سیستم تشخیص نفوذ در شبکه های نرم افزار محور
با استفاده از شبکه های عصبی عمیق

سمیه جعفری هرستانی[۱]، سید امین حسینی سنو[۲]
[۱]دانشجوی کارشناسی ارشد، گروه مهندسی کامپیوتر، دانشگاه فردوسی مشهد، مشهد، ایران، Somayeh_mz@yahoo.com
[۲]دانشیار گروه مهندسی کامپیوتر، دانشگاه فردوسی مشهد، مشهد، ایران، Hosseini@um.ac.ir

چکیده: در شبکه های کامپیوتری، سیستم های تشخیص نفوذ، ابزاری مفید برای نظارت بر فرآیندهای شبکه و اعلام تهدیدهای احتمالی بوده و معرفی یک سیستم با دقت و صحت بالا برای تشخیص نفوذ از غیر نفوذ، امری حیاتی برای شبکه محسوب می‌شود.

اما چارچوب کلی تمام راه حل‌های پیشنهادی برای حل مسئله تشخیص نفوذ، استفاده از طبقه‌بندی متن است و امروزه شبکه های عصبی عمیق، از برترین طبقه بندها به شمار می آیند. بر این اساس، راهکار پیشنهادی این پژوهش، ارائه یک سیستم تشخیص نفوذ، در شبکه های نرم افزار محور، با استفاده از شبکه های عصبی عمیق می باشد. شبکه عصبی عمیق طراحی شده، مدلی با چیدمان ۱۲ لایه بوده و روی دو مجموعه‌داده جمع آوری شده از شبکه های نرم افزار محور، به نام های NSL-KDD و KDD۹۹ به کار گرفته شده است. لازم به ذکر است، که چیدمان لایه ای منحصر به فرد مدل پیشنهادی برای هر دو مجموعه‌داده تغییر نکرده، که این از نقاط قوت مدل به شمار می رود. اما برای ارزیابی راهکار پیشنهادی، ۶ مدل شبکه عصبی دیگر طراحی و مقادیر معیارهای ارزیابی از جمله صحت، دقت، فراخوانی، معیارF و تابع زیان، در هر یک مورد بررسی قرار گرفته است. همچنین همه معیارها با مقاله وینیاکومار ۲۰۱۹، بهترین مقاله این حوزه، مقایسه شده و برتری راهکار پیشنهادی و بهبود همه نتایج نشان داده شده است. برای پیاده سازی راهکار پیشنهادی نیز، از بسته یادگیری عمیق تنسور فلو۱، کراس و زبان برنامه نویسی پایتون۳، روی ابزار گوگل کولب بهره گرفته شده است.

کلمات کلیدی: سیستم تشخیص نفوذ، شبکه عصبی عمیق، شبکه نرم افزار محور، یادگیری عمیق، تشخیص ناهنجاری.

۱ مقدمه و کلیات پژوهش

در تولید سیستم های کامپیوتری وجود ضعف امنیتی قابل چشم پوشی نیست و بر این اساس بررسی زمینه های مختلف تشخیص نفوذ در این سیستم ها دارای اهمیت می باشد. یک سیستم تشخیص نفوذ (IDS[۱])، به صورت سخت افزاری و نرم افزاری قابل ارائه می باشد و عملکرد آن نظارت بر جریان ها و فعالیت های کل شبکه یا کامپیوتر میزبان بوده و اگر نقض سیاست های مدیریتی و امنیتی را تشخیص دهد، به مدیر شبکه گزارش خواهد داد[۱،۲،۳،۱۱،۱۹،۳۰].

در مقوله یادگیری ماشین، شبکه های عصبی، از پرکاربردترین طبقه بندها هستند. این شبکه ها تکنیک های محاسباتی پیشرفته ای بوده که در بازنمایی دانش دریافتی و اعمال این دانش در جهت اعلام پیش بینی های مورد نیاز خروجی و تخمین توابع پیچیده ریاضی بسیار مورد استفاده قرار می گیرند. یادگیری عمیق(ژرف)[۲]، نیز یکی از زیر مجموعه های یادگیری ماشین بوده و از محبوب ترین و داغ ترین علوم حوزه هوش مصنوعی می باشد، که در آن شبکه سعی می کند داده ها را به کمک لایه های مخفی، از یک سطح به سطحی دیگر نگاشت کند، به گونه ای که بتوان به کمک یک خط، داده ها را از هم تفکیک کرد و روی آن ها طبقه بندی انجام داد. اما یادگیری عمیق یک مسئله کلاس بندی است. یعنی معمولا در آن روی یک مسئله که ذاتا بر پایه سیستم نظارت شده هست، تمرکز می شود و مجموعه داده های جمع آوری شده روی شبکه های نرم افزار محور(SDN[۳]) مثل NSL-KDD[۴]، KDD۹۹، Kyoto-UNSW، NB۱۵، ISCX۱۴ و... در واقع مسئله کلاس بندی را توضیح داده اند، به این صورت که یک کلاس با عنوانY و چندین ویژگی با عنوانX در آن ها آورده شده است. بر این اساس، سیستم پیشنهادی این پژوهش نیز بر پایه شبکه های نرم افزار محور انتخاب و ارائه شده است.

