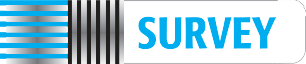


دریافت شده ۲۲ مارس ۲۰۲۴، پذیرفته شده ۱۳ آوریل ۲۰۲۴، تاریخ از انتشار ۱۸ آوریل ۲۰۲۴، تاریخ از فعلی نسخه ۲۶ آوریل ۲۰۲۴.

*دیجیتال شیء شناسه ‎۱۰.۱۱۰۹/دسترسی.۲۰۲۴.۳۳۹۰۸۴۴‎*

**

ابر شبکه ناهنجاری تشخیص استفاده از تکنیک‌های یادگیری ماشین و عمیق - اخیر تحقیق پیشرفت‌ها

امیرا ماهات عبدالله [](https://orcid.org/0000-0001-9896-5676)۱ ، عایشه سیف راشد عبید الکعبی ۱ ، قایا بارک ناصر دومان آلامری ۱ ، صیدا حفصه رفیق [](https://orcid.org/0000-0002-2445-3798)۱ ،

نورا شفا موسی [](https://orcid.org/0000-0001-7343-4000)۱،۲​ و تانگاول مورگان [](https://orcid.org/0000-0002-2510-8857)۱ ، (ارشد عضو، IEEE)

۱ دانشکده اطلاعات فناوری، یونایتد امارات متحده عربی دانشگاه، آل عین، ابو دبی، یونایتد امارات متحده عربی

۲ کالج از مهندسی، آل عین دانشگاه، آل عین، ابو دبی، یونایتد عرب امارات

متناظر نویسنده: تانگاول موروگان [(thangavelm@uaeu.ac.ae)](mailto:(thangavelm@uaeu.ac.ae)

این کار تا حدودی توسط دانشگاه امارات متحده عربی از طریق طرح پیشنهادی استارت‌آپ تحقیقاتی تحت حمایت قرار گرفت. گرانت G00004612/12T048.

 **چکیده** در چشم‌انداز به سرعت در حال تحول محاسبات و شبکه، مفاهیم شبکه‌های ابری داشته باشند به دست آورد قابل توجه برجستگی اگرچه ‎‏ ... ابر شبکه پیشنهادات بنا به تقاضا دسترسی به منابع مشترک، ناهنجاری‌ها ژست گرفتن پتانسیل خطرات به ‎‏ ... صداقت و امنیت از ابر شبکه‌ها. با این حال، محافظت از ابر شبکه علیه ناهنجاری‌ها باقی مانده است الف چالش. برخلاف سنتی تشخیص تکنیک‌ها، یادگیری ماشین (ML) و یادگیری عمیق (DL) روش‌های جدید و قابل تطبیقی را برای تشخیص ناهنجاری‌ها در شبکه‌های ابری ارائه می‌دهند. عینی از این مطالعه است به به طور جامع کاوش کردن موجود میلی لیتر /دی ال روش‌ها برای تشخیص متفاوت ناهنجاری‌ها مبتنی بر روی توزیع شده انکار از خدمات ناهنجاری (عدم سرویس توزیع‌شده) و نفوذ تشخیص سیستم‌های (IDS) در شبکه‌های ابری. این مطالعه به دنبال پرداختن به شکاف‌های موجود در تشخیص ناهنجاری برای شبکه‌های ابری است و راه‌حل‌های بالقوه‌ای را برای تشخیص ناهنجاری در این محیط‌های ابری پیشنهاد می‌دهد. هدف نهایی، مشارکت در ... ارزشمند بینش‌ها و عملی راه حل ها به افزایش ‎‏ ... امنیت و قابلیت اطمینان از ابر شبکه‌ها از طریق ناهنجاری مؤثر تشخیص توسط ML/ دی ال تکنیک‌ها. روش‌شناسی‌ها برای ML/DL هستند توضیح داده شده، همراه با آنها مزایا، معایب، و مربوطه رویکردها. در علاوه بر این، الف خلاصه از ‎‏ ... مقایسه بین مدل‌های مختلف یادگیری ماشین/یادگیری عمیق نیز گنجانده شده است.

 **اصطلاحات شاخص** شبکه ابری، رایانش ابری، می‌تواند، یادگیری ماشین (ML)، یادگیری عمیق (DL)، انکار سرویس توزیع‌شده (DDoS)، سیستم تشخیص نفوذ (IDS)، تشخیص ناهنجاری، امنیت.

1. **مقدمه**

در حوزه گسترده محاسبات، یک شبکه ابری، زیرساخت توزیع‌شده پیچیده و پیشرفته‌ای را نشان می‌دهد که از قابلیت‌های سرورهای راه دور و شبکه‌های به‌هم‌پیوسته برای ذخیره‌سازی، مدیریت و ... بهره می‌برد. پردازش از داده‌ها تسهیل شده توسط اینترنت اتصال. شبکه‌های ابری با کنار گذاشتن وابستگی سنتی به سرورهای محلی یا دستگاه‌های شخصی برای توابع محاسباتی، از منابع گسترده‌ای که در دسترس قرار گرفته‌اند، بهره می‌برند . از طریق الف پیچیده شبکه از به هم پیوسته سرورها مستقر در از نظر استراتژیک موقعیت یابی شده داده‌ها مراکز. این پارادایم شیفت در

[](https://orcid.org/0000-0002-0917-2277) وابسته ویرایشگر هماهنگ کننده ‎‏ ... بررسی از این نسخه خطی و ییمینگ تانگ آن را برای انتشار تأیید کرد .

معماری محاسباتی نشان‌دهنده‌ی فاصله گرفتن از معماری محلی و وابسته به سخت‌افزار است. عملیات به الف در سطح جهانی به هم پیوسته، سرشار از منابع مدل که دارد تبدیل شدن مترادف با مدرن تکنولوژیکی منظره. ابر محاسبات شامل می‌شود سه لایه‌ها، الف سیستم لایه، الف پلتفرم لایه، و یک لایه کاربردی. دو لایه اولیه بر روی ماشین‌های مجازی تمرکز دارند (ماشین‌های مجازی) و عملیاتی سیستم‌ها [[1] ،](#_bookmark98) [[2] .](#_bookmark99) روشن ‎‏ ... از سوی دیگر، لایه سوم با برنامه‌های کاربردی میزبانی شده توسط ابر سروکار دارد، مانند به عنوان مبتنی بر وب برنامه های کاربردی. این نکات برجسته ‎‏ ... مزایا و پذیرش گسترده رایانش ابری [[3] .](#_bookmark100) اگرچه ابر شبکه‌ها شامل شدن چندین امنیت اقدامات، آنها امنیت را نباید دست کم گرفت. شبکه ابری، مانند بسیاری از فناوری‌های جدید، دائماً مورد حمله دشمنان قرار می‌گیرد. سازمان بهداشت جهانی هستند همیشه آمدن بالا با جدید راه‌ها به دریافت

جلد ۱۲، ۲۰۲۴

© ۲۰۲۴ نویسندگان. این کار است دارای مجوز تحت الف خلاق عوام انتساب مجوز ۴.۰

برای برای اطلاعات بیشتر، به https://creativecommons.org/licenses/by/4.0/ 56749 مراجعه کنید.

دسترسی به پایان کاربران دستگاه‌ها و داده‌ها [[4] .](#_bookmark101) با این حال، با مزایا​ و پهن محبوبیت از ابر خدمات، فعلی مطالعات، مسائل و نگرانی‌های مربوط به امنیت و ارائه خدمات ناشی از سرویس‌های ابری را برجسته کرده‌اند. حوادث ابری چنین به عنوان شکست‌ها، از دست دادن داده‌ها، و حریم خصوصی تخلفات داشته باشید پتانسیل به هزینه کسب و کارها میلیاردها از دلار، به ویژه آنهایی که سازمان بهداشت جهانی استفاده اینها خدمات به فروشگاه مهم شرکت داده‌ها و کاربردها. چندین مثال این اصل را نشان می‌دهند. برای مثال، روی فوریه بیست و هشتم، ۲۰۱۷، یک آمازون اس۳ اختلال در سرویس در شمالی ویرجینیا تحت تأثیر قرار گرفته خدمات وب آمازون خدمات، متحمل شدن قابل توجه هزینه‌ها به دلیل غیرمجاز حذف از سرورها به دلیل یک خطای دستوری، طیف وسیعی از مشتریان و کاربران نهایی که از آن سرویس‌ها استفاده می‌کنند را تحت تأثیر قرار داده و منجر به اختلال در سرویس می‌شود. اختلال و پتانسیل داده‌ها دسترسی نگرانی‌ها درون آسیب دیده آمازون اس۳ زیرسیستم‌ها [[5] .](#_bookmark102) علاوه بر این، روشن ۵ مارس ۲۰۲۴، هزاران نفر گزارش دادند که خود به خود دچار سرگیجه شده‌اند. خروج‌ها از متا فیسبوک و اینستاگرام پلتفرم‌ها ، بنابراین، آنجا بود الف گسترده قطع برق در ‎‏ ... یک ابرشبکه جهانی که به نظر می‌رسید کل زیرساخت شرکت را مختل کرده و حساب‌های کاربران را غیرقابل دسترس کرده و آنها قادر به بازیابی دسترسی نبودند. با این حال، گمانه‌زنی‌های اجتناب‌ناپذیری نیز وجود داشت مبنی بر اینکه ممکن است متا یک حمله سایبری را تجربه کرده باشد [[6] .](#_bookmark103) بنابراین، مهم‌ترین چالش که ابر خدمات ارائه دهندگان صورت است کنترل کردن وقوع حوادث و تهدیدات مرتبط با ابر برای ارائه به مصرف‌کنندگان با الف قابل اعتماد و با کیفیت بالا خدمات. با این حال، متعدد مطالعات روی ناهنجاری تشخیص داشته باشند از ML/DL برای شناسایی ناهنجاری‌ها استفاده کرد.

جی و ال. [[7]](#_bookmark104) مقابله شده چالش‌ها در ناهنجاری تشخیص در داده‌های سری زمانی چند متغیره، با تمرکز بر ابعاد بالا، نویز و ناهنجاری‌های ناهمزمان. هدف آنها توسعه یک کارآمد تعبیه فضا استراتژی برای ناهنجاری تشخیص (SES-AD) در سری‌های زمانی چند متغیره، قادر به شناسایی دقیق ناگهانی تغییرات بدون تکیه کردن روی خاص توزیع سیگنال. SES-AD از یک استراتژی تعبیه فضا برای تصویر کردن داده‌ها برای محاسبه عدم تشابه استفاده کرد و امکان محلی‌سازی دقیق تغییرات را فراهم کرد. نتایج تجربی نشان داد که SES-AD بالا دقت روی عمومی مجموعه داده‌ها، عملکرد بهتری نسبت به مدل‌های موجود دارد و اثربخشی آن را در تشخیص ناهنجاری در زمان واقعی نشان می‌دهد .

هو و همکاران [[8]](#_bookmark105) محدودیت‌های شناسایی‌شده در تشخیص ناهنجاری فعلی تکنیک‌ها برای چند متغیره زمان سری (ام تی اس) داده‌ها، مانند به عنوان فقدان از مداوم یادگیری توانایی و طولانی زمان‌های یادگیری برای ابعاد بالا مجموعه داده‌ها. هدف قرار دادند. به توسعه یک چارچوب محاسباتی جدید، مبتنی بر بازگشت محلی مبتنی بر نرخ اختلاف و نفاق جستجو (LRRDS) به تشخیص ناهنجاری‌های موجود در داده‌های MTS. LRRDS شامل تولید نمودارهای بازگشتی، قطعه‌بندی MTS خام برای زیرتوالی دقیق ناهماهنگی بود . شناسایی، و ارزیابی کردن ‎‏ ... رویکرد روی مجموعه داده‌های مختلف.

اقبال و امین [[9]](#_bookmark106) متمرکز بر رسیدگی به چالش‌ها در حوزه ناهنجاری‌ها تشخیص و زمان سری پیش‌بینی با استفاده از دی ال مدل‌ها . آنها اهداف شامل شدن در حال بهبود دقت در تشخیص ناهنجاری، بهبود پیش‌بینی سری‌های زمانی و بررسی تأثیر تکنیک‌های پیش‌پردازش بر عملکرد مدل . پیشنهادی سیستم شامل می‌شود ناهنجاری تشخیص با استفاده از متغیر-

تکنیک‌های یادگیری عمیق متنوع مانند حافظه کوتاه‌مدت بلندمدت (LSTM)، خودرمزگذار LSTM مجتمع مدل‌ها، شبکه مولد تخاصمی (GAN) و معماری‌های ترانسفورماتور.

همچنین، هی و همکاران [[10]](#_bookmark107) یک آشکارساز ناهنجاری سری زمانی چند متغیره آگاه از توپولوژی (TopoMAD) ارائه دادند، یک روش یادگیری عمیق که ناهنجاری‌ها را در سیستم‌های ابری بدون نظارت تشخیص می‌دهد. اهداف آنها شامل یکپارچه‌سازی سیستم بود توپولوژی، استخدام گراف عصبی شبکه‌ها (جی ان ان) و شبکه‌های حافظه کوتاه‌مدت بلند (LSTM) و استقرار- ایجاد یک مدل تصادفی seq2seq. نتایج، بهبود قابل توجهی در دقت و صحت نشان می‌دهد که اثربخشی یادگیری ماشینی (DL) را در مدیریت داده‌های پیچیده برجسته می‌کند.

با این حال، ‎‏ ... استفاده از دی ال/ میلی لیتر رویکردها در ناهنجاری همانطور که در [11 [] توضیح داده شده است،](#_bookmark108) تشخیص در سیستم‌های ابری هم پتانسیل و هم چالش را به همراه دارد [.](#_bookmark108) یکی از مهمترین مسائل این است پیچیدگی ذاتی و تنوع داده‌های ابری، که شامل موارد زیر می‌شود مختلف منابع چنین به عنوان شبکه ترافیک، سیستم لاگ‌ها و رفتار کاربر. این ناهمگونی، استخراج ویژگی و آموزش مدل را پیچیده می‌کند، زیرا داده‌ها ممکن است حاوی الگوهای غیرخطی و ناهنجاری‌های جزئی باشند که تشخیص آنها دشوار است. علاوه بر این، ماهیت پویای سیستم‌های ابری، که شامل می‌شود سریع مقیاس‌بندی، منبع تخصیص، و تغییرات حجم کار، وظیفه حفظ انعطاف‌پذیری مدل را پیچیده می‌کند و انطباق بیش از زمان. همچنین، ‎‏ ... مقیاس‌پذیری و الزامات پردازش مرتبط با روش‌های یادگیری ماشین/یادگیری عمیق. علاوه بر این، اطمینان از ‎‏ ... حریم خصوصی و امنیت از حساس داده‌های مورد استفاده برای آموزش دی‌ال/ام‌ال مدل‌ها در چند مستاجری ابر محیط‌ها باقی مانده است الف برترین نگرانی، ایجاب کننده رمزگذاری قوی، کنترل‌های دسترسی و تکنیک‌های حفظ حریم خصوصی برای کاهش خطر نقض داده‌ها و حملات خصمانه. پرداختن به این چالش‌ها نیازمند تلاش‌های بین رشته‌ای برای توسعه روش‌های مقیاس‌پذیر، کارآمد از نظر منابع و آگاه از حریم خصوصی است. الگوریتم‌های DL/ML متناسب با ویژگی‌های منحصر به فرد محیط‌های ابری، ضمن تقویت ... همکاری بین دانشگاه، صنعت، و نهادهای نظارتی برای ایجاد بهترین شیوه‌ها و استانداردها برای تشخیص ناهنجاری ایمن و مؤثر در ابر.

این کاغذ فراهم می‌کند الف ادبیات نمای کلی از میلی لیتر/ دی ال مدل‌ها برای مبتنی بر ابر ناهنجاری تشخیص. مقاله روش‌های یادگیری ماشین/یادگیری عمیق (ML/DL) و کاربردهای آنها در تشخیص شبکه‌های ابری را شرح می‌دهد. ناهنجاری‌ها آن تمرکزها روی مربوطه مطالعات در مورد استفاده از ML/DL برای تشخیص انکار توزیع‌شده حملات سرویس (DDoS) و سیستم‌های تشخیص نفوذ (IDS).

تحقیقات ما بر روی نشریاتی متمرکز بود که معیارهای استاندارد را رعایت می‌کردند و از «شبکه‌های ابری»، «محاسبات ابری» و «...» استفاده می‌کردند. ''می‌تواند'' «ماشین» یادگیری (ML) ، '' عمیق یادگیری (DL) توزیع شده انکار از خدمات (DDoS) « سیستم تشخیص نفوذ (IDS)،» «تشخیص ناهنجاری» و «امنیت » به عنوان کلمات کلیدی. به طور خاص، ما در جدیدترین فناوری‌های پیشرفته، ارزش قائلیم. کاغذها، به عنوان آنها آدرس پرطرفدار این مقاله به عنوان یک منبع آکادمیک جامع برای کسانی که علاقه‌مند به بررسی تشخیص ناهنجاری در محیط‌های ابری در حوزه‌های یادگیری ماشین/یادگیری عمیق هستند، طراحی شده است. بنابراین، قابل توجه است اهمیت است داده شده به فراهم کردن مفصل توضیحات​ از ‎‏ ... ام ال/دی ال روش‌ها، بحث ‎‏ ... مزایا و

معایب سیستم‌های پیشنهادی مختلف و مشخص کردن فرصت‌ها برای آینده تحقیق و توسعه. اثربخشی از اینها سیستم‌ها در شناسایی و آدرس‌دهی حملات DDoS و آی دی اس، تأکید می‌کند ‎‏ ... نیاز برای ارتقاء دهنده روش‌های تشخیص و کاهش ناهنجاری‌ها در شبکه‌های ابری. با این حال، استراتژی‌های مدرن برای تشخیص ناهنجاری‌ها در شبکه‌های ابری معمولاً شامل استفاده از فناوری‌های پیشرفته است. فناوری‌ها و دنبال کردن ‎‏ ... بهترین مبتنی بر ابر روش‌های تشخیص ناهنجاری

مشارکت‌ها از این بررسی عبارتند از: (من) الف جزئیات بررسی و بحث از میلی لیتر/ دی ال تکنیک‌ها در حملات انسداد سرویس (DDOS) تشخیص و IDS ناهنجاری مبتنی بر هستند معرفی شده، (ii) مختلف ابر سناریوهای شبکه استخدام میلی لیتر / دی ال برای حملات انسداد سرویس (DDOS) حمله تشخیص و IDS هستند تحلیل شده، (۳) نقد و بررسی از ابر شبکه مجموعه داده‌ها برای تشخیص ناهنجاری‌ها در یک شبکه ابری استفاده می‌شود، (iv) ویژگی‌ها و مزایا از هر کدام ام ال/دی ال مدل در ناهنجاری تشخیص خلاصه شده است، (v) شکاف تحقیقاتی نیز مورد بحث قرار گرفته است، و (vi) دامنه پیشرفت‌ها برای تحقیقات آینده نیز مورد بررسی قرار گرفته است.

استراحت از این بررسی است ساختار یافته به عنوان به شرح زیر است: بخش [سوم](#_bookmark12) بر مسائل امنیتی در شبکه‌های ابری تمرکز دارد. بخش [چهارم](#_bookmark21) تشخیص ناهنجاری مبتنی بر شبکه ابری را معرفی می‌کند. بخش [پنجم](#_bookmark31) منبع مجموعه داده‌ها را شرح می‌دهد. بخش‌های [ششم](#_bookmark32) و [هفتم](#_bookmark70) توصیف شده ‎‏ ... روش‌ها و مرتبط کاغذها برای میلی لیتر و دی ال در حملات انسداد سرویس (DDOS) تشخیص و شناسه‌ها ناهنجاری مبتنی بر. بخش [هشتم](#_bookmark92) شکاف تحقیقاتی را مورد بحث قرار می‌دهد. بخش [نهم](#_bookmark94) دامنه بهبود را معرفی کرد. بخش [دهم](#_bookmark97) نتیجه‌گیری ارائه می‌دهد.

1. **تحقیق روش‌شناسی**

این مطالعه استفاده می‌کند الف ادبیات بررسی به شناسایی کاغذها مربوط به ‎‏ ... تحقیق موضوع یا به آدرس خاص تحقیق متمرکز روی ابر ناهنجاری‌ها، با الف اصلی تمرکز روی حملات انسداد سرویس (DDOS) حمله تشخیص و شناسه‌ها مبتنی بر ناهنجاری تکنیک‌ها. در این ادبیات در این بررسی، ما از مناسب‌ترین و قابل اعتمادترین روش برای مستندسازی و ارزیابی مطالعات تحقیقاتی موجود استفاده کردیم. تکنیک بررسی متون قادر می‌سازد محققان به بررسی هر دو ‎‏ ... مزایا و معایب مطالعات تحقیقاتی قبلی، انجام یک بررسی کامل مطالعه به شناسایی آینده‌نگر تحقیق شکاف‌ها به عنوان و همچنین روندها و مشکلات آینده، و یک ساختار و نقطه شروع عالی برای ایجاد یک موضوع تحقیقاتی جدید فراهم می‌کند. به طور کلی فرآیند برای انتخاب کردن کاغذها، دنبال کردن ایجاد رشته‌های جستجو، در شکل [1 نشان داده شده است](#_bookmark22) .

ما انجام شده الف سخت‌گیرانه و سیستماتیک ادبیات بررسی شامل مختلف معتبر دیجیتال پایگاه‌های داده، از جمله IEEE اکسپلور، اسپرینگر، الزویر، وایلی، تیلور و فرانسیس، MDPI، و هنداوی انتخاب شده برای آنها اثبات شده آهنگ سابقه ارائه جدیدترین و معتبرترین مقالات در زمینه مسائل مربوط به شبکه‌های ابری و راه‌حل‌های امنیتی تثبیت‌شده.

با در نظر گرفتن بازه زمانی ۲۰۲۰ تا ۲۰۲۴، محدوده زمانی ما بر آن بود تا جدیدترین پیشرفت‌ها در این حوزه را به تصویر بکشیم. با استفاده از مجموعه‌ای دقیق از عبارات جستجو مانند «ابر» شبکه، «ابر» محاسبات، ''می‌تواند'' « یادگیری ماشین» (ML) ، '' عمیق یادگیری (دی‌ال)،'' توزیع شده حملات انکار سرویس (DDoS)، سیستم تشخیص نفوذ (IDS)، تشخیص ناهنجاری و امنیت. ما مخازن کتابخانه‌های اصلی را به طور کامل بررسی کردیم.

در نتیجه، ۲۷۰۲ مقاله که می‌توانند بالقوه مرتبط باشند بودند شناسایی شد. دنبال کردن این، مقالات منتشر شده قبل از ۲۰۲۰ (372) بودند حذف شده، پیشرو به الف تمرکز روی ۲۳۳۰ مقالات منتشر شده بین سال‌های ۲۰۲۰ تا ۲۰۲۴. برای محدود کردن بیشتر ‎‏ ... انتخاب، مقالات نه مرتبط به ماشین یادگیری یا یادگیری عمیق (۸۶۳) به همراه مقالات کنفرانس، کتاب‌ها، کارگاه‌ها و مجلات حذف شدند که در نتیجه ۷۰۲ مقاله در حوزه هوش مصنوعی (AI) قرار گرفتند. از طریق الف بررسی از عناوین و چکیده‌ها، ۴۴۲ مقالات حذف شدند و 260 مقاله باقی ماندند که تأیید شد منحصراً در مجلات معتبر منتشر می‌شوند. پس از حذف نظرسنجی و بررسی مقالات (82)، ما همچنین هر کدام را مستثنی کرد مقالات مرتبط به SDN، مه، و لبه محیط‌ها

(114). مجموعه نهایی برای تجزیه و تحلیل دقیق شامل 64 مقاله بود (به شکل [1 مراجعه کنید](#_bookmark22) ).

1. **امنیت مسائل در شبکه‌های ابری**

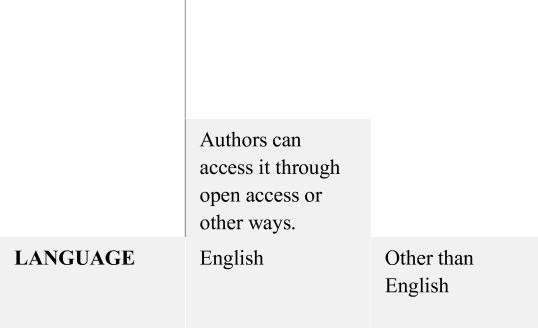
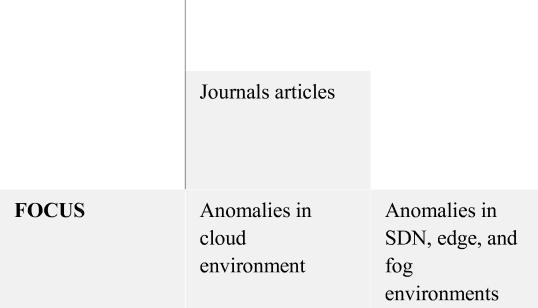
معماری از ابر محاسبات شامل می‌شود دو اجزای اصلی، بخش جلویی (front end) و بخش پشتی (back end). بخش جلویی به عنوان رابطی عمل می‌کند که از طریق آن کاربران با سیستم تعامل دارند. در همین حال، ‎‏ ... برگشت پایان شامل می‌شود مختلف مدل‌های سرویس ابری، یعنی زیرساخت به عنوان سرویس (IaaS)، پلتفرم به عنوان سرویس (PaaS) و نرم‌افزار به عنوان سرویس (SaaS). شکل [2](#_bookmark29) انواع کاربران مرتبط با هر مدل را به همراه نمونه‌هایی از برنامه‌های کاربردی مورد استفاده در آنها نشان می‌دهد.

* 1. *نرم‌افزار به عنوان سرویس (نرم‌افزار به عنوان سرویس)*

این است ‎‏ ... اول لایه از ‎‏ ... خدمات مدل. در این ابر در این مدل، ارائه‌دهندگان دسترسی به پایگاه داده و نرم‌افزار را ارائه می‌دهند، اما نرم‌افزار به عنوان سرویس (SaaS) با چالش‌های امنیتی مواجه است و مسئولیت را بر دوش کاربران می‌گذارد. کاربران باید در مورد اطلاعات و دسترسی‌های مشترک محتاط باشند.

