک سیستم تشخیص نفوذ کارآمد بر اساس معماری اینترنت اشیا ارائه می‌دهد. در بخش II کارهای مرتبط در زمینه تشخیص حملات در اینترنت اشیا ارائه می‌دهد. در بخش III، سیستم تشخیص نفوذ پیشنهادی در اینترنت اشیا و بر اساس یادگیری عمیق و الگوریتم بهینه‌سازی ببر سیبری توسعه داده شده است. در بخش IV، روش پیشنهادی پیاده‌سازی و با روش‌های مشابه مقایسه می‌شود. در بخش V نتایج تحقیق و یافته‌های تحقیق به همراه پیشنهادها آتی ارائه می‌گردد.

[1] Very Deep Convolutional Networks (VGG)

۲- کارهای مرتبط

سیستم تشخیص نفوذ در شناسایی حملات سایبری احتمالی بسیار مؤثر است. سیستم تشخیص نفوذ از الگوریتم‌هایی برای طبقه‌بندی و شناسایی حملات استفاده می‌کند. دودسته از سیستم‌های تشخیص نفوذ وجود دارد، به نام‌های سیستم تشخیص نفوذ مبتنی بر امضا و سیستم تشخیص نفوذ مبتنی بر ناهنجاری. سیستم تشخیص نفوذ بر پایه تشخیص ناهنجاری حملات را بر اساس الگوهای شناخته شده قبلی، توالی‌ها یا مجموعه‌ای از قوانین تعریف شده برای حملات شناسایی می‌کند و توانایی بیشتری نسبت به روش‌های غیرپویا و مبتنی بر امضا یا لیست سیاه دارند. سیستم تشخیص نفوذ بر پایه میزان می‌تواند با بازرسی داده‌های سیستم‌عامل، گزارش‌های فایروال و گزارش‌های پایگاه‌داده یا ممیزی برنامه‌ها، حملات را از داخل سیستم شناسایی کند. سیستم تشخیص نفوذ مبتنی بر شبکه می‌تواند حملات خارجی را قبل از ورود به شبکه کامپیوترها شناسایی کند. سیستم تشخیص نفوذ بر شبکه ترافیک استخراج شده از منابع داده‌های مختلف شبکه را برای شناسایی هرگونه تهدیدی برای شبکه استفاده می‌کند] ۱۴] انواع مختلفی از سیستم‌های تشخیص نفوذ مبتنی بر اعضاء[2] و مبتنی بر ناهنجاری[3] وجود دارد که در شکل(۱)، نمایش داده می‌شود.



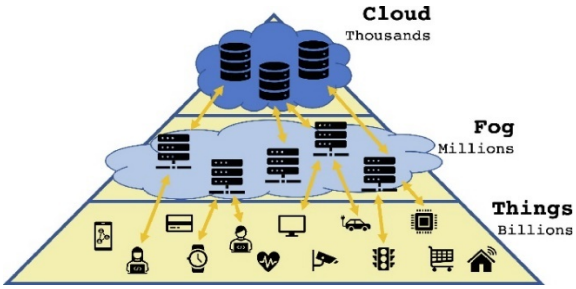
شکل (۱): تقسیم بندی سیستمهای تشخیص نفوذ [۱۴]

روش‌های مبتنی بر دانش یا مبتنی بر آمار و یادگیری ماشین عمیق، رویکردهای ساخته شده توسط هستند. معیارهای آماری مانند میانه، حالت، میانگین و انحراف معیار برای رویکرد مبتنی بر آمار استفاده می‌شود. مدل‌های مشابه مدل‌های تک‌متغیره، چندمتغیره و سری زمانی هستند. برای یک رویکرد مبتنی بر دانش، مجموعه‌ای از قوانین با استفاده از دانش انسانی ایجاد می‌شود. ماشین‌های حالت محدود، زبان‌های توصیف و سیستم‌های خبره نمونه‌هایی از سیستم‌های تشخیص نفوذ مبتنی بر دانش هستند. رویکردهای یادگیری ماشین را می‌توان به یادگیری تحت نظارت، نیمه نظارت و بدون نظارت طبقه بندی کرد. یادگیری نظارت شده از داده‌های ورودی برچسب گذاری

[2] Sig-IDS
[3] Anom-IDS

شده برای آموزش استفاده می‌کند، درحالی‌که یادگیری بدون نظارت از داده‌های ورودی بدون برچسب برای آموزش استفاده می‌کند. یادگیری نیمه نظارت شده از برخی داده های برچسب دار و تعداد زیادی از داده‌های ورودی بدون برچسب برای آموزش استفاده می‌کند[۱۴].

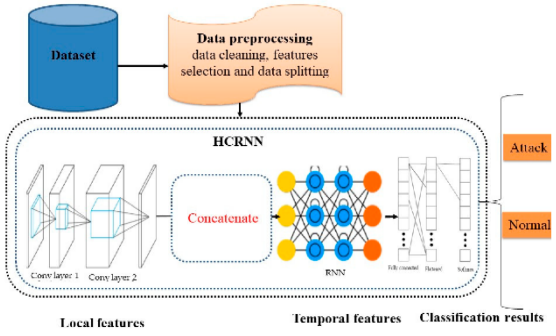
ارائه سیستم‌های تشخیص نفوذ در اینترنت اشیا داری چالش‌های زیادی است؛ زیرا در این شبکه حجم زیادی از ترافیک وجود دارد که از نوع کلان‌داده است. تحلیل همه ترافیک شبکه اینترنت اشیا توسط یک معماری متمرکز ممکن نمی‌باشد. برای تحلیل ترافیک بزرگ اینترنت اشیا نیاز به بسترهای توزیع شده مانند محاسبات مه است. اینترنت اشیا به‌سرعت در حال استفاده بیشتر و گسترده‌تر در زمینه‌های صنعت، درمان پزشکی و حمل‌ونقل است و به بخش مهمی از عصر "اینترنت همه چیز" تبدیل شده است. درحالی‌که رایانش ابری مقدار زیادی از پشتیبانی منابع را برای برنامه‌های IoT فراهم می‌کند، ویژگی‌های آن مانند سلف‌سرویس برحسب تقاضا، شبکه گسترده، خدمات اندازه‌گیری شده و کشش سریع نیز توسعه IoT را ارتقا می‌دهند. بااین‌حال، اتصال از راه دوربین گره‌های ابری و دستگاه‌های انتهایی در لبه شبکه از طریق اینترنت مشکلاتی مانند عملکرد، امنیت، تأخیر و پایداری را ایجاد می‌کند. ظهور این مشکلات باعث توسعه محاسبات مه شده است. محاسبات مه گسترش محاسبات ابری به لبه شبکه است که بین گره‌های ابری و دستگاه‌های انتهایی قرار دارد و اینترنت اشیا را با محاسبات ابری - مه ترکیبی شکل می‌دهد، همان‌طور که در شکل (۲)، نشان‌داده‌شده است[۱۶] گره‌های مه منابع را نزدیک به لبه شبکه مستقر می‌کنند. شبکه، به برنامه‌های اینترنت اشیا امکان می‌دهد منابع را به‌صورت ایمن و پایدار با تأخیر کم به دست آورند. این امر محاسبات مه را به راه‌حل بهینه برای ارائه خدمات کارآمد و ایمن اینترنت اشیا تبدیل می‌کند. کارهایی که نیاز به منابع فشرده دارند همچنان برای اجرا در لایه ابر آپلود می‌شوند؛ اما کارها و وظایفی که بلادرنگ بوده و به تأخیر حساس هستند در لایه مه اجرا می‌شوند. اینترنت اشیا با محاسبات ابری هیبریدی به طور گسترده در خودروهای هوشمند، ساختمان های هوشمند، شبکه های هوشمند، شهرهای هوشمند، سلامت هوشمند، کشاورزی هوشمند، صنعت هوشمند و سایر زمینه‌ها استفاده می‌شود[۱۷].



شکل (۲): لایه های اینترنت اشیا و مه محاسباتی [۱۶]

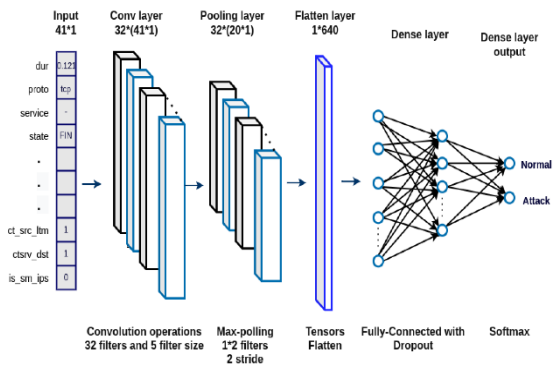
دستگاه‌های اینترنت اشیا به دلیل کاستی‌هایشان و به روزرسانی مداوم حملات شبکه، در برابر حملات آسیب‌پذیر هستند. استفاده از فناوری یادگیری عمیق برای ساخت نسل جدیدی از سیستم تشخیص نفوذ به یک نیاز امنیتی اینترنت اشیا با محاسبات ابری - مه‌آلود ترکیبی تبدیل شده است. سیستم تشخیص نفوذ با شناسایی داده‌های جمع آوری‌شده در زمان واقعی حملات را شناسایی می‌کند و به پرسنل امنیتی شبکه هشدار می‌دهد. سیستم تشخیص نفوذ با یادگیری عمیق و یادگیری ماشین این امکان را به لایه ابر یا مه می‌دهد که ترافیک حملات روز صفر را تشخیص دهند.

در شکل(۳)، به‌کارگیری روش یادگیری عمیق برای تشخیص حملات در اینترنت اشیا نشان‌داده‌شده است. برای تشخیص حملات با روش‌های یادگیری عمیق نیاز است که مجموعه‌داده متعادل‌سازی شود و در ادامه فاز انتخاب ویژگی اجرا شود تا یادگیری روی ویژگی‌های بااهمیت انجام شود.



شکل (۳): تشخیص حملات با یادگیری عمیق[۱۸]

برای تشخیص حملات به شبکه اینترنت اشیا، روش‌های یادگیری عمیق از جمله شبکه عصبی کانولوشن دارای کاربردهای زیادی است. شبکه عصبی کانولوشن از لایه‌های پیچشی یک‌بعدی، لایه‌های ادغام، لایه‌های حذف و توابع فعال‌سازی برای مدیریت داده‌های یک‌بعدی تشکیل شده است. در شکل(۴)، یک شبکه عصبی کانولوشن و لایه‌های آن برای تشخیص حملات نمایش‌داده‌شده است[۱۹].



