Journal of New Achievements in Electrical, Computer and Technology
Vol. 2, No. 3, Jun-Sep 2022,( 49- 64)
WWW.JNAECT.IR

مجله دستاوردهای نوین در برق،کامپیوتر و فناوری
دوره۲، شماره ۳، تابستان ۱۴۰۱ (۶۴-۴۹)

# مروری بر الگوریتم های یادگیری عمیق به کار برده شده در سیستم های تشخیص نفوذ

**مهشید صالحی**[1*]

دپارتمان مهندسی کامپیوتر،واحد مشهد، دانشگاه ازاد اسلامی ، مشهد،ایران salehy.md@gmail.com

**چکیده**

پیشرفت های سریع در زمینه اینترنت و ارتباطات باعث افزایش زیادی در اندازه شبکه و داده های مربوط به ان شده است. در نتیجه، بسیاری از حملات جدید در حال ایجاد هستند و امنیت شبکه را برای شناسایی دقیق نفوذها با چالش هایی مواجه کرده اند. علاوه بر این، حضور هکر ها با هدف انجام حملات مختلف در داخل شبکه را نمی توان نادیده گرفت. سیستم های تشخیص نفوذ یک ابزار حفاظتی مهم برای تشخیص نفوذ در شبکه است. سیستم های تشخیص نفوذ طبقه بندی کننده ای است که رکورد های ورودی را دریافت و کلاس انواع حملات را پیش بینی می کند. در حملات شبکه الگوریتم‌های مختلف یادگیری عمیق وجود داشته است که برای اجرای سیستم های تشخیص نفوذ پیشنهاد شده است. در دهه‌های گذشته، محققان از یادگیری عمیق مختلفی با رویکردهایی برای طبقه‌بندی و تشخیص ترافیک غیرعادی از ترافیک نرمال در شبکه بدون قبلی دانش قبلی در مورد الگوی حملات استفاده کردند. در این مقاله مروری بر سیستم های تشخیص نفوذ از دیدگاه یادگیری عمیق است. یک بخش جداگانه را به ارائه مجموعه داده های استفاده شده در زمینه سیستم های تشخیص نفوذ به طور خاص، دو مجموعه داده اصلی، KDDCup99 وNSL-KDD اختصاص می دهیم. همچنین معیار های ارزیابی و ابزار های پیاده سازی در سیستم های تشخیص نفوذ مورد بررسی قرار می گیرند.

**واژه‌های کلیدی:** سیستم های تشخیص نفوذ، یادگیری عمیق ، امنیت شبکه.

.

**۱.مقدمه**

با ادغام عمیق روزافزون اینترنت و جامعه، اینترنت در حال تغییر روشی در زندگی، تحصیل و کار افراد به وجود اورده است اما ما با تهدیدات امنیتی جدی و جدی تری رو به رو میشویم. نحوه شناسایی حملات در شبکه های مختلف، به ویژه شناسایی حملات غیرقابل پیش بینی یک مسئله فنی کلیدی اجتناب ناپذیر است(Yin et al., 2017). ابزار های مختلفی از جمله فایروال ها و سیستم های تشخیص نفوذ برای شناسایی حملات وجود دارند. فایروال می تواند گزینه خوبی برای جلوگیری از حملاتی از راه دور باشد اما برای حملات از داخل شبکه به خوبی کار نمی کند. پس سیستم های تشخیص نفوذ برای کاهش این حملات باید در زیرساخت ها گنجانده شوند(Modi et al., 2013). سیستم تشخیص نفوذ (IDS) یکی از زمینه های مهم برای امنیت سایبری است. سیستم های تشخیص نفوذ ترافیک شبکه را تجزیه و تحلیل میکند و متمرکز است تا علائم مربوط به فعالیت های مخرب را شناسایی کند(Drewek-Ossowicka et al., 2021) . برای دسته بندی انواع سیستم های تشخیص نفوذ میتوان دو نوع دسته بندی کلی مبتنی بر منبع داده و مبتنی بر تشخیص استفاده کرد.

۱/۱ . سیستم های تشخیص نفوذ مبتنی بر منبع داده

در دسته بندی مبتنی بر منبع داده سیستم های تشخیص نفوذ تبدیل به دو دسته میشوند.

۱.۱.۱.سیستم های تشخیص نفوذ مبتنی بر میزبان (HIDS): HIDS یک نرم افزار که بر روی هاست رایانه در شبکه برای نظارت ، تجزیه و تحلیل و جمع آوری فعالیت های ترافیکی در رابط های شبکه است که از میزبان برنامه سیستم نشأت گرفته اند. نمایش این سیستم تشخیص نفوذ محدود است و این سیستم فقط می تواند رفتارهای مخرب را برای یک میزبان مشخص کند.

۱.۱.۲ سیستم های تشخیص نفوذ مبتنی بر شبکه (NIDS): NIDS تشخیص ناهنجاری و تشخیص امضا را انجام می دهد. سیستم تشخیص نفوذ مبتنی بر شبکه با نظارت بر ترافیک هنگام عبور شبکه از زیرساخت شبکه کار می کند. NIDS و HIDS هر دو قابلیت شناسایی و نظارت بر فعالیتهای مخرب را دارند.

۱.۲ سیستم های تشخیص نفوذ مبتنی بر تشخیص

در سیستم های تشخیص نفوذ برای شناسایی حملات از دو روش اصلی استفاده میشود. سیستم تشخیص نفوذ بر اساس روش تشخیص به دو دسته کلی تقسیم می شوند: تشخیص نفوذ مبتنی بر امضا و تشخیص نفوذ مبتنی بر ناهنجاری. یک سیستم تشخیص نفوذ مبتنی بر امضا الگوهای ترافیک شبکه را با الگوهای حمله که قبلاً در پایگاه داده خود ذخیره کرده است مطابقت می دهد. در صورت یافتن شباهت کامل ، هشدار میدهد. سیستم های تشخیص نفوذ مبتنی بر امضا دارای دقت بالا و میزان هشدار کاذب کم است ، با این وجود در تشخیص حملات جدید توانایی لازم را ندارد. سیستم های تشخیص نفوذ مبتنی بر ناهنجاری به دلیل توانایی در شناسایی حملات جدید ، بر سیستم های تشخیص نفوذ مبتنی بر امضا ترجیح داده می شود(Verma & Ranga, 2020).

۱.۲.۱. روش مبتنی بر ناهنجاری :

از نکات مثبت استفاده از این روش (الف) مفید برای حمله ناشناخته (ب)وابستگی کم در سیستم عامل های دیگر و سیستم های نرم افزاری دیگر را میتوان نام برد. از معایب ان میتوان به (الف) دقت نسبت به کار مکرر کم است . (ب)توانایی سرویس هنگام بازسازی پروفایل رفتاری متوقف میشود. (ج) در تهیه به موقع هشدار ضعیف است ، اشاره کرد.