طی سال های اخیر، با به کارگیری تکنیک های مختلف نام برده شده، راهکارهای متعددی برای مسئله تشخیص نفوذ پیشنهاد شده است[۵-۵۱]، اما هر کدام از آن ها چالش ها و مشکلاتی به همراه داشته اند. به عنوان مثال اکثر پژوهش ها نرخ صحت خوبی گزارش داده اند، ولی معیارهای دیگر از جمله دقت، فراخوانی و... را گزارش نکرده اند، که این امر می تواند حاکی از آن باشد که احتمالا مقادیر پایینی در این موارد به دست آورده اند. یا اینکه برخی پژوهش ها معیارهای دیگر هم گزارش کرده اند، ولی مقادیر بسیار پایینی می باشد. از چالش های دیگر راهکار پیشنهادی پژوهش ها، کار کردن روی فقط یک مجموعه داده می باشد، که یکی از دلایل این امر نیز می تواند نداشتن احتمالا کارکردی خوب روی مجموعه داده های دیگر، بزرگتر و جدیدتر باشد. همچنین، بعضی از مقالات نیز مقادیر معیارهای گزارش داده خود را با کلاس بندهای ساده و معمولی مقایسه کرده و برتری خود را اینگونه سنجیده و اعلام داشته اند، که واضح است، این مقایسه از سطح خوب و کیفیت لازم برخوردار نمی باشد. به این ترتیب، با توجه به چالش های مطرح شده، هدف این پژوهش ارائه راهکاری مناسب برای تشخیص نفوذ، در شبکه های نرم افزار محور، با استفاده از شبکه های عصبی عمیق می-باشد. در ادامه پیشینه ای از پژوهش جاری مطرح شده، راهکار پیشنهادی را شرح می دهیم و در انتها هم به ارزیابی و نتیجه گیری از پژوهش خواهیم پرداخت.

۲ مبانی نظری و پیشینه پژوهش

۲-۱ شبکه های نرم افزار محور(SDN)

این روزها نیز نوعی از شبکه ها گسترش پیدا کرده، که به شبکه های نرم افزار محور(SDN) معروف می باشد. به کمک شبکه های نرم افزار محور، مدیریتی آسان، منعطف و یکپارچه خواهیم داشت و اگر در ساختار شبکه تغییر یا ناهنجاری احتمالی رخ دهد، می توان به سرعت و در لحظه آن را تشخیص داده، مدیریت کرده و امنیت و پایداری شبکه را به خوبی تضمین نمود.

همچنین امروزه شبکه های بسیار زیادی وجود دارند، از جمله VANET ،WSN ، MPLS ،SDN...که هر کدام مجموعه داده های مختلفی مختص به خود دارند و اکثرا ارائه روش، مدل و سیستم تشخیص نفوذ برای هر یک به صورت اختصاصی می باشد. به این ترتیب، ما نیز در این پژوهش سعی کردیم، روی مجموعه داده های مختص شبکه های نرم افزار محور(SDN) مثلNSL-KDD و KDD۹۹ تمرکز کنیم. در ادامه به بررسی پژوهش های پیشین انجام شده روی تکنیک های مرتبط با پژوهش جاری خواهیم پرداخت.

۲-۲ پژوهش های پیشین

در این بخش پژوهش های پیشین را دسته بندی کرده و طی دو مبحث آن ها را ذکر می کنیم: ۱) مبحث پژوهش های انجام شده روی معماری های کم عمق و ۲) مبحث پژوهش های انجام شده روی معماری های عمیق.

جدول(۱)، پژوهش‌هایی که تکنیک تشخیص نفوذ خود را مبنی بر معماری های کم عمقی مانند: الگوریتم های ماشین بردار پشتیبان(SVM)، درخت تصمیم(DT)، جنگل های تصادفی(RF)، خوشه بندی(Clustering)، K امین نزدیک ترین همسایه(KNN)، بهینه سازی اجتماع ذرات(PSO)، شبیه سازی ذوب(SA)، شبکه های عصبی مصنوعی(ANN) و روش هایEnsemble(جمعی) قرار داده اند[۵،۶،۱۰،۱۱،۱۲،۱۴،۱۵،۱۸،۴۵]، آورده شده و برتری ها و چالش های این دسته ذکر شده است:

جدول۱: برتری ها و چالش های پژوهش های انجام شده روی معماری های کم عمق

پژوهش های انجام شده روی معماری های کم عمق	مزایا و برتری ها	معایب و چالش ها
[۵،۶،۱۰،۱۱،۱۲،۱۴،۱۵،۱۸،۴۵]	• استفاده از مزیت های الگوریتم های کم عمق • گزارش فاکتورهای صحت یا دقت تشخیص خوب	• گزارش فقط یک معیار صحت یا دقت و عدم ارائه معیارهای دیگر • به کارگیری فقط یک مجموعه داده برای ارزیابی • مقایسه نتایج فقط با کلاس بندهای معمولی

اما پژوهش های انجام شده روی معماری های عمیق نیز در جدول(۲)، به صورت جداگانه دسته بندی شده و برتری ها و چالش های دسته ها نیز به ترتیب بیان شده است:

جدول۲: برتری ها و چالش های پژوهش های انجام شده روی معماری های عمیق

	مراجع	مزایا و برتری ها	معایب و چالش ها
دسته پژوهش های انجام شده روی تکنیک های CNN	[۱۶،۲۵،۳۶،۳۴]	• استفاده از تکنیکی خوب برای تشخیص و آماده سازی داده ها • در برخی مقالات استفاده از لایه های کم و در نتیجه داشتن سرعت پردازش بالاتر و در نهایت ارائه میزان صحتی قابل قبول	• گزارش یک یا دو معیار ارزیابی • به کارگیری فقط یک مجموعه داده برای ارزیابی • مقایسه نتایج با کلاس بندهای ساده و معمولی
دسته پژوهش های انجام شده روی تکنیک های RNN و یا GRU-RNN	[۱۳۰،۳۹،۴۲]	• بهره گیری از RNN های Gate دار • ارائه میزان صحت بالا	• استفاده از لایه های زیاد و نیاز به پردازش های فراوان • به کارگیری مجموعه داده متفاوت که در مقالات اندکی استفاده شده • گزارش فقط یک یا دو معیار ارزیابی
دسته پژوهش انجام شده روی تکنیک LSTM	[۳۲]	• استفاده از حافظه های کوتاه مدت شبکه های LSTM	• گزارش نرخ صحت نسبتا پایین • به کارگیری فقط یک مجموعه داده
دسته پژوهش های انجام شده روی تکنیک های CNN+RNN	[۴۱،۲۲]	• شرح بسیار خوب معماری و مدل تکنیک برخی مقالات	• استفاده از مجموعه داده ای خاص • استفاده از کلاس بندی فقط باینری
دسته پژوهش های انجام شده روی تکنیک های CNN+LSTM	[۴۰،۲۱،۱۷]	• به دست آوردن نرخ صحت بالا روی مجموعه داده انتخابی • استفاده از حافظه های کوتاه مدت LSTM	• به کارگیری فقط یک مجموعه داده برای ارزیابی • به کارگیری مجموعه داده ای خاص
دسته پژوهش های انجام شده روی تکنیک های RNN+LSTM	[۳۰]	• استفاده از متدی هوشمند برای تشخیص حمله	• گزارش یک معیار ارزیابی و عدم ارائه معیارهای دیگر
دسته پژوهش های انجام شده روی تکنیک های Auto Encoder	[۳۵،۲۹،۳۸،۳۷] [۲۷،۲۳۰]	• ارائه چهارچوبی همه جانبه • گزارش صحت خوب و قابل قبول	• استفاده از فقط یک مجموعه داده • فقط مقایسه با کلاس بندهای معمولی • ارائه نرخ متوسطی برای اکثر معیارها
دسته پژوهش های انجام شده روی تکنیک های DNN[۵]	[۵۱،۴۶،۴۴۰، ۴۳،۲۴ [۱۹،۲۰۰	• دستیابی به نرخ بالای صحت در اکثر مقالات این دسته • استفاده از چندین مجموعه داده • استفاده از لایه های معمولی که نیاز به پردازش زیادی ندارد و در نتیجه افزایش سرعت محاسبات	• ذکر نکردن چیدمان لایه ها • فقط استفاده از کلاس بندی باینری • مقایسه نتایج با کلاس بندهای ساده و معمولی
دسته پژوهش های انجام شده روی تکنیک های Ensemble	[۵۰،۴۹،۴۸، ۴۷،۴۵ ۳۳،۲۸، [۱۸۰	• استفاده از تکنیک های Ensemble برای بهبود نرخ صحت • استفاده از رای اکثریت به عنوان یک تصمیم گیرنده نهایی	• فقط گزارش معیار صحت • آزمایش فقط بر روی یک مجموعه‌داده • پردازش های بیشتر به دلیل استفاده از کلاس‌بند های زیاد

به این ترتیب و با توجه به راهکارهای مختلفی که در پژوهش های مذکور مطرح شده، ارائه مدل و چیدمان لایه ای منحصر به فرد این پژوهش به کمک شبکه های عصبی عمیق(DNN)، برای مسئله تشخیص نفوذ در شبکه‌های نرم افزار محور(SDN)، نوآوری پژوهش جاری محسوب می شود و نمونه ی ترکیب و توالی لایه ها و چیدمان مدل DNN طراحی شده، در هیچ یک از پژوهش های پیشین مشاهده نشده است.