شکل (۴): لایه های شبکه عصبی کانولوشن در تشخیص حملات [۱۹]

شبکه عصبی کانولوشن با استفاده از فراپارامترهای تعداد لایه‌های کانولوشن، نورون‌ها در هر لایه، اندازه فیلتر و ضریب نمونه برداری هر لایه زیر پیکربندی شده است. لایه پیچیدگی کاربرد اصلی فیلتر برای ورودی است. با استفاده از عملیات فیلترینگ مکرر، یک نقشه ویژگی ایجاد می‌کند که ویژگی‌های خاص مربوط به نقاط داده را نشان می‌دهد. پیچیدگی یک عملیات خطی است که شامل ضرب با ورودی با مجموعه ای از وزن است. برای این مورد، ورودی‌ها با وزن آرایه‌های تک‌بعدی که به‌عنوان هسته شناخته می‌شوند، ضرب می‌شوند. این عملیات برای هر پاس یک مقدار منحصربه فرد می‌دهد و اجرای این عملیات چندین مقدار را به دست می‌دهد که به‌عنوان نقشه ویژگی شناخته می‌شود[۲۰] در ادامه این بخش تعدادی از مطالعات در مورد سیستم‌های تشخیص نفوذ به شبکه مرور و بررسی می‌شود.

در[۲۱] سیستم تشخیص نفوذ شبکه بر اساس رمزگذارهای خودکار پشته‌ای در محاسبات مه ارائه دادند. یک سیستم‌های تشخیص نفوذ شبکه مبتنی بر رمزگذار خودکار پشته ای مستقر در لایه محاسبات مه پیشنهاد دادند. سیستم آنها از آموزش بدون نظارت رمزگذارهای خودکار پشته‌ای برای استخراج ویژگی‌های معنایی عمیق ترافیک عادی و غیرعادی استفاده می کند و به دنبال آن یادگیری نظارت شده با برچسب‌ها برای بهبود ویژگی‌ها و قابلیت‌های طبقه‌بندی است. نتایج نشان می‌دهد که نرخ خطای تشخیص روش پیشنهادی آنها در حدود ۲٪ است. در[۲۲] یک تشخیص نفوذ برای اینترنت اشیا صنعتی از طریق یادگیری حساس به هزینه تکاملی و محاسبات مه ارائه دادند. حملات و نفوذهای سایبری به موانع اصلی برای پذیرش اینترنت صنعتی اشیا در صنایع حیاتی تبدیل شده‌اند. توزیع نامتعادل داده‌ها یک مشکل رایج در محیط های اینترنت اشیا صنعتی است که بر سیستم‌های تشخیص نفوذ مبتنی بر یادگیری ماشین تأثیر منفی می‌گذارد. برای پرداختن به این مشکلات آنها یک مدل ترکیبی از رمزگذارهای خودکار پشته ای و شبکه های عصبی کانولوشنال با یک تابع تلفات جدید وابسته به هزینه ارائه دادند. هدف تابع ضرر بهینه‌سازی پارامترهای مدل است که در آن هزینه‌ها با استفاده از یک الگوریتم تکاملی تعیین می‌شود. ترکیبی از الگوریتم های تکاملی و یادگیری عمیق روی داده‌های بزرگ مانع از مقیاس‌پذیری سیستم‌های تشخیص نفوذ می‌شود. آنها آزمایش‌ها را بر روی مجموعه‌داده‌های ToN-IoT و UNSW-NB15 برای ارزیابی عملکرد روش پیشنهادی اجرا کردند. نتایج نشان می‌دهد که چارچوب‌های آنها می‌توانند به طور مؤثری مشکل عدم تعادل کلاس و مقیاس‌پذیری داده‌های ترافیک بزرگ اینترنت اشیا را در مقایسه با مدل های دیگر مدیریت کنند. مقادیر میانگین یادآوری، دقت و امتیاز F1 برای روش پیشنهادی به ترتیب ۹۳,۳، ۹۷/۶ و ۹۵/۲ درصد است که بالاتر از روش های مقایسه شده است. در[۲۳] تشخیص نفوذ با استفاده از طبقه‌بندی مجموعه بهینه شده در الگوی محاسباتی مه ارائه دادند. این پژوهش یک طبقه‌بندی‌کننده مجموعه مبتنی بر بهینه‌سازی ترکیبی را در یک پلت فرم محاسباتی مه ابداع کرده است. در محاسبات مه، پردازش کامل با استفاده از لایه‌های سه‌گانه انجام می‌شود که شامل لایه ابر، لایه نقطه پایانی و لایه مه است. در لایه ابری، سه روش مانند تبدیل داده‌ها، انتخاب ویژگی‌ها و فرایندهای طبقه‌بندی انجام شده است. یک تبدیل داده با تبدیل log انجام می‌شود. یک ویژگی با استفاده از فیلتر مبتنی بر همبستگی Kolmogorov-Smirnov انتخاب شده است. سپس، طبقه بندی با استفاده از طبقه‌بندی‌کننده‌های گروهی به نام‌های RideNN، شبکه عصبی فازی عمیق و شبکه عصبی کانولوشنال شپرد انجام می‌شود. تنظیم طبقه‌بندی‌کننده گروهی با استفاده از الگوریتم توسعه‌یافته RSLO انجام می‌شود. در لایه مه، تشخیص نفوذ بر اساس یک طبقه بندی گروهی آموزش دیده انجام می‌شود. روش پیشنهادی دارای دقتی در حدود ۹۷/۲٪ است. در[۲۴] یک معماری ترکیبی جدید برای تشخیص نفوذ در محاسبات مه ارائه کرده‌اند که ترکیبی از استفاده از مدل‌های یادگیری عمیق است. باتوجه‌به ابعاد بزرگ‌داده‌های شبکه، در ابتدا از رگرسیون بردار پشتیبانی مبتنی بر تابع مبتنی بر شعاعی برای به‌حداقل‌رساندن ابعاد داده‌ها و کاهش زمان آموزش استفاده می‌شود. سپس، در سرور ابری، از VGG19 و 2DCNN یکپارچه برای تکمیل آموزش مجموعه‌داده و انتقال آن به لایه مه استفاده می‌شود، جایی که انتقال داده‌ها مشاهده می‌شود و تهدیدها شناسایی می‌شوند. آزمایش‌ها با مجموعه‌داده‌های UNSW-NB15، CICIDS2017 و CICIDS2018 نشان می‌دهند که تکنیک‌های ارائه‌شده در این مقاله از نظر نرخ تشخیص، امتیاز F، دقت، فراخوان، FAR و دقت، بهتر از سایر تکنیک‌های قابل‌مقایسه هستند و در نتیجه مشکل تشخیص نفوذ را حل می‌کنند. در[۲۵] تشخیص نفوذ مبتنی بر ناهنجاری مقیاس‌پذیر برای اینترنت اشیا ایمن با استفاده از شبکه‌های متخاصم مولد در محیط مه ارائه می‌شود. در این مقاله، آنها یک روش یادگیری عمیق بدون نظارت جدید را برای شناسایی ناهنجاری ها در برابر شبکه های اینترنت اشیا پیشنهاد دادند که از شبکه‌های متخاصم مولد دوطرفه برای ساخت مدل بر روی داده های عادی اینترنت اشیا استفاده می کند. این مدل فاصله Wasserstein را برای ضبط و یادگیری توزیع داده های خام با ابعاد بالا معرفی می کند و با استفاده از یک طبقه‌بندی‌کننده کمکی بر نمایش های پنهان تمرکز می کند. نتایج تجربی بر روی دو مجموعه‌داده اخیر UNSW-NB15 و CIC-IDS2017 تأیید می کند که روش پیشنهادی به ۴ درصد افزایش دقت و ۴ درصد کاهش در نرخ هشدار نادرست نسبت به روش های پیشرفته و درعین‌حال حفظ کارایی محاسباتی دست می‌یابد. در[۲۶]چارچوب تشخیص نفوذ هوشمند شبکه باقابلیت مه برای برنامه-های کاربردی اینترنت اشیا ارائه شده است. آنها یک چارچوب

شبکه عصبی مصنوعی مبتنی بر بهینه سازی تعادل برای تشخیص حملات شبکه مربوط به سیستم های IoT پیشنهاد دادند. رویکرد پیشنهادی از تکنیک موازنه پویا برای به‌دست‌آوردن تعداد بهینه ویژگی‌ها برای آموزش الگوریتم شبکه عصبی استفاده می کند. برای ارزیابی اثربخشی مدل پیشنهادی، عملکرد آن با چندین مدل پیش بینی پایه مقایسه می شود. یافته‌های تجربی نشان می‌دهد که روش پیشنهادی دارای مقادیر دقت و یادآوری به ترتیب ۰/۹۳۸۹ و ۰/۹۲۴۸ است و دقت کلی ۹۳/۴۷٪ می‌شود. در] ۲۷] از تکنیک تقویت تطبیقی سبک‌وزن و بر پایه الگوریتم AdaBoost برای تشخیص نفوذ در شبکه‌های تعریف‌شده نرم‌افزار استفاده می‌کنند. نتایج تجربی با استفاده از UNSW-NB15 نشان می‌دهد که روش آنها در دقت و سرعت تشخیص بهتر از روش‌های پیشرفته‌تر عمل می‌کند، درحالی‌که پیچیدگی محاسباتی را تا حد زیادی کاهش می‌دهد. در] ۲۸] یک سیستم تشخیص نفوذ توزیع شده برای شناسایی حملات DDoS در شبکه اینترنت اشیا با بلاک‌چین ارائه دادند. این مقاله یک سیستم تشخیص نفوذ توزیع شده جدید را با استفاده از محاسبات مه برای شناسایی حملات DDoS علیه شبکه اینترنت اشیا با بلاک‌چین پیشنهاد می‌کند. عملکرد روش آنها با جنگل تصادفی و سیستم تقویت درخت گرادیان بهینه شده بر روی گره های مه توزیع شده ارزیابی می‌شود. اثربخشی مدل پیشنهادی با استفاده از یک مجموعه داده واقعی مبتنی بر اینترنت اشیا، یعنی BoT-IoT که شامل جدیدترین حملاتی است که در شبکه اینترنت اشیا با بلاک‌چین فعال شده است، ارزیابی می‌شود. نتایج نشان می‌دهد، برای تشخیص حمله باینری، XGBoost بهتر عمل می‌کند درحالی‌که برای تشخیص چند حمله، جنگل تصادفی عملکرد بهتری دارد. به‌طورکلی در گره‌های مه توزیع شده جنگل تصادفی در مقایسه با XGBoost زمان کمتری برای آموزش و آزمایش می‌گیرد. در] ۲۹] یک مدل ترکیبی تشخیص نفوذ گروهی با استفاده از یادگیری عمیق با انتخاب ویژگی کارآمد با استفاده از جنگل‌های تصادفی برای محیط‌های محاسباتی مه با استفاده از دو مدل یادگیری عمیق CNN سنتی و مدل IDS-AlexNet با جنگل تصادفی پیشنهاد شده است. پیاده‌سازی‌های مدل مربوطه بر روی مجموعه داده UNSW-NB15 نشان داده شده‌اند که ۹ کلاس حملات به نام‌های Fuzzers، Analysis، Backdoors، DoS، Exploits، Generic، Reconnaissance، Shellcodes و Worms را با دقتی متوسط در حدود ۹۷٫۵٪ تشخیص می‌دهد.