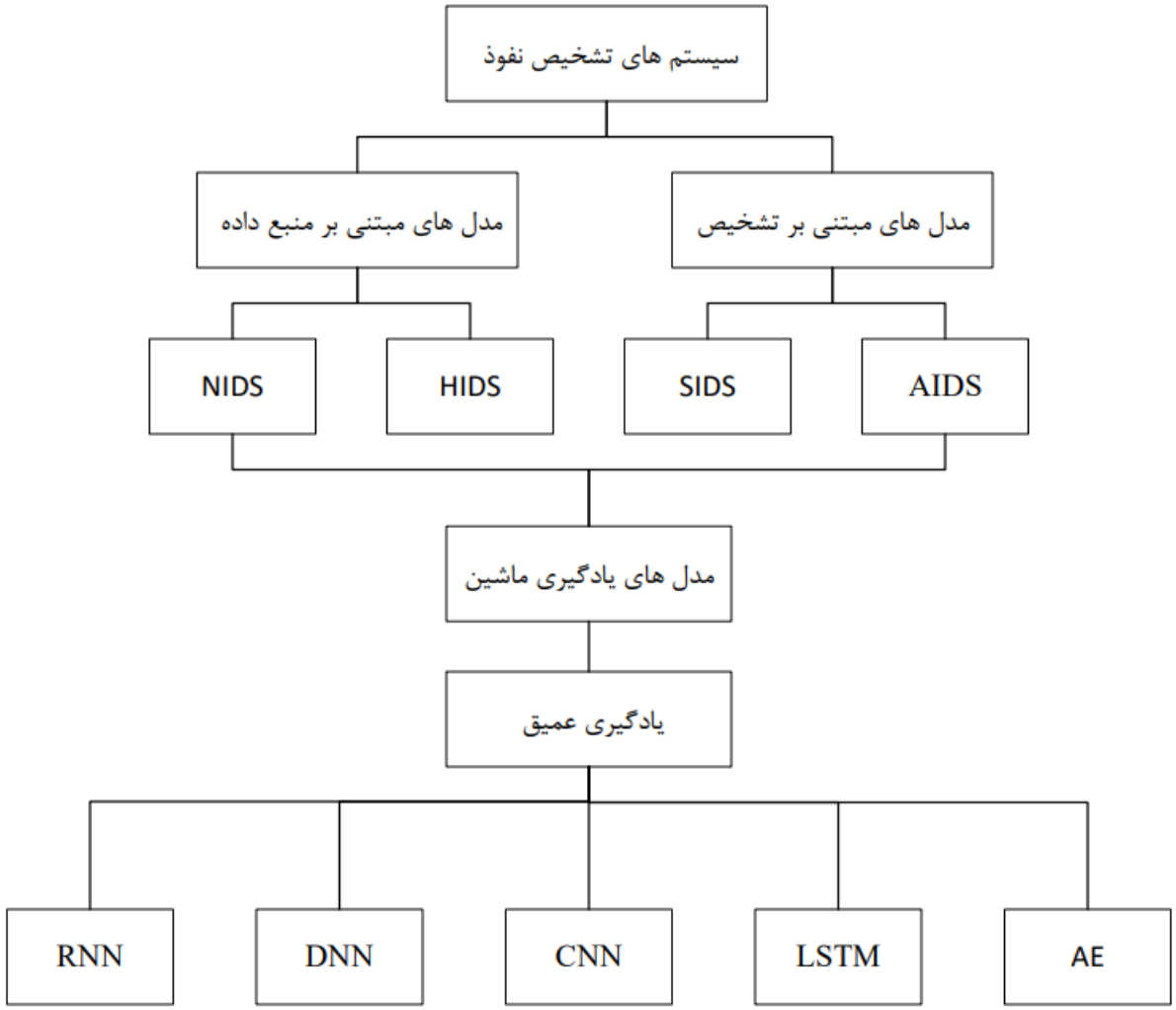
۱.۲.۲. روش مبتنی بر امضا :

از نکات مثبت استفاده از این روش شامل (الف) این روش های ساده ، دقیق و موثر است.(ب) جزئیات تجزیه و تحلیل متن را دارد (ج) تشخیص سریع و پاسخهای متداول را انجام میدهد و از معایب استفاده از این روش (الف)توانایی تشخیص حملات ناشناخته را ندارد. (ب) درک محدودی از پروتکل ها دارد . (ج) به روز رسانی در ان سخت و مکرر است. (د) برای حفظ دانش به زمان بیشتری نیاز دارد(Khan et al., 2020).

یادگیری ماشین تکنیکی است که به کامپیوتر اموزش میدهد. این امر مدل سازی روابط داده ها با شرایط موجود را به رسمیت می شناسد.در نتیجه یادگیری می تواند از طبقه بندی استفاده کند.نام یادگیری ماشین برای اولین بار در سال ۱۹۵۹ مطرح شد. پس از دهه ها مشخص شد که ، پیشرفت قابلیت محاسبات کامپیوترهای دیجیتال به طور قابل ملاحظه ای برای پیشرفت در آموزش مهارت های ماشین آلات نیست. یادگیری ماشین طبقه بندی و پیشبینی را برای داده ها امکان پذیر می کند و میتواند به درصد بالایی از دقت دست یابد که احتمال آن را برای تصمیم گیری صحیح بیشتر می کند (Meng et al., 2020).الگوریتم های مختلف یادگیری ماشین مانند ماشین بردار پشتیبان ، شبکه های عصبی ،naive-bayesian و random forests برای سیستم های تشخیص نفوذ به کار گرفته شده اند. به تازگی، از الگوریتم های مبتنی بر یادگیری عمیق با موفقیت در صدا، تصویر و برنامه های کاربردی پردازش گفتار و تشخیص نفوذ استفاده شده است. هدف این روش های یادگیری نمایش ویژگی خوب از مقدار زیادی از داده های بدون برچسب و متعاقباً اعمال این ویژگی های آموخته شده بر روی مقدار محدودی از داده های برچسب گذاری شده در یک طبقه بندی نظارت شده است. داده‌های دارای برچسب و بدون برچسب ممکن است از منابع مختلفی باشند. با این حال، آنها باید با یکدیگر مرتبط باشند(Niyaz et al., 2015). همانطور که بیان شد سیستم های تشخیص نفوذ را می توان از دیدگاه روش های استقرار منبع داده یا تشخیص حملات طبقه بندی کرد. در شکل ۱ این طبقه بندی ارائه شده است. واژگان مختصر شده در این تحقیق نیز در جدول ۱ بیان شده است. در فصل دوم پایگاه داده های استفاده شده مورد بررسی قرار میگیرند . در فصل سوم معیار های ارزیابی در تشخیص نفوذ بیان میشوند. در فصل چهارم الگوریتم های یادگیری عمیق در تشخیص نفوذ مورد بررسی قرار میگیرند. در فصل پنجم تحلیل نتایج و در فصل ششم نتبجه گیری و کار های اینده در جهت ادامه تحقیقات در زمینه یادگیری عمیق بیان میشود.