تهدیدات سایبری اخیر، جذابیت ارائه دهندگان خدمات ابری را به عنوان هدف برجسته کرده و کاربران را ملزم به بررسی دقیق امنیت ارائه دهندگان خدمات می‌کند [[12] .](#_bookmark109) حملات DDoS تهدیدی قابل توجه برای ... پیاده‌سازی‌های SaaS، که هم ارائه‌دهندگان و هم کاربران را تحت تأثیر قرار می‌دهد. SaaS، بودن الف برجسته مدل در ابر محاسبات، توجه عوامل مخربی را که به دنبال اختلال در خدمات هستند، جلب می‌کند. با SaaS، نرم‌افزار به صورت مرکزی میزبانی می‌شود و از راه دور به آن دسترسی پیدا می‌شود، که آن را در معرض حملات DDoS با هدف سرکوب گسترده قرار می‌دهد. سرورها و رندرینگ خدمات غیرقابل دسترس به کاربران قانونی. این حملات می‌توانند عملیات تجاری را مختل کنند، علت مالی زیان‌ها، و لکه‌دار کردن ‎‏ ... اعتبار ارائه دهندگان SaaS. اجرای اقدامات امنیتی قوی، از جمله آی دی اس، فایروال‌ها، و رمزگذاری پروتکل‌ها، است حیاتی برای کاهش دادن ‎‏ ... ریسک از حملات انسداد سرویس (DDOS) حملات. علاوه بر این، نظارت مداوم و سریع پاسخ مکانیسم‌ها هستند ضروری برای شناسایی و خنثی کردن مؤثر چنین حملاتی، و محافظت از یکپارچگی و در دسترس بودن پلتفرم‌های SaaS برای کاربران [[13] .](#_bookmark110) در همین حال، تشخیص نفوذ در تنظیمات SaaS برای محافظت از ارائه دهنده خدمات و کاربران آن حیاتی است. SaaS شامل موارد زیر است : چندگانه کاربران اشتراک گذاری ‎‏ ... همان کاربرد به عنوان مثال، چالش‌های امنیتی منحصر به فردی را ایجاد می‌کند. IDS سنتی ممکن است به دلیل کنترل محدود بر زیرساخت، با SaaS سازگار نباشد. بنابراین، چند مستاجری شناسه‌ها چارچوب‌ها هستند لازم است. اینها

**جدول ۱.** خلاصه از ‎‏ ... معیارها برای شمول و محرومیت معیارها.



چارچوب‌ها باید ارائه‌دهندگان را قادر سازند تا IDS را به عنوان یک سرویس ارائه دهند، ترافیک شبکه و فعالیت‌های سیستم را رصد کنند تا اقدامات مخرب را به صورت بلادرنگ شناسایی و با آنها مقابله کنند. نفوذ مؤثر تشخیص مکانیسم‌ها کمک نرم‌افزار به عنوان سرویس (SaaS) ارائه دهندگان پلتفرم را ارتقا دهید امنیت، محافظ حساس داده‌ها از دسترسی غیرمجاز [[14] .](#_bookmark111)

* 1. *پلتفرم به عنوان سرویس (PaaS)*

این دوم لایه از ‎‏ ... خدمات مدل [[12]](#_bookmark109) پلتفرم به عنوان الف سرویس (PaaS) یک پلتفرم محاسباتی ارائه می‌دهد که شامل منابع اساسی مانند سیستم عامل‌ها، زبان‌های برنامه‌نویسی، پایگاه‌های داده و سرورهای وب است. این منابع به طور خودکار با تغییرات سازگار می‌شوند. به رسیدگی تغییرات در کاربرد خواسته‌ها در این راه اندازی، توسعه دهندگان استفاده خاص کاربرد رابط‌ها (API ها) به برنامه‌هایی را برای یک محیط خاص بسازید . PaaS همچنین امکان کنترل بر تنظیمات استقرار و پیکربندی نرم‌افزار را فراهم می‌کند [[15] .](#_bookmark112) با این حال، حبیب و همکاران [[16]](#_bookmark113) یک سیستم تشخیص DDoS برای معماری‌های ابری PaaS و Infrastructure-as-a-service (IaaS) پیاده‌سازی کردند که از یک طبقه‌بندی‌کننده‌ی ترکیبی یادگیری ماشین از پیش آموزش‌دیده شامل مدل‌هایی مانند جنگل تصادفی، درخت تصمیم‌گیری، ماشین بردار پشتیبان و XGBoost استفاده می‌کند.

* 1. *زیرساخت به عنوان سرویس (اینترنت به عنوان سرویس)*

زیرساخت به عنوان سرویس (IaaS) یک مدل رایانش ابری است که اجازه می‌دهد مشتریان به استفاده کردن مجازی سازی شده منابع محاسباتی چنین به عنوان مجازی ماشین آلات، ذخیره سازی، و شبکه سازی از طریق ‎‏ ... اینترنت. این خدمات قادر می‌سازد سازمان‌ها به اجاره زیرساخت فناوری اطلاعات بر اساس پرداخت انعطاف‌پذیر، که امکان توسعه منابع را بر اساس نیازهای آنها بدون نیاز به سرمایه‌گذاری در یا رسیدگی فیزیکی سخت‌افزار [[17] .](#_bookmark114) سرویس اینترنت به عنوان سرویس (IAAS)، یکی از ‎‏ ... سه ابر خدمات مدل‌ها، است بسیار مستعد به

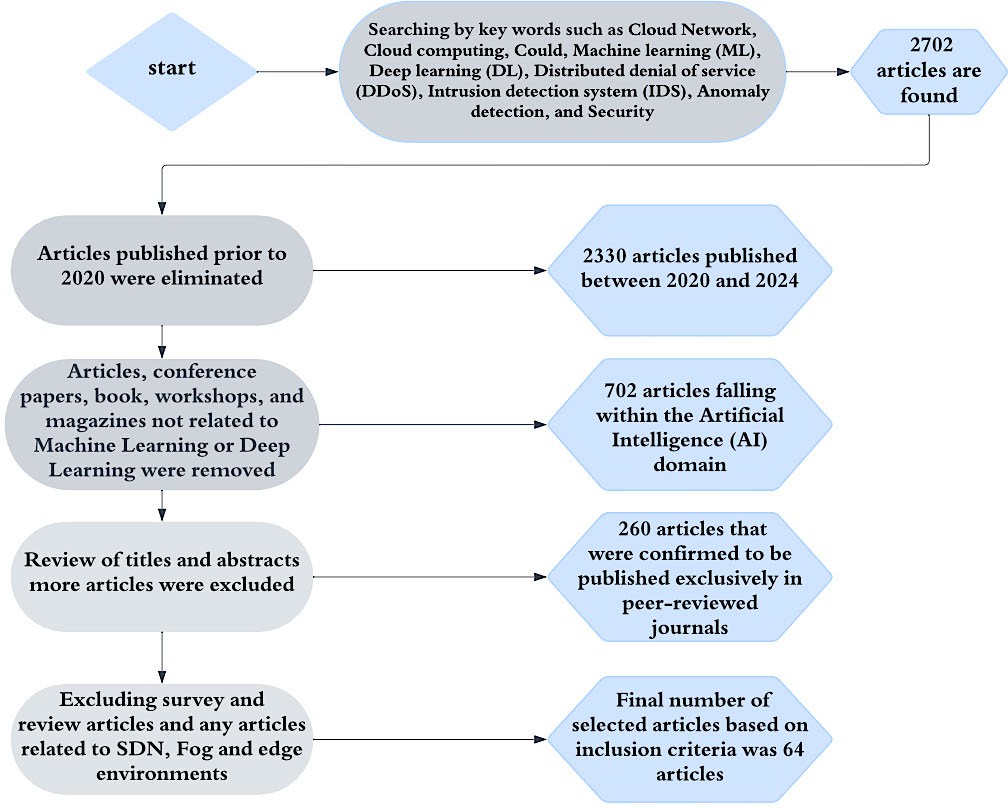
حملات DDoS. ماهیت مشترک این منابع ابری باعث می‌شود آنها الف نخست هدف برای حملات انسداد سرویس (DDOS) حملات، که به دنبال غرق کردن ‎‏ ... زیرساخت و رندر آن غیرقابل دسترس به کاربران قانونی. حملات DDoS با استفاده از فرآیندها و اقدامات متقابل متنوعی مانند پیشگیری از نفوذ، تشخیص نفوذ و پاسخ به نفوذگر [[18] در برابر آنها دفاع می‌شوند .](#_bookmark115) به دلیل خطرات امنیتی مرتبط با IaaS در محاسبات ابری، نیاز مبرمی به نصب IDS برای رسیدگی به آنها وجود دارد. اینها مسائل. آنجا است همچنین الف نیاز برای قوی اقدامات امنیتی برای ایمن‌سازی سرویس‌های زیرساخت مبتنی بر ابر ، و IDS متمرکز بر IaaS به عنوان امری مهم شناخته شده است [[19] .](#_bookmark116)

1. **ابر شبکه‌ها مبتنی بر تشخیص ناهنجاری**

ناهنجاری‌ها در یک شبکه ابری نشان‌دهنده انحراف از الگوها، رفتارها و رویدادهای مورد انتظار هستند که به طور بالقوه نشان‌دهنده تهدیدات امنیتی، بی‌نظمی‌های عملیاتی یا مشکلات عملکردی هستند. این ناهنجاری‌ها که به انواعی مانند امنیت، ترافیک شبکه، استفاده از منابع، رفتار برنامه، داده‌ها و رفتار کاربر طبقه‌بندی می‌شوند، شامل دسترسی غیرمجاز، انتقال غیرمعمول داده‌ها و منابع غیرطبیعی می‌شوند. استفاده کنید. شناخت و آدرس‌دهی اینها ناهنجاری‌ها حیاتی است برای حفظ کردن ‎‏ ... ابر شبکه صداقت، امنیت، و قابلیت اطمینان، حفاظت علیه سایبری تهدیدها، و تضمین عملکرد بهینه. در حوزه تحقیق، ناهنجاری‌های متنوعی شناسایی شده‌اند که موانع بزرگی را برای زیرساخت امنیتی شبکه‌های ابری ایجاد می‌کنند. موارد زیر را شامل می‌شود:

* 1. *توزیع‌شده انکار از خدمات (DDOS) حمله*

حمله انکار سرویس توزیع‌شده (DDoS) نوعی حمله سایبری است در که چندگانه سیستم‌ها یا دستگاه‌ها هستند استفاده شده



**شکل ۱.** کاغذ انتخاب فرآیند.

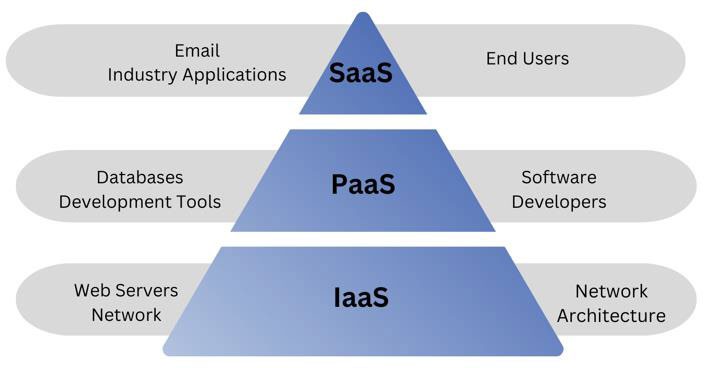
برای پر کردن سرور یا شبکه‌ی هدف با ترافیک زیاد، و خارج کردن آن از دسترس کاربران قانونی [[20] .](#_bookmark117)

در محاسبات ابری، حملات DDoS می‌توانند خسارات قابل توجهی به ارائه دهندگان خدمات ابری و مشتریان آنها وارد کنند و منجر به از کارافتادگی، از دست دادن درآمد و آسیب به اعتبار شوند. بنابراین، داشتن مکانیسم‌های تشخیص و پیشگیری مؤثر برای کاهش تأثیر حملات DDoS در محیط‌های محاسبات ابری بسیار مهم است. انواع حملات DDoS بر اساس آسیب‌پذیری مورد سوءاستفاده، ممکن است به عنوان حملات سیل‌آسا، سوءاستفاده از پروتکل طبقه‌بندی شوند. حملات، تقویت حملات، و بدشکل حملات بسته [[21] .](#_bookmark118) طبق شکل [3](#_bookmark30) ، پیش‌بینی می‌شود تعداد حملات DDoS تا سال 2023 بیش از دو برابر شود و به 15.4 میلیون برسد، همانطور که سیسکو در سال 2020 گزارش داده است [[22] .](#_bookmark119) با این حال، افزایش حملات انسداد سرویس (DDOS) حمله تشخیص و پیشگیری محققان از روش‌های ML/Dl استفاده کرده‌اند که در بخش [VI مورد بحث قرار خواهد گرفت](#_bookmark32) .

* 1. *مبتنی بر ناهنجاری نفوذ تشخیص سیستم‌ها (IDS)*

نفوذها شامل شدن الف توالی از به هم پیوسته فعالیت‌های مخرب اعدام شده توسط داخلی یا خارجی مهاجمان، هدف گیری

به سازش ‎‏ ... هدفمند سیستم [[23] .](#_bookmark120) علاوه بر این، تشخیص نفوذ فرآیندی است که سیستم‌های کامپیوتری را رصد می‌کند. و شبکه ترافیک فیکشن و تحلیل کردن فعالیت به تشخیص سیستم بالقوه تهدیدها [[24] .](#_bookmark121) در اخیر بارها، شناسه‌ها داشته باشند تبدیل شدن به دلیل افزایش فراوانی و شدت حملات شبکه، اجزای جدایی‌ناپذیر چارچوب‌های امنیتی بسیاری از سازمان‌ها هستند. تشخیص الف امنیت نقض شامل می‌شود نظارت و تجزیه و تحلیل دستگاه یا شبکه هدف برای یافتن نشانه‌هایی از دسترسی غیرمجاز. چنین نقض‌هایی به عنوان تلاش برای ... تعریف می‌شوند. سازش ‎‏ ... محرمانگی، صداقت، یا در دسترس بودن از یک کامپیوتر سیستم یا شبکه، یا به دور زدن آن امنیت اقدامات [[25] .](#_bookmark122) با این حال، رایج‌ترین رویکردهای تشخیص نفوذ، مبتنی بر امضا و مبتنی بر ناهنجاری هستند. آنها اغلب با هم، چه به صورت یکپارچه و چه به صورت جداگانه، برای افزایش دقت تشخیص استفاده می‌شوند. از نظر تشخیص مبتنی بر ناهنجاری، انواع مختلفی از تکنیک‌های تشخیص ناهنجاری بر اساس روش مورد استفاده برای شناسایی ناهنجاری‌ها، مانند یادگیری ماشین/یادگیری عمیق، منطق فازی، ماشین بردار پشتیبان (SVM) و داده‌کاوی، طبقه‌بندی می‌شوند. در طول دهه گذشته، مطالعات متعددی این روش‌ها را بررسی کرده‌اند، همانطور که در بخش [هفتم نشان داده شده است. همانطور که در این](#_bookmark70) بررسی بیشتر توضیح داده خواهد شد .



**شکل ۲.** ابر خدمات مدل‌ها.



**شکل ۳.** حملات انسداد سرویس (DDOS) مجموع حملات تاریخ و پیش‌بینی‌ها

1. **منبع از مجموعه داده‌ها**

در این بخش، ما توضیح دهید و دسته‌بندی کردن ‎‏ ... مجموعه داده‌ها مورد استفاده در ‎‏ ... بررسی شده ادبیات مبتنی بر روی ‎‏ ... ابر شبکه داده‌های ترافیک. فراوانی استفاده از مجموعه داده‌ها در ادبیات بررسی شده در شکل [4 نشان داده شده است](#_bookmark38) . بنابراین، انتخاب دقیق مجموعه داده‌ها برای تضمین تشخیص و طبقه‌بندی کارآمد بسیار مهم است. از ناهنجاری‌ها در ابر محیط‌ها. با این حال، در ابر محاسبات امنیت، متفاوت مجموعه داده‌ها هستند مورد استفاده قرار گرفت برای آموزش مدل‌های یادگیری ماشین/یادگیری عمیق. جدول [2](#_bookmark44) توصیفی از پرکاربردترین مجموعه داده‌های مورد استفاده در امنیت محاسبات ابری که در این بررسی استفاده شده است، ارائه می‌دهد.

1. **میلی لیتر و دی ال مبتنی بر برای حملات انسداد سرویس (DDOS) تشخیص در شبکه‌های ابری**

با توجه به زمان‌بر بودن مراحل توسعه، آزمایش و استقرار مبتنی بر ابر ناهنجاری تشخیص سیستم‌ها بعد از

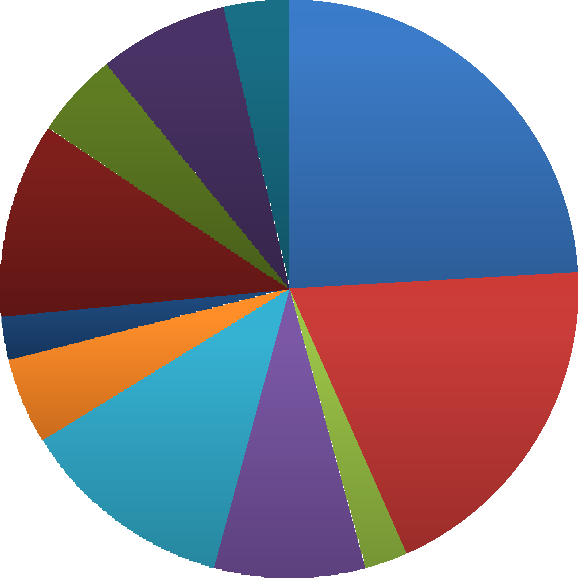
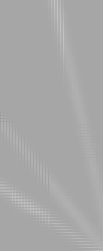
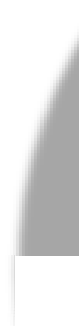
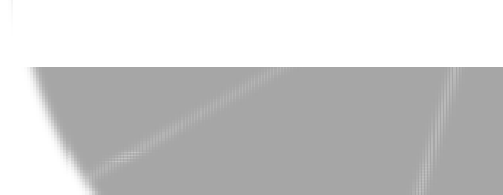
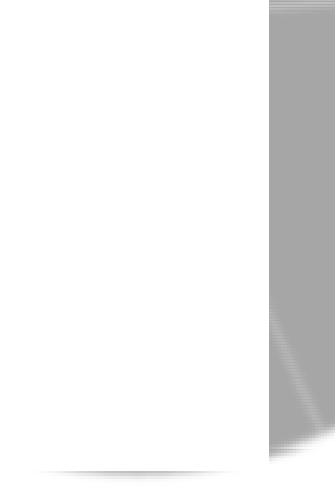
با هر حمله غیرمنتظره، نیاز مبرمی به راه‌حل‌های کمتر وابسته به انسان در تشخیص ناهنجاری وجود دارد. مبتنی بر ابر ناهنجاری تشخیص با استفاده از میلی لیتر فناوری به این موضوع می‌پردازد مسئله توسط فراهم کردن الف سیستم قادر از یادگیری از داده‌ها و تشخیص ناهنجاری‌ها بر اساس الگوهای آموخته‌شده [[35] .](#_bookmark123) از سوی دیگر، DL زیرمجموعه‌ای پیچیده از ML است که شامل از متعدد لایه‌ها از نورون‌ها که منعکس کردن ‎‏ ... فرآیند یادگیری. یادگیری ماشینی (DL) قادر به مدیریت حجم عظیمی از داده‌ها است و اثربخشی خود را در زمینه‌های مختلف نشان داده است [[36] .](#_bookmark124) این بخش رایج‌ترین کاربرد تکنیک‌های یادگیری ماشینی/یادگیری ماشینی را پوشش می‌دهد و پس از آن شرح مفصلی از هر رویکرد مورد استفاده در تشخیص DDoS به همراه انتشارات مرتبط اخیر ارائه می‌شود. جداول [۳](#_bookmark73) و [۴](#_bookmark78) فراهم کردن الف مفصل نمای کلی از روش‌های مختلف یادگیری ماشین/یادگیری عمیق و مزایای آنها برای شناسایی و کاهش حملات DDoS در ابر محیط‌ها. شکل [۵](#_bookmark45) ویترین ها ‎‏ ... ساختار جامع یک سیستم تشخیص ناهنجاری مبتنی بر یادگیری ماشین/یادگیری عمیق.

1. *حملات انسداد سرویس (DDOS) ناهنجاری مبتنی بر روشن ML—موجود کارهای پژوهشی*

کوشوا و همکاران [[37]](#_bookmark125) با تمرکز بر دشواری اساسی تشخیص حملات DDoS در محاسبات ابری، با تأکید بر اهمیت از افزایش یافته امنیت و قابلیت اطمینان در برنامه‌های مبتنی بر ابر. تحقیقات آنها یک سیستم جدید مبتنی بر الگوریتم ماشین یادگیری شدید رأی‌گیری (V-ELM) ارائه داد تا بر محدودیت‌های موجود در تشخیص DDoS غلبه کند. سیستم‌ها در اصطلاحات از دقت، سرعت، و کار سهولت در جابجایی. به طرز چشمگیری، این سیستم از انواع سیستم‌های شناخته شده بهتر عمل می‌کند. ارزیابی تجربی، عملکرد بالایی را نشان داد. تشخیص دقت، حساسیت، ویژگی، و حداقل زمان آموزش، که تأکید بیشتری بر اثربخشی رویکرد پیشنهادی دارد.

سامبانگی و همکاران [[38]](#_bookmark126) از تکنیک‌های یادگیری ماشین برای تشخیص حملات DDoS در محیط‌های محاسبات ابری استفاده کردند. آنها به این موارد پرداختند: ‎‏ ... چالش‌ها مرتبط با حملات انسداد سرویس (DDOS) تشخیص در این محیط‌ها، با تأکید بر نیاز به مکانیسم‌های تشخیص کارآمد و دقیق برای مقابله با تهدیدات امنیتی در زیرساخت‌های شبکه. هدف این تحقیق طراحی یک مدل یادگیری ماشینی است. مبتنی بر روی چندگانه خطی رگرسیون تحلیل برای حمله DDoS تشخیص، با استفاده از داده‌ها تجسم و ویژگی انتخاب​ تکنیک‌ها به افزایش پیش‌بینی دقت. نتایج از آزمایش‌ها شامل معیارهای عملکرد مانند دقت، صحت، به یاد آوردن، امتیاز F1، و گیجی ماتریس، نویدبخش بودن پیامدها با ‎‏ ... پیشنهادی چندگانه خطی رویکرد تحلیل رگرسیون در مقایسه با روش‌های موجود.

ابوبکر و همکاران [[39]](#_bookmark127) با تمرکز بر افزایش فراوانی و تنوع حملات به شبکه‌های کامپیوتری، عمدتاً حملات انسداد سرویس (DDOS) حملات، که ارائه شده الف قابل توجه چالشی به دلیل ماهیت و مکانیسم‌های در حال تکامل آنها. راه‌حل‌های پیشنهادی با هدف توسعه مکانیسمی ارائه شده‌اند که قادر به تشخیص سریع حملات DDoS، شناسایی منشأ آنها و آغازگر کاهش رویه‌ها در ‎‏ ... اوایل مراحل تشخیص. این رویکرد یک الگوریتم طبقه‌بندی بهینه‌شده ماشین بردار پشتیبان (SVM) را با خرناس نفوذ پیشگیری سیستم (آی پی اس) به فراهم کردن



**شکل ۴.** فرکانس – کاربرد از مجموعه داده‌ها جمع‌آوری‌شده تحقیق مقالات.

اقدامات پیشگیرانه در طول حملات DDoS. نتایج تجربی شامل ارزیابی کردن ‎‏ ... پیشنهادی آی پی اس روش در سناریوهای حمله تک منبعی و چند منبعی و مقایسه معیارهای عملکرد مانند بار پردازنده، تأخیر، میانگین بسته‌ها، دقت، نرخ تشخیص، ویژگی و مثبت کاذب نرخ. اینها آزمایش‌ها نشان داده شده ‎‏ ... اثربخشی روش پیشنهادی در تشخیص و کاهش حملات DDoS در مقایسه با راه‌حل‌های موجود.

تحقیق [[40]](#_bookmark128) به مسائل مختلف مربوط به محاسبات ابری، به ویژه آسیب‌پذیری در برابر حملات DDoS، پرداخت. که می‌توانست مختل کردن دسترسی به اطلاعات. آن بر ضرورت وجود یک سیستم تشخیص نفوذ قابل اعتماد برای شناسایی سریع و مقابله با چنین حملاتی در پلتفرم‌های ابری تأکید کردند. پیشنهادی راه حل ها درگیر خلق کردن الف طبقه بندی مدل با استفاده از تصادفی هارمونی جستجو بهینه‌سازی (RHS) و ماشین‌های بولتزمن محدود (RBM) برای بهبود تشخیص حمله DDoS در تنظیمات ابری. نتایج از ‎‏ ... مطالعه نشان داد تقویت‌شده دقت در تشخیص DDoS حملات مقایسه شده به متعارف روش‌ها، همراه با بهبود یافته دقت، به یاد آوردن، و امتیاز F1 معیارها علاوه بر این-

متحد، ‎‏ ... رویکرد رهبری کرد به کاهش یافته نادرست نکات مثبت و افزایش کارایی در شناسایی بلادرنگ حملات DDoS در محیط‌های ابری.

الشماری و همکاران [[41]](#_bookmark129) تحقیقات به دو مسئله اصلی پرداختند، اول، شناسایی غیرطبیعی الگوها در شبکه ترافیک داده‌هایی برای تمایز بین رفتار مخرب و عادی؛ و دوم، در حال توسعه یک میلی لیتر مدل قادر از آموزش شناسه‌ها به رسمیت شناختن متفاوت انواع از ناهنجاری‌ها چنین به عنوان حملات انسداد سرویس (DDOS) در محاسبات ابری شبکه‌ها. راه حل ها پیشنهادی در ‎‏ ... تحقیق شامل ساختمان الف جامع مدل که ترکیب می‌کند تکنیک‌های مختلف یادگیری ماشین مانند g، K-نزدیک‌ترین همسایه (KNN)، پشتیبانی بردار ماشین (ماشین بردار پشتیبان)، تصادفی جنگل (RF)، بیز ساده (NB)، درخت تصمیم (DTREE) و شبکه عصبی مصنوعی (شبکه عصبی مصنوعی) به انتخاب کنید ‎‏ ... بیشترین دقیق طبقه بندی کننده و اشتغال تحت نظارت دستگاه یادگیری روش‌ها. نتایج نشان داد ‎‏ ... اثربخشی از ‎‏ ... مدل در تشخیص الگوهای ترافیک مخرب و بهبود امنیت کلی شبکه. تحقیق [[42]](#_bookmark130) تمرکز بر تشخیص حملات DDoS در محیط‌های محاسبات ابری با استفاده از یک الگوریتم یادگیری افراطی بهینه ماشین. آن هدف قرار داده شده به آدرس ‎‏ ... چالش‌ها از در حال توسعه یک مؤثر سیستم برای حملات انسداد سرویس (DDOS) تشخیص در محاسبات ابری در حالی که ارتقاء دهنده دقت و کارایی. پیشنهادی راه حل ها شامل شدن با استفاده از یک بهینه شده ماشین یادگیری مفرط و پیاده‌سازی یک مدل تکاملی خود-تطبیق‌پذیر افراطی یادگیری ماشین (SAE-ELM) مدل برای بهبود تشخیص دقت. اهداف شامل کردن پیشنهاد دادن ‎‏ ... بهینه شده افراطی یادگیری دستگاه و معرفی سا-ای-ال‌ام مدل به افزایش تشخیص دقت. این تحقیق عملکرد سیستم پیشنهادی را با استفاده از معیارهایی مانند دقت، حساسیت، ویژگی، دقت و امتیاز F ارزیابی کرد. نشان دادن قابل توجه بهبودها بیش از موجود روش‌ها در تشخیص حملات انسداد سرویس (DDOS) حملات در ابر محاسبات

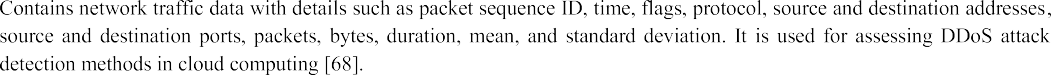
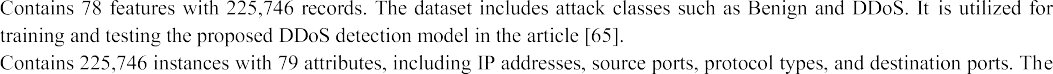
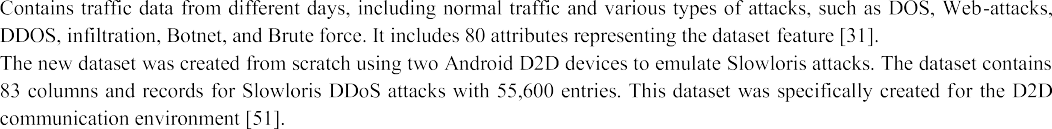
محیط‌ها.