۳ راهکار پیشنهادی

در مدل و راهکار پیشنهادی، از یک شبکه عصبی عمیق منحصر به فرد ۱۲ لایه برای هر دو مجموعه‌داده استفاده شده است. ترکیب لایه‌ها در این شبکه ۱۲ لایه به این صورت می‌باشد: لایهDense ، لایه Dense، لایه فعال ساز، لایه حذف تصادفی، لایه Dense، لایه فعال ساز، لایه حذف تصادفی، لایه Dense، لایه فعال ساز، لایه حذف تصادفی، لایه Dense، لایه فعال ساز یا همان لایه کاملا متصل (Fully Connected-FC) که بر حسب تعداد خروجی کلاس ها از توابع سافت مکس(Softmax) یا تانژانت هیپربولیک(Tanh) برای انتخاب کلاس متناسب، مورد استفاده قرار گرفته است. لازم به ذکر است، که معماری و چیدمان لایه ای مدل DNN پیشنهادی برای هر دو مجموعه‌داده، ۱۲ لایه بوده، که این از نقاط قوت مدل و راهکار پیشنهادی به شمار می رود. در واقع مدل پیشنهادی توانسته بدون تغییر تعداد و چیدمان لایه ها روی دو مجموعه داده مقادیر معیارهای ارزیابی را بهبود داده و بسیار خوب عمل کند.

اما در مورد لایه های مدل پیشنهادی باید عنوان کرد، که مقادیر لایه های Dense، با ورودی هر مجموعه‌داده (به تعداد ویژگی‌های هر مجموعه‌داده) متفاوت بوده و تابع فعال‌سازی را نیز یکی از بهترین توابع آزمایش شده برای شبکه عصبی، یعنی تابع غیر خطی Relu قرار داده ایم. در مدل پیشنهادی بعد از هر لایه Dense یک لایه Drop out با مقادیر ۰.۱۵ تا ۰.۵ در نظر گرفته شده، که در اصل لایه حذف تصادفی(Drop out)، به صورت اتفاقی برخی از نورون ها را حذف و رها کرده و از Overfit شدن شبکه جلوگیری می کند و لایه آخر که یک لایه کاملا متصل (بر خلاف یک لایه Dense) می باشد، لایه‌ای است که به همه نورون های لایه قبل متصل می شود. در واقع این لایه، ورودی لایه قبلی را به عنوان یک پارامتر در نظر گرفته و تعداد کلاس‌ها را برای پیش بینی (برای هر مجموعه‌داده بر حسب تعداد خروجی) به کمک یک تابع فعال ساز، یعنی به وسیله یک تابع Softmax و یا Tanh بر روی شبکه اعمال می‌کند. لازم به ذکر است که، در بسته تنسورفلو به صورت پیش‌فرض تمامی بهینه‌سازها و توابع هزینه(زیان[۶]) تعریف شده‌اند و کافی است فراخوانی شده و مقداردهی شوند. در این پژوهش، بهینه‌ساز Adam، بنا به شرایط دو مجموعه‌داده مورد استفاده در تشخیص نفوذ، با نرخ یادگیری متفاوت و محبوب ترین تابع هزینه یعنی Cross Entropy، به کار گرفته شده است.

۴ ارزیابی راهکار پیشنهادی

۴-۱ معیارهای ارزیابی

مهم‌ترین و پرکاربردترین معیارهایی که تاکنون برای ارزیابی کیفیت نتایج روش‌های تشخیص نفوذ مورد استفاده قرار گرفته‌اند[۱۰،۱۳،۱۵،۱۸،۲۱،۲۲،۲۹،۳۰،۳۱،۳۷،۴۷،۴۸،۵۱]، عبارتند از: ۱)صحت[۷] ۲)دقت[۸]، ۳)فراخوانی[۹]، ۴) معیارF[۱۰] و ۵)تابع خطا یا زیان. در ابتدا لازم است، چهار اصطلاح پایه مورد استفاده در معیارهای مذکور را تعریف کنیم[۸]:

مثبت حقیقی[۱۱] یا TP: بیانگر تعداد رکوردهای اتصالی که به طور صحیح در کلاس نرمال طبقه بندی شده اند.

منفی حقیقی[۱۲] یا TN: بیانگر تعداد رکوردهای اتصالی که به طور صحیح در کلاس حمله طبقه بندی شده اند.

مثبت کاذب[۱۳] یا FP: بیانگر تعداد رکوردهای اتصال حمله ای که به طور اشتباه در رکوردهای اتصال نرمال طبقه بندی شده اند.

منفی کاذب[۱۴] یا FN: بیانگر تعداد رکوردهای اتصال نرمالی که به طور اشتباه در رکوردهای اتصال حمله طبقه بندی شده اند.

در ادامه به توضیح کاربرد این اصطلاحات پایه در معیارهای ارزیابی مذکور می پردازیم.

صحت: این معیار نسبت رکوردهای اتصال درست تشخیص داده شده را به کل رکوردهای مجموعه داده مورد آزمایش تخمین می زند. به عبارت دیگر، معیار صحت، نشان می دهد

که چند درصد از داده ها درست دسته بندی شده اند، که این رابطه در ادامه آورده شده‌است:

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN}$$ رابطه۱)

دقّت: این معیار نسبت رکوردهای اتصال حمله درست شناسایی شده، به تعداد کل رکوردهای اتصال حمله شناسایی شده را تخمین می زند، به عبارت دیگر، نسبت تعداد رکوردهای بازیابی شده مرتبط به تعداد کل رکوردهای بازیابی شده را به دست می آورد، که این رابطه نیز در ادامه آورده شده‌است:

$$Precision = \frac{TP}{TP+FP}$$ رابطه۲)