**جدول ۱- واژگان مختصر شده**

| تعریف | واژه مخفف | تعریف | واژه مخفف |
|---|---|---|---|
| N-BaIoT | NB | KDD Cup1999 | KD |
| UNSW-NB 15 | UN | NSL-KDD | NK |
| CSE-CIC-IDS2018 | C8 | CIC-IDS2017 | C7 |
| Precision | PRE | Accuracy | ACC |
| Recall | REC | F-Measure | F-M |
| False Alarm Rate | FAR | false positive | FP |
| False Positive Rate | FPR | Others | OT |
| Autoencoder | AE | Convolutional Neural Network | CNN |
| Long Short Term Memory | LSTM | Deep Neural Network | DNN |
| Generative adversarial networks | GAN | Network based Intrusion Detection System | NIDS |
| gate recurrent unit | GRU | | |




**شکل ۱- طبقه بندی الگوریتم های یادگیری عمیق و دامنه تحقیق**

## ۲.پایگاه داده های استفاده شده در سیستم های تشخیص نفوذ

مجموعه داده های نقش حیاتی را در اعتبار سنجی هر یک از مدل های پیشنهادی برای سیستم های تشخیص نفوذ را ایفا می کنند و به ما امکان ارزیابی قابلیت روش پیشنهادی را در تشخیص رفتار مهاجمان میدهد. مجموعه داده های مورد استفاده برای بسته های شبکه تجزیه و تحلیل در محصولات تجاری به دلیل حفظ حریم خصوصی به راحتی در دسترس نیست. با این حال، تعداد کمی وجود دارد مجموعه داده های در دسترس عموم مانند KDDCup 99، NSL-KDD به طور گسترده ای استفاده می شود. در این بخش، به تعدادی از شناخته شده ترین مجموعه داده ها در سیستم های تشخیص نفوذ بیان میشوند.

### KDD Cup1999 .2.1

مجموعه داده KDD Cup 1999 (Bolón-Canedo et al., 2011; Divekar et al., 2018) به استفاده از داده های مناسبی که برای ارزیابی سیستم های تشخیص نفوذ نیاز دارد می پردازد. این مجموعه داده به عنوان یک مجموعه داده شبیه سازی در سال ۱۹۹۸ ساخته شد. از آن زمان به طور گسترده در زمینه های داده کاوی و یادگیری ماشین و یادگیری عمیق استفاده شده است. KDDCup1999 شامل داده‌های آموزشی و آزمایشی است و دارای ۴۱ ویژگی است که به ترافیک و ویژگی های محتوایی طبقه‌بندی می‌شوند.

### NSL-KDD .۲.۲

NSL-KDD مجموعه داده ای است که برای حل برخی از مشکلات مجموعه داده KDD Cup99(Bolón-Canedo et al., 2011; Divekar et al., 2018) پیشنهاد شده است. تعداد رکورد های آموزشی و آزمایشی در NSL-KDD معقول است. این مزیت این مجموعه داده، اجرای آن را مقرون به صرفه می کند تا نیازی به انتخاب تصادفی بخش کوچکی به جای آزمایش بر روی مجموعه کامل نداشته باشد. موارد زیر مزایای NSL-KDD (Tavallaee et al., 2009)نسبت به مجموعه داده اصلی KDD Cup99 است (الف) مجموعه داده NSL-KDD (Tavallaee et al., 2009)شامل رکورد های اضافی در مجموعه داده اموزشی نیست پس طبقه بندی بهتری انجام خواهد شد. (ب) تعداد رکورد های انتخاب شده از هر گروه معکوس با درصد سوابق در مجموعه داده های اصلی KDDCUP99 است . در نتیجه ، طبقه بندی روش های یادگیری ماشین در محدوده وسیع تری متفاوت هستند که کارامدی آن را برای ارزیابی دقیق تر از تکنیک های یادگیری بیشتر می کند. (ج) تعداد رکورد های موجود در مجموعه اموزشی و تست منطقی است ، که باعث می شود آزمایش های مناسبی بدون نیاز به انتخاب تصادفی بخش کوچکی روی مجموعه کامل انجام شود. در نتیجه ، نتایج ارزیابی تحقیقات مختلف قابل مقایسه خواهند بود (Chae et al., 2013; Meena & Choudhary, 2017).

### UNSW-NB15 .۲٫۳

مجموعه داده UNSW-NB15 (Moustafa & Slay, 2015) جدید است و در سال ۲۰۱۵ منتشر شد. این مجموعه داده شامل حمله مدرن (۹ نوع حمله در مقایسه با ۱۴ نوع حمله در مجموعه داده KDDCup99). دارای ۴۹ ویژگی و انواع فعالیت های عادی و هجومی است. از جمله با برچسب های کلاس ۲۲۱۸۷۶ رکورد عادی و ۳۲۱۲۸۳ رکورد حمله وجود دارد. ویژگی های مجموعه داده UNSW-NB15 به شش گروه به نام ویژگی های اساسی طبقه بندی می شود. ویژگی‌های جریان، ویژگی‌های زمانی، ویژگی‌های محتوا، ویژگی‌های اضافی تولید شده، و ویژگی‌های برچسب‌گذاری شده. امکانات شمارش از ۳۶-۴۰ به عنوان ویژگی های هدف عمومی شناخته می شود. ویژگی های شمارش شده از ۴۱-۴۷ به عنوان ویژگی های اتصال شناخته می شوند. بعلاوه، مجموعه داده UNSW-NB15 دارای ۹ نوع حمله است که به Analysis, Fuzzers, Backdoors, DoS Exploits, Reconnaissance, Generic, Shellcode و Worms معروف هستند (Choudhary & Kesswani, 2020).

## ۳- معیار های ارزیابی

جهت ارزیابی مدل از ماتریس اغتشاش استفاده شد که یکی از معیار های رایج برای ارزیابی مدل است. عناصر این ماتریس در جدول ۲ ارائه شده است.

**جدول ۲ ماتریس اغتشاش**

| | | رکورد های تشخیص داده شده | |
|---|---|---|---|
| | | حمله | عادی |
| رکورد های واقعی | حمله | TP | FN |
| | عادی | FP | TN |

TN: تعداد دفعاتی که حالت نرمال بوده و مدل پیشنهادی نیز ان را به طور درست پیشبینی کرده است.

TP: تعداد دفعاتی که حالت حمله بوده و مدل پیشنهادی نیز ان را به طور درست پیشبینی کرده است.
FP: تعداد دفعاتی که حالت نرمال انجام شده و مدل پیشنهادی ان را به طور اشتباه حمله نشان داده است.
FN: تعداد دفعاتی که حالت حمله انجام شده و مدل پیشنهادی ان را به طور اشتباه نرمال نشان داده است.

Accuracy به معنی نزدیک بودن مقادیر اندازه گیری شده به مقدار واقعی است و این که مدل پیشنهادی تا چه حد خروجی را به درستی پیشبینی کرده است. که توسط فرمول (۱) قابل محاسبه خواهد بود.

$$Accuracy = (TP + TN)/ (TP + TN + FP + FN) \quad (۱)$$

Precision یا صحت به نزدیکی دو یا چند اندازه گیری با یکدیگر اشاره دارد و زمانی که مدل نتیجه را مثبت پیش بینی میکند این نتیجه تا چه اندازه درست است. که توسط فرمول (۲) قابل محاسبه خواهد بود.

$$Precision = (TP)/ (TP + FP) \quad (۲)$$

Recall یا تشخیص کسری از جوابهای مثبت که درست تشخیص داده شده‌اند. که توسط فرمول (۳) قابل محاسبه خواهد بود.

$$Recall = (TP)/ (TP + FN) \quad (۳)$$

F-measure یک نوع میانگین بین پارامتر Precision و پارامتر Recall است. Precision صحت سیستم در میان داده‌های پیش‌بینی شده‌است Recallنسبت تعداد داده‌های پیش‌بینی شده، به تعداد کل داده‌های مورد انتظار برای پیش‌بینی است که توسط فرمول (۴) قابل محاسبه خواهد بود. در فرمول (۴-۴) Precision و Recall به اختصار به p و r تبدیل شده اند.

$$F1=2*(P*R)/ (P+R) \quad (۴)$$

FAR به عنوان نسبت نمونه های حمله اشتباه پیش بینی شده به تمام نمونه هایی که نرمال هستند تعریف می شود که توسط فرمول (5) قابل محاسبه خواهد بود.

$$FAR=FP/FP+TN \quad (5)$$

در جدول ۳ به خلاصه ای از معیار های ارزیابی و مجموعه داده تعدادی تحقیق که از الگوریتم های یادگیری عمیق در سیستم تشخیص نفوذ استفاده کرده اند، بررسی میشود.