ساچدوا و همکاران [[43]](#_bookmark131) تحقیقات به طبقه‌بندی پرداخت- بررسی حملات در محیط‌های شبکه ابری، با استفاده از یادگیری ماشین و پزشکی قانونی دیجیتال. این مقاله به چالش‌های تشخیص و طبقه‌بندی حملات DDoS در شبکه‌های ابری در بحبوحه پیچیدگی فزاینده تهدیدات و محدودیت‌های سایبری می‌پردازد. از روش‌های تشخیص موجود. راه‌حل‌های پیشنهادی شامل توسعه الف همجوشی الگوریتم که ترکیب می‌کند میلی لیتر تکنیک‌هایی با پزشکی قانونی دیجیتال، که از مصنوعات شاهد برای تجزیه و تحلیل استفاده می‌کنند. تنظیمات تجربی شامل معیارهای عملکردی مانند آماره کاپا، نرخ مثبت کاذب (FPR)، نرخ مثبت واقعی (TPR)، خطای جذر میانگین مربعات (RMSE)، دقت و فراخوانی برای اعتبارسنجی در نظر گرفته شده‌اند. نتایج نشان‌دهنده دقت، صحت و نرخ منفی واقعی بالا در طبقه‌بندی حمله، همراه با بهبود عملکرد در تشخیص است. و طبقه بندی حملات در ابر شبکه‌ها، اعتبارسنجی اثربخشی الگوریتم ادغام در چندین معیار عملکرد.

تحقیق [[44]](#_bookmark132) تمرکز بر تشخیص حملات DDoS در محیط‌های محاسبات ابری با استفاده از یک بردار پشتیبانی کارآمد مبتنی بر ماشین گسسته فیل گله داری بهینه‌سازی (SVM-DEHO) طبقه بندی کننده. آن خطاب شده قابل توجه امنیت سایبری مسائل ژست گرفته توسط حملات انسداد سرویس (DDOS) حملات، که به سرعت اگزوز قربانی​ ارتباط و محاسبه منابع. اهداف

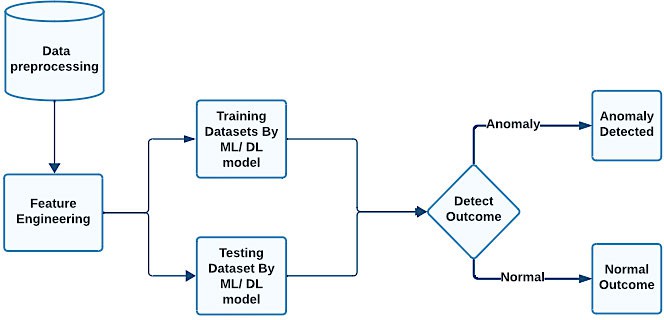
**جدول ۲.** رایج ابر امنیت مجموعه داده‌ها.





شامل کردن پیشنهاد دادن یک SVM-DEHO طبقه بندی کننده برای تشخیص DDoS ، با تجربی نتایج نشان دادن بالا دقیق-

تند و زننده، حساسیت، ویژگی، دقت، و معیار F مقادیر. نتایج نشان دادن ‎‏ ... برتری از ‎‏ ... پیشنهادی رویکرد



**شکل ۵.** تشخیص ناهنجاری مبتنی بر یادگیری ماشین/یادگیری عمیق در فضای ابری شبکه.

بیش از موجود روش‌ها، تأیید کننده آن اثربخشی در کاهش حملات DDoS در محیط‌های ابری.

میشرا و همکاران [[45]](#_bookmark133) تحقیقات متمرکز بر شناسایی آسیب‌پذیری DDoS در ابر محاسبات با استفاده از ‎‏ ... گیج و مبهوت طبقه بندی کننده بیز آن خطاب شده چالش‌ها در شناسایی و سوءاستفاده از آسیب‌پذیری‌ها در محاسبات ابری، به ویژه با تأکید بر ‎‏ ... شدت از حملات انسداد سرویس (DDOS) حملات و آنها تأثیر روی زیرساخت ابری. راه‌حل‌ها شامل پیاده‌سازی تکنیک‌های یادگیری ماشینی، به طور خاص ‎‏ ... گیج و مبهوت بیز طبقه بندی کننده، به حملات DDoS را در محیط‌های ابری شناسایی و کاهش می‌دهد. معیارهای عملکرد مانند دقت، حساسیت و ویژگی برای ارزیابی اثربخشی رویکرد پیشنهادی در شناسایی حملات DDoS استفاده می‌شوند. به طور کلی، نتایج نشان داد که ‎‏ ... گیج و مبهوت بیز طبقه‌بندی‌کننده می‌تواند با موفقیت آسیب‌پذیری‌های DDoS را در محیط ابری شناسایی و کاهش داد .

استفاده از یادگیری ماشین در محاسبات ابری برای شناسایی حملات DDoS موضوع تحقیق است [[46] .](#_bookmark134) کاهش اشتباهات طبقه‌بندی نادرست در تشخیص DDoS مسئله اصلی است، به عنوان آن تأثیرات ‎‏ ... در دسترس بودن از خدمات برای مجاز کاربران. کاهش طبقه‌بندی نادرست خطاها، ارزیابی کردن میلی لیتر تکنیک‌هایی برای تشخیص حمله DDoS، تجزیه و تحلیل طبقه‌بندی‌های نادرست برای اطلاعات بیشتر دقیق اندازه‌گیری‌ها، و انتخاب کردن مهم ویژگی‌ها با استفاده از اطلاعات متقابل (MI) و اهمیت ویژگی جنگل تصادفی (RFFI) رویکردها هستند ‎‏ ... اصلی اهداف از تحقیق . با این حال، ‎‏ ... تصادفی جنگل روش انجام شده از نظر تشخیص حملات DDoS در مقایسه با سایر تکنیک‌ها، بهترین بود. امتیاز F1، یادآوری، دقت و صحت از جمله معیارهای عملکرد بودند.

مطالعه [[47]](#_bookmark135) متمرکز روی تشخیص حملات انسداد سرویس (DDOS) حملات در مدرن​ شبکه زیرساخت‌ها برای صنعت ۴.۰، با استفاده از میلی لیتر مدل‌ها و روش‌های تبدیل ویژگی. این [مطالعه] به امنیت و داده‌ها در دسترس بودن مسائل در مدرن شبکه سازی، به طور قابل توجه در فضای ابری محاسبات، تمرکز کردن روی ‎‏ ... تشخیص از حملات انسداد سرویس (DDOS) حملات در شبکه‌های ابری، که مشکلات جدیدی را برای شبکه ایجاد می‌کنند جامعه. رمان مبتنی بر گاوسی ترافیک توابع شباهت الگو-ویژگی برای خوشه‌بندی ویژگی‌های تکاملی، مانند خب به عنوان مبتنی بر گاوسی شبکه ترافیک شباهت توابع برای ارزیابی کردن شباهت‌ها بین شبکه ترافیک موارد، به عنوان راه حل پیشنهاد شده‌اند. علاوه بر این، این مطالعه ایجاد می‌کند مدل یادگیری ماشین SWASTHIKA برای تشخیص هر دو نرخ پایین و نرخ بالا شبکه تهدیدها نتایج تجربی

نشان می‌دهد که SWASTHIKA از نظر عملکرد، نرخ تشخیص حمله بسیار بالاتری نسبت به طبقه‌بندی‌کننده‌های پیشرفته یادگیری ماشین دارد. اقدامات چنین به عنوان دقت، دقت، نرخ تشخیص و امتیاز F.

مطالعه [[48]](#_bookmark136) خطاب شده ابر امنیت در دولت الکترونیک، شامل تشخیص و کاهش نفوذ به شبکه، به ویژه حملات DDoS. این مطالعه بر چالش‌های امنیتی حیاتی در محاسبات ابری تمرکز داشت و بر ماهیت آسیب‌پذیر سیستم‌های دولت الکترونیک مبتنی بر ابر در برابر حملات از گره‌های آسیب‌پذیر و اهمیت ... از نظارت داخلی به عنوان خب به عنوان خارجی ترافیک در ابر شبکه برای امنیت اهداف. پیشنهادی راه‌حل‌ها شامل معرفی یک روش ML برای خوشه‌بندی دقیق است از داده‌های شبکه برای تشخیص حملات DDoS، با استفاده از تکنیک‌های انتخاب ویژگی برای بهبود کارایی خوشه‌بندی داده‌ها، و با استفاده از خوشه‌بندی الگوریتم‌ها چنین به عنوان مدیر تحلیل مولفه‌ها (PCA)، مبتنی بر تراکم فضایی خوشه‌بندی از کاربردها​ با نویز اسکن پایگاه داده، متراکم کننده خوشه‌بندی، و

نتایج آزمایش نشان می‌دهد که PCA + DBSCAN پیشنهادی از الگوریتم‌های استاندارد بهتر عمل می‌کند.

سوکالینگام و ال. [[49]](#_bookmark137) تحقیق خطاب شده ‎‏ ... پله پله بالا رفتن

فراوانی و پیچیدگی حملات DDoS که سرویس‌های محاسبات ابری را هدف قرار می‌دهند و نارسایی‌های سیستم‌های تشخیص نفوذ سنتی در شناسایی و آدرس‌دهی اینها حملات. به مقابله اینها چالش‌ها، این مطالعه راهکارهایی مانند توسعه یک سیستم تشخیص نفوذ هوشمند که از تکنیک‌های یادگیری ماشین برای افزایش تشخیص حمله DDoS استفاده می‌کند و به‌کارگیری یک ماشین بردار پشتیبان (SVM) با رویکرد ترکیبی الگوریتم بهینه‌سازی هریس هاکس (HHO) و بهینه‌سازی ازدحام ذرات (PSO) برای بهبود دقت و کارایی در محیط‌های ابری را پیشنهاد کرد. ارزیابی تجربی از عملکرد استفاده کرد. معیارها از جمله دقت، حساسیت، گزینش پذیری ، اف۱ امتیاز، دقت، و مساحت زیر ‎‏ ... منحنی (AUC) ارزیابی کردن ‎‏ ... اثربخشی از ‎‏ ... پیشنهادی سیستم، آشکار سازی پیشرفته تشخیص قابلیت‌ها و کارایی در مقابله با حملات DDoS در محیط‌های محاسبات ابری

مطالعه [[50]](#_bookmark138) با هدف افزایش اثربخشی الگوریتم گاوسی ساده‌لوح بیز طبقه بندی کننده به تشخیص حملات منع سرویس دابلیو‌اس حملات در محاسبات ابری. این مقاله شیوع حملات DDOS و DOS علیه سرویس‌های ابری و همچنین دشواری تشخیص این حملات به دلیل ماهیت توزیع‌شده و پتانسیل آنها برای پیامدهای فاجعه‌بار را مورد بحث قرار داد. راه‌حل‌های پیشنهادی برای تشخیص حملات DDOS شامل استفاده از تکنیک‌های یادگیری ماشین، به ویژه طبقه‌بندی‌کننده گاوسی Naïve Bayes، پیش پردازش داده‌ها به آدرس احتمال صفر مسائل، و انتخاب ویژگی‌های بسیار مستقل برای بهبود دقت. چارچوب پیشنهادی دقت ... را بهبود می‌بخشد. طبقه‌بندی‌کننده‌ی گاوسی-بیز ساده در تشخیص حملات DDOS، کاهش می‌دهد ‎‏ ... احتمال صفر مشکل از طریق پیش‌پردازش داده‌ها، کارایی انتخاب ویژگی را بهبود می‌بخشد و عملکرد طبقه‌بندی‌کننده را با استفاده از دقت، فراخوانی و امتیاز F1 اندازه‌گیری می‌کند.

مطالعه [[51]](#_bookmark139) شاغل میلی لیتر به تشخیص حملات انسداد سرویس (DDOS) حملات در اتصالات دستگاه به دستگاه (D2D). راه‌حل‌ها شامل استفاده از میلی لیتر تکنیک‌ها چنین به عنوان تصادفی جنگل، ایکس جی تقویت،

Ada Boost و Light Gradient Boosting Machine (LGBM) برای شناسایی و جلوگیری از حملات DDoS در ارتباطات D2D سیستم‌ها. اهداف شامل شدن فراهم کردن بهبود قابل توجهی از نظر زمان تشخیص و پیشگیری، منابع مورد نیاز و استفاده از باتری دستگاه، و همچنین ارائه یک تکنیک مفید برای مبارزه با حملات DDoS در ارتباطات D2D. سیستم پیشنهادی از تکنیک‌های ML استفاده کرد. به طبقه بندی کردن و تشخیص حملات انسداد سرویس (DDOS) حملات، با یک تأکید بر سین و اسلولوریس حملات. تحقیق شاغل ارزیابی​ معیارها چنین به عنوان دقت، دقت، به یاد آوردن، مساحت تحت منحنی (AUC)، و اف۱ امتیاز به ارزیابی کردن ‎‏ ... عملکرد رویکردهای طبقه‌بندی یادگیری ماشینی در تشخیص حملات DDoS در محیط ارتباطی شبکه D2D. نتایج نشان داده شده قابل توجه عملکرد بهبودها و ارزیابی‌های جامعی از مدل‌های یادگیری ماشین ارائه داد که به اثربخشی روش‌های تشخیص حمله DDoS در سناریوهای دنیای واقعی کمک می‌کند.

نویسندگان در [[52]](#_bookmark140) بر محافظت از محیط‌های محاسبات ابری مجازی در برابر حملات DDOS با استفاده از الگوریتم Naive Bayes ML تمرکز داشتند. آنها به چالش‌های ناشی از افزایش تعداد کاربرانی که به برنامه‌های مبتنی بر ابر دسترسی دارند، پرداختند که منجر به افزایش حملات DDOS با هدف قرار دادن... ابر خدمات. علاوه بر این، آنجا است الف فقدان از قابل اعتماد روش‌ها برای تشخیص و فیلتر کردن اینها حملات، ساختن آنها الف ترجیح داده شده سلاح برای سایبری مهاجمان به آدرس این مسائل، ‎‏ ... تحقیق کاوش می‌کند میلی لیتر تکنیک‌ها و به طور خاص الگوریتم Naive Bayes را برای جلوگیری و تشخیص حملات DDOS در محیط‌های ابری مجازی اعمال می‌کند. به طور قابل توجهی، مدل Naive Bayes بهبود دقت، یادآوری، ویژگی و امتیاز F را نشان داد.

محققان در [[53]](#_bookmark141) متمرکز روی با استفاده از میلی لیتر به تشخیص حملات DDoS در محیط‌های ابری شبکه موردی خودرویی (VANE)T، با هدف پرداختن به چالش‌های شناسایی و کاهش چنین حملاتی در شبکه‌های خودرویی. آنها پیشنهاد کردند راه حل ها چنین به عنوان استخدام میلی لیتر مدل‌ها مانند رگرسیون لجستیک (LR)، درخت تصمیم (DT)، جنگل تصادفی (RF)، K-نزدیکترین همسایه (KNN)، بیز ساده (NB) و ماشین بردار پشتیبان هسته (SVM) برای طبقه‌بندی «نرمال » و ''حمله منع سرویس توزیع‌شده'' سناریوها و پیاده‌سازی فازی‌سازی برای دسته‌بندی درجات همبستگی در محدوده‌های مقدار ویژگی. اهداف شامل بهبود امنیت و ایمنی در شبکه‌های خودرویی با تشخیص حملات DDoS، با استفاده از یک روش ساختاریافته شامل شبیه‌سازی NS2 و تشخیص مبتنی بر ML است. فازها عملکرد معیارها چنین به عنوان دقت امتیاز و امتیاز دقت برای الگوریتم‌های طبقه‌بندی مختلف محاسبه می‌شوند که نشان‌دهنده کاربرد موفقیت‌آمیز یادگیری ماشین به ویژه دی تی و آر اف در علاوه بر این به فازی‌سازی تکنیک‌هایی در افزایش قابلیت‌های تشخیص DDoS در محیط‌های ابری VANET.

الصالح و ال. [[54]](#_bookmark142) تحقیق متمرکز روی ‎‏ ... استفاده از ML به تشخیص حملات انسداد سرویس (DDOS) تهدیدها در ابر محاسبات تنظیمات. این مقاله تهدیدات امنیت سایبری مرتبط با پیاده‌سازی فناوری ابری، از جمله حملات DDoS، را مورد بحث قرار داد و بر محدودیت‌های IDS استاندارد در تشخیص حملات DDoS تأکید کرد. در پویا شبکه محیط‌ها. مطالعه به دنبال آن بود که پاسخ سوالات درباره ‎‏ ... اثربخشی از ‎‏ ... پیشنهادی

مبتنی بر بیز کانولوشن عصبی شبکه مدل (BaysCNN) در تشخیص حملات DDoS، میزانی که داده‌ها فیوژن بیزفوس سی‌ان‌ان رویکرد بهبود می‌بخشد حملات انسداد سرویس (DDOS) تشخیص دقت، قابلیت اطمینان، و عملکرد معیارها، و چگونه مدل‌های پیشنهادی از نظر دقت و کارایی با روش‌های موجود مقایسه می‌شوند. نتایج نشان داد که مدل BaysCNN به طور متوسط میزان دقت 99.66٪ را به دست می‌آورد. در سراسر ۱۳ چند طبقه حملات، در حالی که ‎‏ ... داده‌ها فیوژن بایز، فوس، سی‌ان‌ان مدل می‌شود یک حتی بالاتر میانگین دقت از ۹۹.۷۹٪. این مطالعه بینش‌های مفیدی در مورد توسعه ارائه داد . از مقاوم مبتنی بر یادگیری ماشینی نفوذ تشخیص سیستم‌ها، به عنوان و همچنین بهبود قابلیت اطمینان و مقیاس‌پذیری IDS در محیط‌های محاسبات ابری.

تالپور و همکاران [[55]](#_bookmark143) کاربرد یادگیری ماشین و تکامل را بررسی کرد. الگوریتم‌ها به حملات انسداد سرویس (DDOS) حملات در ابر سیستم‌های محاسباتی. مطالعه نشان داد که مدرن جامعه است به طور فزاینده‌ای در برابر حملات سایبری، به ویژه حملات DDoS، آسیب‌پذیر می‌شوند و بر نیاز به اقدامات تشخیصی و امنیت سایبری بیشتر تأکید می‌کنند. این سیستم حملات DDoS را با استفاده از تاپ با ‎‏ ... ژنتیکی الگوریتم جی.ای. همچنین، میلی لیتر روش‌هایی مانند تقویت گرادیان شدید (XGB)، جنگل تصادفی (RF) و ماشین بردار پشتیبان (SVM) الگوریتم XGB-GA را پیشنهاد می‌کنند. بهینه‌سازی، RF-GA بهینه‌سازی، و روش‌های بهینه‌سازی SVM-GA بررسی شدند. این فناوری به سطوح دقت بالایی رسید و اقدامات امنیت سایبری را به طور قابل توجهی افزایش داد. رویکرد بهینه‌سازی پیشنهادی XGB-GA عملکرد بهتری داشت. دیگر روش‌ها برای شناسایی حملات انسداد سرویس (DDOS) حملات از نظر از دقت، دقت، به یاد آوردن، و اف۱ امتیاز. دستیابی به دقت آزمایش ۹۹.۰۰٪ و بهترین دقت آزمایش خط لوله ۱.۰۰۰٪.

تحقیق [[56]](#_bookmark144) متمرکز بر تشخیص و دسته‌بندی حملات DDoS حملات در توزیع شده شبکه‌ها با استفاده از سلسله مراتبی روش‌های بهینه‌سازی یادگیری ماشین و فراپارامتر. این روش به تهدید رو به رشد حملات DDoS در شبکه‌های توزیع‌شده و چالش شناسایی سریع و جلوگیری از آنها برای محافظت از زیرساخت‌ها و داده‌های شبکه پرداخت. راه‌حل‌ها شامل استفاده از مدل‌های یادگیری ماشین سلسله مراتبی مانند تقویت گرادیان شدید (XGBoost)، ماشین تقویت گرادیان سبک (LGBM) و ... است. کت‌بوست، تصادفی جنگل (RF)، و تصمیم درخت (DT) برای طبقه‌بندی بهتر حمله و بهینه‌سازی پارامترهای فرامتنی برای بهبود دقت و کارایی سیستم تشخیص نفوذ. اهداف شامل پیشنهاد یک ویژگی LASSO است. انتخاب روش با سلسله مراتبی میلی لیتر مدل‌ها، تقسیم فرآیند به مراحل پیش‌پردازش، انتخاب ویژگی و تنظیم بهینه‌سازی‌شده با فراپارامتر برای طبقه‌بندی، و ارزیابی عملکرد با استفاده از معیارهایی مانند یادآوری، دقت، صحت و امتیاز F1. این مطالعه نشان داد که طبقه‌بندی‌کننده LGBM با دستیابی به دقت 99.77٪، مؤثرترین است که موفقیت تکنیک‌های سلسله مراتبی یادگیری ماشین را در پیش‌بینی دقیق حملات DDoS برجسته می‌کند.

1. *حملات انسداد سرویس (DDOS) ناهنجاری مبتنی بر روشن DL—موجود کارهای پژوهشی*

ولیانگیری و ال. [[57]](#_bookmark145) تحقیق متمرکز روی حملات انسداد سرویس (DDOS) حمله تشخیص درون ابر محاسبات محیط‌ها، هدف گیری به آدرس

نیاز مبرم به روش‌های تشخیص مؤثر و غلبه بر محدودیت‌های الگوریتم‌های موجود. اهداف شامل موارد زیر است در حال توسعه الف رمان فازی و تیلور فیل بهینه‌سازی گله (FT-EHO) و طبقه‌بندی‌کننده شبکه باور عمیق (DBN) که به‌طور خاص برای تشخیص حمله DDoS طراحی شده‌اند و مقایسه کردن آن عملکرد علیه مدرن الگوریتم‌ها مانند پشتیبانی بردار ماشین (ماشین بردار پشتیبان)، عصبی شبکه (NN)، EHO و DBN مبتنی بر TEHO. سیستم پیشنهادی از سه پایگاه داده، از جمله پایگاه داده KDD cup، استفاده می‌کند. به تشخیص حملات انسداد سرویس (DDOS) حملات و استخدام می‌کند الف فازی و رویکرد مبتنی بر TEHO در طبقه‌بندی‌کننده شبکه باور عمیق FT-EHO برای طبقه‌بندی. ارزیابی تجربی بر معیارهای عملکرد مانند دقت، صحت تشخیص، دقت و فراخوانی متمرکز بود. نتایج، اثربخشی طبقه‌بندی‌کننده FT-EHO-DBN پیشنهادی را در بین تعداد مختلفی از کاربران نشان داد و نقاط قوت آن را در دستیابی به دقت بالا، دقت تشخیص، دقت و فراخوانی برجسته کرد و در نتیجه به طور قابل توجهی به افزایش تشخیص DDoS در محیط‌های ابری کمک کرد.

بهاردواج و همکاران [[58]](#_bookmark146) متمرکز بر افزایش تشخیص حملات انسداد سرویس (DDOS) حملات در ابر محاسبات محیط‌ها با استفاده از یک شبکه عصبی عمیق تنظیم‌شده با فراباند (Hyperband Tuned Deep Neural Network) همراه با یک رمزگذار خودکار پراکنده انباشته (Stacked Sparse Autoencoder). این روش به چالش‌های مهمی مانند داده‌های آموزشی محدود، مجموعه داده‌های نامتوازن، و ‎‏ ... پیچیده وظیفه از انتخاب کردن بهینه ویژگی‌ها. در حالی که سنتی روش‌ها و میلی لیتر رویکردها مبارزه با تکامل حمله بردارها و پر سر و صدا داده‌ها، ‎‏ ... پیشنهادی هدف این سیستم کاهش این محدودیت‌ها است. اعتبارسنجی تجربی، عملکرد برتر سیستم را در مقایسه با روش‌های موجود، با بهبودهای قابل توجه در دقت، صحت، فراخوانی و امتیاز F1 نشان داد.

در تحقیقات [[59]](#_bookmark147) میشرا و همکارانش بر محاسبات ابری، به ویژه بررسی و پرداختن به آسیب‌پذیری‌ها در برابر حملات DDoS در محیط‌های ابری، در کنار نگرانی‌هایی مانند خطاها و نفوذهای شبکه و مسائل مربوط به تعادل بار، تمرکز کردند. راه‌حل‌های پیشنهادی شامل استفاده از شبکه‌های عصبی (NN) برای ارزیابی عملکرد آموزش و تشخیص دقیق است . و استخدام ازدحام بهینه‌سازی به کوچک کردن خطاها و اطمینان حاصل کردن پاسخ ثبات. نتایج نشان داده شده شبکه کاهش یافته خطاها، تقویت‌شده تشخیص دقت، و بهتر شناسایی نفوذها، با معیارهایی شامل میانگین مربعات نرخ خطا، دقت تشخیص و صحت.

ولیانگیری و همکاران [[60]](#_bookmark148) بر حملات DDoS در محاسبات ابری با استفاده از شبکه‌های عمیق مبتنی بر بهینه‌سازی تمرکز دارد. کلید مشکلات خطاب شده شامل شدن تشخیص حملات انسداد سرویس (DDOS) حملات در محیط‌های ابری، بهبود امنیت پلتفرم ابری در برابر چنین حملاتی، و بهبود دقت و کارایی تکنیک تشخیص. این راه‌حل‌ها شامل ایجاد یک طبقه‌بندی‌کننده شبکه باور عمیق مبتنی بر بهینه‌سازی تیلور-فیل هرد (TEHO-DBN) برای تشخیص DDoS، استفاده از DL برای تشخیص ناهنجاری در ابرها، و استفاده از یک استراتژی مبتنی بر بهینه‌سازی برای بهبود عملکرد سیستم تشخیص. انواع معیارهای ارزیابی مانند تشخیص نرخ، دقت، به یاد آوردن، محاسباتی زمان، و دقت هستند در نظر گرفته شده چه زمانی شبیه‌سازی ‎‏ ... TEHO-DBN طبقه بندی کننده.