در] ۳۰] یک سیستم تشخیص حملات رد سرویس خدمات توزیع شده با استفاده از روش دسته‌بندی گروهی و رویکرد یادگیری فعّال ارائه دادند. در روش پیشنهادی از الگوریتم‌های درخت تصمیم‌گیری، شبکه عصبی پرسپترون چندلایه و جنگل تصادفی به روش گروهی استفاده می‌شود. آزمایش‌ها نشان می‌دهد دقت روش پیشنهادی جهت شناسایی حمله رد سرویس خدمات توزیع شده، ۹۹/۸۱٪ رسیده است. در] ۳۱] یک سیستم تشخیص بات نت‌ها با استفاده از روش‌های یادگیری عمیق ارائه شده است. شبکه عصبی کانولوشنال در این مطالعه برای تشخیص ۱۴ نوع بدافزار و بات نت بکار رفته است. روش آنها در تشخیص بات نت از ماشین بردار پشتیبان و درخت تصمیم‌گیری دقت بیشتری دارد. در] ۳۲] یک روش تشخیص حملات مبتنی بر بدافزار در رایانش ابری با استفاده از یادگیری جمعی ارائه دادند. در این مطالعه روش‌های یادگیری آدابوست، جنگل تصادفی و درخت گرادینت بوستد به‌صورت یادگیری گروهی استفاده شده است. آزمایش‌ها نشان داد دقت روش پیشنهادی برای تشخیص بدافزار برابر با ۹۶/۹۹٪ است. در] ۳۳] یک روش تشخیص نفوذ با استفاده از یادگیری ماشین و انتخاب ویژگی بر اساس الگوریتم سنجاقک ارائه شده است. در] ۳۴] یک روش تشخیص حملات سایبری پیشرفته با استفاده پردازش زبان طبیعی ارائه شده است. در این مقاله از خوشه‌بندی MD_DBSCAN برای تشخیص حملات استفاده شده است و ارزیابی‌ها نشان می‌دهد سطح تشخیص حملات نسبت به روش DBSCAN حدود ۲٪ بهبودیافته است. در جدول(۱)، کارهای مرتبط در زمینه تشخیص نفوذ بررسی و تحلیل شده است.

۳- روش پیشنهادی

بررسی مطالعات و کارهای مرتبط نشان می‌دهد که برای تشخیص نفوذ به شبکه روش‌های مختلفی وجود دارد که یکی از آنها روش‌های یادگیری عمیق از جمله شبکه‌های عصبی است. روش‌های یادگیری عمیق بر پایه شبکه عصبی مصنوعی در تشخص نفوذ چند چالش اساسی دارند که به شرح ذیل است:

- در بیشتر موارد تعداد نمونه‌های عادی از حمله بیشتر است و این موضوع باعث عدم تعادل مجموعه‌داده و کاهش دقت یادگیری می‌شود و ازاین‌جهت در روش پیشنهادی از تئوری بازی و شبکه یادگیری عمیق GAN برای این منظور استفاده می‌شود.
- روش‌های یادگیری عمیق معمولاً در لایه‌های اول عملیات انتخاب ویژگی و کاهش ابعاد را انجام می‌دهند این موضوع باعث افزایش پیچیدگی و افزایش واگرایی در مدل یادگیری شده و نرخ خطا را افزایش می‌دهد ازاین‌جهت در روش پیشنهادی فاز انتخاب ویژگی از یادگیری عمیق مستقل و جدا شده و با روش هوشمندانه ببر سیبری این فرایند انجام می‌شود.
- کاهش ابعاد با الگوریتم بهینه‌سازی ببر سیبری باعث می‌شود تا ورودی کمتری وارد شبکه عصبی شود و زمان یادگیری را کاهش دهد.

- در بیشتر موارد معماری‌های موفق مانند VGG16 و VGG19 در پردازش تصویر استفاده شده است؛ اما به دلیل آنکه ماهیت این معماری‌ها تصاویر و پردازش آنها است تاکنون کمتر در تشخیص نفوذ استفاده شده‌اند. به عبارت بهتر مزیت کدگذاری ترافیک شبکه به تصاویر آن است که می‌توان از معماری یادگیری عمیق که در پردازش تصویر بکار گرفته شده‌اند، استفاده نمود.
- مزیت معماری‌های نظیر VGG16 دارای رویکرد یادگیری انتقالی است و استفاده از کدینگ ترافیک به تصاویر باعث می‌شود از این معماری برای تشخیص نفوذ استفاده نمود و فاز آموزش را حذف نمود.
- انتخاب ویژگی در روش پیشنهادی باعث می‌شود تا ترافیک کاهش ابعاد یافته و تصاویر ورودی VGG16 کاهش یابد و زمان یادگیری نیز کاهش داده شود.

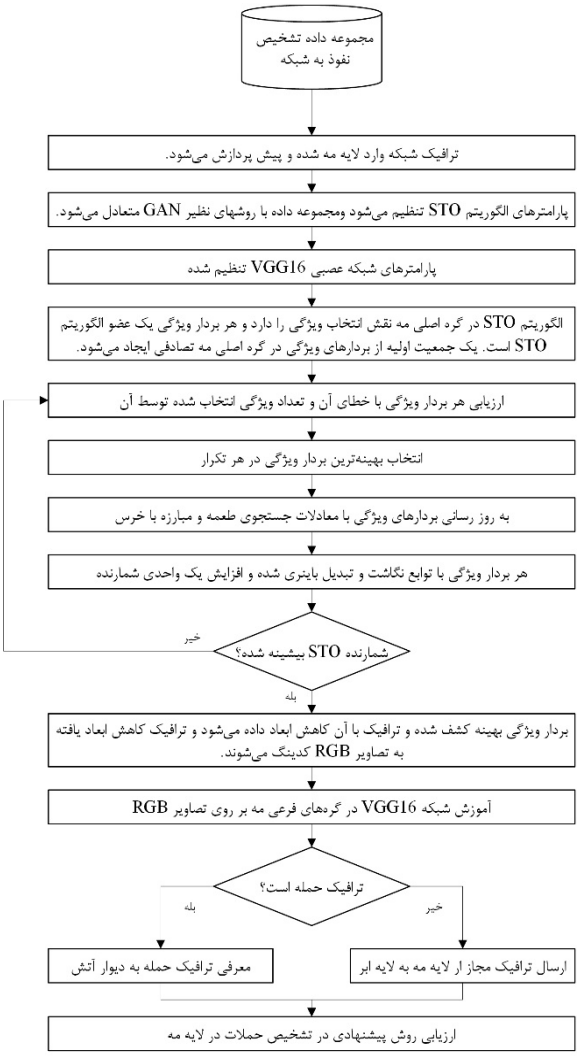
باتوجه‌به مطالب ارائه شده، روش پیشنهادی در این بخش برای تشخیص حملات به شبکه ارائه می‌شود. در روش پیشنهادی، سیستم تشخیص نفوذ در اینترنت اشیا مستقر است و مطابق چارچوب شکل(۵)، حملات به شبکه تشخیص داده می‌شود.

باتوجه‌به چارچوب پیشنهادی برای تشخیص حملات در اینترنت اشیا مراحل ذیل بکار گرفته می‌شود:

- یک گره در لایه مه به‌عنوان گره اصلی در نظر گرفته می‌شود و سایر گره‌ها به‌عنوان گره فرعی فرض می‌شوند. گره اصلی دارای توان پردازشی بیشتری نسبت به سایر گره‌های شبکه در لایه مه است.
- ترافیک شبکه به‌عنوان ورودی به لایه مه وارد شده و توسط گره اصلی پیش‌پردازش و نرمال‌سازی می‌شود.
- گره اصلی مه با استفاده از شبکه عصبی GAN تلاش می‌کند تا ترافیک شبکه را متعادل‌سازی نماید. هدف از متعادل‌سازی آن است که تعداد نمونه‌های حمله و ترافیک عادی یکسان شود.
- در مرحله بعد در گره اصلی مه انتخاب ویژگی با الگوریتم STO انجام می‌شود. نقش الگوریتم STO یافتن ویژگی‌های بهینه ترافیک شبکه و ارسال بردار ویژگی بهینه برای گره‌های فرعی مه است.

جدول (۱): مرور کارهای مرتبط

مرجع	روش	مزیت	چالش
۲۱	رمزگذارهای خودکار پشته‌ای	نرخ خطای تشخیص اندک	عدم تعادل در مجموعه‌داده
۲۲	یادگیری حساس به هزینه تکاملی	مدیریت مشکل عدم تعادل	نرخ خطای قابل‌توجه
۲۳	شبکه عصبی فازی عمیق و شبکه عصبی کانولوشنال شپرد	دقت نسبتاً خوب	پیچیدگی زیاد
۲۴	VGG19 و 2DCNN	ارزیابی دقیق و دقت بالا	پیچیدگی و عدم کاهش ابعاد
۲۵	شبکه‌های متخاصم مولد	۴ درصد افزایش دقت نسبت به روشهای مشابه	عدم کاهش ابعاد هوشمندانه
۲۶	شبکه عصبی مصنوعی مبتنی بر بهینه‌سازی تعادل	کاهش ابعاد قابل‌توجه	دقت اندک
۲۷	تقویت تطبیقی سبک‌وزن و بر پایه الگوریتم AdaBoost	پیچیدگی محاسباتی اندک	دقت کمتر از روش‌هایی مانند LSTM
۲۸	XGBoost	سرعت تشخیص بالا	عدم تعادل مجموعه‌داده آموزشی
۲۹	یادگیری عمیق CNN سنتی و مدل IDS-AlexNet با جنگل تصادفی	دقت بالا	پیچیدگی زیاد
۳۰	یادگیری گروهی	دقت بالا	زمان آموزش زیاد
۳۱	شبکه عصبی کانولوشنال	دقت بیشتر از ماشین بردار پشتیبان و درخت تصمیم‌گیری	عدم کاهش ابعاد ورودی شبکه عصبی و عدم تعادل مجموعه‌داده
۳۲	یادگیری جمعی	دقت بیشتر از روش‌های یادگیری آدابوست، جنگل تصادفی و درخت گرادینت بوستد	عدم تشخیص انواع حملات
۳۳	یادگیری ماشین و انتخاب ویژگی بر اساس الگوریتم سنجاقک	کاهش ابعاد و کاهش زمان یادگیری	عدم قطعیت
۳۴	پردازش زبان طبیعی و خوشه‌بندی	دقت بیشتر از DBSCAN	نرخ خطای قابل‌توجه در ترافیک کد شده



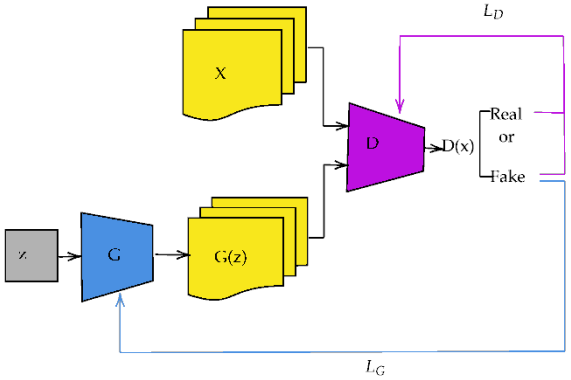
شکل (۵): چارچوب سیستم تشخیص نفوذ به شبکه

- گره‌های فرعی مه ترافیک شبکه را با بردار ویژگی بهینه که توسط الگوریتم STO کشف می‌شود، کاهش ابعاد می‌دهند. هر ترافیک کاهش ابعاد یافته باتوجه‌به مطالبی که در ادامه توضیح داده می‌شود به تصاویر RGB تبدیل می‌شود. از تصاویر RGB حمله و نرمال برای آموزش شبکه عصبی VGG16 استفاده می‌شود.
- گره‌های مه ترافیک حملات را برای دیوار آتش ارسال نموده و ترافیک عادی از لایه مه برای لایه ابر ارسال می‌شود تا از خدمات شبکه استفاده نماید.