فراخوانی: این معیار، نسبت رکوردهای اتصال حمله که به طورصحیح طبقه بندی شده را به تعداد کل رکوردهای اتصال حمله تخمین می زند. به عبارت دیگر، نسبت تعداد رکوردهای بازیابی شده مرتبط به تعداد کل رکوردهای مرتبط واقعی در مجموعه داده را به دست می آورد، که این معیار را به نام نرخ تشخیص(Detection Rate-DR) یا نسبت مثبت حقیقی(TP Rate) نیز می شناسند[۱۳].

$$Recall = \frac{TP}{TP+FN}$$ رابطه۳)

معیارF : این معیار (که F-Score نیز نامیده می شود)، ترکیبی از (سازگار با) معیارهای فراخوانی و دقّت است و سعی می کند trade offی بین معیارهای دقت و فراخوانی برقرار کرده و نمایش دهد و در نتیجه به این معیار، میانگین هارمونیک نیز گفته می شود. در واقع هر چه این معیار بالاتر باشد، مدل یادگیری ماشین بهتری داریم، که از طریق این فرمول قابل محاسبه می باشد:

$$F - Score = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$ رابطه۴)

همچنین معیار دیگری نیز می توان در ارزیابی ها مدنظر قرار داد، که همان تابع زیان(Loss Function) است [۴۲،۲۰] و در واقع هزینه اینکه چقدر خروجی خطا دارد، را نشان می دهد و با بهینه کردن آن می توانیم به جواب های خوبی برسیم.

۲-۴ مجموعه داده های مورد استفاده در این پژوهش

در این پژوهش از دو مجموعه‌داده جمع آوری شده از شبکه های نرم افزار محور، برای مقایسه راهکار پیشنهادی با دیگر روش‌ها، از جمله مقاله پایه وینیاکومار۲۰۱۹[۱۹] استفاده شده است که به نام های NSL-KDD و KDD۹۹ می باشند. مجموعه داده NSL-KDD، از پرکاربردترین مجموعه داده های مرتبط با سیستم های تشخیص نفوذ می باشد، که از شبکه های نرم افزار محور جمع آوری شده و در واقع برای حل بعضی از مشکلات مجموعه داده KDD۹۹ پیشنهاد شده است. لازم به ذکر است که در این پژوهش از آخرین نسخه این مجموعه داده با ۲۳ کلاس استفاده شده است[۷]. مجموعه-داده KDD۹۹ نیز، از مجموعه داده های قدیمی شبکه های نرم افزار محور با ۴۱ کلاس بوده و در واقع الگویی است که قادر به تفکیک اتصالات "بد" با نام نفوذ یا حمله و اتصالات "خوب" با نام نرمال می باشد.

۳-۴ ابزارهای مورداستفاده برای پیاده‌سازی راهکار پیشنهادی

به منظور پیاده سازی راهکار پیشنهادی پژوهش، نرم افزار Jupyter Notebook به عنوان محیط توسعه و کدنویسی برای این پژوهش مورد استفاده قرار گرفته و این نرم افزار، روی ابزار رایگان Google Colaboratory[۱۵] به صورت پیش فرض نصب می باشد. امروزه محبوب ترین و شاید بتوان گفت، تنها زبان برنامه نویسی برای یادگیری عمیق، زبان برنامه نویسی پایتون(Python) می باشد، یعنی هر دو مجموعه‌داده معرفی شده در این پژوهش، با استفاده از لینک گیت‌هاب در زبان پایتون دانلود شده، مورد بررسی قرار گرفته و پیاده‌سازی آن بر روی بسته یادگیری عمیق تنسورفلو۱ (Tensorflow) [۴]، با پشتیبانی کراس(Keras)، روی GPU های قدرتمند ابزار گوگل کولب (با توجه به محاسبات بسیار زیاد لایه های شبکه عصبی عمیق)، انجام می شود.

۴-۴ ارزیابی راهکار پیشنهادی این پژوهش

اما پژوهش های انجام شده در این حوزه، نتایج ارزیابی روش خود را با استفاده از معیارهای ارزیابی، با نتایج ارائه شده از پژوهش‌های معتبر موجود در حوزه مقایسه می-کنند. در این میان، ما نیز نتایج پژوهش خود را با پژوهش ۲۰۱۹ وینیاکومار[۱۹] مقایسه خواهیم کرد. به این ترتیب، در این پژوهش، ابتدا ۶ مدل شبکه عصبی دیگر برای انجام مقایسه روی هر دو مجموعه‌داده، طبق جدول(۳) طراحی شده و در ادامه، هر ۷ مدل با شرایط یکسان، مورد ارزیابی و بررسی قرار می گیرند.