در مقایسه با تکنیک‌های موجود، معیارهای عملکرد بهبود یافته‌ای را نشان داد .

مطالعه [[61]](#_bookmark149) متمرکز روی تشخیص حملات انسداد سرویس (DDOS) و حملات انکار سرویس اقتصادی (EDoS) در محاسبات ابری با ترکیب فناوری‌های شبکه باور عمیق (DBN) و ماشین بردار پشتیبان (SVM). این فناوری به چالش‌هایی از جمله به عنوان به طور دقیق تشخیص متفاوت فرم‌ها از EDoS و حملات DDoS حملات، جلوگیری از حملات از در حال حرکت بین ماشین‌های مجازی (VM) و هایپروایزر، و تخمین درصد حملات ضمن تعیین آستانه‌های حساسیت بر اساس الزامات سیستم. راه‌حل‌های پیشنهادی شامل ابداع الف جامع روش برای شناسایی هر دو حملات EDoS و DDoS، با استفاده از یک رویکرد جهانی برای بهبود تهدید تشخیص. با این حال، چه زمانی شناسایی حملات انسداد سرویس (DDOS) و در حملات EDoS در محاسبات ابری، برخی از معیارهای عملکرد رایج برای ارزیابی مانند زمان گزارش حمله، زمان درخواست-پاسخ، زمان از کارافتادگی سرویس قربانی، هزینه دفاعی/ساعت، نرخ مثبت واقعی (TPR)، نرخ منفی واقعی (TNR) و دقت در نظر گرفته شده‌اند. نتایج به‌دست‌آمده در مورد ترکیب DBN و SVM برای تشخیص حملات DDoS و EDoS در ‎‏ ... ابر نشان دادن چندین قابل توجه نتایج. اینها شامل شدن برتر دقت در شناسایی حملات انسداد سرویس (DDOS) ترافیک حمله، که منجر به کاهش زمان گزارش حمله و پاسخ می‌شود ، به عنوان خب به عنوان کاهش یافته از کارافتادگی برای قربانی خدمات. علاوه بر این ، ‎‏ ... رویکرد منجر می‌شود به پایین‌تر هزینه‌ها مرتبط با تشخیص و کاهش حمله . نکته قابل توجه این است که دقت طبقه‌بندی به‌دست‌آمده فوق‌العاده بالا است و به ۹۹.۷۸٪ می‌رسد. به‌طورکلی، این نتایج، اثربخشی روش پیشنهادی را در افزایش امنیت و تاب‌آوری محیط‌های ابری در برابر حملات DDoS و EDoS برجسته می‌کند.

آلمیانی و همکاران [[62]](#_bookmark150) امنیت شبکه را در کانتینرها بررسی کرد ابر محاسبات پلتفرم‌ها با استفاده از الف مقاوم انتشار معکوس عصبی شبکه. آنها هدف قرار داده شده به آدرس آسیب‌پذیری‌ها​ چنین به عنوان حملات انسداد سرویس (DDOS) حملات روی کانتینر شده میکروسرویس‌ها و ‎‏ ... نیاز برای هوشمند نفوذ تشخیص در محیط‌های بومی ابری . پیشنهادی راه حل شامل می‌شود یک شناسه‌ها مبتنی بر شبکه‌های عصبی (NN) برای شناسایی و کاهش حملات DDoS انعکاسی حملات. اهداف شامل شدن پیشنهاد دادن ‎‏ ... سیستم، ارزیابی کردن آن عملکرد علیه حملات انسداد سرویس (DDOS) حملات، و اطمینان از ملاقات می‌کند ‎‏ ... تأخیر الزامات از کانتینر شده معماری‌های میکروسرویس . نتایج تجربی، پردازش کارآمد را نشان می‌دهند. زمان‌ها و بالا دقت در تشخیص بازتابنده حملات DDoS ، همانطور که با استفاده از معیارهای عملکرد شامل دقت، حساسیت، امتیاز F1، ویژگی، دقت و نرخ مثبت کاذب ارزیابی شده‌اند.

آکگون و ال. [[63]](#_bookmark151) متمرکز روی در حال توسعه نفوذ سیستم‌های تشخیص برای حملات انسداد سرویس (DDOS) حملات. آنها خطاب شده ‎‏ ... تشدید شونده فرکانس و پیچیدگی از چنین حملات، به عنوان خب به عنوان محدودیت‌های روش‌های تشخیص سنتی. وجود دارد- ینگ راه حل ها شامل شدن مبتنی بر امضا و سیستم‌های تشخیص نفوذ مبتنی بر ناهنجاری، همراه با رویکردهای یادگیری ماشینی برای شناسایی تهدیدات بدافزار ناشناخته. اهداف تحقیق شامل ارائه یک مدل تشخیص نفوذ مبتنی بر یادگیری ماشینی، ارزیابی معماری‌های مختلف یادگیری ماشینی مانند شبکه عصبی عمیق است. شبکه‌ها (دی‌ان‌ان)، کانولوشن عصبی شبکه‌ها

(سی‌ان‌ان)، و طولانی کوتاه مدت حافظه (LSTM)، مقایسه مدل‌های پیشنهادی با رویکردهای پایه با استفاده از CIC-DDoS2019 مجموعه داده‌ها. عملکرد ارزیابی مقایسه با مدل‌های پایه، بهبود دقت، صحت، فراخوانی، امتیاز F1 و مساحت زیر منحنی (AUC) را نشان می‌دهد که نشان‌دهنده قابلیت تشخیص حمله DDoS بهبود یافته است. علاوه بر این، معیارهای امنیتی مانند دقت تشخیص، نرخ مثبت کاذب و نرخ منفی کاذب در نظر گرفته شده‌اند.

آیدین و همکاران [[64]](#_bookmark152) با هدف ایجاد یک حافظه بلند مدت کوتاه مدت مبتنی بر (LSTM) حملات انسداد سرویس (DDOS) تشخیص و دفاع سیستم در یک محیط ابری عمومی، با تأکید بر نیاز فوری به شناسایی دقیق و سریع و پیشگیری از حملات DDoS، به ویژه در دوران کووید-۱۹. اهداف شامل موارد زیر است کاردستی یک مبتنی بر LSTM راه حل برای حملات انسداد سرویس (DDOS) تشخیص و دفاع، شامل کردن خودمختار دفاع اجزایی برای مقابله با ناهنجاری‌های شناسایی‌شده و در نهایت بهبود فضای ابری سیستم امنیت سایبری. پیشنهادی رویکرد از تحلیل ترافیک شبکه، امضاهای دیجیتال و استراتژی‌های دفاع خودکار برای شناسایی و مقابله با حملات DDoS استفاده کرد. این سیستم دقت قابل توجهی در طبقه‌بندی حملات نشان داد، رقابتی عملکرد در آموزش و آزمایش مدت زمان‌ها در مقایسه با مطالعات قبلی، و ارزیابی کامل با استفاده از معیارهای حیاتی عملکرد و امنیت مانند دقت، صحت، به یاد آوردن، امتیاز F1، و ‎‏ ... اثربخشی از دفاع مکانیسم‌ها .

سامسو آلیار و همکاران [[65]](#_bookmark153) تحقیقاتی که بر تشخیص حملات DDoS در محیط‌های ابری با استفاده از ویژگی‌های ترکیبی وزن‌دار بهینه‌شده و یک شبکه باور عمیق ترکیبی با معماری واحد بازگشتی دروازه‌دار DBN-GRU متمرکز بودند. آن خطاب شده عملکرد تخریب در نتیجه از این حملات در محاسبات ابری، همراه با چالش حفظ امنیت داده‌ها و حریم خصوصی. راه‌حل‌ها مستلزم توسعه یک رویکرد مبتنی بر DL برای تشخیص خودکار، با استفاده از بهینه شده ویژگی‌ها و ‎‏ ... هیبریدی معماری. تجربی راه اندازی شامل می‌شود ارزیابی کردن عملکرد معیارهایی مانند به عنوان دقت، حساسیت، ویژگی، دقت، اف-۱ نمره، ضریب همبستگی متیو، نرخ مثبت کاذب، نرخ منفی کاذب و نرخ کشف کاذب.

آگراوال و ال. [[66]](#_bookmark154) هدف بود تشخیص و کاهش حملات DDoS در محیط‌های سایبری با استفاده از Mod- سیستم شبکه عصبی باور عمیق (M-DBNN) توسعه‌یافته. بخش اصلی هدف بود ‎‏ ... حفاظت از کاربر شخصی اطلاعات علیه نفوذ یا حملات انسداد سرویس (DDOS) حملات. آگراوال و اهداف دیگر شامل به‌کارگیری MDBNN برای تشخیص رفتارهای نامطلوب، پیش‌پردازش ویژگی‌های مجموعه داده‌ها برای بهبود تشخیص، بهینه‌سازی عملکرد طبقه‌بندی‌کننده با الگوریتم بهینه‌سازی Chimp و مقایسه روش پیشنهادی است. به موجود تکنیک‌ها. نتایج نشان داده شده ‎‏ ... عملکرد برتر M-DBNN از نظر دقت، نرخ خطا، امتیاز F1، نرخ مثبت کاذب، کاپا، ضریب همبستگی متیو، دقت، حساسیت و مقادیر ویژگی.

وارگیس و همکاران [[67]](#_bookmark155) متمرکز بر تشخیص نفوذ در سیستم‌های ابری، به ویژه حملات DDoS، و پرداختن به مسائل امنیتی دشواری‌ها مواجه شد توسط چنین حملات و محافظت کردن داده‌ها در ابر محاسبات. پیشنهادی راه حل ها شامل شدن ‎‏ ...

معرفی یک مدل تشخیص نفوذ جدید مبتنی بر شبکه عصبی تابع بایاس شعاعی (RBF-NN) بهینه شده با وزن‌های تنظیم شده بهینه با استفاده از میانگین هارمونیک ضعیف و غنی بهینه‌سازی (اچ ام پرو) الگوریتم .

نتایج شامل شدن ‎‏ ... برتر عملکرد از ‎‏ ... RBF-NN +

اچ‌ام‌پرو رویکرد چه زمانی با در نظر گرفتن ویژگی، نادرست منفی-

نرخ تشخیص خطا (FNR)، حساسیت، دقت، نرخ تشخیص مثبت کاذب (FPR)، متیو همبستگی ضریب (ام سی سی)، خالص ارزش پیش‌بینی (NPV) و دقت.

امیل سلوان و همکاران [[68]](#_bookmark156) کار متمرکز بر تشخیص و پیشگیری حملات انسداد سرویس (DDOS) حملات در ابر محاسبات محیط‌ها، پرداختن به چالش‌های شناسایی چنین حملاتی در جریان‌های ترافیک دنیای واقعی و در عین حال به حداقل رساندن زمان شناسایی، کاهش پیچیدگی محاسباتی و بهبود مدل‌های تشخیص به رسیدگی متنوع حمله انواع. آن اهداف شامل توسعه یک بهینه‌سازی کسری ضد ویروس کرونا (FACVO) مبتنی بر یک سیستم شبکه عصبی-فازی عمیق (DNFN) است. به طور خاص متناسب سازی شده برای حملات انسداد سرویس (DDOS) حمله تشخیص در ابر، با ترکیب ویژگی‌ها، افزایش داده و تکنیک‌های DL برای افزایش دقت تشخیص، نرخ مثبت واقعی (TPR)، نرخ منفی واقعی (TNR) و دقت. سیستم پیشنهادی با استفاده از فایل‌های لاگ تولید شده از محیط‌های ابری شبیه‌سازی شده و با استفاده از DNFN آموزش دیده توسط FACVO برای شناسایی حملات DDoS، کار می‌کند. تجربی ارزیابی انجام شده با استفاده از ‎‏ ... NSL-KDD و مجموعه داده‌های BoT-IoT شامل مقایسه با تکنیک‌های موجود، با تمرکز بر آزمایش دقت، TPR، TNR و معیارهای دقت است که اثربخشی سیستم DNFN مبتنی بر FACVO توسعه‌یافته را در تشخیص قوی حملات DDoS در محیط‌های ابری نشان می‌دهد.

بالاسوبرامانیام و همکاران [[69]](#_bookmark157) به چالش‌های مطرح شده پرداخت توسط خودی حملات انسداد سرویس (DDOS) حملات تأثیرگذار ابر عملکرد و در دسترس بودن خدمات. اهداف شامل توسعه یک الگوریتم بهینه‌سازی رهبر ترکیبی گرادیان (GHLBO) برای تشخیص کارآمد حمله، ترکیب یک شبکه حداکثر خروجی عمیق (DMN) برای ادغام ویژگی‌ها، نمونه‌برداری بیش از حد برای افزایش داده و ادغام نزول گرادیان با الگوریتم مبتنی بر رهبر ترکیبی است. بهینه‌سازی اچ‌ال‌بی‌او برای تقویت‌شده عملکرد. ارزیابی تجربی، رویکرد مبتنی بر GHLBO را با روش‌های موجود با استفاده از معیارهایی مانند دقت آزمایش، TPR و TNR مقایسه می‌کند و نتایج به ترتیب 0.917، 0.909 و 0.909 است که نشان‌دهنده بهبود معیارهای عملکرد در مجموعه داده‌های مختلف است.

در [[70] ،](#_bookmark158) پاشا و ال. تحقیق هدفمند چگونه به تشخیص حملات DDoS با نرخ پایین در محاسبات ابری با استفاده از الگوریتم DDoS با نرخ پایین حمله تشخیص چارچوب (LRDADF)، ادغام هوش مصنوعی فناوری‌ها مانند دی ال. آن پیشنهاد می‌کند الف هیبریدی رویکردی برای الگوریتم تشخیص DDoS با نرخ پایین HA-LRDD، که شبکه‌های عصبی کانولوشن عمیق (CNN) و خودرمزگذارها را ترکیب می‌کند برای تقویت‌شده دقت. موجود روش‌ها مانند حمله فیلتر کردن هستند مورد بحث، برجسته سازی ‎‏ ... نیاز برای بهبود مکانیسم‌های تشخیص. نتایج تجربی، اثربخشی HA-LRDD را در مقایسه با سایر الگوریتم‌ها نشان داد. تضمین سرویس ابری کیفیتی که نشان می‌دهد نرخ تشخیص بالا ۹۵.۳۲٪ و نرخ مثبت کاذب پایین ۰.۵۶۹۴۳٪.

لیو و ال. [[71]](#_bookmark159) متمرکز روی تشخیص نرخ پایین حملات انسداد سرویس (DDOS) حملات با استفاده از یک ناهمزمان فدرال یادگیری مدل داوری مبتنی بر روی دو جهته طولانی کوتاه مدت حافظه (bi-LSTM) و مکانیسم از توجه لیو و ال. [[71]](#_bookmark159) چالش‌های مرتبط با این حملات را مورد بررسی قرار داد و بر ضرورت سازوکارهای تشخیص مؤثر تأکید کرد و ... محدودیت‌ها در موجود مدل‌ها. اهداف مستلزم طراحی است یک مساوی زمان گام کشویی پنجره روش برای داده‌ها پیش‌پردازش، در حال توسعه الف محلی مدل مبتنی بر روی bi-LSTM و توجه مکانیسم برای حمله تشخیص، و پیشنهاد دادن الف رهبر گره انتخابات الگوریتم در کنار ناهمزمان فدرال یادگیری چارچوب. ارزیابی تجربی شامل می‌شود مقایسه کردن ‎‏ ... پیشنهادی مدل با طبقه‌بندی‌کننده‌های مختلف و مدل‌های DL و ارزیابی معیارهای عملکرد مانند دقت، دقت، به یاد آوردن، و زمان پیچیدگی. مطالعه [[72]](#_bookmark160) متمرکز بر تشخیص حملات DDoS در فضای ابری محیط‌ها با استفاده از یک مبتنی بر هوش مصنوعی شناسه‌ها چارچوب، با یک اولیه هدف از در حال بهبود دقت در حالی که کوچک سازی آلارم‌های کاذب پیشنهادی راه حل ها شامل کردن استخدام گروه ویژگی​ انتخاب به شناسایی کلید ویژگی‌ها و ساختن الف مدل شبکه عصبی عمیق (DNN) برای تشخیص دقیق DDoS. نتایج نشان‌دهنده اثربخشی مدل FEwDN پیشنهادی است ، نشان دادن برتر دقت مقایسه شده به تکنیک‌های مرسوم یادگیری ماشین و پیشی گرفتن از روش‌های موجود در مختلف عملکرد معیارها تحقیق بر کارایی چارچوب IDS مبتنی بر هوش مصنوعی با عملکرد بالا تأکید کرد. ارزیابی معیارها چنین به عنوان دقت، دقت، یادآوری، اف۱ امتیاز، مساحت زیر ‎‏ ... منحنی (AUC)، و گیرنده

عملیاتی مشخصه (آر او سی) استفاده شده برای تکامل.

مطالعه [[73]](#_bookmark161) متمرکز روی پیش‌بینی حملات سایبری مانند Brute\_Force، DDoS، ICMP Flood، Port\_Scan و Web Crawling در محیط‌های محاسبات ابری با استفاده از یک شبکه عصبی بسیار تقویت‌شده. هدف آن خودکارسازی تشخیص و شناسایی سناریوهای حمله سایبری چند مرحله‌ای و در عین حال افزایش دقت و کارایی پیش‌بینی بود. پیشنهادی راه حل ها شامل کردن با استفاده از ‎‏ ... تقویت شده عصبی شبکه (NN) برای پیش‌بینی دقیق‌تر و پیاده‌سازی پیشرفته میلی لیتر تکنیک‌ها به بهبود بخشیدن امنیت سایبری اقدامات در ابر سیستم‌ها. سیستم عمل شده توسط آموزش ‎‏ ... شبکه عصبی روی داده‌های حمله تاریخی، با استفاده از الگوریتم‌های پیچیده برای تحلیل و پیش‌بینی در زمان واقعی، و به طور مداوم در حال بهبود از طریق تطبیقی یادگیری و مکانیسم‌های بازخورد . نظارت مختلف عملکرد معیارها امکان ارزیابی دقت، حساسیت، ویژگی و اثربخشی کلی را فراهم می‌کند. نتایج، بهبود دقت در پیش‌بینی را نشان دادند. چند مرحله‌ای حملات سایبری، تقویت‌شده کارایی در تهدید تشخیص و کاهش، و اعتبارسنجی از ‎‏ ... NN تقویت‌شده اثربخشی از طریق تجربی شبیه‌سازی‌ها و ارزیابی‌ها.

پاندیتورای و ال. [[74]](#_bookmark162) متمرکز روی پیش‌بینی حملات انسداد سرویس (DDOS) حملات در الف ابر محیط زیست با استفاده از الف ترکیب از عسل الگوریتم بهینه‌سازی گورکن و حافظه کوتاه‌مدت بلندمدت دوطرفه (دوگانه-LSTM) فناوری. آنها خطاب شده چالش‌های مرتبط با ابر فرزندخواندگی چنین به عنوان حریم خصوصی مسائل و نشت داده‌ها ، با تأکید بر محدودیت‌های موجود در سیستم تشخیص. آزمایش‌ها به نمایش گذاشته شده برتر دقت. نتایج حاضر

عملکردهای مختلفی از جمله نرخ مثبت کاذب (FPR)، حساسیت، دقت، صحت، ویژگی، امتیاز F1، خطا و کاپا را نشان داد. با این حال، Bi-LSTM حساسیت 95٪، دقت 94٪، کاپا 88٪، FPR 5٪ و امتیاز F1 87٪ را به دست آورد.

آرانگو-لوپز و همکاران [[75]](#_bookmark163) متمرکز بر افزایش تشخیص و پیش‌بینی حملات سایبری DDoS در زمان واقعی با استفاده از یک سیستم ابری دی ال معماری. آنها خطاب شده چالش‌ها مانند​ دستیابی به زمان واقعی تشخیص، کاهش دهنده ارزیابی معیارهایی با مجموعه داده‌های استاندارد، و تمرکز بر دسته‌های خاص حمله در میان نویز شبکه. راه‌حل‌ها شامل تجزیه و تحلیل حمله هستند. دسته‌ها با استفاده از ابزارها مانند وایرشارک، اعمال کردن فیلترها به ایزوله کردن خاص حمله انواع، و در حال توسعه الف معماری DL مبتنی بر ابر مانند شبکه‌های عصبی عمیق (DNN) و شبکه‌های عصبی پیچشی (CNN). سیستم پیشنهادی به طور مداوم داده‌های جدید را برای هر کلاس حمله DDoS وارد می‌کند. به بهبود بخشیدن زمان واقعی تشخیص، با دقت تحلیل می‌کند هر دسته حمله، و تمرکز بر حملاتی که بر پروتکل HTTP تأثیر می‌گذارند بندر ۸۰. (یا: ۸۰.) تجربی نتایج نشان داده شده دقت بهینه معیارها به دست آمده توسط ‎‏ ... دی‌ان‌ان، با در نظر گرفتن دقت، صحت، امتیاز F1 و حساسیت به عنوان معیارهای عملکرد.

اوحسینی و ال. [[76]](#_bookmark164) خطاب شده حملات انسداد سرویس (DDOS) حمله تشخیص و پیشگیری در محیط‌های ابری از طریق چارچوب Deep-Defend، که چالش‌هایی مانند بهره‌وری منابع و محدودیت‌های سیستم‌های موجود را برطرف می‌کند. راه‌حل‌ها شامل موارد زیر است: اجزا مانند ترافیک مجموعه، آنتروپی پیش‌بینی، و حمله پیش‌بینی اهداف شامل شدن ارائه یک استراتژی برای تشخیص و پیشگیری، با استفاده از پیش‌بینی آنتروپی، و بهبود، رمزگذارهای خودکار، عصبی شبکه‌ها (CNN) و مدل درخت تصمیم (DT). این سیستم پردازش می‌کند داده‌ها از طریق مختلف مراحل و استخدام می‌کند دی ال روش‌هایی مانند CNNها، شبکه‌های حافظه کوتاه‌مدت بلندمدت (LSTM)، رمزگذارهای خودکار، و ترانسفورماتورها برای وظایف مانند پیش‌بینی آنتروپی و ویژگی استخراج. آزمایش با مجموعه داده CICIDS-001 و معیارهای عملکرد مانند دقت، صحت، فراخوانی و امتیاز F1 برای ارزیابی استفاده می‌شوند. ‎‏ ... اثربخشی از ‎‏ ... دیپ دیفند چارچوب در تشخیص و جلوگیری از حملات انسداد سرویس (DDOS) حملات. پیامدها برجسته شده دیپ دیفند چارچوب‌ها اثربخشی و دقت در تشخیص و جلوگیری از حملات DDoS در محیط‌های ابری

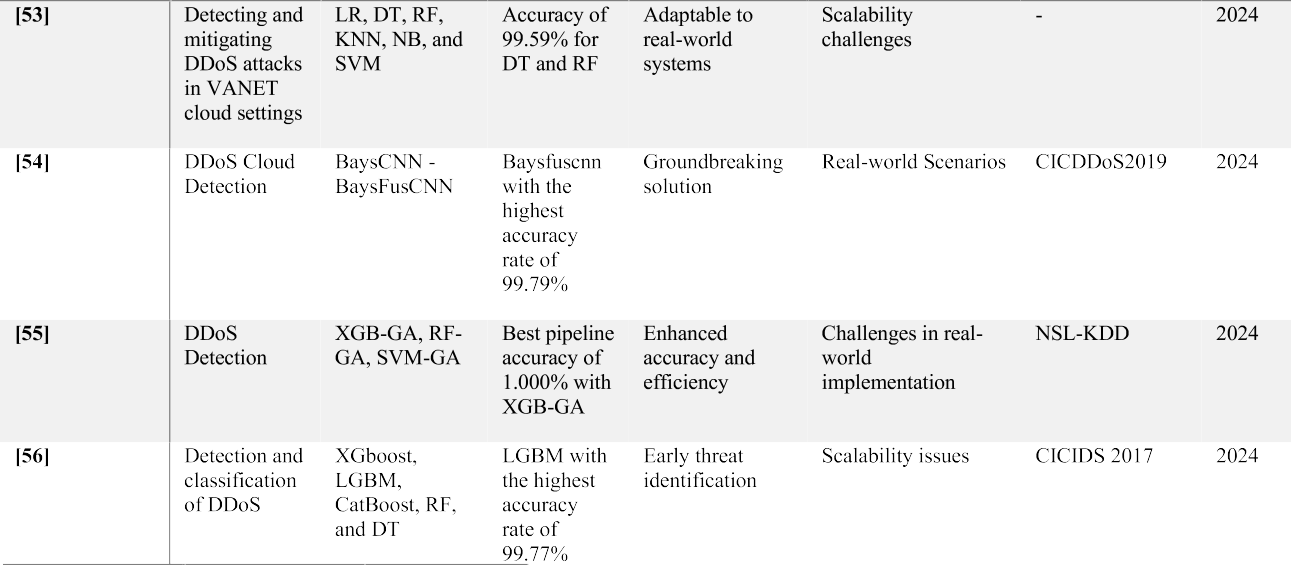
1. **میلی لیتر و دی ال مبتنی بر برای شناسه‌ها در ابر شبکه‌ها**

از آنجایی که الف مبتنی بر امضا شناسه‌ها می‌گیرد قابل توجه زمان به ساخت، آزمایش، و مستقر کردن هر کدام زمان یک غیرمنتظره حمله یک IDS مبتنی بر ناهنجاری مبتنی بر فناوری یادگیری ماشین، سیستمی را ارائه می‌دهد که می‌تواند از داده‌ها یاد بگیرد و در مورد موارد نادیده پیش‌بینی‌هایی انجام دهد. داده‌ها توسط اعمال کردن ‎‏ ... یاد گرفت داده‌ها [[77] .](#_bookmark165) با این حال، مبتنی بر یادگیری ماشین اولیه نفوذ تشخیص تکنیک‌ها بودند مورد انتقاد قرار گرفت به دلیل داشتن توان عملیاتی محدود و نرخ بالای مثبت کاذب. هودو و ال. [[78]](#_bookmark166) مطالعه روی نفوذ تشخیص روش‌ها دریافتند که روش‌های یادگیری عمیق مانند شبکه‌های عمیق، از روش‌های معمول مبتنی بر یادگیری ماشین بهتر عمل می‌کنند. تشخیص رویکردها. الف تکنیک است شاغل تربیت کردن سلسله مراتبی شبکه لایه‌ها با استفاده از بدون نظارت یادگیری در الف گام به گام شیوه، نقاشی الهام از ‎‏ ... ساختار​ از ‎‏ ... انسان مغز. علاوه بر این، میلی لیتر/ دی ال الگوریتم‌ها از یادگیری خودکار برای پیش‌بینی خروجی‌های نهایی استفاده کنید . برای مثال، IDS می‌تواند استخدام اینها الگوریتم‌ها به محافظت ابر شبکه‌ها

**جدول ۳.** حملات انسداد سرویس (DDOS) تشخیص در ابر شبکه با استفاده از ام ال.



**جدول ۳.** *(ادامه دارد.)* حملات انسداد سرویس (DDOS) تشخیص در ابر شبکه با استفاده از ام ال.



از مختلف حملات، چنین به عنوان حملات انسداد سرویس (DDOS) حملات. علاوه بر این، توضیح جامعی از هر روش به کار رفته در IDS ارائه شده است. اراده باش ارائه شده، همراه با اخیر مرتبط مطالعات در این بخش. جداول [۵](#_bookmark91) و [۶](#_bookmark93) روش و مزایای IDS مبتنی بر ML/DL را به تفصیل شرح دهید.