۳- ۱- متعادلسازی با روش GAN

در بیشتر موارد مجموعه‌داده‌های بکار رفته برای آموزش روش‌های یادگیری ماشین و یادگیری عمیق فاقد تعادل هستند و منظور از تعادل آن است که تعداد نمونه‌های آموزشی نرمال به‌مراتب بیشتر از تعداد نمونه‌های حمله است. در این حالت برای رفع این چالش نیاز است که مجموعه‌داده متعادل‌سازی شود و تعداد نمونه‌های حمله افزایش داده شوند. یک روش برای‌آنکه به مجموعه‌داده ترافیک حمله آموزشی اضافه نمود آن است که تعدادی ترافیک نفوذ به‌صورت مصنوعی ایجاد نمود و آنها را به مجموعه‌داده اضافه نمود. مزیت این روش در آن است که ترافیک‌های جدید و پیش‌بینی‌نشده از نوع حمله اضافه می‌شود و مجموعه‌داده غنی‌تر شده و مدل آموزش‌یافته نیز دقت بالایی را به دست خواهد آورد. در روش پیشنهادی از شبکه GAN استفاده می‌شود که دارای دو بخش مختلف برای تولید نمونه‌های جعلی و مصنوعی باکیفیت و اضافه نمودن آنها به مجموعه‌داده است.

معماری پایه GAN در شکل(۶)، ارائه شده است. در اینجا، X مجموعه‌داده آموزشی واقعی را در قالب دسته‌ای حاوی نمونه‌هایی که GANها برای درک توزیع آماری آن استفاده می‌کنند، نشان می‌دهد که سپس هنگام تولید داده‌های مصنوعی اعمال می‌شود. سپس G آن را به نمونه‌های مصنوعی موردنظر تبدیل می‌کند. برای این، G یک شبکه عصبی فرض می‌شود که نقش تولید داده‌ها را بر عهده دارد.



شکل (۶): معماری شبکه GAN برای متعادل‌سازی مجموعه‌داده

سپس این آموزش برای یادگیری توزیع X و در نتیجه تبدیل Z برای تولید نمونه‌های مصنوعی با تقلید از نمونه‌های استخراج‌شده از X آموزش داده می‌شود؛ بنابراین، در پایان فرایند آموزش، هدف این است که نمونه‌های مصنوعی با G(z) در نهایت توزیعی دارد که از توزیع X غیرقابل‌تشخیص است. Z یک بردار نویز است که از فضای پنهان به دست می‌آید و از یک توزیع شناخته شده مانند توزیع نرمال یا یکنواخت نمونه‌برداری می‌شود. فضای پنهان نشان‌دهنده ورودی خام به مولد (G) است. D همچنین نشان‌دهنده یک شبکه عصبی است، شبکه‌ای که مربوط به تمایز کننده است. برای تمایز نمونه‌های گرفته شده از داده‌های واقعی، X، و داده‌های تولید شده، G(z) آموزش‌دیده است. توجه داشته باشید که X و G(z) ورودی‌های تشخیص‌دهنده هستند که یک تصمیم طبقه‌بندی واقعی یا جعلی باینری را خروجی می‌دهد. تمایز کننده و مولد هر دو در تلاش هستند تا تلفات خود را به حداقل برسانند - به ترتیب با Ld و Lg نشان داده می‌شود. آنها به طور هم زمان با روش‌های نزول گرادیان (با گرادیان‌های

محاسبه‌شده با کمک پس انتشار) از طریق تغییربردارهای وزن شبکه عصبی متناظرشان بهبود می‌یابند.

۳- ۲- کاهش ابعاد

در بیشتر موارد تعداد ویژگی‌های مجموعه‌داده برای یادگیری زیاد است و این موضوع باعث می‌شود تا تعداد ورودی شبکه عصبی برای یادگیری افزایش یابد. کاهش ابعاد به فرایندی گفته می‌شود که هدف آن کم‌کردن تعداد ویژگی‌ها و حذف برخی از ویژگی‌ها است که در فرایند یادگیری اهمیت زیادی ندارند. برای کاهش ابعاد از روش‌های انتخاب ویژگی و بهینه‌سازی استفاده می‌شود به‌گونه‌ای که فقط ویژگی‌های مهم ترافیک به‌عنوان ورودی یادگیری عمیق استفاده می‌شود. انتخاب ویژگی یک مسئله بهینه‌سازی است و حداقل دارای مزایای ذیل است:

- انتخاب ویژگی باعث کاهش ابعاد ورودی روش‌های یادگیری عمیق می‌شود و سرعت تشخیص نفوذ را افزایش می‌دهد.
- انتخاب ویژگی باعث کاهش‌یافتن خطای تشخیص نفوذ توسط روش‌های یادگیری عمیق می‌شود؛ زیرا روش‌های یادگیری بر روی ویژگی‌های مهم متمرکز می‌شوند نه همه ویژگی‌ها که برخی از آنها اهمیت زیادی ندارند.

نکته قابل‌توجه آن است که کاهش ابعاد باعث کاهش کیفیت نمونه‌ها نمی‌شود؛ زیرا ویژگی‌های غیراصلی را حذف نمود و برعکس باعث افزایش کیفیت می‌شود؛ زیرا فقط ویژگی‌های مهم و تأثیرگذار در تشخیص نفوذ را نگهداری می‌کند. الگوریتم بهینه-سازی ببر سیبری بر اساس رفتار شکارکردن این حیوانات درنده مدل‌سازی می‌شود. الگوریتم STO یک روش فراابتکاری برای حل مسائل بهینه‌سازی است[۱۵] ببرهای سیبری به دلیل اختلاف بر سر طعمه و دفاع از خود با خرس سیاه و خرس قهوه‌ای می-جنگند. رفتارهای ببرهای سیبری در طبیعت شامل استراتژی آنها برای شکار طعمه و مبارزه با خرس قهوه‌ای است. فرایندهای هوشمندانه‌ای است که می‌تواند مبنایی برای طراحی یک الگوریتم فراابتکاری جدید باشد. در روش پیشنهادی هر ببر سیبری یک بردار ویژگی است. برای ارزیابی هر ببر سیبری یا بردار ویژگی معادل از معادله(۱)، استفاده می‌شود.

$$F(X_i) = \theta_1 . E + \theta_2 \frac{size(X_i)}{Dim} \quad (۱)$$

در این معادله، E خطای تشخیص حملات به‌ازای بردار ویژگی i-ام یا X_i است و $size(X_i)$ تعداد ویژگی انتخاب شده بردار ویژگی X_i است. ابعاد بردارهای ویژگی و تعداد ویژگی‌های انتخاب شده در مجموعه داده با Dim نمایش داده می‌شود. θ_1 و θ_2 دو ضریب وزنی بین صفر و یک است که مجموع آنها برابر یک است. در مرحله اول از الگوریتم STO یک جمعیت اولیه از راه‌حلها یا بردارهای ویژگی تصادفی مطابق معادله(۲) ایجاد می‌شود.

$$X = \begin{bmatrix} X_1 \\ \vdots \\ X_i \\ \vdots \\ X_N \end{bmatrix}_{N\times m} = \begin{bmatrix} x_{1,1} & \cdots & x_{1,f} & \cdots & x_{1,\,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{i,1} & \cdots & x_{i,j} & \cdots & x_{i,\,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{N,1} & \cdots & x_{N,j} & \cdots & x_{N,\,m} \end{bmatrix}_{N\times m} \quad (۲)$$

که در آن X ماتریس جمعیت ببرهای سیبری است، Xi ببر سیبری شماره i و N تعداد کل ببرهای سیبری جمعیت است. موقعیت اولیه ببرهای سیبری در فضای جستجو در ابتدای اجرای STO به طور تصادفی با استفاده از (۳) محاسبه می‌شود.

$$x_{I,j} = lb_j + r_{I,j} \cdot (ub_j - lb_j),\ i = 1,2,\dots,N, j = 1,2,\dots,m \quad (۳)$$

$x_{i,j}$ راه‌حل iام در بعد j است. m تعداد متغیرهای مسئله است، $r_{i,j}$ اعداد تصادفی در بازه [۰،۱] هستند، lbj و ubj کران پایین و کران بالای متغیر مسئله j است. مجموعه مقادیر محاسبه شده برای تابع هدف به ازای جمعیت بردارهای ویژگی یا ببرهای سیبری در معادله(۴)، را می‌توان با استفاده از بردار به نام بردار تابع هدف مطابق (۴) نمایش داد.

$$F = \begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} F(X_1) \\ \vdots \\ F(X_i) \\ \vdots \\ F(X_N) \end{bmatrix}_{N\times 1} \quad (۴)$$

که در آن F بردار مقادیر تابع هدف و Fi مقدار تابع هدف به دست آمده برایi امین ببر سیبری است. کمینه شدن تابع هدف در فاز انتخاب ویژگی مطلوب است. بهترین عضو Xbest (بهترین راه حل نامزد) را تعیین می‌کندبهترین عضو در هر تکرار باید با مقایسه مقدار تابع هدف با این مقادیر جدید نیز به روز شود. در مرحله اول، جمعیت STO بر اساس شبیه‌سازی استراتژی شکار ببرهای سیبری به روز می‌شوند. در این استراتژی، ببر سیبری پس از انتخاب طعمه به آن حمله می‌کند و سپس در یک فرآیند تعقیب و گریز، طعمه را می‌کشد. این مرحله باعث تغییرات ناگهانی و گسترده در موقعیت اعضای STO می‌شود و در نتیجه توانایی جستجوی سراسری و کاوش را افزایش می‌دهد. در طراحی STO، موقعیت‌های طعمه راه‌حلهای هستند که تابع هدف به ازای آنها بهینه‌تر شده است. مجموعه موقعیت طعمه‌ها در معادله (۵) فرموله می‌شود.

$$PP_i = \{X_k \mid k \in \{1,2,\dots,N\} \wedge F_k < F_i\} \cup \{X_{best}\} \quad (۵)$$

که در آن Xbest بهترین راه‌حل یا بهینه‌ترین بردار ویژگی است و N تعداد کل اعضای جمعیت STO است. یک عضو این مجموعه به‌عنوان TPi نشان داده می‌شود و به طور تصادفی به‌عنوان هدف مورد حمله توسط ببر سیبری انتخاب می‌شود و موقعیت جدید آن بر اساس شبیه‌سازی محاسبه می‌شود. در الگوریتم STO حمله به طعمه با استفاده از معادله(۶) شبیه‌سازی می‌شود.

$$x_{I,j}^{P1S1} = x_{I,j} + r_{I,j} \cdot (TP_{I,j} - I_{I,j} \cdot x_{I,j}),\ i = 1,2,\dots,N \text{ and } j = 1,2,\dots,m, \quad (۶)$$

که در آن $TPi_{,j}$، بعد j راه‌حل TPi است، $x_{i,j}^{P1S1}$ موقعیت جدید

عضو i در بعد j در مرحله ۱ از فاز ۱ الگوریتم STO است. m تعداد متغیرهای مسئله است. $r_{i,j}$ اعداد تصادفی در بازه [۰،۱] هستند و $I_{i,j}$ اعداد تصادفی از مجموعه {۱،۲} هستند. در فرآیند به روز رسانی اعضای STO، موقعیت محاسبه شده جدید در صورتی قابل قبول است که مقدار تابع هدف را بهبود بخشد از معادله(۷) برای این منظور استفاده می‌شود.