**جدول ۳ – خلاصه ای از مجموعه داده ها و معیار های ارزیابی در تحقیق های سیستم تشخیص نفوذ**

| منبع | مجموعه داده | | | | | | | معیار ارزیابی | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | KD | NK | NB | UN | C7 | C8 | OT | ACC | PRE | REC | F-M | FAR | FPR |
| (Vinayakumar et al., 2019) | ✓ | ✓ | | ✓ | | | | ✓ | ✓ | | ✓ | | ✓ |
| (Yu & Bian, 2020) | | ✓ | | ✓ | | | | ✓ | ✓ | ✓ | ✓ | ✓ | |
| (Yang et al., 2020) | | ✓ | | ✓ | | | | ✓ | ✓ | ✓ | ✓ | | |
| (K. Jiang et al., 2020) | | ✓ | | | | | | ✓ | | | | ✓ | |
| (S. Kim et al., 2020) | | | | | | | ✓ | ✓ | | | | | |
| (J. Kim et al., 2020) | ✓ | | | | | ✓ | | ✓ | | | | | |
| (Cheng et al., 2021) | | | ✓ | | | | | ✓ | ✓ | ✓ | ✓ | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| (Li et al., 2020) | | ✓ | | | | | ✓ | ✓ | | | | |
| (Yang et al., 2019) | | ✓ | | ✓ | | | | ✓ | ✓ | ✓ | ✓ | | ✓ |
| (Potluri et al., 2018) | | ✓ | | ✓ | | | | ✓ | | | | | |
| (B. Zhang et al., 2018) | | ✓ | | | | | | | ✓ | ✓ | ✓ | | |
| (H. Zhang et al., 2019) | ✓ | | | | | | | ✓ | ✓ | ✓ | ✓ | | |
| (C. Xu et al., 2018) | ✓ | ✓ | | | | | | ✓ | | | | | |
| (Fu et al., 2018) | | ✓ | | | | | | ✓ | | | | ✓ | |
| (F. Jiang et al., 2020) | | ✓ | | | | | | ✓ | | | | ✓ | |
| (Lin et al., 2018) | ✓ | | | | | | | ✓ | | | | | |
| (Otoum et al., 2022) | | ✓ | | | | | | ✓ | ✓ | ✓ | ✓ | | |
| (W. Xu et al., 2021) | | ✓ | | | | | | ✓ | ✓ | ✓ | ✓ | | |
| (Kunang et al., 2021) | | ✓ | | | | ✓ | | ✓ | | | | | ✓ |
| (Almiani et al., 2020) | | ✓ | | | | | | ✓ | ✓ | ✓ | ✓ | | ✓ |
| (A. Kim et al., 2020) | | | | | ✓ | | | ✓ | ✓ | ✓ | ✓ | | |
| (Al-Emadi et al., 2020) | | ✓ | | | | | | ✓ | ✓ | ✓ | ✓ | | |

### ۴. الگوریتم های یادگیری عمیق

یادگیری عمیق زیرمجموعه ای از یادگیری ماشین است که شامل بسیاری از لایه های پنهان برای بدست آوردن ویژگی های شبکه عمیق است. این تکنیک ها به دلیل ساختار عمیق و توانایی در یادگیری ویژگی های مهم از یادگیری ماشین کارآمدتر هستند و به تنهایی بتوانند ویژگی های مهم تر را استخراج و خروجی را تولید کند. این بخش رویکردهای یادگیری عمیق اتخاذ شده برای پیشنهاد سیستم های تشخیص نفوذ مبتنی بر الگوریتم های یادگیری عمیق را ارائه می‌کند.

#### CNN .۴٫۱

CNN نوعی شبکه عصبی مصنوعی است که به یک لایه کانولوشنال نیاز دارد اما می‌تواند انواع لایه‌های دیگری مانند لایه‌های غیرخطی، ادغام‌شده و کاملاً متصل را برای ایجاد یک شبکه عصبی کانولوشنال عمیق داشته باشد. بسته به کاربرد، CNN می تواند کارامد باشد. با این حال، پارامترهای اضافی را برای آموزش اضافه میکند. در CNN، فیلترهای کانولوشنال با استفاده از روش انتشار پس زمینه آموزش داده می شوند. شکل ساختار فیلتر به وظیفه داده شده بستگی دارد. به عنوان مثال، در برنامه‌ای مانند تشخیص چهره، یک فیلتر می‌تواند استخراج لبه را انجام دهد، در حالی که فیلتر دیگر می‌تواند استخراج چشم را انجام دهد. با این حال، ما این فیلترها را به طور کامل در CNN کنترل نمی کنیم و مقادیر آنها از طریق یادگیری تعیین می شود(Albawi et al., 2018).

#### AE .٤,۲

AE یک فید فوروارد بدون نظارت است. AE شبکه عصبی مورد استفاده برای بازسازی ورودی های خودش میباشد. AE از یک لایه ورودی، یک لایه خروجی و یک یا چند لایه های مخفی بیشتر تشکیل شده است. یک الگوی متقارن دارد . خروجی لایه دارای همان تعداد نورون است که لایه ورودی دارد. در حالی که هر لایه پنهان معمولاً نورون های کمتری نسبت به لایه ورودی و لایه خروجی دارد. لایه گلوگاه که به آن فضای نهفته نیز می گویند.یکی از لایه های پنهان است که کمترین تعداد نورون ها را دارد. می توان از آن برای به دست آوردن نمایشی از ورودی با ابعاد کاهش یافته استفاده کرد. فضای نهفته شامل

بازنمای فشرده شده دریافت ورودی است. مکانیسم تلاش های AE برای بازسازی ورودی در خروجی، برای دریافت ورودی و خروجی مشابه است(W. Xu et al., 2021).

### DNN .۴/۳

DNN ها از ساختار شبکه های عصبی مصنوعی با تعداد زیادی لایه پنهان ایجاد می شوند. در استقرار متعارف، داده ها به لایه ورودی وارد می شوند و سپس به صورت غیر خطی به چندین لایه مخفی تبدیل می شود و در لایه خروجی نتایج نهایی محاسبه و تولید می شود. نورون های لایه پنهان و خروجی به تمام نورون های لایه قبلی متصل هستند(Bai et al., 2019).

### LSTM .۴/۴

داده های سری زمانی به داده هایی اطلاق می شود که به ترتیب زمانی مرتب شده اند. مشخصه این نوع داده ها این است که یک همبستگی قوی بین داده های قبل و بعد وجود دارد. یک شبکه LSTM مشکلات گرادیان را تا حد معینی از طریق کنترل گیت حل می کند. که می تواند به طور موثر اطلاعاتی را در مورد وابستگی های طولانی مدت یاد بگیرد. LSTM نتایج خوبی در تعداد زیادی از مسائل سری زمانی دست یافته است و توجه فزاینده ای از محققین را به خود جلب کرده است (Liu et al., 2020).