* 1. *شناسه‌ها ناهنجاری مبتنی بر روشن میلی لیتر - موجود کارهای پژوهشی*

مطالعه [[79]](#_bookmark167) متمرکز روی با استفاده از میلی لیتر برای مبتنی بر لاگ تشخیص نفوذ در ابر وب برنامه های کاربردی، هدف گیری به افزایش امنیت ابری. این [طرح/طرح‌ریزی/اجرا] به چالش‌هایی مانند نیاز به سازگاری پرداخت. امنیت سیستم‌ها در ‎‏ ... پیچیده ابر محیط زیست، پیچیدگی از استقرار چندگانه مخصوص پلتفرم آی دی اس، و تقاضا برای مدل‌های تشخیص ساده‌تر و با به‌روزرسانی آسان‌تر. تحقیق هدف قرار داده شده به معرفی کردن الف انعطاف‌پذیر میلی لیتر رویکرد مانند تصادفی درخت، نماینده درخت، جی۴۸، کیسه کشی، تقویت، جنگل تصادفی و شبکه‌های عصبی برای تشخیص حمله با استفاده از برنامه‌های کاربردی وب سیاهههای مربوط، پیشنهاد دادن پیکربندی‌ها از میلی لیتر الگوریتم‌هایی با عملکرد بالا و حداقل سربار زمانی. این مطالعه اثربخشی الگوریتم‌های یادگیری ماشین مانند درخت‌های تصمیم‌گیری و شبکه‌های عصبی را در تشخیص حملات نشان داد. روی مبتنی بر ابر برنامه های کاربردی. نتایج، اندازه‌گیری شده از میان، برجسته کردن ‎‏ ... پتانسیل از میلی لیتر تکنیک‌ها در ارتقاء دهنده تشخیص نفوذ برای برنامه‌های کاربردی وب ابری، که روشی سازگارتر ارائه می‌دهد و کارآمد رویکرد مقایسه شده به سنتی سیستم‌های مبتنی بر قانون

جابر و همکاران [[80]](#_bookmark168) تحقیقات متمرکز بر بهبود IDS برای فضای ابری محاسبات محیط‌ها، هدف گیری به بهبود بخشیدن دقت تشخیص از طریق الف هیبریدی فازی سی معنی خوشه‌بندی الگوریتم (FCM) با ‎‏ ... پشتیبانی بردار ماشین (ماشین بردار پشتیبان) روش . تحقیق خطاب شده ‎‏ ... فشار دادن نیاز برای تقویت‌شده تشخیص سیستم‌ها در ‎‏ ... صورت از در حال افزایش سایبری تهدیدها در ابر تنظیمات. این مقابله شده چالش‌ها در به طور موثر شناسایی و خنثی کردن موارد مختلف حمله انواع مانند عدم ارائه خدمات (داس)، از راه دور به محلی (R2L)، کاربر به ریشه (U2R)، و عادی ترافیک درون

شبکه‌های ابری. نتایج شامل معیارهای عملکرد مختلفی مانند به عنوان دقت، نادرست طبقه بندی نرخ، نادرست نرخ منفی، درست مثبت نرخ، دقت، به یاد آوردن، و اف۱ امتیاز در سراسر مختلف حمله انواع. هیبریدی FCM-SVM سیستم نشان داده شده چشمگیر دقت نرخ‌ها و کم نادرست منفی نرخ‌هایی که از سایر روش‌های IDS پیشی می‌گیرند.

تحقیق [[81]](#_bookmark169) متمرکز روی ارتقاء دهنده شناسه‌ها در ‎‏ ... امنیت سایبری دامنه توسط آدرس‌دهی ‎‏ ... چالش‌ها ژست گرفته توسط مجموعه داده‌های با ابعاد بالا، شامل پیچیدگی محاسباتی، زمان پیچیدگی، سیستم یادگیری پیچیدگی، منبع مصرف و تأخیرهای هشدار. اهداف این مطالعه شامل معرفی یک روش انتخاب ویژگی مبتنی بر نظریه مجموعه‌های راف و قضیه بیز برای بهبود عملکرد IDS است. پیشنهادی سیستم شامل می‌شود داده‌ها نرمال‌سازی، ویژگی انتخاب مبتنی بر روی تخمین زده شده احتمالات، و طبقه‌بندی با استفاده از بیزی خشن مجموعه روش‌ها به دستیابی به الف نرخ تشخیص بالا و نرخ هشدار کاذب پایین. نتایج نشان دهنده کاهش در زمان و فضا پیچیدگی، بالا تشخیص نرخ‌ها، و نرخ‌های پایین هشدار کاذب، با پارامترهای آماری از ماتریس‌های سردرگمی که برای ارزیابی عملکرد سیستم استفاده می‌شوند.

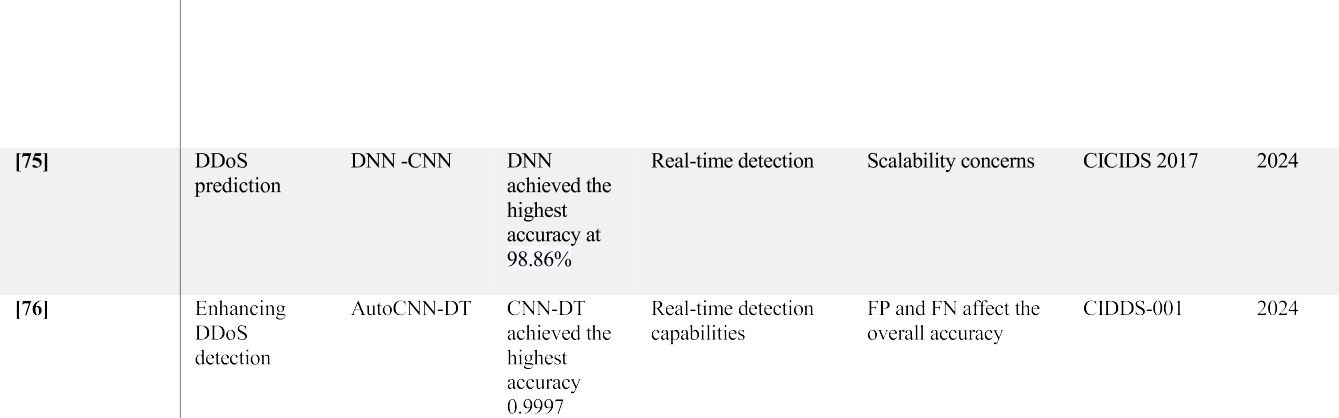
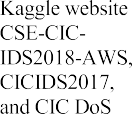
تحقیق [[82]](#_bookmark170) به امنیت سایبری پرداخت، به طور خاص با تمرکز بر IDS در محاسبات ابری، با استفاده از تکنیک‌های یادگیری ماشین. با توجه به پذیرش گسترده سیستم‌های ابری، بر آسیب‌پذیری فزاینده آنها در برابر حملات سایبری تمرکز داشت. توسط سازمان‌ها، بانک‌ها و دولت‌ها، و نیاز مبرم برای مقاوم امنیت اقدامات به محافظت حساس داده‌هایی مانند بهداشت و درمان سوابق از غیرمجاز دسترسی. این مطالعه یک IDS مؤثر با استفاده از الگوریتم‌های یادگیری ماشین مانند الگوریتم‌های ژنتیک (GA) و ماشین‌های بردار پشتیبان (SVM) پیشنهاد کرد. به بهبود بخشیدن امنیت در ابر محاسبات نتایج آزمایش ، نرخ دقت بالایی را در طبقه‌بندی ترافیک عادی و غیرعادی در انواع مختلف حمله نشان داد و اثربخشی سیستم را در کاهش مثبت‌های کاذب و بهبود نرخ تشخیص در تنظیمات محاسبات ابری برجسته کرد.

**جدول ۴.** حملات انسداد سرویس (DDOS) تشخیص در ابر شبکه با استفاده از دی ال.





**جدول ۴.** *(ادامه دارد.)* حملات انسداد سرویس (DDOS) تشخیص در ابر شبکه با استفاده از دی ال.



وانگ و همکاران [[83]](#_bookmark171) مطالعه‌ای متمرکز بر محاسبات ابری، به ویژه در توسعه IDS با استفاده از تکنیک‌های DL مانند Stacked انقباضی رمزگذار خودکار (SCAE) و پشتیبانی ماشین بردار (SVM). این مطالعه به چالش‌هایی مانند با افزایش ترافیک شبکه در محیط‌های ابری، افزایش حملات مخرب که شبکه‌های ابری را هدف قرار می‌دهند و نیاز مبرم به IDS قوی برای محافظت از منابع محاسبات ابری. برای مقابله با این مسائل، این تحقیق استفاده از روش SCAE را برای استخراج ویژگی و کاهش ابعاد، همراه با ادغام الگوریتم SVM پیشنهاد کرد. برای طبقه بندی، هدف گیری به افزایش ‎‏ ... عملکرد تشخیص از ابر نفوذ تشخیص سیستم‌ها. نتایج حاصل از ‎‏ ... آزمایش‌ها شامل ‎‏ ... ارزیابی از مختلف معیارهایی مانند دقت نرخ، دقت نرخ، به یاد بیاورید نرخ، معیار F، گیجی ماتریس، و گیرنده عملیاتی مشخصه (ROC) برای ارزیابی اثربخشی مدل SCAE-SVM. تجزیه و تحلیل مقایسه‌ای با سایر رویکردها، برتری مدل پیشنهادی را در استخراج ویژگی، کاهش ابعاد و تشخیص نفوذ در محیط‌های ابری نشان داد.

یانگ و ال. [[84]](#_bookmark172) متمرکز روی امنیت سایبری، به ویژه توسعه‌ی IDS با استفاده از تکنیک‌های یادگیری ماشین. آن‌ها به افزایش حجم و مخرب بودن حملات سایبری در شبکه‌های مدرن، محدودیت دسترسی به کد عمومی و کامل برای IDSهای مبتنی بر یادگیری ماشین و چالش تشخیص مؤثر حملات شناخته‌شده و روز صفر پرداختند. اهداف شامل شدن در حال توسعه IDS-ML، یک متن‌باز مخزن کد برای توسعه IDS، ارائه راه‌حل‌هایی برای فرآیند کلی توسعه IDS، نشان دادن چگونگی استفاده از الگوریتم‌های یادگیری ماشین برای طراحی انواع مختلف IDSها، و بهبود عملکرد تشخیص نفوذ با تکنیک‌های پیشرفته مانند یادگیری جمعی، یادگیری انتقالی (TL) و بهینه‌سازی فراپارامتر (HPO). راه‌اندازی آزمایشی شامل استفاده از IDS-ML، پیاده‌سازی مختلف میلی لیتر الگوریتم‌ها و تکنیک‌ها، و ارزیابی کردن شناسه‌ها عملکرد با استفاده از مربوطه معیارها چنین به عنوان دقت، صحت، فراخوانی، امتیاز F1، مساحت زیر منحنی (AUC) و مشخصه عملیاتی گیرنده (ROC)، با در نظر گرفتن نرخ تشخیص برای انواع مختلف حملات سایبری.

مطالعه [[85]](#_bookmark173) متمرکز بر IDS در محاسبات ابری توزیع‌شده، هدف گیری به بهبود بخشیدن امنیت از طریق هیبریدی روش‌های خوشه‌بندی و طبقه‌بندی. چالش‌های کلیدی شامل نیاز به افزایش دقت تشخیص IDS در تنظیمات ابری توزیع‌شده و محدودیت‌های مدل‌های سنتی IDS بود. در شناسایی مؤثر حملات شناخته‌شده و ناشناخته. برای پرداختن به این مسائل، این تحقیق استفاده از مدل‌های ترکیبی مبتنی بر یادگیری ماشین را برای بهبود دقت IDS و پیاده‌سازی IDS مبتنی بر ناهنجاری با تکنیک‌های ترکیبی خوشه‌بندی و طبقه‌بندی مانند خوشه‌بندی K-Means و مدل مخلوط گاوسی (GMM) و جنگل تصادفی (RF) پیشنهاد کرد. نتایج آزمایش، بهبود قابل توجهی در دقت کلی، نرخ تشخیص و نسبت هشدار اشتباه در مقایسه با مدل‌های سنتی IDS نشان داد که نشان‌دهنده عملکرد بهبود یافته در تشخیص انواع مختلف نفوذها است.

باکرو و همکاران [[86]](#_bookmark174) بر افزایش IDS در امنیت ابری تمرکز داشت و به نگرانی‌های مربوط به حریم خصوصی و امنیت داده‌ها در محیط‌های ابری در بحبوحه افزایش تهدیدات سایبری پرداخت. با بهره‌گیری از مدل‌های یادگیری ماشین، سیستم پیشنهادی شبکه را طبقه‌بندی کرد. بسته‌ها به طور دقیق به شناسایی نفوذها و داده‌های کاربر را به طور مؤثر حفظ کنید . مشارکت‌های کلیدی شامل ادغام مصنوعی اقلیت نمونه‌گیری بیش از حد تکنیک (SMOTE) برای مدیریت داده‌های نامتوازن، با استفاده از انتخاب ویژگی ترکیبی رویکرد ترکیب کردن اطلاعات سود (اینگرید)، کای-اسکوئر (CS) و بهینه‌سازی ازدحام ذرات (PSO) برای انتخاب زیرمجموعه بهینه ویژگی، و با استفاده از فرمول تصادفی مدل est (RF) برای تشخیص حمله. نتایج تجربی دقت بالایی بیش از ۹۸٪ و ۹۹٪ را در سناریوهای طبقه‌بندی چند کلاسه نشان داد که از رویکردهای موجود بهتر عمل می‌کند. نتایج همچنین به نمایش گذاشته شده بالا تشخیص نرخ‌ها و نرخ‌های پایین هشدار کاذب، نشان‌دهنده اثربخشی سیستم پیشنهادی است.

این تحقیق [[87] تشخیص نفوذ در محاسبات ابری را](#_bookmark175) با تمرکز بر شناسایی ناهنجاری‌ها در سری‌های زمانی بررسی کرد. داده‌ها با استفاده از میلی لیتر تکنیک‌ها. آن خطاب شده نگرانی‌ها مانند آسیب‌پذیری سیستم‌های ابری در برابر حملات به دلیل ماهیت باز آنها، و همچنین چالش‌های مربوط به حریم خصوصی و امنیت که برای موفقیت محاسبات ابری حیاتی هستند. راه‌حل‌های پیشنهادی درگیر اعمال نفوذ شناسه‌ها به محافظت ابر حسادت

گزارش‌ها، معرفی تشخیص ناهنجاری سری‌های زمانی به عنوان یک راه‌حل مناسب، و ادغام یادگیری ماشین برای تشخیص ناهنجاری پیشرفته و اقدامات امنیتی. نتایج شامل ارزیابی‌های عملکرد بر اساس معیارهایی مانند زمان پویا بود. تاب برداشتن (DTW)، میانگین مطلق خطا (MAE)، میانگین مربعات خطا (MSE)، جذر میانگین مربعات خطا (RMSE)، میانگین مطلق درصد خطا (MAPE)، میانه خطای درصد مطلق (MdAPE). با این حال، سیستم پیشنهادی نشان داد که عملکرد بهبود یافته در تشخیص و جلوگیری از تهدیدات امنیتی در محیط‌های محاسبات ابری.

اتو و همکاران [[88]](#_bookmark176) تحقیقاتی که بر روی پرداختن به چالش‌های مرتبط با تشخیص نفوذ در سیستم‌های مبتنی بر ابر متمرکز بودند محیط‌ها توسط پیشنهاد دادن یک نوآورانه مدلی که الگوریتم جنگل تصادفی (RF) را با تکنیک‌های مهندسی ویژگی ترکیب می‌کند. هدف این مطالعه افزایش امنیت در شبکه‌های ابری، با در نظر گرفتن مسائل مربوط به دقت... سیون، مقیاس‌پذیری، و سازگاری مواجه شد توسط متعارف IDS و IDS مبتنی بر یادگیری ماشین. این مدل عملکرد قابل تحسینی را نشان می‌دهد و به دقت، صحت و فراخوانی بالایی نسبت به راه‌حل‌های تثبیت‌شده دست می‌یابد.

در تحقیق [[89] وی](#_bookmark177) آشیشتا و ال. متمرکز روی در حال توسعه یک مدل تشخیص نفوذ ترکیبی (HIDM) برای مراقبت‌های بهداشتی مبتنی بر ابر سیستم‌ها، هدف گیری به آدرس ‎‏ ... چالش‌ها از تشخیص بالا نرخ‌ها برای شناخته شده حملات، ‎‏ ... ناتوانی به تشخیص ناشناخته جدید حملات، و افزایش یافته نادرست زنگ هشدار نرخ‌ها برای ناشناس یا جدید حملات. پیشنهادی مدل مشارکت می‌کند با ارائه الف هیبریدی رویکرد که ترکیب می‌کند روش‌های تشخیص مبتنی بر امضا و مبتنی بر ناهنجاری، که امکان تشخیص حملات شناخته شده و ناشناخته را فراهم می‌کنند. تنظیمات آزمایشی شامل می‌شود ارزیابی کردن عملکرد مبتنی بر روی دقت و کارایی معیارها نتایج نشان داد ‎‏ ... پیشنهادی HIDM عملکرد بهتری داشت دیگر مدل‌ها در اصطلاحات از دقت، با عملکرد معیارها از جمله دقت نرخ‌ها و امنیت تمرکز بر معیارها روی ‎‏ ... توانایی به تشخیص شناخته شده و ناشناخته حملات. مطالعه [[90]](#_bookmark178) به امنیت سایبری، به ویژه با تمرکز بر روی ساختن شناسه‌ها متناسب سازی شده برای ابر محیط‌ها با استفاده از الهام گرفته از طبیعت ویژگی انتخاب الگوریتم‌ها در حرف ربط با یک مدل جنگل تصادفی (RF). اهداف اصلی توسعه یک سیستم تشخیص نفوذ ابری با استفاده از انتخاب ویژگی ترکیبی الهام گرفته از زیست بود. الگوریتم‌ها در کنار یک آر اف مدل و به مقابله با چالش‌ها مرتبط با مجموعه داده‌ها توسعه و ویژگی انتخاب در ‎‏ ... قلمرو از نفوذ تشخیص سیستم‌ها ضمن نمایش عملکرد و اثربخشی بهبود یافته در مقایسه با به موجود روش‌شناسی‌ها نتایج از ‎‏ ... آزمایش‌ها نشان داده شده بهبود یافته عملکرد در دقت، به یاد آوردن،

و نادرست زنگ هشدار نرخ.

* 1. *شناسه‌ها ناهنجاری مبتنی بر روشن دی ال - موجود کارهای پژوهشی*

تحقیق [[91]](#_bookmark179) تمرکز بر بهبود IDS در محاسبات ابری محیط‌ها به آدرس امنیت سایبری چالش‌ها. این مقاله یک IDS مبتنی بر شبکه‌های عصبی فازی Min-Max (FMMNN-IDS) را برای تشخیص حملات متنوع شبکه، مانند حملات انکار سرویس (DoS) و آلودگی‌های بدافزاری، پیشنهاد کرد. شناسه‌های FMMNN عمل شده توسط پردازش شبکه ترافیک

داده‌ها از طریق مراحل انبساط و انقباض هایپرباکس به طور دقیق تشخیص نفوذها آن نشان داده شده برتر عملکرد در دقت و نرخ تشخیص در مقایسه با رویکردهای موجود.

مطالعه [[92]](#_bookmark180) توسعه یافته یک کارآمد شناسه‌ها برای ابر محاسبات ، هدف گیری به آدرس امنیت آسیب‌پذیری‌ها و کاهش بیش‌برازش. این روش از یک تکنیک DL ترکیبی استفاده کرد که بهینه‌سازی بهبود یافته هیپ (IHO) را برای پیش‌پردازش داده‌ها و بهینه‌سازی Chaotic Red Deer (CRDO) را برای انتخاب ویژگی ادغام می‌کرد. شبکه عصبی عمیق کرونکر (DKNN) پیشنهادی، به نام EOS-IDS، دقت تشخیص نفوذ و طبقه‌بندی را افزایش داد. EOS-IDS از طریق آزمایش دقیق روی مجموعه داده‌های معیار، عملکرد رقابتی را در برابر طبقه‌بندی‌کننده‌های پیشرفته نشان داد. معیارهای ارزیابی چنین به عنوان دقت، درست مثبت نرخ (تی پی آر)، درست نرخ منفی (TNR)، دقت و معیار f برای ارزیابی استفاده شدند. ‎‏ ... شناسه‌ها در ابر محاسبات محیط‌ها. قابل ذکر است، EOS-IDS مدل ارائه شده قابل توجه مشارکت‌ها، دستیابی​ بالا دقت نرخ‌ها از ۹۷.۲۲۱٪ برای دارپا شناسه‌ها مجموعه داده‌ها و ۹۷.۱۱۸٪ برای مجموعه داده‌های CSE-CIC-IDS2018.

پاندی و همکاران [[93]](#_bookmark181) تحقیقاتی که بر تشخیص نفوذ در حوزه کلان‌داده در محاسبات ابری متمرکز شده‌اند، به بررسی ... ‎‏ ... محدودیت‌ها از سنتی شناسه‌ها در مقابله با حملات خارجی که بر رفتار شبکه تأثیر می‌گذارند. هدف آن افزایش امنیت شبکه از طریق یک شبکه حداکثر خروجی عمیق مبتنی بر الگوریتم بهینه‌سازی نمایی شپرد (ExpSSOA) برای تشخیص نفوذ بود که Exponentially را ادغام می‌کرد. وزنی حرکت میانگین (EWMA) و چوپان سرگردان بهینه‌سازی الگوریتم (اس‌اس‌او‌ای) برای بهبود یافته عملکرد. توسط با استفاده از اطلاعات از بزرگ داده‌ها منابع مانند اینترنت اشیا (IoT) و داده‌های وب سرور آپاچی. آزمایشی ارزیابی با استفاده از ‎‏ ... آپاچی وب سرور مجموعه داده نمایش داده شده برتر دقت، معیار F، دقت، و

یادآوری در مقایسه با روش‌های تثبیت‌شده مانند پرسپترون چندلایه ام‌ال‌پی، و بلند-کوتاه مدت حافظه LSTM + Spark. تحقیق [[94]](#_bookmark182) با تمرکز بر ارائه یک IDS هوشمند جدید مدل با استفاده از دی ال الگوریتم‌ها برای ارتقاء دهنده ابر محاسبات امنیت. آن هدف قرار داده شده به مقابله ‎‏ ... دشواری‌ها از در حال بهبود

تشخیص نفوذ در محیط‌های ابری و بهینه‌سازی ویژگی‌ها انتخاب به به طور دقیق شناسایی در حال تکامل تهدیدها اهداف شامل معرفی یک مدل IDS جدید بود که با هم ادغام شده بود. ‎‏ ... شعاعی اساس عملکرد عصبی شبکه (RBFNN) و جنگل تصادفی (RF) برای افزایش دقت و کارایی در نفوذ تشخیص. با این حال، ‎‏ ... تحقیق از معیارهای عملکرد در سیستم تشخیص نفوذ هوشمند برای شناسایی فعالیت‌های مخرب در محاسبات ابری، مانند دقت، صحت، فراخوانی و ضریب همبستگی متیو، استفاده کردند. این مدل به طور موثر نفوذها را شناسایی کرد و توانایی خود را در تشخیص و طبقه‌بندی دقیق فعالیت‌های مخرب نشان داد و پتانسیل خود را برای بهبود امنیت سایبری در سیستم‌های مبتنی بر ابر نشان داد.

تحقیق [[95]](#_bookmark183) هدف آن بهبود عملکرد IDS در محیط‌های ابری با استفاده از شبکه‌های عصبی عمیق (DNN)، الگوریتم‌های پس‌انتشار و بهینه‌سازی ازدحام ذرات (PSO) بود. این پروژه به دنبال پرداختن به شکاف‌های موجود در ادبیات موضوع بود، رفتار الف مفصل تحلیل از ‎‏ ... CSE-CIC- IDS-

مجموعه داده‌های ۲۰۱۸، و مقایسه مدل‌های پیشنهادی با رویکردهای قبلی. اهداف شامل انجام یک مطالعه تجربی گسترده بود. تحقیق و تفحص روی سیستم‌های تشخیص نفوذ (IDS) با استفاده از چند لایه پرسپترون (MLP) و پس انتشار MLP-BP و MLP با تکنیک‌های PSO برای افزایش معیارهای عملکرد در محیط‌های ابری. نتایج آزمایش‌ها، نمرات بهبود یافته معیارهای عملکرد، از جمله دقت و صحت را نشان داد .

تحقیق [[96]](#_bookmark184) به چالش‌های مختلفی که در محیط‌های محاسبات ابری با آن مواجه می‌شوند، از جمله افزایش موارد نفوذ، نقض‌های امنیتی در فضای مجازی، پرداخت. شرکت لایه، محدودیت‌ها از متعارف سیستم‌های تشخیص نفوذ، و ضرورت معماری بهبود یافته در توزیع شده محاسبات تنظیمات. آن اهداف درگیر توسعه از مبتنی بر فیلتر گروه ویژگی انتخاب (FEFS) و مدل DL (DLM) برای تشخیص نفوذ در ابر محاسبات. دی ال ام است الف ترکیب شده رویکرد از شبکه عصبی بازگشتی (RNN) و بهینه‌سازی شیطان تاسمانی (TDO). ارزیابی عملکرد از معیارهایی مانند معیار F، ویژگی، حساسیت و دقت برای ارزیابی اثربخشی استراتژی پیشنهادی. نتایج حاصل از ‎‏ ... تحقیق نشان داده شده ‎‏ ... اثربخشی از ‎‏ ... رویکرد پیشنهادی در در حال بهبود امنیت اقدامات برای نفوذ تشخیص در محیط‌های محاسبات ابری.

ماهسواری و ال. [[97]](#_bookmark185) تحقیق مورد بررسی قرار گرفت چالش‌ها مرتبط با بهبود امنیت در محیط‌های محاسبات ابری و افزایش عملکرد IDS. اهداف آن شامل معرفی یک رویکرد ترکیبی است که بهینه‌سازی یادگیری معلم را با شبکه‌های عصبی بازگشتی عمیق ترکیب می‌کند . (TL-DRNN) برای آی دی اس، استخدام اصلاح‌شده بهینه‌سازی جستجوی غذا توسط مانتا-ری (MMFO) برای انتخاب ویژگی، و اعتبارسنجی روش پیشنهادی با استفاده از مجموعه داده‌های استاندارد. نتایج نشان‌دهنده بهبود عملکرد در مورد نرخ مثبت کاذب، نرخ منفی کاذب، دقت، صحت، یادآوری، ویژگی و معیار F در مقایسه با رویکردهای IDS موجود بود.