(۷)
$$X_i = \begin{cases} X_i^{P1S1}, & F_i^{P1S1} < F_i \\ X_i, & else, \end{cases}$$

که در آن F_i^{P1S1} مقدار تابع هدف به ازای عضو X_i^{P1S1} است.

در مرحله دوم، موقعیت اعضای جمعیت بر اساس فرایند تعقیب‌وگریز به‌روز می‌شود. در این فرایند، ببر سیبری موقعیت خود را در منطقه‌ای که در حال حمله به طعمه است تغییر می‌دهد. برای شبیه‌سازی فرایند تعقیب، ابتدا موقعیت جدیدی برای ببر سیبری در نزدیکی محل حمله با استفاده از معادله(۸) محاسبه می‌شود. سپس مطابق معادله (۹) اگر مقدار تابع هدف بهبود یابد، این موقعیت جدید محاسبه شده جایگزین موقعیت قبلی عضو متناظر می‌شود.

$$x_{i,j}^{P_1S2} = x_{ij} + \frac{r_{i,j}\cdot(ub_j - lb_j)}{t}, i = 1,2,\dots,N, j = 1,2,\dots,m, \text{ and } t = 1,2,\dots,T, \quad (۸)$$

(۹)
$$X_i = \begin{cases} X_i^{P1S2}, & F_i^{P1S2} < F_i; \\ X_i, & else, \end{cases}$$

که در آن F_i^{P1S2} موقعیت جدید ببر سیبری بر اساس مرحله دوم از فاز اول الگوریتم STO است. ri,j اعداد تصادفی یکنواخت در بازه [۰،۱] و t شمارنده تکرار الگوریتم است.

بنابراین، در مرحله دوم اعضای STO بر اساس شبیه‌سازی استراتژی ببرهای سیبری هنگام مبارزه با خرس‌ها به‌روز می‌شوند. استراتژی مبارزه ببر سیبری با خرس در دو مرحله حمله و درگیری شبیه‌سازی می‌شود. در مرحله اول برای مدل‌سازی از حمله ببر سیبری به خرس، سایر اعضای جمعیت مجموعه خرس‌ها در نظر گرفته می‌شوند. از این مجموعه خرس‌های احتمالی، موقعیت خرس مورد حمله به طور تصادفی انتخاب می‌شود و این موقعیت با k نشان داده می‌شود. این مرحله منجر به تغییرات قابل‌توجه و ناگهانی در موقعیت اعضای STO می‌شود که می‌تواند قابلیت جستجو سراسری و اکتشافی را افزایش دهد. ابتدا یک موقعیت جدید برای i امین عضو STO، i=1,2,…,N بر اساس معادله (۱۰) محاسبه می‌شود.

$$x_{ij}^{P2SI} = \begin{cases} x_{i,j} + r_{i,j}\cdot\left(x_{kj} - I_{i,j}\cdot x_{i,j}\right), & F_k < F_i; \\ x_{i,j} + r_{i,j}\cdot\left(x_{i,j} - I_{i,j}\cdot x_{kj}\right), & else, \end{cases} \quad (۱۰)$$

که در آن x_{kj} بعد یک مکان خرس است سپس طبق (۱۱) اگر مقدار تابع هدف بهبود یابد، این موقعیت تازه محاسبه شده جایگزین موقعیت قبلی عضو متناظر می‌شود.

$$X_i = \begin{cases} X_i^{P2S2}, & F_i^{P2S2} < F_i; \\ X_i, & else, \end{cases} \quad (۱۱)$$

در آن Fk مقدار تابع هدف خرس، F_i مقدار تابع هدف به ازای موقعیت ببر و F_i^{P2S2} مقدار تابع هدف X_i^{P2S2} است. در مرحله دوم، موقعیت اعضای جمعیت بر اساس مدلسازی درگیری‌های به روز می‌شود. این رفتار باعث تغییرات کوچکی در موقعیت اعضای جمعیت می‌شود که منجر به بهبود جستجوی محلی STO و توانایی بهره برداری می‌شود. برای مدل‌سازی این رفتار، ابتدا یک موقعیت تصادفی در نزدیکی محل مبارزه با استفاده از معادله (۱۲) محاسبه می‌شود.

$$x_{i,j}^{P2S2} = x_{i,j} + \frac{r_{ij}}{t}\left(ub_j - lb_j\right), i - 1,2,\dots,N, j = 1,2,\dots,m, \text{ and } t = 1,2,\dots,T, \quad (۱۲)$$

که در آن $x_{i,j}^{P2S2}$ موقعیت جدید ببر سیبری i بر اساس مرحله دوم از فاز دوم الگوریتم STO است اگر مقدار تابع هدف را مطابق معادله(۱۳) بهبود بخشد.

$$X_i = \begin{cases} X_i^{P2S2}, & F_i^{P2S2} < F_i; \\ X_i, & else, \end{cases}, \quad (۱۳)$$

۳- ۳- باینری نمودن بردارهای ویژگی

با تکرار الگوریتم ببر سیبری، بردارهای ویژگی به‌روزرسانی می‌شوند و در نهایت بردار ویژگی در تکرار آخر الگوریتم STO به‌عنوان جواب نهایی به خروجی این مرحله ارسال می‌شود. در هر تکرار الگوریتم STO، بردارهای ویژگی به‌روزرسانی شده و فضای ویژگی به دلیل روابط و به‌روزرسانی الگوریتم STO از حالت باینری خارج شده و به حالت اعشاری تبدیل می‌شود. برای‌آنکه بردارهای ویژگی در هر تکرار الگوریتم STO مجدد باینری شوند از توابع تبدیل S و V استفاده می‌شود که چهار نمونه از آنها در معادلات(۱۴)، (۱۵)، (۱۶) و (۱۷) فرموله می‌شود. این توابع مقدار بردارهای ویژگی را بین صفر و یک نرمالیزه می‌کنند و بر اساس یک آستانه مانند ۰،۵، مقدارهای کوچک‌تر به صفر و مقادیر بزرگ‌تر از آستانه به یک نگاشت داده می‌شود.

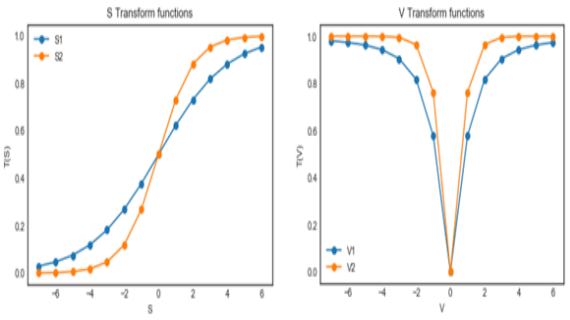
$$S_1 = \frac{1}{1+e^{\left(\frac{-x}{2}\right)}} \quad (۱۴)$$

$$S_2 = 1 - \frac{1}{1+e^{x}} \quad (۱۵)$$

$$V_1 = \frac{x}{\sqrt{2+x^2}} \quad (۱۶)$$

$$V_2 = \tan x \quad (۱۷)$$

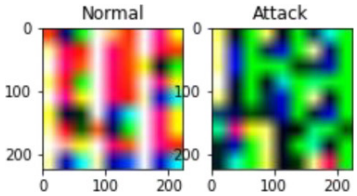
شکل توابع تبدیل از نوع S و V در شکل(۷)، نمایش‌داده‌شده است و مشاهده می‌شود مقدار برد آنها بین صفر و یک است.



شکل (۷): توابع تبدیل S و V

۳- ۴- کدینگ ترافیک به تصاویر

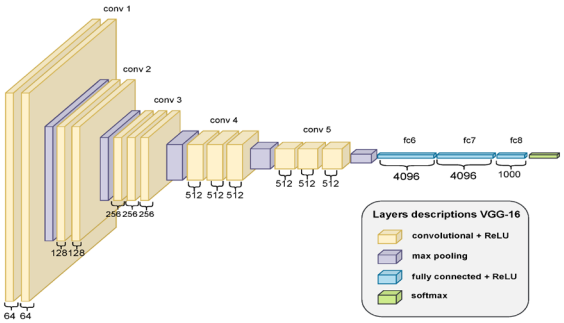
شبکه عصبی کانولوشن یک روش یادگیری عمیق برای پردازش تصاویر و طبقه‌بندی تصاویر است و ورودی آن باید از نوع تصاویر باشد. برای به‌کارگیری یک شبکه عصبی کانولوشن مانند VGG16 در طبقه‌بندی ترافیک شبکه، ترافیک ورودی به تصاویر حمله و تصاویر عادی به‌گونه‌ای کارآمد کدینگ می‌شود. فرض کنید در مرحله انتخاب ویژگی K ویژگی از مجموعه‌داده انتخاب شود. اگر K نمونه از کلاس حملات از مجموعه‌داده جدا شود آنگاه یک ماتریس K در K ایجاد می‌شود. هر ستون این ماتریس یک ویژگی انتخاب شده است. اگر مقادیر ماتریس K در K بین صفر تا ۲۵۵ نرمالیزه شود آنگاه یک تصویر خاکستری ایجاد می‌شود. در روش پیشنهادی سه ماتریس K در K برای سه کانال R، G و B در نظر گرفته می‌شود تا یک تصویر رنگی از مجموعه‌داده ایجاد شود. برای نمونه‌های کلاس ترافیک عادی مانند ترافیک حملات عمل می‌شود. مجموعه‌ای از نمونه‌های ترافیک عادی به‌عنوان تصاویر عادی رنگی و نمونه‌های ترافیک حمله به‌عنوان تصاویر حمله ایجاد می‌شود. از تصاویر حمله و تصاویر عادی برای آموزش شبکه عصبی کانولوشن استفاده می‌شود. با تبدیل نمونه‌های ترافیک به تصاویر رنگی حمله و ترافیک عادی، می‌توان یک شبکه عصبی CNN را آموزش داد(شکل(۸۶)).