### GRU .۴/۵

GRU یک نوع LSTM با معماری ساده تر است. واحد GRU دارای دو گیت به شرح زیر است: به روز رسانی و تنظیم مجدد. گیت به روز رسانی تعیین می کند که آیا حالت مخفی باید با یک حالت مخفی جدید به روز شود، در حالی که گیت تنظیم مجدد تصمیم می گیرد که آیا حالت قبلی حالت پنهان باید نادیده گرفته شود(Zhao et al., 2019).

### RNN .۴/۶

شبکه عصبی بازگشتی معروف ترین مدل برای آموزش داده های توالی RNN معمولی دارد مشکل زمانی که از آن برای تمرین با اندازه گام بلند استفاده می شود . RNN توسعه یک شبکه عصبی فید فوروارد قراردادی است . بر خلاف فید فوروارد شبکه های عصبی، RNN دارای اتصالات چرخه ای هستند که آنها را تبدیل به الگوریتمی قدرتمند برای مدل سازی دنباله ها میکند. RNN قراردادی برای آموزش انتشار مجدد استفاده می شود زمان رسیدگی به ورودی توالی با طول متغیر است (J. Kim et al., 2016).

در جدول ۴ به ارائه الگوریتم پیشنهادی هر تحقیق و ابزاری که از ان برای پیاده سازی در هر تحقیق استفاده شده است میپردازیم.

**جدول ۴ – ابزار های استفاده شده برای پیاده سازی و الگوریتم های پیشنهادی**

| الگوریتم پیشنهادی | ابزار های استفاده شده برای پیاده سازی | | | | | منبع |
|---|---|---|---|---|---|---|
| | OT | Scikit-learn | MATLAB | TensorFlow | Keras | |
| DNN | | | | ✓ | ✓ | (Vinayakumar et al., 2019) |
| FSL using DNN + CNN | | | | | | (Yu & Bian, 2020) |
| SAVAER + DNN | | | | ✓ | | (Yang et al., 2020) |
| LSTM +RNN | | | | ✓ | | (K. Jiang et al., 2020) |
| AE | ✓ | | | | | (S. Kim et al., 2020) |
| CNN | | | | | ✓ | (J. Kim et al., 2020) |

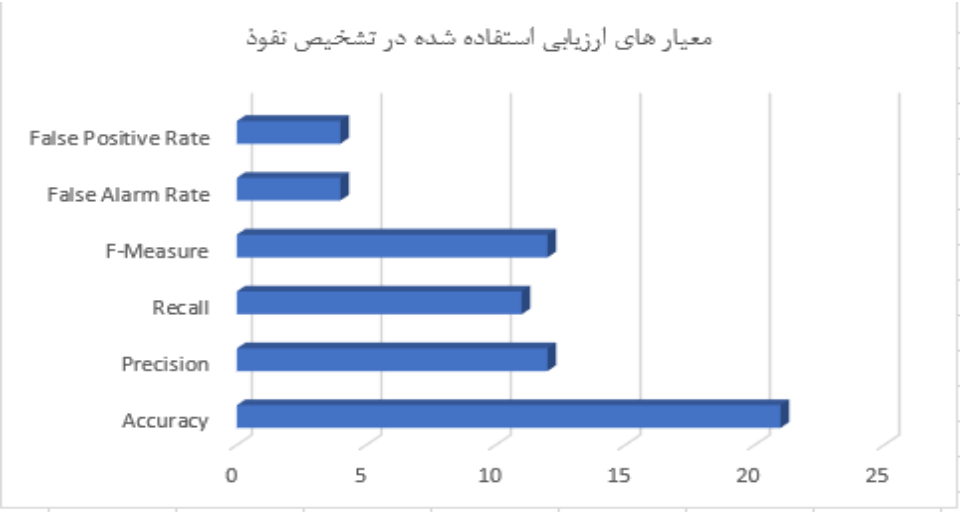
| | | | | | | |
|---|---|---|---|---|---|---|
| CNN | | | ✓ | | ✓ | (Cheng et al., 2021) |
| CNN | | | ✓ | ✓ | | (Li et al., 2020) |
| VAE + DNN | | | ✓ | | | (Yang et al., 2019) |
| CNN | | | ✓ | | | (Potluri et al., 2018) |
| AE + XGBoost | | | | | | (B. Zhang et al., 2018) |
| GAN | | | | | | (H. Zhang et al., 2019) |
| GRU/BGRU + MLP | | | ✓ | | | (C. Xu et al., 2018) |
| LSTM + RNN | | | ✓ | | | (Fu et al., 2018) |
| LSTM + RNN | | | ✓ | | | (F. Jiang et al., 2020) |
| CNN | | | ✓ | | | (Lin et al., 2018) |
| SMO+SDPN | | | ✓ | | | (Otoum et al., 2022) |
| AE | | ✓ | | | | (W. Xu et al., 2021) |
| AE+DNN | | | ✓ | ✓ | | (Kunang et al., 2021) |
| RNN | | ✓ | | | | (Almiani et al., 2020) |
| CNN+LSTM | | | ✓ | ✓ | | (A. Kim et al., 2020) |
| CNN | | | ✓ | | | (Al-Emadi et al., 2020) |

## ۵. تحلیل نتایج

در این فصل به تحلیل مجموعه داده استفاده شده و مدل پیشنهادی مختلف و ابزار و نرم افزار استفاده شده برای ارزیابی و معیار های ارزیابی و تحلیل و ارزیابی نتایج میپردازیم.

### ۵.۱. بررسی و ارزیابی معیار های ارزیابی مورد استفاده قرار گرفته شده

بررسی و ارزیابی معیار های ارزیابی مورد استفاده قرار گرفته شده به شرح زیر است :