تحقیق [[98]](#_bookmark186) متمرکز روی آدرس‌دهی چندین چالش‌های مرتبط به امنیت سایبری در اینترنت اشیا-ابر سیستم‌ها، از جمله حساسیت آنها به حملات سایبری به دلیل به گسترده اتصال و ‎‏ ... بحرانی نیاز برای مقاوم امنیت اقدامات به از دستگاه‌های اینترنت اشیا و سرویس‌های ابری محافظت کنید . برای مقابله با این مشکلات، این مطالعه پیشنهادی راه حل ها چنین به عنوان با استفاده از ازدحام الگوریتم‌های هوشمند همراه با شبکه‌های عصبی عمیق (DNN) برای تشخیص نفوذ کارآمد، با استفاده از DNN برای استخراج داده‌های بهینه ویژگی‌ها از اینترنت اشیا شناسه‌ها داده‌ها، و معرفی کردن الف انتخاب ویژگی تکنیک مبتنی بر روی ‎‏ ... کاپوچین جستجو الگوریتم (CapSA) برای افزایش قابلیت‌های تشخیص نفوذ. نتایج از ‎‏ ... آزمایش‌ها شامل عملکرد معیارها مانند میانگین دقت، میانگین فراخوانی، میانگین دقت و نرخ بهبود عملکرد، همراه با مقایسه‌های CNN-CapSA مدل با دیگر بهینه‌سازی الگوریتم‌ها، در نهایت نتیجه‌گیری روی ‎‏ ... رقابتی عملکرد از رویکرد پیشنهادی در مجموعه داده‌های مختلف.

تحقیق [[99]](#_bookmark187) هدف قرار داده شده به افزایش شناسه‌ها برای ابر امنیت محاسباتی، پرداختن به مسائلی مانند حریم خصوصی، محرمانگی، و در دسترس بودن در ابر سیستم‌ها، به عنوان خب به عنوان تشخیص جدید

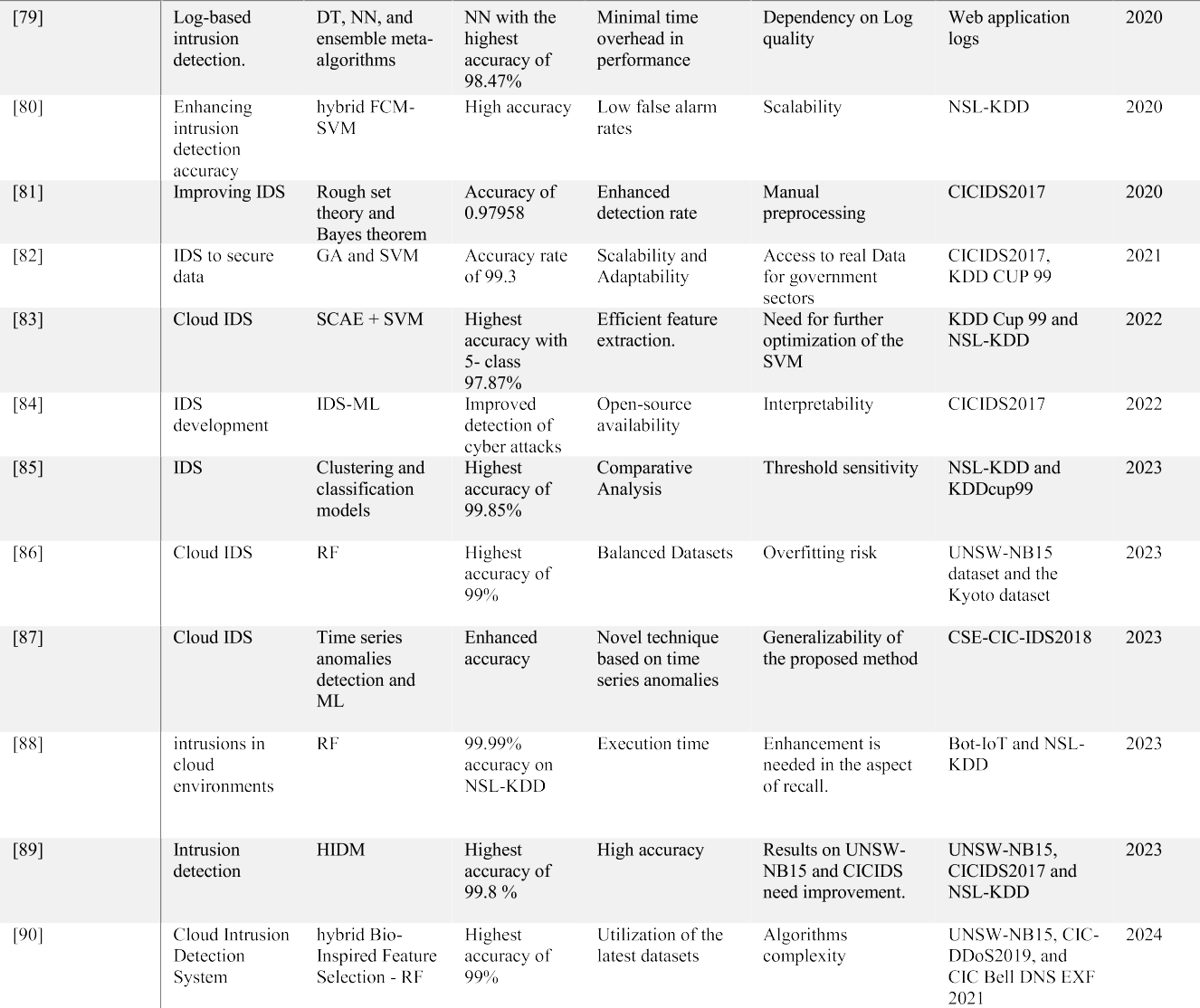
انواع نفوذ و کاهش حملات محاسبات کوانتومی. پیشنهادی گروه نفوذ تشخیص مدل برای محاسبات ابری با استفاده از عمیق یادگیری (EICDL) متمرکز روی بهبود​ دقت و کارایی در نفوذ تشخیص. آن معایب IDS موجود را تجزیه و تحلیل کرد ، و یک روش افزایش دقت معرفی نمود. مدل، و مقایسه شده EICDL عملکرد با روش‌های مدرن یادگیری ماشین و IDS موجود. سیستم داده‌های ورودی را پیش‌پردازش کرد، ویژگی‌ها را استخراج کرد و با استفاده از مدل‌های یادگیری ماشین طبقه‌بندی نمود. مانند دروازه‌دار مکرر واحدها (جی آر یو) و شبکه عصبی کانولوشن (CNN) و پیش‌بینی‌هایی ارائه داد. ارزیابی معیارها شامل دقت، دقت، به یاد آوردن، و اف۱ امتیاز در مجموعه داده‌ها. این مطالعه عملکرد EICDL را با سایر الگوریتم‌ها مقایسه کرد و به طور مداوم دقت ، صحت و فراخوانی بالاتری را نشان داد.

مقاله [[100]](#_bookmark188) در مورد اعمال تشخیص نفوذ بحث شد در آموزش موسیقی آنلاین با استفاده از شبکه‌های عصبی عمیق (DNN) در شبکه‌های ابری عمومی. هدف این تحقیق مقابله با چالش‌های تشخیص نفوذ در این حوزه بود. چارچوب پیشنهادی شامل ویژگی‌های مبتنی بر منطق فازی بود. انتخاب، بهینه‌سازی با استفاده از ‎‏ ... سالپ ازدحام الگوریتم، ادغام واحد بازگشتی دروازه‌دار (GRU) و شبکه عصبی کانولوشنی (CNN). معیارهای ارزیابی شامل دقت، دقت، به یاد آوردن، و اف۱ امتیاز در سراسر مجموعه داده‌ها. نتایج نشان داده شده بالاتر دقت در تشخیص نفوذها با مدل‌های پیشنهادی

تحقیق [[101]](#_bookmark189) مقابله شده نفوذ تشخیص در شبکه‌های کامپیوتری در چارچوب امنیت شبکه، با تمرکز بر چالش‌هایی مانند پیچیدگی فزاینده حملات شبکه و محدودیت‌های از سنتی فایروال ها. هدف بود به توسعه دادن بهینه‌سازی فعال دی ال مدل موش صحرایی ازدحام بهینه‌سازی شکارچی-پری-شبکه حداکثر خروجی عمیق (RSHPO-DMN) برای رسیدگی به مسائل تشخیص نفوذ. این شامل وظایفی مانند پیش‌پردازش داده‌ها، استخراج ویژگی مبتنی بر شبکه عصبی متعارف (CNN)، استفاده از DMN برای نفوذ است. تشخیص، و ارتقاء دهنده عملکرد از طریق بهینه‌سازی RSHPO. ارزیابی نشان داده شده ‎‏ ... برتر عملکرد RSHPO-DMN نسبت به سایر روش‌ها از نظر دقت، صحت، فراخوانی و امتیاز F1.

جوراویا و همکاران [[102]](#_bookmark190) چندین مسئله کلیدی را بررسی کرد، از جمله پرداختن به چالش‌های امنیتی ناشی از کانتینری شدن در محیط‌های ابری و بهبود اثربخشی سیستم‌های تشخیص نفوذ برای نظارت و شناسایی حملات درون کانتینر شده محیط‌ها. راهکارهای پیشنهادی شامل کردن استخدام دی ال روش‌ها، به طور خاص شبکه‌های عصبی کانولوشنی (CNNs)، برای تشخیص ناهنجاری در سیستم تماس بگیرید توالی‌ها و تصاویر مشتق شده از اینها نتایج حاصل از ارزیابی تجربی سیستم تشخیص نفوذ میزبان مبتنی بر DL-DL-(HIDS) شامل مقایسه دقت تشخیص، نرخ مثبت کاذب و خطاهای احتمالی است . منفی نرخ با موجود روش‌ها، همراه با تجزیه و تحلیل کردن ‎‏ ... تأثیر از متغیر تصویر اندازه‌ها، سیستم تماس بگیرید پارامترها و معماری‌های CNN بر عملکرد تشخیص. علاوه بر این، ‎‏ ... ارزیابی ارزیابی می‌کند ‎‏ ... سیستم قابلیت به شناسایی حملات شناخته شده و ناشناخته در محیط‌های ابری کانتینری، و در نهایت با هدف پیاده‌سازی DL-HIDS برای بهبود امنیت در چنین محیط‌هایی.

**جدول ۵.** شناسه‌ها ناهنجاری مبتنی بر در ابر شبکه با استفاده از ام ال.



1. **تحقیق گپ**

بر اساس فهرست گسترده مقالات پژوهشی ارائه شده، چندین تحقیق شکاف‌ها و مناطق برای بیشتر تحقیق و تفحص در حوزه ناهنجاری‌های انکار سرویس توزیع‌شده (DDoS) و نفوذ تشخیص سیستم‌ها (IDS) می‌تواند باش شناسایی شد. اولاً، شکاف قابل توجهی در آزمایش و اعتبارسنجی در دنیای واقعی وجود دارد. از روش‌های تشخیص، که بسیاری از مطالعات عمدتاً بر توسعه و ارزیابی با استفاده از شبیه‌سازی یا معیار تمرکز دارند مجموعه داده‌ها مانند NSL-KDD، سیسیدها، و کی دی دی جام، بنابراین فاقد اعتبارسنجی گسترده در محیط‌های محاسبات ابری دنیای واقعی یا با داده‌های ترافیک شبکه زنده است. ثانیاً، مقیاس‌پذیری نگرانی‌ها پافشاری کردن، به ویژه در در مقیاس بزرگ محیط‌های ابری که کاوش در تشخیص نفوذ مقیاس‌پذیر را تضمین می‌کنند تکنیک‌ها قادر از به طور کارآمد رسیدگی افزایش یابنده داده‌ها حجم و شبکه ترافیک. سوم اینکه، آنجا است الف نیاز به شناسه‌ها که می‌تواند سازگار شدن به پویا تهدیدها، به عنوان بسیاری مطالعات

آدرس شناخته شده حمله انواع اما سقوط کوتاه در تشخیص الگوهای حمله نوظهور و در حال تکامل. علاوه بر این، در حالی که بسیاری از تشخیص‌ها روش‌ها دستیابی به بالا دقت نرخ‌ها، آنجا است از نظر کارایی محاسباتی و استفاده از منابع، جای بهبود وجود دارد. علاوه بر این، در توسعه IDS شکاف وجود دارد. مقاوم علیه گریز تکنیک‌ها شاغل توسط مهاجمان می‌توانند مکانیسم‌های تشخیص را دور بزنند و این امر نیاز به تحقیق با تمرکز بر روش‌های تشخیص مقاوم در برابر گریز را برجسته می‌کند. علاوه بر این، به عنوان سازمان‌ها مستقر کردن چندگانه امنیت برای راه‌حل‌ها، نیاز به تحقیق در مورد قابلیت همکاری و ادغام یکپارچه بین IDS و سایر ابزارهای امنیتی وجود دارد. به افزایش به طور کلی تهدید تشخیص و پاسخ قابلیت‌ها. در نهایت، پرداختن به نگرانی‌های مربوط به حریم خصوصی و ملاحظات اخلاقی مربوط به جمع‌آوری، پردازش و اشتراک‌گذاری داده‌ها در IDS توسعه است ضروری، برجسته کردن ‎‏ ... اهمیت در حال توسعه حفظ حریم خصوصی شناسه‌ها تکنیک‌ها اولویت بندی-

**جدول ۶.** شناسه‌ها ناهنجاری مبتنی بر در ابر شبکه با استفاده از دی ال.



ینگ کاربر حریم خصوصی در حالی که نگهداری مؤثر تهدید تشخیص. آدرس‌دهی اینها تحقیق شکاف‌ها می‌تواند مشارکت به طور قابل توجهی به​ پیشرفت از حملات انسداد سرویس (DDOS) پیشگیری و شناسه‌ها فناوری‌ها، در نهایت ارتقاء دهنده ‎‏ ... امنیت وضعیت بدن از ابر سیستم‌های محاسباتی و شبکه‌ای.

1. **محدوده از بهبود**

میدان از ماشین یادگیری (میلی لیتر) نگه می‌دارد گسترده پتانسیل، به ویژه مربوط به ناهنجاری تشخیص در ابر خالص-

با پیشرفت‌های مداوم در چندین زمینه کلیدی، کار می‌کند. اینها شامل شدن در حال بهبود داده‌ها کیفیت و کمیت برای آموزش مدل‌های تشخیص ناهنجاری قوی، افزایش قابلیت تفسیر مدل برای درک بهتر فرآیندهای تصمیم‌گیری، رفع سوگیری و تضمین انصاف در الگوریتم‌ها به جلوگیری از تبعیض آمیز پیامدها، و اصلاح- انتقال قابلیت‌های یادگیری برای بهره‌برداری از دانش از حوزه‌های مرتبط، ضمن تضمین مقیاس‌پذیری و کارایی برای در مقیاس بزرگ استقرار در ابر محیط‌ها.

انسان-ماشین همکاری است حیاتی برای پالایش سیستم‌های تشخیص ناهنجاری ، در حالی که راه‌حل‌های AutoML پذیرش فناوری را تسریع می‌کنند. در حوزه یادگیری عمیق (DL)، پیشرفت بر نوآوری‌های معماری، قابلیت تفسیر، انتقال یادگیری، کارایی، استحکام، امنیت، و مداوم یادگیری. کاوش کوانتومی میلی لیتر نشان دهنده یک نوآوری مرز برای هل دادن ناهنجاری تشخیص قابلیت‌های بیشتر در شبکه‌های ابری. این پیشرفت‌ها در مجموع به تکامل مداوم روش‌های تشخیص ناهنجاری کمک می‌کنند و بهبود مستمر در محیط‌های ابری را تضمین می‌کنند. از سوی دیگر، مدل‌های زبان بزرگ (LLM) می‌تواند باش استفاده شده به طور موثر برای ناهنجاری تشخیص توسط گرفتن​ مزیت از آنها پیشرفته توانایی‌ها در طبیعی پردازش زبان . آنها می‌تواند تحلیل کردن متن داده‌ها و تشخیص الگوهایی که با آنچه معمولاً انتظار می‌رود متفاوت هستند. علاوه بر این، ادغام سیستم تشخیص ناهنجاری مبتنی بر LLM با تنظیمات نظارت و امنیت ابری موجود برای ارائه دفاع جامع در برابر تهدیدات سایبری برای افزایش قابلیت اطمینان زیرساخت‌های ابری در مواجهه با تهدیدات امنیتی فزاینده ضروری است. با این حال، LLM به عنوان یک محافظ اضافی عمل می‌کند و روش‌های سنتی تشخیص ناهنجاری مبتنی بر قانون یا آماری را تکمیل می‌کند. برای مثال، علی و ال. [[103]](#_bookmark191) پیشنهاد شده راه حل ها شامل ادغام LLM ها و توسعه نمونه اولیه HuntGPT است که ترکیب می‌کند مبتنی بر یادگیری ماشینی ناهنجاری تشخیص با هوش مصنوعی قابل توضیح برای ارائه بینش‌های عملی برای پاسخ‌دهندگان به تهدیدات. پاسخ‌های چت‌بات سیستم، دانش فنی امنیت سایبری و توضیحات واضحی برای ناهنجاری‌های شناسایی‌شده ارائه می‌دهد و... به کاربران با محدود امنیت سایبری تجربه. علاوه بر این، زمان سری تحلیل می‌تواند باش استفاده شده به طور کارآمد به شناسایی ناهنجاری‌ها، کمک به تشخیص و پیشگیری از موارد غیرعادی رفتارها در ابر محیط‌ها. علاوه بر این، ادغام LLM ها با تکنیک‌های تحلیلی سری زمانی می‌تواند فراهم کند الف بیشتر جامع راه حل به ناهنجاری تشخیص با بهره‌گیری از ویژگی‌های مکمل هر دو روش. این ادغام می‌تواند منجر به بهبود دقت و اثربخشی سیستم‌های تشخیص ناهنجاری شود. لیو و همکاران. [[104]](#_bookmark192) تحقیقات با پیشنهاد AnomalyLLM که برای استخراج دانش استفاده می‌شد، به چالش‌های تشخیص ناهنجاری سری‌های زمانی پرداخت. از الف آموزش دیده لیسانس حقوق آنومالی LLM از رویکردهای پیشرفته‌تر بهتر عمل می‌کند و اثربخشی LLM را در بهبود شناسایی ناهنجاری‌های سری زمانی نشان می‌دهد.

1. **نتیجه‌گیری**

این مقاله به چالش‌ها و تهدیدهای امنیتی پیش روی شبکه‌های ابری می‌پردازد و استفاده از تکنیک‌های ML/DL را به عنوان یک راه حل پیشنهاد می‌کند. این مقاله شیوع توزیع‌شده را مورد بحث قرار می‌دهد. انکار از خدمات (عدم سرویس توزیع‌شده) حملات در ابر محاسبات، محدودیت‌های اقدامات امنیتی فعلی و ضرورت برای پیشرفته امنیت راه حل ها. پیشنهادی راه‌حل‌ها شامل تکنیک‌های یادگیری ماشین/یادگیری عمیق برای تشخیص ناهنجاری در شبکه‌های ابری هستند، به‌ویژه از طریق یک سیستم تشخیص نفوذ (IDS) که چندین الگوریتم یادگیری ماشین/یادگیری عمیق را ترکیب می‌کند. برای تشخیص و طبقه‌بندی دقیق تهدید. این مقاله یک مدل امنیتی نوآورانه را معرفی می‌کند که طبقه‌بندی را بهبود می‌بخشد. دقت و نشان دادن ‎‏ ... اثربخشی از

سیستم‌های پیشنهادی. با این حال، این [مطالعه] همچنین شکاف‌های تحقیقاتی را برجسته می‌کند که فراهم کردن فرصت‌ها برای آینده مطالعات به تشخیص ناهنجاری در محیط‌های ابری را افزایش می‌دهد و در نهایت به تقویت تاب‌آوری شبکه ابری در برابر تهدیدات سایبری در حال تحول و حفاظت از داده‌ها و سرویس‌های حیاتی کمک می‌کند .

**منابع**

1. م. ندیم، الف. ارشد، س. ریاض، س. س. گروه موسیقی، و الف. موسوی، رهگیری ‎‏ ... ابر شبکه از وحشیانه نیرو و حملات انسداد سرویس (DDOS) حملات از طریق نفوذ تشخیص و پیشگیری سیستم،'' *IEEE دسترسی* ، جلد ۹، ص. ۱۵۲۳۰۰–۱۵۲۳۰۹، ۲۰۲۱، دی آی: [‎۱۰.۱۱۰۹/دسترسی.۲۰۲۱.۳۱۲۶۵۳۵‎](http://dx.doi.org/10.1109/ACCESS.2021.3126535)
2. الف. فتانی، م. الف. العزیز، الف. داهو، م. الف. الف. القانس، و س. لو، اینترنت اشیا سیستم تشخیص نفوذ با استفاده از یادگیری عمیق و حالت گذرای بهبود یافته بهینه‌سازی جستجو، « *IEEE Access* »، جلد ۹، صفحات. ۱۲۳۴۴۸–۱۲۳۴۶۴، ۲۰۲۱، دی آی: [‎۱۰.۱۱۰۹/دسترسی.۲۰۲۱.۳۱۰۹۰۸۱‎](http://dx.doi.org/10.1109/ACCESS.2021.3109081)
3. SM Kasongo، "یک سیستم تشخیص نفوذ پیشرفته برای IIoT مبتنی بر روی جی ای و درخت مبتنی بر الگوریتم‌ها، *IEEE دسترسی* ، جلد ۹،

ص. ۱۱۳۱۹۹–۱۱۳۲۱۲، ۲۰۲۱، دی آی: [‎۱۰.۱۱۰۹/دسترسی.۲۰۲۱.۳۱۰۴۱۱۳‎](http://dx.doi.org/10.1109/ACCESS.2021.3104113)

1. ای. سینگ و کی. چاترجی، «مسائل و چالش‌های امنیتی ابری: الف» «نظرسنجی»، *مجله محاسبات کاربردی شبکه* ، جلد ۷۹، صفحات ... ۸۸–۱۱۵، فوریه ۲۰۱۷، doi: [‎۱۰.۱۰۱۶/j.jnca.۲۰۱۶.۱۱.۰۲۷‎](http://dx.doi.org/10.1016/j.jnca.2016.11.027)
2. آمازون. *خلاصه‌ای از اختلال در سرویس S3 آمازون در شمال منطقه ویرجینیای شرقی (US-EAST-1)* . دسترسی: ۲۸ فوریه ۲۰۲۴. [آنلاین].

موجود است: https://aws.amazon.com/message/41926/

1. بن لاوجوی. (2024). *قطعی سراسری متا: چه می‌دانیم، و چه بود ‎‏ ... احتمالاً علت*​ دسترسی‌ها: فوریه ۲۸، ۲۰۲۴. [آنلاین]. موجود است: https://9to5mac.com/2024/03/06/global-meta-outage-what-happened/
2. ز. جی، ی. وانگ، ک. یان، ایکس. شی، ی. شیانگ، و جی. هوانگ، «الف» استراتژی تعبیه فضا برای تشخیص ناهنجاری در زمان چند متغیره سری، '' *Expert Syst. Appl.* ، جلد 206، نوامبر 2022، ماده. نه. ۱۱۷۸۹۲، doi: [‎۱۰.۱۰۱۶/j.eswa.۲۰۲۲.۱۱۷۸۹۲‎](http://dx.doi.org/10.1016/j.eswa.2022.117892)
3. ام. هو، ایکس. فنگ، زد. جی، کی. یان، و اس. ژو، «یک روش محاسباتی جدید» رویکرد برای اختلاف و نفاق جستجو با محلی عود نرخ‌ها در چند متغیره- «سری‌های زمانی»، *مجله علوم پایه* ، جلد ۴۷۷، صفحات ...». ۲۲۰–۲۳۳، مارس ۲۰۱۹، doi: [‎۱۰.۱۰۱۶/j.ins.۲۰۱۸.۱۰.۰۴۷‎](http://dx.doi.org/10.1016/j.ins.2018.10.047)
4. الف. اقبال و آر. امین، «زمان» سری پیش‌بینی و ناهنجاری تشخیص- با استفاده از یادگیری عمیق، « *مهندسی شیمی کامپیوتر* ، جلد ۱۸۲، مارس ۲۰۲۴» شماره ماده ۱۰۸۵۶۰، doi: [10.1016/j.compchemeng.2023.108560.](http://dx.doi.org/10.1016/j.compchemeng.2023.108560)
5. ز. هی، پ. چن، ایکس. لی، وای. وانگ، جی. یو، سی. چن، ایکس. لی، و زد. ژنگ، یک رویکرد یادگیری عمیق مکانی-زمانی برای ناهنجاری‌های بدون نظارت تشخیص در سیستم‌های ابری، « *سیستم یادگیری شبکه عصبی ترانس IEEE »* ، جلد ۳۴، نه. ۴، ص. ۱۷۰۵–۱۷۱۹، آوریل ۲۰۲۳، دی آی: [‎۱۰.۱۱۰۹/TNNLS.۲۰۲۰‎](http://dx.doi.org/10.1109/TNNLS.2020.3027736)

[۳۰۲۷۷۳۶.](http://dx.doi.org/10.1109/TNNLS.2020.3027736)

1. ام. ام. بلال و دی. ام. ساندرام، «مروری جامع بر اطلاعات» دفاع‌های امنیتی قدرتمند در فضای ابری: طبقه‌بندی، مسائل امنیتی، یادگیری ماشین/یادگیری یادگیری عمیق تکنیک‌ها، چالش‌ها و آینده روندها، *جی. پادشاه سعود دانشگاه کام- قرار دهید. Inf. Sci.* ، جلد 34، شماره 10، صفحات. ۹۱۰۲–۹۱۳۱، نوامبر ۲۰۲۲، doi: [‎۱۰.۱۰۱۶/j.jksuci.‎‏ ‏۲۰۲۲.۰۸.۰۳۵‎‏.](http://dx.doi.org/10.1016/j.jksuci.2022.08.035)
2. ای. شاجان و اس. رنگاسوامی، «بررسی تهدیدات امنیتی و راهکارهای مقابله با آنها» اقدامات در ابر محاسبات، *یونایتد بین المللی جی. پژوهش فناوری* ، جلد ۲، نه. ۷،

ص. ۲۰۱–۲۰۷، ۲۰۲۱. (یا: ۲۰۲۱)