جدول ۳: مقایسه مدل راهکار پیشنهادی با ۶ مدل شبکه عصبی دیگر

لایه ها	مدل اول	مدل دوم	مدل سوم	مدل چهارم	مدل پنجم	مدل ششم	مدل پیشنهادی
لایه ۱	Dense(۱۲۸)	Embedding	Embedding	Dense(۱۲۸)	Embedding	Embedding	**Dense(۶۴)**
لایه ۲	Dense(۶۴)	Dropout	Dropout	Dense(۶۴)	Dropout	Dropout	**Dense(۳۲)**
لایه ۳	Dense(۱۲۸)	Conv(۲۵۶)	Conv(۳۲)	Dense(۱۲۸)	Conv(۶۴)	Conv(۶۴)	**Activation**
لایه ۴	Dropout	Dense(۱۰۰)	Dense(۶۴)	Conv(۶۴)	Dense(۱۰۰)	Dropout	**Dropout**
لایه ۵	Dense(۶۴)	Dropout	Dropout	Dense(۶)	Conv(۱۲۸)	Dropout	**Dense(۳۲)**
لایه ۶	Dropout	Conv(۱۲۸)	LSTM(۱۲۸)	Dense(۱۲۸)	Conv(۱۲۸)	Conv(۶۴)	**Activation**
لایه ۷	Dense(۶)	Dense(۱۰۰)	Dense(۱۰۰)	FC	Dense(۱۰۰)	Dropout	**Dropout**
لایه ۸	Dropout	Dropout	Dropout	---	Dropout	LSTM(۳۰۰)	**Dense(۳۲)**
لایه ۹	FC	Conv(۲۵۶)	Dense(۱۰۰)	---	Conv(۱۲۸)	Dense(۱۰۰)	**Activation**
لایه ۱۰	---	Dense(۱۰۰)	FC	---	Dense(۱۰۰)	Dropout	**Dropout**
لایه ۱۱	---	Dropout	---	---	Dense(۱۰۰)	Dense(۱۰)	**Dense(۳۲)**
لایه۱۲	---	Dense(۲۰۰)	---	---	Dropout	FC	**FC**
لایه۱۳	---	Dropout	---	---	Dense(۲۰۰)	---	---
لایه۱۴	---	Dense(۱۰۰)	---	---	Conv(۳۲)	---	---
لایه۱۵	---	Conv(۳۲)	---	---	Conv(۶۴)	---	---
لایه۱۶	---	Max-pool	---	---	Conv(۱۲۸)	---	---
لایه۱۷	---	Dropout	---	---	Dense(۱۰۰)	---	---
لایه۱۸	---	Dense(۲۵۶)	---	---	Dropout	---	---
لایه۱۹	---	Dropout	---	---	Dense(۲۵۶)	---	---
لایه۲۰	---	Dense(۱۰۰)	---	---	Dropout	---	---
لایه۲۱	---	Dropout	---	---	FC	---	---
لایه۲۲	FC	---	---	---	---	---	---

۱-۴-۴ ارزیابی ۷ مدل در مجموعه‌داده KDD ۹۹

جدول۴: مقایسه عملکرد راهکار پیشنهادی و ۶ مدل شبکه عصبی دیگر در مجموعه داده KDD ۹۹

معیارها	مدل اول	مدل دوم	مدل سوم	مدل چهارم	مدل پنجم	مدل ششم	مدل پیشنهادی
صحت	۵۳/۹۶	۹۸/۹۳	۵۰/۸۷	۶۱/۱۰	۹۸/۹۰	۸۸/۳۲	**۹۹/۰۲**
دقت	۸۳/۷۹	۸۸/۶۷	۷۸/۵۴	۹۸/۲۷	۸۸/۳۸	۶۳/۱۷	**۹۹/۱۴**
فراخوانی	۷۶/۱۹	۸۶/۳۴	۷۹/۰۰	۴۱/۲۴	۸۵/۹۴	۵۸/۷۷	**۹۸/۹۳**
معیار F	۷۸/۷۸	۸۷/۴۹	۷۸/۷۴	۵۸/۰۸	۸۷/۱۴	۶۰/۰۰	**۹۹/۰۴**
تابع زیان	۰/۰۴۵۹	**۰/۰۳۰۴**	۰/۰۵۴۴	۰/۴۱۴۶	۰/۰۳۰۶	۰/۰۷۷۳	**۰/۱۰۶۷**

با ملاحظه مقادیر معیارهای ارزیابی به دست آمده در جدول(۴)، کاملا واضح است که راهکار پیشنهادی در ۴ معیار صحت، دقت، فراخوانی و معیارF بیشترین مقدار را داشته است که این بهبود، نشان از چیدمان درست لایه ها و کنترل خوب بیش برازش می باشد. با این حال تابع زیان مدل پیشنهادی برای این مجموعه داده از مدل دوم بیشتر است، یعنی مدل دوم با مقدار ۰/۰۳۰۴ به عنوان کمترین تابع زیان مطرح می باشد. در حالت کلی، درست است مدل پیشنهادی کمترین تابع زیان به نسبت دیگر مدل‌ها را ندارد، اما با مقایسه تابع اعتبارسنجی مناسبی که مدل پیشنهادی ارائه کرده و با مشاهده مقادیر بالای معیارهای ارزیابی دیگر، می‌توان عملکرد بسیار خوب مدل پیشنهادی در این مجموعه‌داده را اثبات نمود.