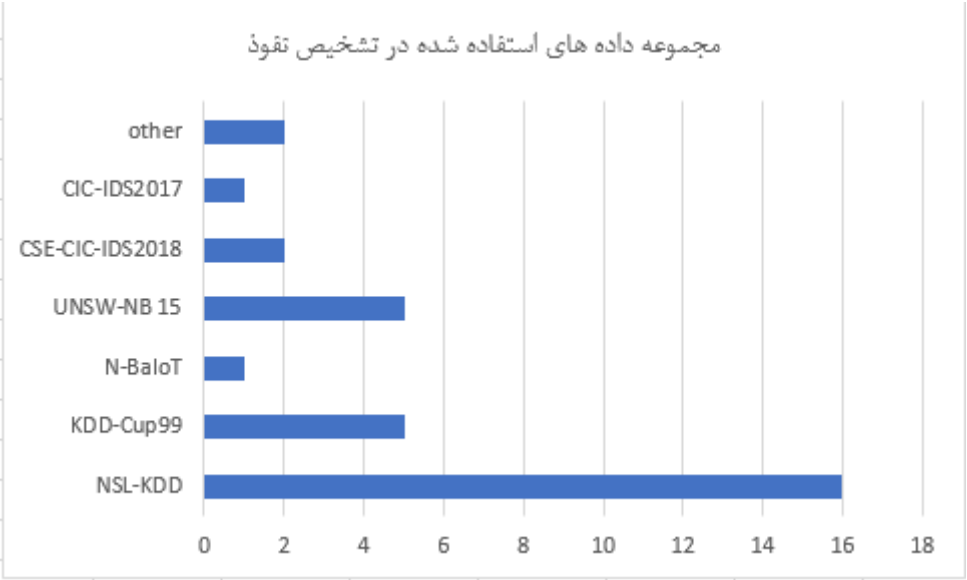



**شکل ۲- معیار های ارزیابی استفاده شده در تشخیص نفوذ**

همانطور که در شکل ۲ مشاهده میشود مجموعه داده های مختلفی برای انتخاب ویژگی و طبقه بندی و مسائل یادگیری عمیق استفاده شده اند .به طور کلی معیار Accuracy در ۲۱ تحقیق و Precision در ۱۲ تحقیق و Recall در ۱۱ تحقیق و معیار F در ۱۲ تحقیق و سایر معیار ها در کمتر از پنج تحقیق مورد بررسی قرار گرفته اند. در برخی از تحقیق ها نیز چندین معیار ارزیابی مورد بررسی قرار گرفته اند. Accuracy با اختلاف بیشترین معیار به کار برده شده در تحقیق ها است.

### ۵.۲. بررسی و ارزیابی مجموعه داده های مورد استفاده قرار گرفته شده

بررسی و ارزیابی مجموعه داده های مورد استفاده قرار گرفته شده به شرح زیر است :

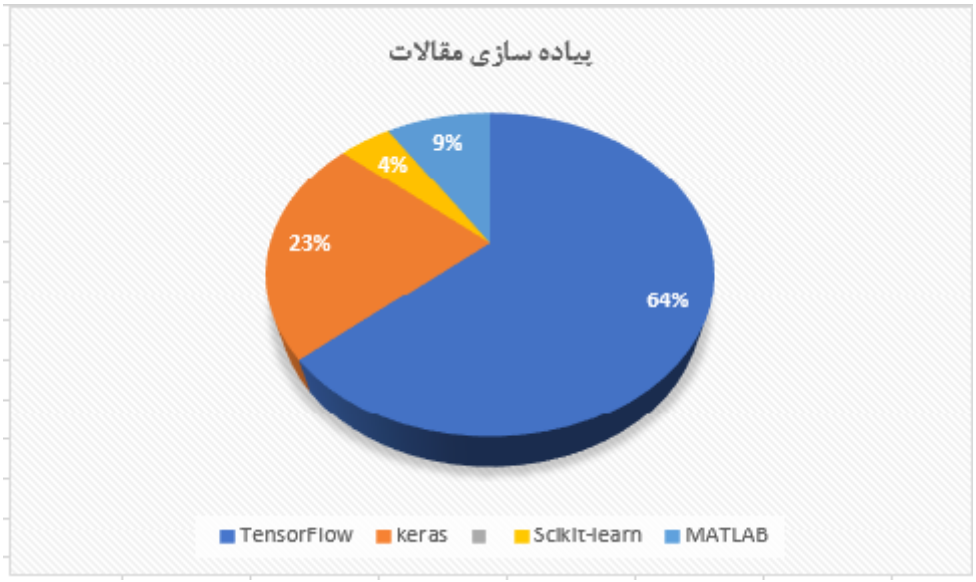



**شکل ۳- تعداد مجموعه داده های استفاده شده**

همانطور که در شکل ۳ مشاهده میشود در ستون هر یک مجموعه داده و سطر ها بیانگر تعداد دفعاتی که یک مجموعه داده در مقالات تکرار شده میباشد و مراحل انجام مدل پیشنهادی باید بر روی مجموعه ای از داده ها اعمال شود. مجموعه داده های مختلفی برای انتخاب ویژگی و طبقه بندی و مسائل یادگیری عمیق استفاده شده اند . به طور کلی مجموعه داده NSL-KDD شانزده بار مجموعه داده KDDCUP پنج بار مجموعه داده UNSW-NB15 پنج بار مجموعه داده CSE-CIC-IDS2018 دو بار و بقیه مجموعه داده ها تنها یک بار در تحقیق ها استفاده شده اند. و این نکته را باید در نظر داشت که در برخی از مقالات چندین مجموعه داده مورد بررسی قرار گرفته اند. پس NSL-KDD مجموعه داده ای است که بیشتر از سایر مجموعه داده ها برای پیاده سازی مورد استفاده قرار گرفته شده است .

### ۵.۳. بررسی و ارزیابی ابزار های مورد استفاده قرار گرفته شده

بررسی و ارزیابی ابزار های مورد استفاده قرار گرفته شده به شرح زیر است :

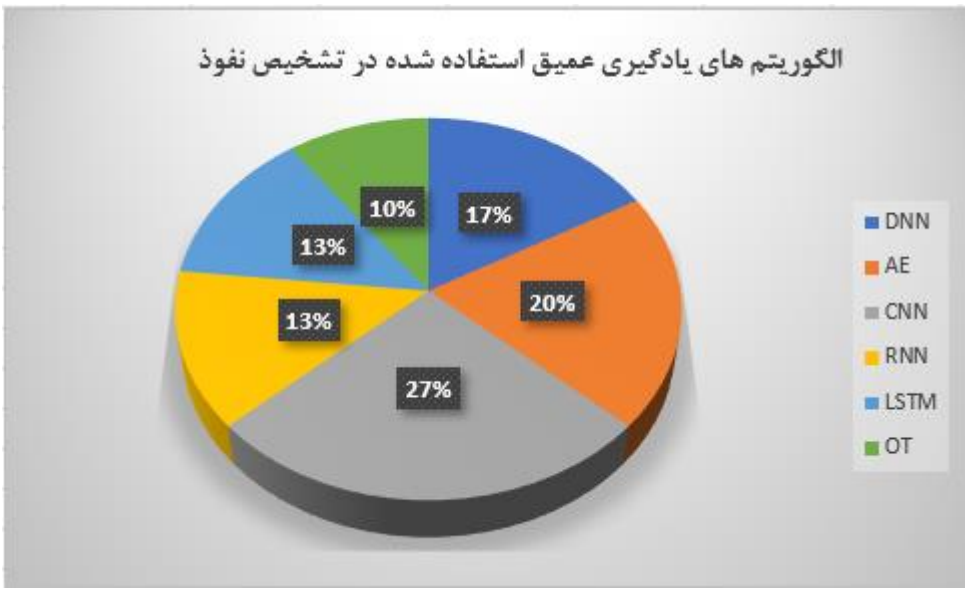



**شکل ۴- درصد استفاده از نرم افزار ها در مقالات برای پیاده سازی**

همانطور که در شکل ۴ مشاهده میشود برای پیاده سازی روش پیشنهادی به کمک یکی از نرم افزار های شبیه سازی انجام میشود. این نرم افزار ها شامل سه نرم افزارSkit-learn, keras, Tensorflow, MATLAB میباشند. طور کلی 64٪ مقالات پیاده سازی شده با Tensorflow و 23٪ مقالات پیاده سازی شده با keras و 9٪ مقالات پیاده سازی شده با MATLAB هستند و در سه تحقیق ابزار پیاده سازی مدل پیشنهادی معرفی نشده اند پس Tensorflow ابزاری است که بیشتر از سایر ابزار ها برای پیاده سازی مورد استفاده قرار گرفته شده است .