1. الف. س. روماله و دی. ن. چودهاری، «ابر» محاسبات: نرم‌افزار به عنوان «یک سرویس»، در *مجموعه مقالات دومین کنفرانس بین‌المللی برق، کامپیوتر، ارتباطات و فناوری. (ICECCT)* ، فوریه ۲۰۱۷، صفحات ۱-۶، doi: [10.1109/ICECCT.2017.8117817.](http://dx.doi.org/10.1109/ICECCT.2017.8117817)
2. م. یاسین، ه. اولد-سلیمان، س. طلحی، و ه. بوشنب، «چند- چارچوب تشخیص نفوذ مستاجر به عنوان سرویسی برای SaaS، *IEEE خدمات کامپیوتری ترانس* ، جلد 15، شماره 5، صفحات. ۲۹۲۵–۲۹۳۸، سپتامبر ۲۰۲۲، doi: [‎۱۰.۱۱۰۹/TSC.۲۰۲۱.۳۰۷۷۸۵۲‎](http://dx.doi.org/10.1109/TSC.2021.3077852)
3. س. ک. سمیه، پ. دیپیکا، جی. نارن، و # ب فنی. (۲۰۱۴). *قرار دادن- بررسی اجمالی Cloud-IaaS، PaaS و SaaS* . [آنلاین]. موجود در: [www.ijcsit.com](http://www.ijcsit.com/)
4. ب. حبیب و ف. خورشید، «تشخیص DDoS مبتنی بر REST-API با استفاده از طبقه‌بندی‌کننده جنگل تصادفی در یک محیط ابری پلتفرم به عنوان سرویس، *بین المللی جی. محاسبه. رقم سیستم.* ، جلد ۱۴، نه. ۱، صفحات ۱۰۷۵–۱۰۸۹، سپتامبر ۲۰۲۳، دی آی: [‎۱۰.۱۲۷۸۵/ijcds/۱۴۰۱۸۴‎](http://dx.doi.org/10.12785/ijcds/140184)
5. D. Gonzales، JM Kaplan، E. Saltzman، Z. Winkelman و D. Woods، «ابر-اعتماد—A» امنیت ارزیابی مدل برای زیرساخت به عنوان الف خدمات ابرهای (IaaS)، « *IEEE Trans. Cloud Comput.»* ، جلد ۵، شماره ۳، صفحات. ۵۲۳–۵۳۶، ژوئیه 2017، doi: [10.1109/TCC.2015.2415794.](http://dx.doi.org/10.1109/TCC.2015.2415794)
6. س. الف. وارما و ک. جی. ردی، «الف» بررسی از حملات انسداد سرویس (DDOS) حملات و آن اقدامات متقابل در ابر محاسبات، در *مجموعه مقالات پنجم بین المللی کنفرانس. اطلاعات. سیستم. محاسبات. شبکه. (ISCON)* ، اکتبر 2021، صفحات. ۱–۶، doi: [‎۱۰.۱۱۰۹/ISCON۵۲۰۳۷.۲۰۲۱.۹۷۰۲۳۸۸‎](http://dx.doi.org/10.1109/ISCON52037.2021.9702388)
7. J. Snehi, M. Snehi, A. Bhandari, V. Baggan, and R. Ahuja, ''Intro- تماشا کردن نفوذ تشخیص سیستم‌ها در معامله با امنیت باهم- سرن‌ها در محیط ابری، در *مجموعه مقالات دهمین کنفرانس بین‌المللی مدل سیستم. پژوهش‌های پیشرفت. روندها (SMART)* ، دسامبر ۲۰۲۱، صفحات. ۳۴۵–۳۴۹، doi: [10.1109/SMART52563.2021.9676258.](http://dx.doi.org/10.1109/SMART52563.2021.9676258)
8. MA Al-Shareeda، S. Maniccam و MA Saare، ''حملات DDoS تشخیص با استفاده از دستگاه یادگیری و عمیق یادگیری تکنیک‌ها: تحلیل و مقایسه،'' *گاو نر. برق مهندس اطلاعات.* ، جلد ۱۲، نه. ۲، ص. ۹۳۰–۹۳۹، آوریل 2023، doi: [10.11591/eei.v12i2.4466.](http://dx.doi.org/10.11591/eei.v12i2.4466)
9. سی. دولیگریس و ای. میتروکوتسا، «حملات DDoS و مکانیسم‌های دفاعی» نیسم‌ها: طبقه‌بندی و مدرن،'' *محاسبه. شبکه* ، جلد ۴۴، نه. ۵،

ص. ۶۴۳–۶۶۶، آوریل ۲۰۰۴، دی آی: [‎10.1016/j.comnet.2003.10.003‎‏. (این عبارت به نظر مجموعه‌ای تصادفی از حروف و اعداد است و معنای قابل ترجمه‌ای ندارد.)](http://dx.doi.org/10.1016/j.comnet.2003.10.003)

1. سیسکو. (۲۰۲۳). *سیسکو سالانه اینترنت گزارش (۲۰۱۸–۲۰۲۳) گزارش رسمی* . [آنلاین]. موجود در: [https://www.cisco.com/](http://www.cisco.com/) c/en/us/solutions/collateral/executive-perspectives/annual-internet- گزارش/گزارش-سفید-c11-741490.html.
2. سی. کروگل، اف. والور، و جی. ویگنا، *تشخیص نفوذ و همبستگی: چالش‌ها و راه‌حل‌ها* ، جلد ۱۴. چام، سوئیس: اشپرینگر، ۲۰۰۴.
3. کی. اسکارفون و پی. مل، «راهنمای تشخیص و پیشگیری از نفوذ» سیستم‌ها (IDPS) *نات موسسه استانداردها فناوری* ، جلد ۸۰۰، ص. ۹۴، فوریه ۲۰۰۷. (۱۳۸۶)
4. الف. مومند، س. یو. جان، و ن. رمضان، «الف» سیستماتیک و جامع بررسی پیشرفت‌های اخیر در سیستم‌های تشخیص نفوذ با استفاده از ماشین یادگیری: یادگیری عمیق، مجموعه داده‌ها و طبقه‌بندی حمله، *مجله حسگرها* ، جلد ۲۰۲۳، صفحات ۱ تا ۱۸، فوریه ۲۰۲۳، doi: [10.1155/2023/6048087.](http://dx.doi.org/10.1155/2023/6048087)
5. م. تولایی، ای. باقری، دبلیو. لو، و الف. الف. قربانی، «الف» مفصل تحلیل از ‎‏ ... کی دی دی جام ۹۹ داده‌ها تنظیم شده،'' در *مجموعه مقالات IEEE علامت محاسبه. هوش. امن. مجله کاربردی دفاع* ، ژوئیه ۲۰۰۹، صفحات ۱ تا ۶، doi: [10.1109/CISDA.2009.5356528.](http://dx.doi.org/10.1109/CISDA.2009.5356528)
6. (۲۰۱۷). *مجموعه داده‌های ارزیابی تشخیص نفوذ (CIC-IDS۲۰۱۷)* . دسترسی: ۱۰ مارس ۲۰۲۴. [آنلاین]. موجود در: https://www.unb. ca/cic/datasets/ids-2017.html
7. ع. شیروی، ح. شیروی، م. تولایی و ع.ع.قربانی، «به سوی توسعه عملیات الف سیستماتیک رویکرد به تولید کردن معیار مجموعه داده‌ها برای نفوذ تشخیص، '' *Comput. Secur.* ، جلد ۳۱، شماره ۳، صفحات. ۳۵۷–۳۷۴، مه ۲۰۱۲، doi: [‎۱۰.۱۰۱۶/j.cose.۲۰۱۱.۱۲.۰۱۲‎](http://dx.doi.org/10.1016/j.cose.2011.12.012)
8. ن. مصطفی و جی. اسلی، «UNSW-NB15: یک مجموعه داده جامع برای» سیستم‌های تشخیص نفوذ شبکه (مجموعه داده‌های شبکه UNSW-NB15) در *مجموعه مقالات میل. ارتباطات اطلاعات سیستم کنفرانس (MilCIS)* ، نوامبر ۲۰۱۵، ص. ۱–۶، دی آی: [‎۱۰.۱۱۰۹/MilCIS.۲۰۱۵.۷۳۴۸۹۴۲‎](http://dx.doi.org/10.1109/MilCIS.2015.7348942)
9. (۲۰۱۹). *حملات انسداد سرویس (DDOS) ارزیابی مجموعه داده‌ها (CIC- DDoS2019* )

دسترسی: ۱۰ مارس ۲۰۲۴. [آنلاین]. موجود در: [https://www.unb.ca/cic/datasets/ddos-2019.html.](http://www.unb.ca/cic/datasets/ddos-2019.html)

1. (۲۰۱۸). *CSE-CIC-IDS2018 روی خدمات وب آمازون: الف مشارکتی پروژه بین ‎‏ ... ارتباطات امنیت تأسیس (سی اس ای) و ‎‏ ... کانادایی موسسه برای امنیت سایبری (CIC)* . دسترسی: 11 مارس 2024. [آنلاین]. موجود در: [https://www.unb.ca/cic/datasets/ids-2018.html.](http://www.unb.ca/cic/datasets/ids-2018.html)
2. اُ. اوسانایه، اچ. کای، ک.-ک.-ر. چو، الف. دهقانتنها، ز. خو، و

ام. دلودلو، «روش انتخاب ویژگی چند فیلتری مبتنی بر گروه برای» تشخیص DDoS در محاسبات ابری، *مجله ارتباطات بی‌سیم EURASIP. شبکه* ، جلد ۲۰۱۶، نه. ۱، ص. ۱–۱۰، دسامبر ۲۰۱۶، دی آی: [۱۰.۱۱۸۶/s۱۳۶۳۸- ۰۱۶-](http://dx.doi.org/10.1186/s13638-016-0623-3)

[۰۶۲۳- ۳.](http://dx.doi.org/10.1186/s13638-016-0623-3)

1. ی. فروند و آر. ای. شاپیر، «تعمیم نظریه تصمیم‌گیری از «یادگیری آنلاین و کاربردی برای تقویت یادگیری»، *مجله علوم کامپیوتر* ، جلد ۵۵، شماره ۱، صفحات ۱۱۹-۱۳۹، اوت ۱۹۹۷، doi: [10.1006/jcss.1997.1504.](http://dx.doi.org/10.1006/jcss.1997.1504)
2. *ترافیک داده‌ها از کیوتو دانشگاه عسل- گلدان‌ها* . دسترسی: ۱۱ مارس ۲۰۲۴. [آنلاین]. موجود در: [https://www.takakura.com/Kyoto\_data/](http://www.takakura.com/Kyoto_data/)
3. الف. ب. ناصیف، م. الف. طالب، س. نصیر، اچ. البدانی، و

ف. م. داکلباب، «یادگیری ماشین برای امنیت ابری: یک رویکرد سیستماتیک» مرور، « *IEEE Access* »، جلد ۹، صفحات. ۲۰۷۱۷–۲۰۷۳۵، ۲۰۲۱، doi: [‎۱۰.۱۱۰۹/دسترسی.۲۰۲۱.۳۰۵۴۱۲۹‎](http://dx.doi.org/10.1109/ACCESS.2021.3054129)

1. ای. آلدویش، ای. درهاب، و ای. زد. امام، «رویکردهای یادگیری عمیق» برای مبتنی بر ناهنجاری نفوذ تشخیص سیستم‌ها: الف نظرسنجی، طبقه بندی، و شماره‌های باز، « *سیستم مبتنی بر دانش»* ، جلد ۱۸۹، فوریه ۲۰۲۰، ماده. نه. ۱۰۵۱۲۴، دی آی: [‎۱۰.۱۰۱۶/j.knosys.۲۰۱۹.۱۰۵۱۲۴‎](http://dx.doi.org/10.1016/j.knosys.2019.105124)
2. جی. س. کوشوا و وی. رنگا، «رأی‌گیری» افراطی یادگیری دستگاه تشخیص حمله انکار سرویس توزیع‌شده مبتنی بر محاسبات ابری «،» *J. Inf. Secur. Appl.* ، جلد ۵۳، اوت ۲۰۲۰، ماده. نه. ۱۰۲۵۳۲، doi: [‎۱۰.۱۰۱۶/j.jisa.۲۰۲۰.۱۰۲۵۳۲‎](http://dx.doi.org/10.1016/j.jisa.2020.102532)
3. س. سامبانگی و ل. گوندی، «یک رویکرد یادگیری ماشینی برای DDoS» تشخیص حمله (انکار سرویس توزیع‌شده) با استفاده از الگوریتم‌های خطی چندگانه رگرسیون، *مجموعه مقالات* ، جلد ۶۳، شماره ۱، ص. ۵۱، ۲۰۲۰، doi: [10.3390/pro-](http://dx.doi.org/10.3390/proceedings2020063051) [ceedings2020063051.](http://dx.doi.org/10.3390/proceedings2020063051)
4. آر. ابوبکر، الف. آلدگیشم، م. ف. مجید، الف. محمود، اچ. مریم،

ن. الف. الراجح، سی. افرا، و م. جواد «آن» مؤثر مکانیکی- آنیسم به کاهش دادن زمان واقعی حملات انسداد سرویس (DDOS) حمله،'' *IEEE دسترسی* ، جلد ۸،

ص. ۱۲۶۲۱۵–۱۲۶۲۲۷، ۲۰۲۰، دی آی: [‎۱۰.۱۱۰۹/ACCESS.۲۰۲۰.۲۹۹۵۸۲۰‎](http://dx.doi.org/10.1109/ACCESS.2020.2995820)

1. M. Mayuranathan، M. Murugan، و V. Dhanakoti، «بازگشت مقاله: بهترین ویژگی‌ها مبتنی بر نفوذ تشخیص سیستم توسط آر بی ام مدل برای تشخیص حملات انسداد سرویس (DDOS) در ابر محیط زیست،'' *جی. محیط هوش. انسانی‌سازی شده محاسبه.* ، جلد ۱۲، نه. ۳، ص. ۳۶۰۹–۳۶۱۹، مارس ۲۰۲۱، دی آی: [۱۰.۱۰۰۷/s۱۲۶۵۲-](http://dx.doi.org/10.1007/s12652-019-01611-9)

[۰۱۹-۰۱۶۱۱- ۹.](http://dx.doi.org/10.1007/s12652-019-01611-9)

1. الف. الشماری و الف. آلدریبی، «به‌کارگیری تکنیک‌های یادگیری ماشینی در تشخیص بدخواه شبکه ترافیک در ابر محاسبات، *جی. بزرگ داده‌ها* ، جلد ۸، شماره ۱، صفحه ۹۰، دسامبر ۲۰۲۱، doi: [10.1186/s40537-021-00475-1.](http://dx.doi.org/10.1186/s40537-021-00475-1)
2. جی. س. کوشوا و وی. رنگا، ''بهینه‌سازی شده'' افراطی یادگیری دستگاه برای تشخیص حملات DDoS در محاسبات ابری، « *محاسبات امنیتی* »، جلد ۱۰۵، ژوئن 2021، هنر. نه 102260، doi: [10.1016/j.cose.2021.102260.](http://dx.doi.org/10.1016/j.cose.2021.102260)
3. اس. ساچدوا و ای. علی، «یادگیری ماشین با پزشکی قانونی دیجیتال برای» طبقه‌بندی حمله در محیط شبکه ابری، « *Int. J. Syst. Assurance» مدیریت مهندسی* ، جلد ۱۳، شماره S1، صفحات ۱۵۶–۱۶۵، مارس ۲۰۲۲، doi: [‎۱۰.۱۰۰۷/s۱۳۱۹۸-۰۲۱-۰۱۳۲۳-۴‎](http://dx.doi.org/10.1007/s13198-021-01323-4)
4. MMG Alam، SJN Kumar، RU Mageswari، و TFM Raj، یک طبقه‌بندی‌کننده DEHO کارآمد مبتنی بر SVM برای تشخیص حمله DDoS در محیط محاسبات ابری، *مجله محاسبات شبکه* ، جلد ۲۱۵، اکتبر ۲۰۲۲ شماره ماده ۱۰۹۱۳۸، doi: [10.1016/j.comnet.2022.109138.](http://dx.doi.org/10.1016/j.comnet.2022.109138)
5. ن. میشرا، آر. کی. سینگ، و اس. کی. یاداو، «تشخیص DDoS» آسیب‌پذیری در محاسبات ابری با استفاده از طبقه‌بندی بیز پیچیده fier,'' *Comput. هوشمند نوروسک.* ، جلد 2022، صص. ۱–۱۳، ژوئیه ۲۰۲۲، doi: [‎۱۰.۱۱۵۵/۲۰۲۲/۹۱۵۱۸۴۷‎](http://dx.doi.org/10.1155/2022/9151847)
6. م. الدویلیج، س. دبلیو. خان، م. طاهر، م. سرداراز، م. الدویلیج، و

ف. مالک، «مبتنی بر یادگیری ماشین» حملات انسداد سرویس (DDOS) حمله تشخیص با استفاده از متقابل اطلاعات و روش اهمیت ویژگی جنگل تصادفی، '' *تقارن* ، جلد ۱۴، شماره ۶، صفحه ۱۰۹۵، مه ۲۰۲۲، doi: [10.3390/sym14061095.](http://dx.doi.org/10.3390/sym14061095)

1. س. سامبانگی، ل. گوندی، و س. الجوارنه، «الف» ویژگی شباهت دستگاه مدل یادگیری برای تشخیص حمله DDoS در محیط شبکه مدرن مانت برای صنعت ۴.۰، *محاسبه. برق مهندس* ، جلد ۱۰۰، مه ۲۰۲۲، شماره ماده ۱۰۷۹۵۵، doi: [10.1016/j.compeleceng.2022.107955.](http://dx.doi.org/10.1016/j.compeleceng.2022.107955)
2. ف. جی. عبدالله اوا، توزیع شده انکار از خدمات حمله تشخیص در «ابر دولت الکترونیک از طریق خوشه‌بندی داده‌ها»، *مجله Array* ، جلد ۱۵، سپتامبر ۲۰۲۲ شماره ماده ۱۰۰۲۲۹، doi: [10.1016/j.array.2022.100229.](http://dx.doi.org/10.1016/j.array.2022.100229)
3. س. سوکالینگام و آر. راماکریشنان، «آن» هوشمند نفوذ تشخیص سیستم برای توزیع شده انکار از خدمات حملات: الف پشتیبانی بردار دستگاه با هیبریدی بهینه‌سازی الگوریتم مبتنی بر رویکرد، *همزمانی کام- putation، Pract. Exper.* ، جلد ۳۴، شماره ۲۷، دسامبر ۲۰۲۲، شماره ماده e7334، doi: [‎۱۰.۱۰۰۲/cpe.۷۳۳۴‎](http://dx.doi.org/10.1002/cpe.7334)
4. س. نعیم، الف. ای. خضر، الف. م. ادریس، و م. من. ماری، ''بهبودبخشی'' کارایی طبقه‌بندی‌کننده یادگیری ماشین گاوسی-بیز ساده در ‎‏ ... تشخیص از حملات منع سرویس دابلیو‌اس در ابر محاسبات، *IEEE دسترسی* ، جلد ۱۱،

ص. ۱۲۴۵۹۷–۱۲۴۶۰۸، ۲۰۲۳، دی آی: [‎۱۰.۱۱۰۹/ACCESS.۲۰۲۳.۳۳۲۸۹۵۱‎](http://dx.doi.org/10.1109/ACCESS.2023.3328951)

1. س. وی. جی. رانی، من. ایوانو، پ. ناگارادجانه سی. کریستوفورو، وی. واسیلیو،

س. چاران، س. پراکاش، ن. پارخ، و الف. پیتسیلیدها تشخیص حملات DDoS در ارتباطات D2D با استفاده از یادگیری ماشین رویکرد، « *ارتباطات کامپیوتری»* ، جلد ۱۹۸، صفحات. ۳۲–۵۱، ژانویه ۲۰۲۳، doi: [‎۱۰.۱۰۱۶/j.comcom.۲۰۲۲.۱۱.۰۱۳‎](http://dx.doi.org/10.1016/j.comcom.2022.11.013)

1. ی. شانگ، پیشگیری و تشخیص از حملات منع سرویس دابلیو‌اس حمله در مجازی محیط محاسبات ابری با استفاده از الگوریتم ساده بیز ماشین یادگیری، '' *اندازه گیری، حسگرها* ، جلد ۳۱، فوریه ۲۰۲۴، ماده. نه. ۱۰۰۹۹۱، doi: [‎۱۰.۱۰۱۶/j.measen.۲۰۲۳.۱۰۰۹۹۱‎](http://dx.doi.org/10.1016/j.measen.2023.100991)
2. اچ. ستیا، الف. چابرا، س. ک. سینگ، س. کومار، س. شارما، وی. آریا،

ب. ب. گوپتا و جی. وو، «تضمین مسیر پیش رو: یادگیری ماشینی» رانده شده حملات انسداد سرویس (DDOS) حمله تشخیص در ونت ابر محیط‌ها، *امنیت سایبری. ضمیمه* ، جلد ۲، ژانویه ۲۰۲۴، ماده. نه. ۱۰۰۰۳۷، doi: [‎۱۰.۱۰۱۶/j.csa.۲۰۲۴.۱۰۰۰۳۷‎](http://dx.doi.org/10.1016/j.csa.2024.100037)

1. آی. الصالح، ای. السماوی، و ال. نصیرات، «یادگیری ماشینی نوین» رویکردی برای تشخیص ابری DDoS: CNN و داده‌های مبتنی بر بیزی «بهبودهای همجوشی»، « *حسگرها »* ، جلد ۲۴، شماره ۵، ص. ۱۴۱۸، فوریه ۲۰۲۴، doi: [‎۱۰.۳۳۹۰/s۲۴۰۵۱۴۱۸‎](http://dx.doi.org/10.3390/s24051418)
2. F. Talpur، IA Korejo، AA Chandio، A. Ghulam، و M. س. اچ. تالپور، تشخیص حملات DDoS مبتنی بر یادگیری ماشین با استفاده از الگوریتم‌های تکاملی بهینه‌سازی، « *حسگرها »* ، جلد ۲۴، شماره ۵، ص. ۱۶۷۲، مارس ۲۰۲۴، doi: [‎۱۰.۳۳۹۰/s۲۴۰۵۱۶۷۲‎](http://dx.doi.org/10.3390/s24051672)
3. س. داساری و آر. کلوری، «آن» مؤثر طبقه بندی از حملات انسداد سرویس (DDOS) حملات در الف توزیع شده شبکه توسط اتخاذ کردن سلسله مراتبی دستگاه یادگیری و هایپرپارامترها بهینه‌سازی تکنیک‌ها، *IEEE دسترسی* ، جلد ۱۲،

ص. ۱۰۸۳۴–۱۰۸۴۵، ۲۰۲۴، دی آی: [‎۱۰.۱۱۰۹/ACCESS.۲۰۲۴.۳۳۵۲۲۸۱‎](http://dx.doi.org/10.1109/ACCESS.2024.3352281)

1. اس. ولیانگیری و اچ. ام. پاندی، «بهینه‌سازی گله فیل فازی-تیلور» شبکه باور عمیق الهام گرفته از mization برای تشخیص حمله DDoS و مقایسه با الگوریتم‌های پیشرفته، « *محاسبات عمومی آینده». سیستم* ، جلد ۱۱۰، صفحات ۸۰-۹۰، سپتامبر ۲۰۲۰، doi: [10.1016/j.future.2020.03.049.](http://dx.doi.org/10.1016/j.future.2020.03.049)
2. ای. بهاردواج، وی. منگات، و آر. ویگ، «شبکه‌های عصبی عمیق تنظیم‌شده با ابرباند» شبکه‌ای با AutoEncoder پراکنده انباشته شده با وضعیت مناسب برای تشخیص حملات انسداد سرویس (DDOS) حملات در ابر،'' *IEEE دسترسی* ، جلد ۸، ص. ۱۸۱۹۱۶–۱۸۱۹۲۹، ۲۰۲۰، دی آی: [‎۱۰.۱۱۰۹/ACCESS.۲۰۲۰.۳۰۲۸۶۹۰‎](http://dx.doi.org/10.1109/ACCESS.2020.3028690)
3. ن. میشرا و آر کی سینگ، «تحلیل و کاهش آسیب‌پذیری‌های DDoS» مدل در محاسبات ابری، *مجله ریاضی گسسته، علوم، رمزنگاری* ، جلد ۲۳ شماره ۲، صفحات ۵۳۵–۵۴۵، فوریه ۲۰۲۰، doi: [10.1080/09720529.2020.1729503.](http://dx.doi.org/10.1080/09720529.2020.1729503)
4. س. ولیانگیری، پ. کارتیکیان، و وی. وینوت کومار، تشخیص از توزیع شده انکار از خدمات حمله در ابر محاسبات با استفاده از ‎‏ ... مبتنی بر بهینه‌سازی عمیق شبکه‌ها، *جی. آزمایش. تئوری آرتیف. هوشمند* ، جلد 33، شماره 3، صص ۴۰۵–۴۲۴، مه ۲۰۲۱، doi: [‎۱۰.۱۰۸۰/۰۹۵۲۸۱۳x.۲۰۲۰.۱۷۴۴۱۹۶‎](http://dx.doi.org/10.1080/0952813x.2020.1744196)
5. جی بی دنیس و ام اس پریا، «شبکه باور عمیق و بردار پشتیبانی» دستگاه همجوشی برای توزیع شده انکار از خدمات و اقتصادی انکار از تشخیص حمله به سرویس در ابر، *محاسبات همزمان، کارشناس عملی* ، جلد ۳۴، شماره ۱، ژانویه ۲۰۲۲، شماره ماده e۶۵۴۳، doi: [10.1002/cpe.6543.](http://dx.doi.org/10.1002/cpe.6543)
6. م. المیانی، ا. ابوغزله، ی. جراروه، و ا. رزاق، «تاب‌آور» برگشت انتشار عصبی شبکه امنیت مدل برای کانتینر شده محاسبات ابری، " *شبیه‌سازی مدل، عمل، نظریه* "، جلد ۱۱۸، ژوئیه ۲۰۲۲ هنر نه 102544، doi: [10.1016/j.simpat.2022.102544.](http://dx.doi.org/10.1016/j.simpat.2022.102544)
7. دی. آکگون، س. هیزال، و یو. چاووش اوغلو، «الف» جدید حملات انسداد سرویس (DDOS) حملات نفوذ تشخیص مدل مبتنی بر روی عمیق یادگیری برای امنیت سایبری- rity،'' *Comput. Secur.* ، جلد ۱۱۸، ژوئیه ۲۰۲۲، ماده. نه. ۱۰۲۷۴۸، doi: [‎۱۰.۱۰۱۶/j.cose.2022.102748‎‏. (این عبارت به نظر مجموعه‌ای تصادفی از حروف و اعداد است و نیازی به ترجمه ندارد.)](http://dx.doi.org/10.1016/j.cose.2022.102748)
8. H. Aydın، Z. Orman و MA Aydın، ''یک حافظه کوتاه مدت طولانی مبتنی بر (LSTM) توزیع شده انکار از خدمات (عدم سرویس توزیع‌شده) تشخیص و دفاع طراحی سیستم در محیط شبکه ابری عمومی، " *امنیت محاسباتی "* ، جلد 118، ژوئیه 2022، هنر. نه 102725، doi: [10.1016/j.cose.2022.102725.](http://dx.doi.org/10.1016/j.cose.2022.102725)
9. ای.اس. آلیار، ام. آگورامورثی، و وای. جاستینهاس، «یک دستگاه خودکار تشخیص حمله DDoS در ابر با استفاده از الگوریتم‌های ترکیبی وزن‌دار بهینه‌شده ویژگی‌ها و معماری ترکیبی DBN-GRU، « *سایبرن. سیستم»* ، صفحات ... ۱–۴۲، ژانویه 2023، doi: [10.1080/01969722.2022.2157603.](http://dx.doi.org/10.1080/01969722.2022.2157603)
10. آ. آگراوال، آر. سینگ، ام. خاری، اس. ویمال، و اس. لیم، «خودرمزگذار» برای طراحی مدل کاهش حملات DDOS از طریق M-DBNN، " *Wire- " کمتر، ارتباطات. محاسبات سیار.* ، جلد. 2022، صفحات. ۱ تا ۱۴ آوریل ۲۰۲۲، doi: [‎۱۰.۱۱۵۵/۲۰۲۲/۹۸۵۵۰۲۲‎](http://dx.doi.org/10.1155/2022/9855022)
11. ام. وارگیسه و ام. ویکتور خوزه، «یک تابع بایاس شعاعی بهینه شده» شبکه عصبی برای تشخیص نفوذ در حملات انکار سرویس توزیع‌شده حمله در ‎‏ ... ابر،'' *همزمانی محاسبه.، عمل. تجربه* . جلد ۳۴، نه. ۲۷، دسامبر ۲۰۲۲، شماره ماده e7321، doi: [10.1002/cpe.7321.](http://dx.doi.org/10.1002/cpe.7321)
12. GSRE Selvan، R. Ganeshan، IDJ Jingle، و JP Ananth، ''FACVO-DNFN: عمیق مبتنی بر یادگیری ویژگی همجوشی و تشخیص حمله انکار سرویس توزیع‌شده در محاسبات ابری، *نظام مبتنی بر دانش* ، جلد ۲۶۱، فوریه ۲۰۲۳، ماده. نه. ۱۱۰۱۳۲، doi: [‎۱۰.۱۰۱۶/j.knosys.2022.110132‎‏. (این عبارت به نظر مجموعه‌ای تصادفی از حروف و اعداد است و نیازی به ترجمه ندارد.)](http://dx.doi.org/10.1016/j.knosys.2022.110132)
13. س. بالاسوبرامانیام، سی. ویجش جو، تی. الف. سیواکومار، الف. پراسانت،