شکل (۸): کدینگ ترافیک حمله و عادی به تصاویر RGB

۳- ۵- طبقه بندی با یادگیری انتقالی

در روش پیشنهادی از تصاویر حملات و تصاویر ترافیک عادی به‌عنوان ورودی شبکه عصبی [۳۵VGG16] به‌عنوان یک معماری شبکه عصبی کانولوشن استفاده می‌شود. شکل(۹)، معماری VGG16 طبقه‌بندی تصاویر حمله و عادی را نمایش می‌دهد.



شکل (۹): معماری شبکه عصبی VGG16 برای طبقه‌بندی ترافیک شبکه در لایه مه

در این معماری پیشنهادی VGG16، لایه‌های درگیر ۱۶ لایه است که شامل ۱۳ لایه کانولوشن به همراه لایه max-pooling و ۳ لایه کاملا متصل که در شکل(۸)، نشان داده شده است. مزیت اصلی موجود در معماری VGG16 در مقایسه با AlexNet، استفاده از فیلترهای کوچکتر است که روی هم قرار می‌گیرند نه یک فیلتر بزرگ. مفهوم پشت این رویکرد ارتباط نزدیکی با زمینه های حساس فیلترهای کانولوشن دارد. با این حال، هر پیکسل اطلاعات ۴۹ پیکسل لایه قبلی را از طریق هسته دریافت می‌کند. از این رو، میدان‌های حساس بالاتر می‌توانند نقوش بیشتری را در یک منطقه بزرگ در هنگام از دست دادن جزئیات ثبت کنند، در حالی که میدان‌های دریافتی کمتر قادر به گرفتن الگوهای معمولی نیستند. بنابراین، معماری VGG16 شامل لایه های کانولوشن، لایه‌های حداکثر تجمعی و لایه‌های کاملاً متصل است. اگرچه تفاوت های بیشتری وجود دارد، مدلی که در این سهام پیاده‌سازی می‌شود شامل فیلترهای کانولوشنی است. پیچیدگی‌های کاملاً متصل فقط ترکیب خطی یک مکان پیکسل را بر روی لایه ها نشان می‌دهد. در واقع، استفاده از فعال سازی غیرخطی و ReLU در AlexNet ترجیح داده شده است. مدل‌های از پیش آموزش دیده این شبکه در Keras و چارچوب ها و کتابخانه‌های مختلف یادگیری عمیق موجود هستند.

۴- نتایج تجربی

در این بخش سیستم تشخیص نفوذ پیشنهادی برای تشخیص حملات به شبکه هوشمند پیاده‌سازی و ارزیابی می‌شود. برای پیاده‌سازی از پایتون و کتابخانه Keras و Tensorfolw استفاده می‌شود. اندازه جمعیت الگوریتم STO برابر ۱۵ و تعداد تکرار بیشینه STO برابر ۵۰ تنظیم شده است. تعداد آزمایشات برابر ۲۵ و اندازه داده‌های آموزشی و آزمون به ترتیب برابر ۷۰٪ و ۱۵٪ در نظر گرفته می‌شود. ۱۵٪ از نمونه‌ها نیز از نوع ترافیک اعتبارسنجی است.

۴- ۱- مجموعه داده

در این پژوهش برای آزمایش‌ها از مجموعه‌داده NSL-KDD استفاده

می‌شود که به‌عنوان یک نسخه مدرن از مجموعه‌داده KDD CUP 99 است. برای هر ورودی، از ۴۱ ویژگی مختلف پشتیبانی خواهید کرد، که هر کدام ممکن است به نوع حمله رکورد یا نوع عادی آن اختصاص داده شود. مقادیر مشخصه می‌توانند اسمی، باینری یا عددی باشند. با این حال، بر خلاف KDD CUP 99، مجموعه آموزشی مجموعه داده NSL-KDD حاوی هیچ ورودی تکراری نیست. بنابراین، طبقه‌بندی‌کننده‌ها نسبت به رکوردهای متداول‌تر مشکلی ندارند. بنابراین، در NSL-KDD، تکنیک‌هایی با نرخ تشخیص بهتر رکوردهای مکرر در مجموعه‌های آزمایشی بر عملکرد فراگیران تأثیر نمی گذارند. یعنی ۴۱ ویژگی موجود در این مجموعه داده دارای سه ویژگی نوع اسمی، Protocol_type، Service و Flag می‌باشند، در حالی که سایر ویژگی‌ها همه از نوع دوگانه هستند. این مجموعه داده دارای انواع حملات و از جمله حملات انکار سرویس (DoS)، حملات از راه دور به محلی (R2L)، کاربر به ریشه (U2R) و حملات کاوشگر چهار دسته اصلی حملات سایبری هستند[۳۶]. این مجموعه داده مطابق جدول(۲)، دارای ۴۱ ویژگی ورودی است و این ویژگی‌ها به شرح ذیل است:

- ویژگی‌های اساسی (۱-۹): اینها اطلاعات اولیه بسته مانند "مدت"، "نوع پروتکل"، "سرویس" و "پرچم" را نشان می‌دهند.
- ویژگی‌های محتوا (۱۰-۲۲): آنها بر اساس اطلاعات محتوای بسته هستند و برای شناسایی حملات R2L و U2R، مانند چندین تلاش ناموفق برای ورود استفاده می‌شوند.
- ویژگی‌های مبتنی بر زمان (۲۳-۳۱): شامل ویژگی‌هایی مانند «شمارش» و «شمارش *srv*». آنها در یک پنجره ۲ ثانیه محاسبه می شوند. این ویژگی‌ها نشان دهنده الگوهای اتصالات شبکه هستند.

جدول (۲): لیست ویژگی‌های مجموعه داده NSL-KDD [۳۸]

F#	Feature name	F#	Feature name	F#	Feature name
F1	Duration	F15	Su attempted	F29	Same srv rate
F2	Protocol type	F16	Num root	F30	Diff srv rate
F3	Service	F17	Num file creations	F31	Srv diff host rate
F4	Flag	F18	Num shells	F32	Dst host count
F5	Source bytes	F19	Num access files	F33	Dst host srv count
F6	Destination bytes	F20	Num outbound cmds	F34	Dst host same srv rate
F7	Land	F21	Is host login	F35	Dst host diff srv rate
F8	Wrong fragment	F22	Is guest login	F36	Dst host same src port rate
F9	Urgent	F23	Count	F37	Dst host srv host rate
F10	Hot	F24	Srv count	F38	Dst host serror rate
F11	Number failed logins	F25	Serror rate	F39	Dst host srv serror
F12	Loggeed in	F26	Srv serror ratte	F40	Dst host serror rate
F13	Num compromised	F27	Rerror rate	F41	Dst host srv serror rate
F14	Root shell	F28	Srv rerror rate	F42	Class lable

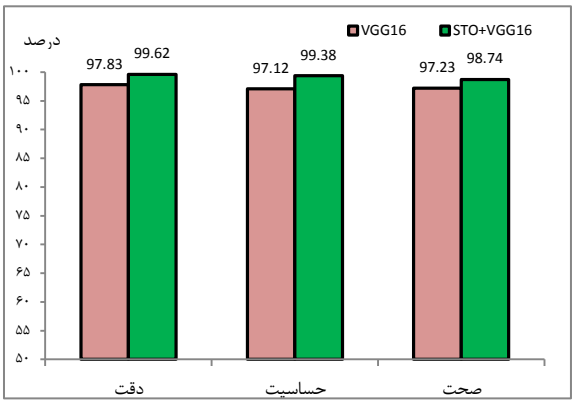
- ویژگی‌های مبتنی بر میزبان (۳۲-۴۱): با ویژگی‌هایی مانند «تعداد میزبان dst» و «تعداد srv میزبان dst»، این ویژگی‌ها در پنجره‌هایی با بیش از ۲ ثانیه محاسبه می‌شوند و الگوهای حمله را از مقصدی به میزبان دیگر نشان می‌دهند.

مجموعه‌داده UNSW-NB15 نشان‌دهنده یک منبع مهم و جامع است که برای سیستم‌های تشخیص نفوذ شبکه طراحی شده است و در بخشی از آزمایش‌ها ما نیز بکار گرفته می‌شود. این مخزن که برای رفع محدودیت‌های مجموعه‌داده‌های موجود توسعه‌یافته است، مجموعه‌ای متنوع و واقعی از داده‌های ترافیک شبکه را فراهم می‌کند که به طور خاص برای کمک به ارزیابی و پیشرفت IDS طراحی شده است. برای تولید مجموعه‌داده UNSW-NB15 از ابزارها و روش‌های پیشرفته استفاده شده است. در این مجموعه‌داده ابزار IXIA Perfect Storm برای ایجاد ترکیبی از فعالیت‌های شبکه مدرن معتبر و رفتارهای حمله مصنوعی معاصر استفاده شده است. متعاقباً، ابزار tcpdump برای ضبط ۱۰۰ گیگابایت ترافیک خام، ذخیره شده در فایل‌های pcap استفاده شد، که منجر به ایجاد مجموعه‌ای شد که دینامیک شبکه در دنیای واقعی را با دقت بیشتری منعکس می‌کند. یکی از نقاط قوت کلیدی مجموعه داده UNSW-NB15 در نمایش جامع انواع حملات مختلف است. این شامل نه دسته حمله مجزا از جمله Fizzers، Analysis، Backdoors، DoS، Exploits، Generic، Reconnaissance، Shellcode و Worms است. با در بر گرفتن طیف گسترده‌ای از سناریوهای حمله، مجموعه داده به محققان امکان می‌دهد تا عملکرد IDS ها را در برابر تهدیدات مختلف ارزیابی کنند. مجموعه داده شامل ابزارهای Argus و Bro-IDS برای تولید مجموعه ای از ۴۹ ویژگی است که هر کدام با یک برچسب کلاس خاص مرتبط هستند. این ویژگی‌ها در فایل UNSW-NB15_features.csv به تفصیل آمده است، و به محققان درک عمیق‌تری از ویژگی‌های مجموعه داده ارائه می‌دهد و تجزیه و تحلیل مبتنی بر ویژگی را تسهیل می‌کند[۳۹].

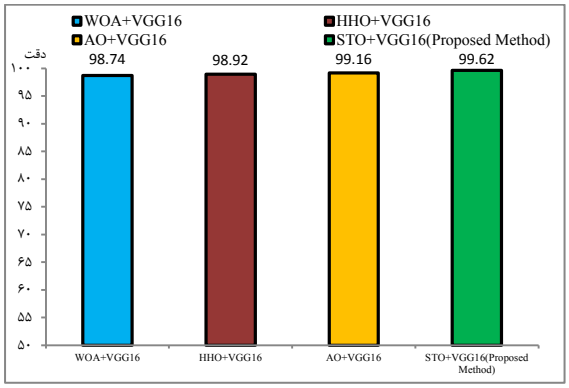
در این مطالعه، دسته‌بندی با استفاده از برچسب‌های باینری انجام می‌شود، به این معنی که تمام مقادیر مرتبط با ویژگی برچسب به

حمله یا امن تبدیل می‌شوند. در نمودار شکل(۱۰)، شاخص دقت، حساسیت و صحت روش پیشنهادی در تشخیص حملات در دو حالت VGG16 و STO+VGG16 با هم مقایسه شده است تا تأثیر انتخاب ویژگی در تشخیص حملات مشخص شود.