۲-۴-۴ ارزیابی ۷ مدل در مجموعه‌داده NSL-KDD

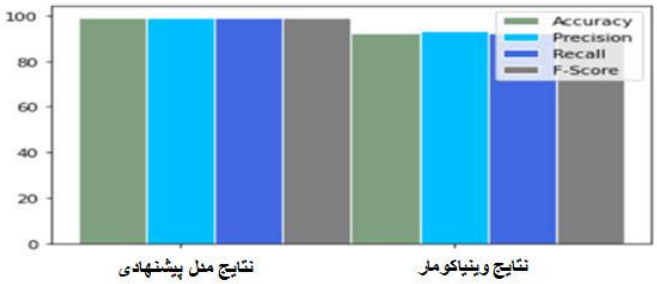
جدول ۵: مقایسه عملکرد راهکار پیشنهادی و ۶ مدل شبکه عصبی دیگر در مجموعه داده NSL-KDD

معیارها	مدل اول	مدل دوم	مدل سوم	مدل چهارم	مدل پنجم	مدل ششم	مدل پیشنهادی
صحت	۷۱/۷۵	۹۵/۹۵	۹۶/۵۳	۶۷/۰۸	۹۵/۹۵	۶۱/۳۲	**۹۹/۳۹**
دقت	۸۳/۵۱	۵۳/۲۶	۹۳/۲۵	۹۱/۱۷	۵۳/۴۸	۸۰/۳۳	**۹۹/۴۹**
فراخوانی	۶۹/۷۹	۵۳/۲۳	۷۰/۲۳	۷۸/۴۰	۵۳/۴۴	۸۴/۱۱	**۹۹/۳۳**
معیارF	۷۵/۶۳	۵۳/۲۴	۷۹/۹۸	۸۳/۸۹	۵۳/۴۶	۸۱/۷۴	**۹۹/۴۱**
تابع زیان	۰/۰۶۸۳	۰/۰۸۷۶	۰/۰۸۴۱	۰/۰۹۳۵	۰/۰۸۷۸	۰/۰۷۶۳	**۰/۰۲۲۴**

با توجه به جدول (۵) برای مجموعه‌داده NSL-KDD با ۲۳ کلاس، کاملا واضح است که راهکار پیشنهادی در همه معیارهای ارزیابی، حتی در تابع زیان نیز از دیگر مدل‌ها با اختلاف بسیار خوبی بهتر عمل کرده است. به عبارت دیگر، بالاتر از ۹۹ درصد بودن مقادیر معیارهای ارزیابی در مدل پیشنهادی و کاهش بسیار خوب تابع زیان روی آن، نشان از عملکرد بسیار عالی راهکار پیشنهادی و طراحی چیدمان مناسب لایه های شبکه عصبی در آن، نسبت به مدل های دیگر می باشد.

۴-۵ مقایسه مقادیر معیارهای ارزیابی راهکار پیشنهادی با مقاله پایه (وینیاکومار۲۰۱۹)

همانطور که پیش‌تر نیز ذکر شد، مقاله وینیاکومار۲۰۱۹ [۱۹]، از بهترین، به روزترین و جسورانه ترین مقالاتی هست، که با استفاده از شبکه های عصبی عمیق(DNN)، مقادیر معیارهای ارزیابی بسیار خوبی را روی ۶ مجموعه داده این حوزه که از شبکه های نرم افزار محور جمع آوری شده اند، کسب کرده و اکثر چالش‌های تشخیص نفوذ را تحت پوشش قرار داده است. لازم به ذکر است که تکنیک استفاده شده در مقاله وینیاکومار نیز، DNN بوده و وجه تمایز راهکار پیشنهادی ما و مقاله وینیاکومار در چیدمان، تعداد، ترکیب و توالی لایه های مختلفی است که در مدل شبکه عصبی عمیق خود به کار برده ایم. در ادامه سعی شده راهکار پیشنهادی پژوهش با نتایج این مقاله نیز مقایسه و بررسی گردد.



شکل ۱: مقایسه راهکار پیشنهادی با مقاله وینیاکومار در مجموعه داده **KDD ۹۹**

همانطور که در شکل(۱) ملاحظه می کنید، با توجه به اینکه مجموعه‌داده KDD۹۹ مد نظر می باشد، مدل و راهکار پیشنهادی در همه مقادیر معیارهای ارزیابی از جمله: صحت، دقت، فراخوانی و معیار F، توانسته از مقاله وینیاکومار بهتر عمل کند و در واقع مقادیر معیارهای ارزیابی این مقاله بسیار خوب را بهبود دهد.

شکل ۲: مقایسه راهکار پیشنهادی با مقاله وینیاکومار در مجموعه داده NSL-KDD

همچنین با ملاحظه شکل(۲) و مقایسه مقادیر معیارهای ارزیابی مدل و راهکار پیشنهادی با مقاله وینیاکومار۲۰۱۹[۱۹] روی مجموعه داده NSL-KDD، واضح است که در این مجموعه‌داده حتی اختلاف مقادیر معیارها روی مدل پیشنهادی با مقاله وینیاکومار، نسبت به مقادیر کسب شده روی مجموعه داده ۹۹ KDD، بیشتر هم شده است و تقریبا همه معیارها به نزدیک صد در صد رسیده‌اند و اختلاف تقریبا ۲۰ درصدی معیارهای صحت، دقت، فراخوانی و معیار F مشهود می باشد.