### ۵.۴. بررسی و ارزیابی الگوریتم های مورد استفاده قرار گرفته شده

بررسی و ارزیابی الگوریتم های مورد استفاده قرار گرفته شده به شرح زیر است :




**شکل ۵ – الگوریتم های استفاده شده در تشخیص نفوذ**

همانطور که در شکل ۵ مشاهده میشود الگوریتم های مختلف یادگیری عمیق برای حل مسائل مربوط به سیستم های تشخیص نفوذ به کار گرفته شده اند. CNN با ٪۲۷ و بعد از ان AE با ٪۲۰ و بعد از ان DNN با 17% و RNN و LSTMبا 13% الگوریتم های بعدی هستند. CNN بیشترین استفاده را در بین الگوریتم های یادگیری عمیق دارد اما به طور کلی اختلاف بین الگوریتم های به کار برده شده بالا نیست. تعداد ۲۲ تحقیق مورد بررسی قرار گرفتند که در نیمی از تحقیق ها مدل های پیشنهادی ترکیبی پیشنهاد شده بود . در مدل های ترکیبی یکی از الگوریتم ها به عنوان الگوریتمی برای انتخاب ویژگی ارائه میشود.

## ۶. نتیجه گیری و کار های آینده

سیستم تشخیص نفوذ ابزاری برای محافظت از سیستم ها و تشخیص استفاده های غیر مجاز از سیستم در برابر تهدید های امنیتی است. یادگیری عمیق یکی از روش هایی است که میتوان به کمک ان اطلاعات استراتژیک و مخفی در مجموعه داده ها با ابعاد بالا را کشف کرد که الگوریتم های مختلف یادگیری عمیق ارائه شده تا توانایی تشخیص حملات و یا حالت نرمال را در سیستم های تشخیص نفوذ با دقتی بالا از طریق مجموعه داده ورودی به سیستم داشته باشد.در این تحقیق مروری بر الگوریتم های یادگیری عمیق در تشخیص نفوذ انجام شد و الگوریتم ها و مجموعه داده ها و معیار های ارزیابی و ابزار های پیاده سازی برای مدل های پیشنهادی در تشخیص نفوذ مورد بررسی قرار گرفتند. برای تحقیق و پژوهش های اینده پیشنهاد میشود که الگوریتم های یادگیری عمیق در حوزه های جزئی تری مثل کاربرد الگوریتم های یادگیری عمیق در سیستم های تشخیص نفوذ مبتنی بر ناهنجاری یا شبکه و کاربرد الگوریتم های یادگیری عمیق در طبقه بندی تصاویر و تصویر های پزشکی یا تشخیص اشیا مورد بررسی قرار گیرند.

منابع :

Al-Emadi, S., Al-Mohannadi, A., & Al-Senaid, F. (2020). Using Deep Learning Techniques for Network Intrusion Detection. *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies, ICIoT 2020*, 171–176. https://doi.org/10.1109/ICIoT48696.2020.9089524

Albawi, S., Bayat, O., Al-Azawi, S., & Ucan, O. N. (2018). Social touch gesture recognition using convolutional neural network. *Computational Intelligence and Neuroscience*, *2018*. https://doi.org/10.1155/2018/6973103

Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S., & Razaque, A. (2020). Deep recurrent neural network for IoT intrusion detection system. *Simulation Modelling Practice and Theory*, *101*, 102031. https://doi.org/10.1016/j.simpat.2019.102031

Bai, F., Hong, D., Lu, Y., Liu, H., Xu, C., & Yao, X. (2019). Prediction of the Antioxidant Response Elements' Response of Compound by Deep Learning. *Frontiers in Chemistry*, *7*(MAY), 385. https://doi.org/10.3389/fchem.2019.00385

Bolón-Canedo, V., Sánchez-Maroño, N., & Alonso-Betanzos, A. (2011). Feature selection and classification in multiple class datasets: An application to KDD Cup 99 dataset. *Expert Systems with Applications*, *38*(5), 5947–5957. https://doi.org/10.1016/J.ESWA.2010.11.028

Chae, H., Jo, B., Choi, S., & Park, T. (2013). Feature Selection for Intrusion Detection using NSL-

KDD. *Recent Advances in Computer Science 20132*, 184–187.

Cheng, Y., Xu, Y., Zhong, H., & Liu, Y. (2021). Leveraging Semisupervised Hierarchical Stacking Temporal Convolutional Network for Anomaly Detection in IoT Communication. *IEEE Internet of Things Journal*, *8*(1), 144–155. https://doi.org/10.1109/JIOT.2020.3000771

Choudhary, S., & Kesswani, N. (2020). Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT. *Procedia Computer Science*, *167*(2019), 1561–1573. https://doi.org/10.1016/j.procs.2020.03.367

Divekar, A., Parekh, M., Savla, V., Mishra, R., & Shirole, M. (2018). Benchmarking datasets for Anomaly-based Network Intrusion Detection: KDD CUP 99 alternatives. *Proceedings on 2018 IEEE 3rd International Conference on Computing, Communication and Security, ICCCS 2018*, 1–8. https://doi.org/10.1109/CCCS.2018.8586840

Drewek-Ossowicka, A., Pietrołaj, M., & Rumiński, J. (2021). A survey of neural networks usage for intrusion detection systems. *Journal of Ambient Intelligence and Humanized Computing*, *12*(1), 497–514. https://doi.org/10.1007/s12652-020-02014-x

Fu, Y., Lou, F., Meng, F., Tian, Z., Zhang, H., & Jiang, F. (2018). An intelligent network attack detection method based on RNN. *Proceedings - 2018 IEEE 3rd International Conference on Data Science in Cyberspace, DSC 2018*, 483–489. https://doi.org/10.1109/DSC.2018.00078

Jiang, F., Fu, Y., Gupta, B. B., Liang, Y., Rho, S., Lou, F., Meng, F., & Tian, Z. (2020). Deep Learning Based Multi-Channel Intelligent Attack Detection for Data Security. *IEEE Transactions on Sustainable Computing*, *5*(2), 204–212. https://doi.org/10.1109/TSUSC.2018.2793284

Jiang, K., Wang, W., Wang, A., & Wu, H. (2020). Network Intrusion Detection Combined Hybrid Sampling with Deep Hierarchical Network. *IEEE Access*, *8*, 32464–32476. https://doi.org/10.1109/ACCESS.2020.2973730

Khan, K., Mehmood, A., Khan, S., Khan, M. A., Iqbal, Z., & Mashwani, W. K. (2020). A survey on intrusion detection and prevention in wireless ad-hoc networks. *Journal of Systems Architecture*, *105*(September 2019), 101701. https://doi.org/10.1016/j.sysarc.2019.101701

Kim, A., Park, M., & Lee, D. H. (2020). AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection. *IEEE Access*, *8*, 70245–70261. https://doi.org/10.1109/ACCESS.2020.2986882

Kim, J., Kim, J., Kim, H., Shim, M., & Choi, E. (2020). CNN-Based Network Intrusion Detection against Denial-of-Service Attacks. *Electronics 2020, Vol. 9, Page 916*, *9*(6), 916. https://doi.org/10.3390/ELECTRONICS9060916