باتوجه‌به مقایسه انجام شده اگر انتخاب ویژگی در کنار طبقه‌بندی با معماری VGG16 انجام شود آنگاه دقت، حساسیت و صحتی به ترتیب برابر ۹۹/۶۲٪، ۹۹/۳۸٪ و ۹۸/۷۴٪ است و اگر از انتخاب ویژگی استفاده نشود آنگاه دقت، حساسیت و صحت روش پیشنهادی به ترتیب برابر ۹۷/۸۳٪، ۹۷/۱۲٪ و ۹۷/۲۳٪ است. به عبارت بهتر بکارگیری انتخاب ویژگی باعث می‌شود تا دقت، حساسیت و صحت روش پیشنهادی نسبت به معماری VGG16 در حدود ۱/۷۹٪، ۲/۲۶٪ و ۱/۵۱٪ افزایش یابد. در شکل(۱۱)، روش پیشنهادی از نظر شاخص دقت با چند روش فراابتکاری در فاز انتخاب ویژگی با هم مقایسه شده است. در این نمودار روش پیشنهادی با روشهای نظیر الگوریتم بهینه‌سازی وال[1]، بهینه‌سازی شاهین[2] و بهینه‌سازی عقاب طلایی[3] در شاخص دقت با هم مقایسه شده است.



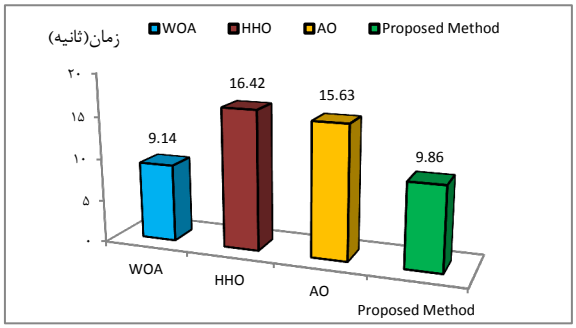
شکل (۱۰): مقایسه دقت، حساسیت و صحت در تشخیص نفوذ



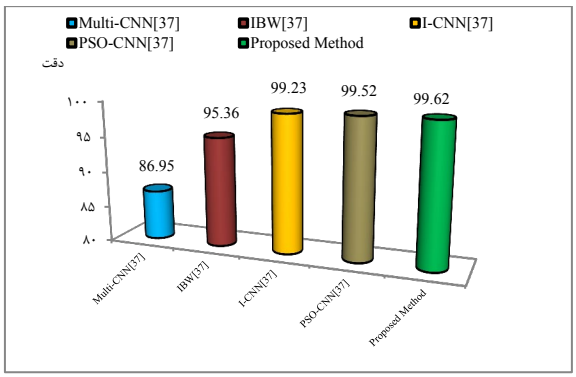
شکل (۱۱): مقایسه دقت، روش پیشنهادی با روش‌های فراابتکاری در انتخاب ویژگی و تشخیص نفوذ

آزمایش‌ها نشان می‌دهد روش پیشنهادی در تشخیص حملات به لایه مه دارای دقتی برابر ۹۹/۶۲٪ است و این درحالی است که دقت الگوریتم بهینه‌سازی وال، بهینه‌سازی شاهین و بهینه‌سازی عقاب طلایی به ترتیب برابر ۹۸/۷۴٪، ۹۸/۹۲٪ و ۹۹/۱۶٪ است. ارزیابی‌ها نشان داد روش پیشنهادی به دلیل دقت بیشتر در فاز انتخاب ویژگی از الگوریتم بهینه‌سازی وال، بهینه‌سازی شاهین و بهینه‌سازی عقاب طلایی در تشخیص حملات موفق‌تر است. روش پیشنهادی را می‌توان در فاز انتخاب ویژگی از نظر زمان اجرا با الگوریتم بهینه‌سازی وال، بهینه‌سازی شاهین و بهینه‌سازی عقاب طلایی مطابق نمودار شکل(۱۲)، نیز مقایسه نمود. با توجه به آزمایشات انجام شده شاخص زمان اجراء در روش پیشنهادی برابر ۹/۸۶ ثانیه در فاز انتخاب ویژگی است. زمان انتخاب ویژگی در تشخیص حملات در روش پیشنهادی فقط از الگوریتم وال بدتر شده است اما نسبت به الگوریتم شاهین و عقاب طلایی دارای زمان کمتری در تشخیص حملات است. پیچیدگی الگوریتم پیشنهادی از الگوریتم وال بیشتر است اما این پیچیدگی صرف افزایش دقت روش پیشنهادی شده است.

در نمودار شکل(۱۳)، روش پیشنهادی با چند روش تشخیص حملات بر پایه یادگیری عمیق از نظر شاخص دقت اجرا با هم مقایسه شده است[۳۷].



شکل (۱۲): مقایسه زمان انتخاب ویژگی در روش پیشنهادی و روش‌های فراابتکاری



شکل (۱۳): مقایسه دقت روش پیشنهادی با روش‌های یادگیری عمیق[۳۷]

آزمایش‌ها و مقایسه‌ها نشان می‌دهد روش پیشنهادی در تشخیص حملات به شبکه از روش‌های یادگیری عمیق نظیر CNN، Multi-CNN، IBW، I-CNN، PSO-CNN دارای دقت

[1] WOA
[2] HHO
[3] AO

بیشتری در تشخیص حملات به شبکه است. روش پیشنهادی این مزیت را دارد که دارای دقت بیشتری نسبت به روش‌های رایج یادگیری عمیق است و از طرفی هوشمندانه ترافیک شبکه را دچار کاهش ابعاد می‌دهد تا سرعت تشخیص حملات را افزایش دهد. در جدول(۳)، روش پیشنهادی در مجموعه‌داده UNSW-NB15 با چند روش انتخاب ویژگی مقایسه شده است.

آزمایش‌ها نشان می‌دهد روش پیشنهادی در مجموعه‌داده UNSW-NB15 موفق شده با ۱۴ ویژگی به دقتی حدود ۹۶/۸۲٪ برسد و دقت آن از روشهای مانند XGBoost، RAO ، جنگل تصادفی، کاهش مولفه اساسی و روش IG در تشخیص حملات بیشتر شود.

جدول (۳): مقایسه با روشهای انتخاب ویژگی در مجموعه تشخیص نفوذ UNSW-NB15

مرجع	روش انتخاب ویژگی	تعداد ویژگی انتخاب شده	دقت
[۳۸]	XGBoost	۱۹	۹۰/۵۸
[۳۹]	Rao Optimization Algorithm	۱۹	۹۲/۵
[۴۰]	Genetic Algorithm	۱۶	۸۷/۶۱
[۴۱]	IG, RF and RFE	۲۳	۸۴/۲۴
[۴۲]	RFE and PCA	۱۵	۹۴/۳
روش پیشنهادی	STO	۱۴	۹۶/۸۲

۵- نتیجه‌گیری

افزایش تعداد دستگاه‌های اینترنت اشیا در عصر جدید منجر به افزایش آسیب‌پذیری‌های امنیتی و حملات روز صفر شده است که بر اهمیت سیستم‌های تشخیص نفوذ شبکه تأکید می‌کند. دستگاه‌های اینترنت اشیا دارای منابع محدودی هستند که این موضوع باعث شده است تا این گره‌ها در مقابل حملات بسیار آسیب‌پذیر باشند. امنیت شبکه به یک جنبه ضروری از زندگی دیجیتال مدرن تبدیل شده است، زیرا تهدیدات و حملات سایبری همچنان در حال تکامل هستند. سازمان‌ها و افراد در حفاظت از دارایی‌های دیجیتال و اطلاعات حساس خود با چالش‌های مهمی روبرو هستند. این خطرات را می‌توان با استفاده از یک سیستم تشخیص نفوذ شبکه که می‌تواند فعالیت‌های مخرب و نقض‌های امنیتی احتمالی را در زمان واقعی شناسایی کند، تا حدی کاهش داد.

یک سیستم تشخیص نفوذ شبکه که سنتی بر تکنیک های تشخیص مبتنی بر قانون یا امضا متکی است. بااین حال، این تکنیک‌ها اغلب در انطباق با تهدیدات جدید و نوظهور شکست می‌خورند. با افزایش پیچیدگی حملات سایبری، تکنیک‌های مختلف یادگیری ماشین و یادگیری عمیق برای بهبود اثربخشی سیستم تشخیص نفوذ شبکه که معرفی شده‌اند. در میان مدل‌های مختلف یادگیری عمیق شبکه‌های عصبی کانولوشن تاکنون برای کاربردهای مختلف موفق بوده‌اند؛ لذا در این مقاله یک سیستم تشخیص نفوذ بر پایه معماری VGG16 که یک معماری موفق از شبکه عصبی کانولوشن است ارائه شده است. سیستم تشخیص نفوذ پیشنهادی در اینترنت اشیا استقرار دارد. سیستم تشخیص نفوذ پیشنهادی با الگوریتم ببر سیبری ویژگی‌های مهم را استخراج کرده و این بردار ویژگی را برای گره‌های مه فرعی ارسال می‌کند. گره‌های فرعی مه ترافیک را با بردار ویژگی بهینه کاهش ابعاد داده و ترافیک را به فرمت تصاویر RGB تبدیل می‌کنند و از این طریق شبکه VGG16 را آموزش می‌دهند تا ترافیک حملات را تشخیص دهد. روش پیشنهادی در مجموعه‌داده NSL-KDD مورد ارزیابی قرار گرفت و آزمایش‌ها نشان داد الگوریتم ببر سیبری نسبت به الگوریتم وال، شاهین و عقاب طلایی توانایی و دقت بیشتری در تشخیص حملات دارد. معماری پیشنهادی هزینه‌ای برای توزیع داده‌ها اضافه نمی‌کند؛ زیرا معماری اینترنت اشیا توزیع شده است و هر سیستم تشخیص نفوذ بخشی از ترافیک را دریافت نموده و آن را برای تشخیص نفوذ تجزیه‌وتحلیل می‌کند. از طرفی روش پیشنهادی نسبت به روش‌های CNN، Multi-CNN، IBW، I-CNN، PSO-CNN دقت بیشتری دارد. در پژوهش آتی معماری VGG16 و BiLSTM با هم ترکیب شده تا از توانایی آنها برای تشخیص دقیق حملات در IoT استفاده شود.

۶- مراجع

[1] B. Kaur, S. Dadkhah, F. Shoeleh, E. C. P. Neto, P. Xiong, S. Iqbal,... & A. A. Ghorbani, "Internet of things (IoT) security dataset evolution: Challenges and future directions," Internet of Things, vol. 22, pp. 100780, 2023, https://doi.org/10.1016/j.iotcps.2023.12.003.

[2] Z. Ahmad, A. S. Khan, K. Zen & F. Ahmad, "MS-ADS: Multistage Spectrogram image-based Anomaly Detection System for IoT security," Transactions on Emerging Telecommunications Technologies, vol. 34, 2023, https://doi.org/10.1002/ett.4810.