ک. س. Kumar، V. Kavitha، و RK Dhanaraj، "بهینه سازی فعال شد تشخیص حمله DDoS مبتنی بر یادگیری عمیق در محاسبات ابری، *مجله بین‌المللی سیستم اطلاعاتی* ، جلد ۲۰۲۳، ص. ۱–۱۶، فوریه ۲۰۲۳، doi: [10.1155/2023/2039217 .](http://dx.doi.org/10.1155/2023/2039217)

1. م. جی. پاشا، ک. پ. رائو، الف. مالا ردی، و وی. باند، نیروی دفاع مردمی (LRDADF): یک هوش مصنوعی فعال شده چارچوب برای تشخیص نرخ پایین حملات انسداد سرویس (DDOS) حملات در ابر محاسبه- ینگ محیط‌ها، *اندازه گیری.، حسگرها* ، جلد ۲۸، اوت ۲۰۲۳، هنر. نه. ۱۰۰۸۲۸، دی آی: [‎۱۰.۱۰۱۶/j.measen.۲۰۲۳.۱۰۰۸۲۸‎](http://dx.doi.org/10.1016/j.measen.2023.100828)
2. ز. لیو، سی. گو، دی. لیو، و ایکس. یین، «آن» ناهمزمان فدرال یادگیری مدل داوری برای تشخیص حمله DDoS با نرخ پایین، IEEE *Access* جلد ۱۱، صفحات ۱۸۴۴۸–۱۸۴۶۰، ۲۰۲۳، doi: [10.1109/ACCESS.2023.3247512.](http://dx.doi.org/10.1109/ACCESS.2023.3247512)
3. س. الف. وارما و ک. جی. ردی، «آن» هوش مصنوعی مبتنی بر شناسه‌ها چارچوب برای تشخیص حملات DDoS در محیط ابری، *اطلاعات امنیتی. جی.، چشم‌انداز جهانی* ،

صفحات 1-13، نوامبر 2023، doi: [10.1080/19393555.2023.2279535.](http://dx.doi.org/10.1080/19393555.2023.2279535)

1. س. دلال، پ. مانوهاران، یو. ک. لیلور، ب. ست، دی. م. آلسکایت،

س. سیمیا، م. حمدی، و ک. راحمی فر، ''فوق العاده تقویت شده نو- شبکه ral برای پیش‌بینی دقیق‌تر حمله سایبری چند مرحله‌ای در «محیط محاسبات ابری»، *مجله محاسبات ابری* ، جلد ۱۲، شماره ۱، ص. ۱۴، ژانویه 2023، doi: [10.1186/s13677-022-00356-9.](http://dx.doi.org/10.1186/s13677-022-00356-9)

1. اُ. پاندیتوری، سی. ونکاتایا س. تیواری، و ن. رامانجانیولو حملات منع سرویس توزیع‌شده (DDoS) پیش‌بینی حمله با استفاده از الگوریتم بهینه‌سازی گورکن عسلی مبتنی بر ویژگی انتخاب و دو-LSTM در ابر محیط زیست،'' *متخصص سیستم کاربردی* ، جلد 241، مه 2024، هنر. نه 122544، doi: [10.1016/j.eswa.2023.122544.](http://dx.doi.org/10.1016/j.eswa.2023.122544)
2. جی. آرانگو-لوپز جی. ایسازا، ف. رامیرز، ن. دوک، و جی. مونتس، «ابر-» معماری مبتنی بر یادگیری عمیق برای پیش‌بینی حمله سایبری DDoS *سیستم متخصص* ، ژانویه ۲۰۲۴، شماره ماده e13552، doi: [10.1111/exsy.13552.](http://dx.doi.org/10.1111/exsy.13552)
3. م. اوحسینی، ک. افدل، ای. آغرابی، م. آکوهر، و ا. ابردا، «دیفند عمیق: چارچوبی جامع برای تشخیص حملات DDoS» بخش و پیشگیری در ابر محاسبات، *جی. پادشاه سعود دانشگاه کام- قرار دهید. Inf. Sci.* ، جلد ۳۶، شماره ۲، فوریه ۲۰۲۴، ماده. نه. ۱۰۱۹۳۸، doi: [‎۱۰.۱۰۱۶/j.jksuci.۲۰۲۴.۱۰۱۹۳۸‎](http://dx.doi.org/10.1016/j.jksuci.2024.101938)
4. الف. آر. وانی، س. پ. رانا، یو. ساکسنا، و ن. پاندی، تحلیل و تشخیص- بررسی حملات DDoS به محیط محاسبات ابری با استفاده از ماشین «تکنیک‌های یادگیری»، در *مجموعه مقالات کنفرانس بین‌المللی هنر و اطلاعات آمیتی (AICAI)* ، فوریه 2019، صفحات 870–875، doi: [10.1109/AICAI.2019.8701238.](http://dx.doi.org/10.1109/AICAI.2019.8701238)
5. E. Hodo، X. Bellekens، A. Hamilton، C. Tachtatzis، و R. Atkinson، «کم‌عمق» و عمیق شبکه‌ها نفوذ تشخیص سیستم: الف طبقه بندی و «نظرسنجی»، ۲۰۱۷، *arXiv:1701.02145* .
6. J. Fontaine، C. Kappler، A. Shahid، و E. De Poorter، "بر اساس گزارش نفوذ تشخیص برای وب ابری کاربردها با استفاده از دستگاه یادگیری،'' در *پیشرفت‌ها در محاسبات P2P، موازی، شبکه‌ای، ابری و اینترنتی: مجموعه مقالات چهاردهمین کنفرانس بین‌المللی P2P، موازی، شبکه، ابر و اینترنت محاسبات (3PGCIC-2019) ۱۴. (یا: ۱۴* ) اسپرینگر، ۲۰۲۰،

ص. ۱۹۷–۲۱۰.

1. AN Jaber و SU Rehman، "تشخیص نفوذ مبتنی بر FCM-SVM". سیستمی برای محیط محاسبات ابری، « *محاسبات خوشه‌ای »* ، جلد ۲۳، شماره ۴، صفحات ۳۲۲۱–۳۲۳۱، دسامبر ۲۰۲۰، doi: [10.1007/s10586-020-03082-6.](http://dx.doi.org/10.1007/s10586-020-03082-6)
2. م. پراساد، س. تریپاتی، و ک. دهال، «آن» کارآمد ویژگی انتخاب- بخش مبتنی بر بیزی و خشن مجموعه رویکرد برای نفوذ تشخیص- «»، « *محاسبات نرم کاربردی»* ، جلد ۸۷، فوریه ۲۰۲۰، ماده. نه. ۱۰۵۹۸۰، doi: [‎۱۰.۱۰۱۶/j.asoc.۲۰۱۹.۱۰۵۹۸۰‎](http://dx.doi.org/10.1016/j.asoc.2019.105980)
3. ای. آلدالال و اف. آلیسا، «سیستم تشخیص نفوذ مؤثر برای ایمن‌سازی» داده‌ها در ابر با استفاده از دستگاه یادگیری،'' *تقارن* ، جلد ۱۳، نه. ۱۲، ص. ۲۳۰۶، دسامبر ۲۰۲۱، doi: [10.3390/sym13122306.](http://dx.doi.org/10.3390/sym13122306)
4. دبلیو. وانگ، ایکس. دو، دی. شان، آر. شین، و ن. وانگ، «ابر» نفوذ تشخیص- بخش روش مبتنی بر روی انباشته شده انقباضی رمزگذار خودکار و پشتیبانی بردار ماشین، « *IEEE Trans. Cloud Comput.* »، جلد 10، شماره 3، صفحات. ۱۶۳۴–۱۶۴۶، ژوئیه 2022، doi: [10.1109/TCC.2020.3001017.](http://dx.doi.org/10.1109/TCC.2020.3001017)
5. ال. یانگ و ای. شامی، «IDS-ML: یک کد متن‌باز برای نفوذ» توسعه سیستم تشخیص با استفاده از یادگیری ماشین، « *اثرات نرم‌افزاری »* ، جلد 14، دسامبر 2022، هنر. نه 100446، doi: [10.1016/j.simpa.2022.100446.](http://dx.doi.org/10.1016/j.simpa.2022.100446)
6. K. Samunnisa، GSV Kumar، و K. Madavi، "تشخیص نفوذ سیستم در محاسبات ابری توزیع‌شده: خوشه‌بندی و طبقه‌بندی ترکیبی روش‌های سنجش، « *اندازه‌گیری‌ها، حسگرها* »، جلد ۲۵، فوریه ۲۰۲۳، ماده. نه. ۱۰۰۶۱۲، doi: [‎۱۰.۱۰۱۶/j.measen.۲۰۲۲.۱۰۰۶۱۲‎](http://dx.doi.org/10.1016/j.measen.2022.100612)
7. م. باکرو، آر. آر. کومار، الف. آلابراه، ز. اشرف، م. ن. احمد،

م. شمیم و ا. عبدالسلام، «طراحی بهبود یافته برای ابر» سیستم تشخیص نفوذ با استفاده از رویکرد انتخاب ویژگی ترکیبی «طبقه‌بندی‌کننده یادگیری ماشین»، *IEEE Access* ، جلد ۱۱، صفحات. ۶۴۲۲۸–۶۴۲۴۷، ۲۰۲۳، doi: [‎۱۰.۱۱۰۹/دسترسی.۲۰۲۳.۳۲۸۹۴۰۵‎](http://dx.doi.org/10.1109/ACCESS.2023.3289405)

1. الف.-ر. الغویری، ی. شراب، دی. الفریحات، م. آل الایمات،

الف. السرحان، و الف. الگارنی، «تشخیص نفوذ در محاسبات ابری» بر اساس ناهنجاری‌های سری زمانی با استفاده از یادگیری ماشین، " *جی. کلود" محاسبات* ، جلد ۱۲، شماره ۱، صفحه ۱۲۷، اوت ۲۰۲۳، doi: [10.1186/ s13677-023-](http://dx.doi.org/10.1186/s13677-023-00491-x) [۰۰۴۹۱-ایکس.](http://dx.doi.org/10.1186/s13677-023-00491-x)

1. H. Attou، A. Guezzaz، S. Benkirane، M. Azrour، and Y. Farhaoui، ''Cloud- رویکرد تشخیص نفوذ مبتنی بر استفاده از تکنیک‌های یادگیری ماشین، *تحلیل کلان‌داده‌کاوی* ، جلد ۶، شماره ۳، صفحات ۳۱۱-۳۲۰، سپتامبر ۲۰۲۳، doi: [‎۱۰.۲۶۵۹۹/BDMA.۲۰۲۲.۹۰۲۰۰۳۸‎](http://dx.doi.org/10.26599/BDMA.2022.9020038)
2. ل. ک. واشیشتا، الف. پ. سینگ، و ک. چاترجی، اچ‌آی‌دی‌ام: الف هیبریدی نفوذ سیون تشخیص مدل برای ابر مبتنی بر سیستم‌ها، *بی‌سیم پرس. ارتباطات* . جلد ۱۲۸، شماره ۴، صفحات ۲۶۳۷–۲۶۶۶، فوریه ۲۰۲۳، doi: [10.1007/ s11277-022-](http://dx.doi.org/10.1007/s11277-022-10063-y) [۱۰۰۶۳-ی.](http://dx.doi.org/10.1007/s11277-022-10063-y)
3. م. باکرو، آر. آر. کومار، م. حسین، ز. اشرف، الف. علی، س. من. یعقوب،

م. ن. احمد، و ن. پروین، ساختمان الف شناسه‌های ابری توسط هیبریدی الهام گرفته از طبیعت ویژگی انتخاب الگوریتم‌ها همراه با تصادفی مدل جنگل، « *IEEE Access* »، جلد ۱۲، صفحات. ۸۸۴۶–۸۸۷۴، ۲۰۲۴، doi: [‎۱۰.۱۱۰۹/دسترسی.۲۰۲۴.۳۳۵۳۰۵۵‎](http://dx.doi.org/10.1109/ACCESS.2024.3353055)

1. الف. کومار، آر. س. اومورزوکوویچ، ن. دی. دونگ، پ. کنعانی،

A. Kuppusamy، M. Praneesh، و MN Hieu، "یک نفوذ شناسایی و پیشگیری برای رایانش ابری: از دیدگاه یادگیری عمیق، « *اپتیک* ، جلد ۲۷۰، نوامبر ۲۰۲۲، ماده ...». نه. ۱۷۰۰۴۴، doi: [‎۱۰.۱۰۱۶/j.ijleo.۲۰۲۲.۱۷۰۰۴۴‎](http://dx.doi.org/10.1016/j.ijleo.2022.170044)

1. م. مایوراناتان، س. ک. سراوانان، ب. موتوسنتیل، و الف. سامیدورای، «آن» کارآمد بهینه امنیت سیستم برای نفوذ تشخیص در ابر محاسبات محیط زیست با استفاده از هیبریدی عمیق یادگیری فناوری- nique،'' *Adv. مهندس نرم افزار* ، جلد 173، نوامبر 2022، هنر. نه. ۱۰۳۲۳۶، doi: [‎۱۰.۱۰۱۶/j.advengsoft.۲۰۲۲.۱۰۳۲۳۶‎](http://dx.doi.org/10.1016/j.advengsoft.2022.103236)
2. بی. کی. پاندی، اس. احمد، سی. رودریگز، و دی. اسنارو، «ExpSSOA- حداکثر خروجی عمیق: بهینه‌سازی نمایی شپرد بر زده شده عمیق مبتنی بر حداکثر شبکه برای نفوذ تشخیص با استفاده از بزرگ داده‌ها در ابر محاسبات چارچوب، '' *Comput. Secur.* ، جلد ۱۲۴، ژانویه ۲۰۲۳، ماده. نه. ۱۰۲۹۷۵، doi: [‎۱۰.۱۰۱۶/j.cose.2022.102975‎‏. (این عبارت به نظر مجموعه‌ای تصادفی از حروف و اعداد است و نیازی به ترجمه ندارد.)](http://dx.doi.org/10.1016/j.cose.2022.102975)
3. اچ. آتو، م. محی الدین، الف. گوئزاز، س. بنکیران، م. آزرور،

الف. Alabdultif، و N. Almusallam، ''به سوی یک نفوذ هوشمند تشخیص سیستم به تشخیص بدخواه فعالیت‌ها در ابر محاسبات، *کاربرد* *علوم* ، جلد ۱۳، شماره ۱۷، صفحه ۹۵۸۸، آگوست ۲۰۲۳، doi: [10.3390/app13179588.](http://dx.doi.org/10.3390/app13179588)

1. س. الزغیبی و س. الخدیری، «سیستم‌های تشخیص نفوذ ابری» مبتنی بر DNN با استفاده از پس انتشار و PSO روی CSE-CIC- مجموعه داده‌های IDS2018، « *علوم کاربردی»* ، جلد ۱۳، شماره ۴، ص. ۲۲۷۶، فوریه ۲۰۲۳، doi: [‎۱۰.۳۳۹۰/app۱۳۰۴۲۲۷۶‎](http://dx.doi.org/10.3390/app13042276)
2. سی. کاویتا، م. سراوانان، تی. آر. گادکالو، ک. نیمالا، ب. پ. کاوین، و

دبلیو سی لای، «انتخاب ویژگی گروهی مبتنی بر فیلتر و یادگیری عمیق» مدلی برای تشخیص نفوذ در محاسبات ابری، « *الکترونیک* ، جلد ۱۲»، شماره ۳، صفحه ۵۵۶، ژانویه ۲۰۲۳، doi: [10.3390/electronics12030556.](http://dx.doi.org/10.3390/electronics12030556)

1. کی. جی. ماهسواری، سی. سیوا، و جی. نالینیپریا، «خوشه‌بندی بهینه مبتنی بر ویژگی انتخاب برای نفوذ تشخیص سیستم در وب و ابر محاسبه- ینگ محیط زیست با استفاده از هیبریدی معلم یادگیری بهینه‌سازی قادر می‌سازد عمیق «شبکه عصبی بازگشتی»، *مجله ارتباطات محاسباتی* ، جلد 202، صفحات 100-110. ۱۴۵–۱۵۳، مارس 2023، doi: [10.1016/j.comcom.2023.02.003.](http://dx.doi.org/10.1016/j.comcom.2023.02.003)
2. م. الف. العزیز، م. الف. الف. القانس، الف. داهو، آر. الف. ابراهیم، و الف. الف. الف. اللطیف، ''نفوذ'' تشخیص رویکرد برای ابر و محیط‌های اینترنت اشیا با استفاده از یادگیری عمیق و جستجوی کاپوچین الگوریتم، '' *Adv. مهندس نرم افزار* ، جلد 176، فوریه 2023، هنر. نه. ۱۰۳۴۰۲، doi: [‎۱۰.۱۰۱۶/j.advengsoft.۲۰۲۲.۱۰۳۴۰۲‎.](http://dx.doi.org/10.1016/j.advengsoft.2022.103402)
3. DB Salvakkam، V. Saravanan، PK Jain، و R. Pamula، ''Enhanced امنیت کوانتومی گروه نفوذ تشخیص تکنیک‌ها برای ابر مبتنی بر روی عمیق یادگیری،'' *شناختی محاسبه.* ، جلد ۱۵، نه. ۵، ص. ۱۵۹۳–۱۶۱۲، سپتامبر ۲۰۲۳، doi: [10.1007/s12559-023-10139-2.](http://dx.doi.org/10.1007/s12559-023-10139-2)
4. جی. ژانگ، جی. دی. پیتر، ای. شانکار، و دبلیو. ویریاسیتاوا، «ابر عمومی» شبکه‌های عصبی عمیق جهت‌دار برای تشخیص نفوذ مؤثر در آموزش آنلاین موسیقی، '' *مهندسی کامپیوتر. برق.* جلد. 115، آوریل 2024، شماره ماده ۱۰۹۰۹۵، doi: [10.1016/j.compeleceng.2024.109095.](http://dx.doi.org/10.1016/j.compeleceng.2024.109095)
5. الف. پارامسواری، آر. گانشان، وی. راگاوی، و م. شریشا، هیبریدی موش صحرایی شکارچی ازدحام، بهینه‌سازی شکار، یادگیری عمیق آموزش‌دیده برای نفوذ به شبکه سیون تشخیص با استفاده از سی‌ان‌ان ویژگی‌ها،'' *محاسبه. امن* . جلد ۱۳٩، آوریل ۲۰۲۴، هنر نه 103656، doi: [10.1016/j.cose.2023.103656.](http://dx.doi.org/10.1016/j.cose.2023.103656)
6. N. Joraviya، BN Gohil، و UP Rao، "DL-HIDS: Deep Learning- سیستم تشخیص نفوذ مبتنی بر میزبان با استفاده از فراخوانی‌های سیستمی به تصویر برای کانتینر شده ابر محیط زیست،'' *جی. ابررایانه* . ص. ۱–۲۹، فوریه ۲۰۲۴، دی آی: [‎۱۰.۱۰۰۷/s۱۱۲۲۷-۰۲۴-۰۵۸۹۵-۳‎](http://dx.doi.org/10.1007/s11227-024-05895-3)
7. تی. علی و پی. کاستاکوس، «HuntGPT: یکپارچه‌سازی مبتنی بر یادگیری ماشین» تشخیص ناهنجاری و هوش مصنوعی قابل توضیح با مدل‌های زبانی بزرگ (LLMs)،'' 2023، *arXiv:2309.16021* .
8. سی. لیو، اس. هی، کیو. ژو، اس. لی، و دبلیو. منگ، «مدل زبان بزرگ» تقطیر دانش هدایت‌شده برای تشخیص ناهنجاری سری‌های زمانی، «۲۰۲۴» *arXiv:2401.15123* . (آرشیوی از نسخه ۲۴۰۱.۱۵۱۲۳)

امیرا ماهات عبدالله دریافت شده ‎‏ ...

کارشناسی مدرک در کامپیوتر علم از طیبه یونی- دانشگاه، عربستان سعودی، در سال ۲۰۱۸. او در حال حاضر دنبال کردن مدرک کارشناسی ارشد در رشته امنیت اطلاعات ریتی با یونایتد عرب امارات دانشگاه، یونایتد امارات متحده عربی. علایق پژوهشی او شامل موارد زیر است: امنیت ابری، سیستم‌های تشخیص نفوذ و مصنوعی هوش.

عایشه سیف راشد عبید الکعبی است فعلاً در حال تعقیب ‎‏ ... کارشناسی مدرک تحصیلی در امنیت اطلاعات با یونایتد دانشگاه امارات متحده عربی، یونایتد امارات متحده عربی. علایق تحقیقاتی او شامل امنیت ابری، تشخیص نفوذ است. سیستم‌های اطلاعاتی و هوش مصنوعی.

قایا بارک ناصر دومان آلامری است فعلاً در حال تعقیب ‎‏ ... مدرک کارشناسی در رشته علوم کامپیوتر از دانشگاه امارات متحده عربی، یونایتد عرب امارات. او تحقیق علایق شامل شدن ابر امنیت، نفوذ سیستم‌های تشخیص و هوش مصنوعی

صیدا حفصه رفیق دریافت شده ‎‏ ... کارشناسی مدرک در سلولی و مولکول- زیست‌شناسی جانوری از دانشگاه امارات متحده عربی (UAEU)، امارات متحده عربی امارات، در سال ۲۰۱۹، و اولین مدرک کارشناسی ارشد در علوم جنایی از دانشگاه استراتکلاید، انگلستان، در سال ۲۰۲۰. او در حال حاضر مشغول تحصیل در مقطع دکترا است. دومین مدرک کارشناسی ارشد خود را در رشته امنیت اطلاعات از دانشگاه امارات متحده عربی دریافت کرد. تحقیقات او علایق شامل شدن ابر امنیت، ‎‏ ... اینترنت اشیا امنیت، مصنوعی هوش، دیجیتال پزشکی قانونی، و علوم جنایی.

نورا شفا موسی مدرک لیسانس خود را دریافت کرد مدرک مهندسی کامپیوتر از دانشگاه قطر دانشگاه کوئینزلند (QU)، قطر، و مدرک کارشناسی ارشد در اطلاعات امنیت از ‎‏ ... کالج از اطلاعات- بخش فناوری، یونایتد عرب امارات دانشگاه (امارات متحده عربی)، امارات متحده عربی. او در حال حاضر یک سرپرست ارشد آزمایشگاه از دانشکده از مهندسی، آل عین دانشگاه (AAU)، یونایتد امارات متحده عربی. نشان دادن یک فداکاری عمیق کاتیون به در حال پیشرفت سایبری امنیت اقدامات، او

تحقیق علایق شامل شدن در حال توسعه نوآورانه راه حل ها به افزایش دیجیتال امنیت، تحقیق و تفحص سایبری تهدیدها، کاوش ابر محاسبات فناوری، و انجام تحقیقات پزشکی قانونی دیجیتال. او جوایزی دریافت کرد و افتخارات

تانگاول موروگان (عضو ارشد، IEEE) مدرک کارشناسی ارشد (Hons.) را در رشته‌های مرتبط دریافت کرد. کامپیوتر علم و مهندسی از ‎‏ ... م. الف.

کالج مهندسی ام.، تریچی، هند، تحت نظر آنا دانشگاه، چنای، هند، ‎‏ ... من مدرک (عالیجناب) در کامپیوتر علم و مهندسی از کالج مهندسی و فناوری جی‌جی، تریچی، تحت نظر دانشگاه آنا، و دارای مدرک دکترا. مدرک از مدرس موسسه از فناوری (دانشگاه ام آی تی) پردیس، آنا دانشگاه. او است فعلاً یک

دستیار استاد با ‎‏ ... دپارتمان از اطلاعات سیستم‌ها و امنیت- ریت، کالج از اطلاعات فناوری، یونایتد عرب امارات دانشگاه. او همچنین نگه می‌دارد بیشتر از ۱۱ سال‌ها از تدریس و تحقیق تجربه از مؤسسات دانشگاهی مختلف. او بیش از ده مقاله در ... منتشر کرده است. بین‌المللی مجلات، بیشتر از ۱۵ کتاب فصل‌ها در بین‌المللی منتشر کردن- اره، بیشتر از ۲۵ در ‎‏ ... دادرسی از بین‌المللی کنفرانس‌ها، و سه در ‎‏ ... دادرسی از ملی کنفرانس‌ها/سمینارها. او دانشگاهی و تحقیق علایق شامل شدن اطلاعات امنیت، عملکرد بالا محاسبات، اخلاقی هک کردن، سایبری پزشکی قانونی، بلاکچین، امنیت سایبری هوش، و آموزش- وابسته فناوری.