Kim, J., Kim, J., Thu, H. L. T., & Kim, H. (2016, April 19). Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection. *2016 International Conference on Platform Technology and Service, PlatCon 2016 - Proceedings*. https://doi.org/10.1109/PlatCon.2016.7456805

Kim, S., Hwang, C., & Lee, T. (2020). Anomaly Based Unknown Intrusion Detection in Endpoint Environments. *Electronics 2020, Vol. 9, Page 1022*, *9*(6), 1022. https://doi.org/10.3390/ELECTRONICS9061022

Kunang, Y. N., Nurmaini, S., Stiawan, D., & Suprapto, B. Y. (2021). Attack classification of an intrusion detection system using deep learning and hyperparameter optimization. *Journal of Information Security and Applications*, *58*, 102804. https://doi.org/10.1016/j.jisa.2021.102804

Li, Y., Xu, Y., Liu, Z., Hou, H., Zheng, Y., Xin, Y., Zhao, Y., & Cui, L. (2020). Robust detection for

network intrusion of industrial IoT based on multi-CNN fusion. *Measurement: Journal of the International Measurement Confederation*, *154*, 107450. https://doi.org/10.1016/j.measurement.2019.107450

Lin, W. H., Lin, H. C., Wang, P., Wu, B. H., & Tsai, J. Y. (2018). Using convolutional neural networks to network intrusion detection for cyber threats. *Proceedings of 4th IEEE International Conference on Applied System Innovation 2018, ICASI 2018*, 1107–1110. https://doi.org/10.1109/ICASI.2018.8394474

Liu, L., Song, D., Geng, Z., & Zheng, Z. (2020). A Real-Time Fault Early Warning Method for a High-Speed EMU Axle Box Bearing. *Sensors*, *20*(3), 823. https://doi.org/10.3390/s20030823

Meena, G., & Choudhary, R. R. (2017). A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA. *2017 International Conference on Computer, Communications and Electronics (Comptelix)*, 553–558. https://doi.org/10.1109/COMPTELIX.2017.8004032

Meng, T., Jing, X., Yan, Z., & Pedrycz, W. (2020). A survey on machine learning for data fusion. *Information Fusion*, *57*(2), 115–129. https://doi.org/10.1016/j.inffus.2019.12.001

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in Cloud. In *Journal of Network and Computer Applications* (Vol. 36, Issue 1, pp. 42–57). Academic Press. https://doi.org/10.1016/j.jnca.2012.05.003

Moustafa, N., & Slay, J. (2015, December 7). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). *2015 Military Communications and Information Systems Conference, MilCIS 2015 - Proceedings*. https://doi.org/10.1109/MilCIS.2015.7348942

Niyaz, Q., Sun, W., Javaid, A. Y., & Alam, M. (2015). A deep learning approach for network intrusion detection system. *EAI International Conference on Bio-Inspired Information and Communications Technologies (BICT)*. https://doi.org/10.4108/eai.3-12-2015.2262516

Otoum, Y., Liu, D., & Nayak, A. (2022). DL-IDS: a deep learning–based intrusion detection framework for securing IoT. *Transactions on Emerging Telecommunications Technologies*, *33*(3), e3803. https://doi.org/10.1002/ett.3803

Potluri, S., Ahmed, S., & Diedrich, C. (2018). Convolutional neural networks for multi-class intrusion detection system. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11308 LNAI*, 225–238. https://doi.org/10.1007/978-3-030-05918-7_20

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. *IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2009*. https://doi.org/10.1109/CISDA.2009.5356528

Verma, A., & Ranga, V. (2020). Machine Learning Based Intrusion Detection Systems for IoT Applications. *Wireless Personal Communications*, *111*(4), 2287–2310. https://doi.org/10.1007/s11277-019-06986-8

Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access*, *7*, 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334

Xu, C., Shen, J., Du, X., & Zhang, F. (2018). An Intrusion Detection System Using a Deep Neural Network with Gated Recurrent Units. *IEEE Access*, *6*, 48697–48707. https://doi.org/10.1109/ACCESS.2018.2867564

Xu, W., Jang-Jaccard, J., Singh, A., Wei, Y., & Sabrina, F. (2021). Improving Performance of

Autoencoder-Based Network Anomaly Detection on NSL-KDD Dataset. *IEEE Access*, *9*, 140136–140146. https://doi.org/10.1109/ACCESS.2021.3116612

Yang, Y., Zheng, K., Wu, B., Yang, Y., & Wang, X. (2020). Network Intrusion Detection Based on Supervised Adversarial Variational Auto-Encoder with Regularization. *IEEE Access*, *8*, 42169–42184. https://doi.org/10.1109/ACCESS.2020.2977007

Yang, Y., Zheng, K., Wu, C., & Yang, Y. (2019). Improving the Classification Effectiveness of Intrusion Detection by Using Improved Conditional Variational AutoEncoder and Deep Neural Network. *Sensors 2019, Vol. 19, Page 2528*, *19*(11), 2528. https://doi.org/10.3390/S19112528

Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. *IEEE Access*, *5*, 21954–21961. https://doi.org/10.1109/ACCESS.2017.2762418

Yu, Y., & Bian, N. (2020). An Intrusion Detection Method Using Few-Shot Learning. *IEEE Access*, *8*, 49730–49740. https://doi.org/10.1109/ACCESS.2020.2980136

Zhang, B., Yu, Y., & Li, J. (2018). Network intrusion detection based on stacked sparse autoencoder and binary tree ensemble method. *2018 IEEE International Conference on Communications Workshops, ICC Workshops 2018 - Proceedings*, 1–6. https://doi.org/10.1109/ICCW.2018.8403759

Zhang, H., Yu, X., Ren, P., Luo, C., & Min, G. (2019). *Deep Adversarial Learning in Intrusion Detection: A Data Augmentation Enhanced Framework*. https://doi.org/10.13140/RG.2.2.19731.73762

Zhao, H., Chen, Z., Jiang, H., Jing, W., Sun, L., & Feng, M. (2019). Evaluation of Three Deep Learning Models for Early Crop Classification Using Sentinel-1A Imagery Time Series—A Case Study in Zhanjiang, China. *Remote Sensing*, *11*(22), 2673. https://doi.org/10.3390/rs11222673

# Deep Learning algorithm for Intrusion Detection System: a survey

**Mahshid Salehi[1]***

[1]Department of Computer Engineering, Mashhad Branch, Islamic Azad University, Mashhad, Iran. salehy.md@gmail.com

Abstract:

Rapid advances in the Internet and communications have greatly increased the size of the network and networks related data. As a result, many new attacks are emerging, challenging network security to accurately identify intrusions. In addition, the presence of hackers with the aim of carrying out various attacks within the network cannot be ignored. Intrusion detection systems are an important protection tool for the network. Intrusion detection systems are classifiers that receive input records and predict the class of types of attacks. In network attacks, there are various deep learning algorithms that have been proposed for intrusion detection systems. Over the past decades, researchers have used a variety of deep learning algorithms to classify and detect malicious traffic from normal traffic without prior knowledge of attack pattern. This article provides an overview of deep learning algorithms that use for intrusion detection systems. A separate section is dedicated to presenting the datasets used in intrusion detection systems in particular, the two main datasets, KDDCup99 and NSL-KDD. Evaluation criteria and implementation tools in intrusion detection systems are also examined.

**Keywords:** deep learning, intrusion detection system, network security.