[3] D. Jin, S. Chen, H. He, X. Jiang, S. Cheng, & J. Yang, "Federated Incremental Learning based Evolvable Intrusion Detection System for Zero-Day Attacks," IEEE Network, vol. 37, pp. 125-132, 2023, https://doi.org/10.1109/MNET.018.2200349.

[4] K. He, D. D. Kim & M. R. Asghar, "Adversarial machine learning for network intrusion detection systems: a comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 25, pp. 538-566, 2023, https://doi.org/10.1109/COMST.2022.3233793.

[5] R. Chinnasamy & M. Subramanian, "Detection of Malicious Activities by Smart Signature-Based IDS," In Artificial Intelligence for Intrusion Detection Systems, pp. 63-78, Chapman and Hall/CRC, 2023, https://doi.org/10.1201/9781003346340-3.

[6] S. Alem, D. Espes, L. Nana, E. Martin, & F. De Lamotte, "A novel bi-anomaly-based intrusion detection

11, 2022, https://doi.org/10.3390/electronics11040515.
[20] E. U. H. Qazi, A. Almorjan & T. Zia, "A one-dimensional convolutional neural network (1d-cnn) based deep learning system for network intrusion detection," Applied Sciences, vol. 12, 2022, https://doi.org/10.3390/app12167986.
[21] S. Tu, M. Waqas, A. Badshah, M. Yin & G. Abbas, "Network intrusion detection system (NIDS) based on pseudo-siamese stacked autoencoders in fog computing," IEEE Transactions on Services Computing, vol. 16, https://doi.org/10.1109/TSC.2023.3319953.
[22] A. Telikani, J. Shen, J. Yang, & P. Wang, "Industrial IoT intrusion detection via evolutionary cost-sensitive learning and fog computing," IEEE Internet of Things Journal, vol. 9, pp. 23260-23271, 2022, https://doi.org/10.1109/JIOT.2022.3188224.
[23] M. P. Ramkumar, T. Daniya, P. M. Paul & S. Rajakumar, "Intrusion detection using optimized ensemble classification in fog computing paradigm, " Knowledge-Based Systems, vol. 252, 2022, https://doi.org/10.1016/j.knosys.2022.109364.
[24] A. Binbusayyis, "Hybrid VGG19 and 2D-CNN for intrusion detection in the FOG-cloud environment," Expert Systems with Applications, vol. 238, https://doi.org/10.1016/j.eswa.2023.121758.
[25] W. Yao, H. Shi & H. Zhao, "Scalable anomaly-based intrusion detection for secure Internet of Things using generative adversarial networks in fog environment," Journal of Network and Computer Applications, vol. 214, 2023, https://doi.org/10.1016/j.jnca.2023.103622.
[26] S. Bebortta, S. K. Das & S. Chakravarty, "Fog-enabled Intelligent Network Intrusion Detection Framework for Internet of Things Applications," In 2023 13th International Conference on Cloud Computing, Data Science & Engineering, 2023.
[27] Z. Abou El Houda & L. Khoukhi, "A hierarchical fog computing framework for network attack detection in sdn," In ICC 2022-IEEE International Conference on Communications, 2022.
[28] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg & M. M. Hassan, "A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network," Journal of Parallel and Distributed Computing, vol. 164, pp. 55-68, 2022, https://doi.org/10.1016/j.jpdc.2022.01.030.
[29] K. Kaliyaperumal, C. Murugaiyan, D. Perumal, G. Jayaraman & K. Samikannu, "Combined Ensemble Intrusion Detection Model using Deep learning with Feature Selection for Fog Computing Environments," Acta Scientiarum. Technology, vol. 45, 2022, https://doi.org/10.4025/actascitechnol.v45i1.60551.
[30] M. Khorram, and M. Rahmani-manesh, "DDoS Attack Detection System Using Ensemble Method Classification and Active Learning Approach," in Electronic and Cyber Defense, 2023, https://doi.org/20.1001.1.23224347.1402.11.2.1.4.)In Persian).
[31] M. Ghanavati Nasab, M. Ghazvini, F. Ghasemian, "Mobile botnets detection using deep learning techniques," in Electronic and Cyber Defense Quarterly, vol. 11, pp. 31-43, 2023. https://doi.org/20.1001.1.23224347.1402.11.2.3.6.)In Persian).
[32] M. Hesabi, M. Deypir, "An Improved Method for Malware Attack Detection in Cloud Computing Using Collective Learning," in Electronic and Cyber Defense , vol. 10, pp. 33-39, 2022, system approach for industry 4.0," Future Generation Computer Systems, vol. 145, pp. 267-283, 2023, https://doi.org/10.1016/j.future.2023.03.024.
[7] G. H. An & T. H. Cho, "Improving Sinkhole Attack Detection Rate through Knowledge-Based Specification Rule for a Sinkhole Attack Intrusion Detection Technique of IoT," Int. J. Comput. Netw. Vol. 9. pp. 169-178, 2022, https://doi.org/10.22247/ijcna/2022/212333.
[8] S. Roy, J. Li, & Y. Bai, "A two-layer fog-cloud intrusion detection model for IoT networks," Internet of Things, vol. 19, 100557, 2022, https://doi.org/10.1016/j.iot.2022.100557.
[9] S. Ahmad, I. Raza, M. H. Jamal, S. Djuraev, S. Hur & I. Ashraf, "Central Aggregator Intrusion Detection System for Denial of Service Attacks. Computers," Materials & Continua, vol. 74, pp. 2363-2377, 2023, https://doi.org/10.32604/cmc.2023.032694.
[10] M. Premkumar, T. V. P. Sundararajan, & G. Mohanbabu, "Dynamic defense mechanism for DoS attacks in wireless environments using hybrid intrusion detection system and statistical approaches," Tehnički vjesnik, vol. 29, pp. 965-970, 2022, https://doi.org/10.17559/TV-20210604113859.
[11] A. O. Alzahrani & M. J. Alenazi, "MLIDSDN: Machine learning based intrusion detection system for software-defined network," Concurrency and Computation: Practice and Experience, vol. 35, 2023, https://doi.org/10.1002/cpe.7438.
[1] [12] K. Hussain, Y. Xia, A. N. Onaizah, T. Manzoor & K. Jalil, "Hybrid of WOA-ABC and proposed CNN for intrusion detection system in wireless sensor networks," Optik, vol. 271, 2022, https://doi.org/10.1016/j.ijleo.2022.170145.
[2] [13] A. S. Alqahtani, "FSO-LSTM IDS: hybrid optimized and ensembled deep-learning network-based intrusion detection system for smart networks," The Journal of Supercomputing, vol. 78, pp. 9438-9455, 2022, https://doi.org/10.1007/s11227-021-04285-3.
[3] [14] S. Gautam, A. Henry, M. Zuhair, M. Rashid, A. R. Javed & P. K. R. Maddikunta, "A composite approach of intrusion detection systems: hybrid RNN and correlation-based feature optimization," Electronics, vol. 11, 2022, https://doi.org/10.3390/electronics11213529.
[4] [15] P. Trojovský, M. Dehghani & P. Hanuš, "Siberian tiger optimization: A new bio-inspired metaheuristic algorithm for solving engineering optimization problems," Ieee Access, vol. 10, pp. 132396-132431, 2022,https://doi.org/10.1109/ACCESS.2022.3229964.
[5] [16] C. Guerrero, I. Lera, & C. Juiz, "Genetic-based optimization in fog computing: Current trends and research opportunities," Swarm and Evolutionary Computation, vol. 72, 2022, https://doi.org/10.1016/j.swevo.2022.101094.
[6] [17] G. Zhao, Y. Wang & J. Wang, "Lightweight Intrusion Detection Model of the Internet of Things with Hybrid Cloud Fog Computing," Security and Communication Networks, 2023, https://doi.org/10.1155/2023/7107663.
[7] [18] M. A. Khan, "HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system," Processes, vol. 9, 2021, https://doi.org/10.3390/pr9050834.
[8] [19] A. Meliboev, J. Alikhanov & W. Kim, "Performance evaluation of deep learning based network intrusion detection system across multiple balanced and imbalanced datasets," Electronics, vol.

Applied Sciences, vol. 14, 2024, https://doi.org/10.3390/app14020479.
[39] S. M. Kasongo, & Y. Sun, "Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset, " Journal of Big Data, vol. 7, 2020, https://doi.org/10.1186/s40537-020-00379-6.
[40] S. N. Abd, M. Alsajri, & H. R. Ibraheem, "Rao-SVM machine learning algorithm for intrusion detection system," Iraqi Journal For Computer Science and Mathematics, vol. 1, pp. 23-27, 2020, https://doi.org/10.52866/ijcsm.2019.01.01.004.
[41] S. M. Kasongo, "An advanced intrusion detection system for IIoT based on GA and tree based algorithms," IEEE Access, vol. 9, pp. 113199-113212, 2021,https://doi.org/10.1109/ACCESS.2021.3104113.
[42] Y. Yin, J. Jang-Jaccard, W. Xu, A. Singh, J. Zhu, F. Sabrina, & J. Kwak, "IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset," Journal of Big Data, vol. 10, 2023, https://doi.org/10.1186/s40537-023-00694-8.
[43] H. Ghani, S. Salekzamankhani, & B. Virdee, "A hybrid dimensionality reduction for network intrusion detection," Journal of Cybersecurity and Privacy, vol. 3, pp. 830-843. 2023, https://doi.org/doi.org/10.3390/jcp3040037.
https://doi.org/20.1001.1.23224347.1401.10.4.4.4.)In Persian).
[33] https://dor.isc.ac/dor/20.1001.1.23224347.1401.10.3.4.2
[34] K. Dadashtabar Ahmadi, M. Kheirkhah, A. J. Rashidi, "Detection of advanced Cyber Attacks, Using Behavior Modeling Based on Natural Language Processing," in Electronic and Cyber Defense Quarterly, vol. 6, pp. 141-151, 2018, https://doi.org/20.1001.1.23224347.1397.6.3.12.2.)In Persian).
[35] F. G. da Silva, L. P. Ramos, B. G. Palm & R. Machado, "Assessment of Machine Learning Techniques for Oil Rig Classification in C-Band SAR Images," Remote Sensing, vol. 14, 2022, https://doi.org/10.3390/rs14132966.
[36] M. H. Alwan, Y. I. Hammadi, O. A. Mahmood, A. Muthanna & A. Koucheryavy, "High Density Sensor Networks Intrusion Detection System for Anomaly Intruders Using the Slime Mould Algorithm," Electronics, vol. 11, 2022, https://doi.org/10.3390/electronics11203332.
[37] D. Kilichev & W. Kim, "Hyperparameter Optimization for 1D-CNN-Based Network Intrusion Detection Using GA and PSO," Mathematics, vol. 11, 2023, https://doi.org/10.3390/math11173724.
[38] H. R. Sayegh, W. Dong, & A. M. Al-madani, "Enhanced Intrusion Detection with LSTM-Based Model, Feature Selection, and SMOTE for Imbalanced Data,"