۵ نتیجه گیری و راهکارهای آتی

دراین پژوهش سعی کردیم در جهت ارتقای سطح امنیت و جلوگیری از حملات مختلف به شبکه ها، گامی برداشته و نیازی از جامعه را حل کنیم. راهکار پیشنهادی این پژوهش، سیستم تشخیص نفوذی است، که بر پایه یک شبکه عصبی عمیق منحصر به فرد ۱۲ لایه بوده و روی دو مجموعه داده جمع آوری شده از شبکه های نرم افزار محور(SDN) به نام های NSL-KDD و KDD۹۹ اعمال شده است. در واقع ترکیب و چیدمان این ۱۲ لایه به این صورت می‌باشد: لایهDense ، لایه Dense، لایه فعال ساز، لایه حذف تصادفی، لایه Dense، لایه فعال ساز، لایه حذف تصادفی، لایه Dense، لایه فعال ساز یا همان لایه کاملا متصل (Fully Connected-FC) که بر حسب تعداد خروجی کلاس ها از توابع سافت مکس(Softmax) یا تانژانت هیپربولیک(Tanh) برای انتخاب کلاس متناسب، مورد استفاده قرار گرفته است. لازم به ذکر است، که معماری و چیدمان لایه ای مدل DNN پیشنهادی برای هر دو مجموعه‌داده، ۱۲ لایه بوده و تعداد و چیدمان لایه ها تغییر نکرده، که این از نقاط قوت مدل و راهکار پیشنهادی به شمار می رود.

اما راهکار پیشنهادی روی هر کدام از این مجموعه‌داده‌ها، در جداول جداگانه ای با ۶ مدل شبکه عصبی دیگر مورد مقایسه و بررسی قرار گرفت، که نتایج به دست آمده برای مجموعه‌داده NSL-KDD با ۲۳ کلاس، مشخص کرد که راهکار پیشنهادی در همه معیارهای ارزیابی، حتی در تابع زیان، از دیگر مدل‌ها با اختلاف زیادی بهتر عمل کرده است، که این بالاتر از ۹۹ درصد بودن مقادیر معیارهای ارزیابی مدل پیشنهادی و کاهش بسیار خوب تابع زیان روی آن، نشان از عملکرد بسیار خوب راهکار پیشنهادی نسبت به مدل های دیگر می باشد. همچنین نتایج عملکرد راهکار پیشنهادی برای مجموعه‌داده KDD ۹۹ نیز، مشخص کرد که راهکار پیشنهادی در چهار معیار مذکور، بیشترین مقادیر معیارهای ارزیابی را به دست آورده، در عین اینکه تنها تابع زیان مدل پیشنهادی برای این مجموعه‌داده، از مدل دوم بیشتر بود، که با توجه به اینکه راهکار پیشنهادی بسیار خوب توانسته، بیش‌برازش را با چیدمان درست لایه ها کنترل نماید، این خطای ناچیز قابل اغماض می باشد. در نهایت نیز، مدل پیشنهادی روی دو مجموعه‌داده مشترک با مقاله وینیاکومار۲۰۱۹[۱۹]، که از بهترین مقالات انجام شده در این حوزه بوده، مورد مقایسه قرار گرفت. به این ترتیب که با در نظر گرفتن مجموعه داده KDD۹۹، مشخص شد که راهکار پیشنهادی در همه معیارهای مذکور بهتر از مقاله وینیاکومار۲۰۱۹ عمل کرد و توانست همه معیارهای ارزیابی مذکور را به میزان بسیار خوبی نسبت به مقاله پایه بهبود بخشد. همچنین با در نظر گرفتن مجموعه داده NSL-KDD، حتی اختلاف مقادیر معیارها روی مدل پیشنهادی با مقاله وینیاکومار، نسبت به مقادیر کسب شده روی مجموعه داده ۹۹ KDD، بیشتر هم شد و تقریبا همه معیارها به نزدیک صد در صد رسیدند و اختلاف تقریبا ۲۰ درصدی معیارهای صحت، دقت، فراخوانی و معیار F روی این مجموعه داده کاملا مشهود بود. در نهایت، با توجه به مقادیر معیارهای ارزیابی کسب شده، می توان نتیجه گرفت که مدل پیشنهادی عملکردی بسیار مناسب برای تشخیص نفوذ روی دو مجموعه‌داده مختلف معرفی شده از شبکه های نرم افزار محور داشته و توانسته نتایج بهترین مقاله این حوزه را به میزان بسیار خوبی بهبود بخشد.

در انتها، برای پژوهشگرانی که علاقه مند هستند در این حوزه فعالیت کنند، می توان تحقیق و بررسی روی راهکارهای زیر را پیشنهاد داد:

- مجموعه‌داده‌های جمع آوری شده روی شبکه های نرم افزار محور، بیشتر از ۲۰ مورد هستند، که در این پژوهش دو مجموعه‌داده پرکاربرد از این حوزه به نام های ۹۹ KDD وNSL-KDD استفاده شدند. اما می توان مجموعه داده های دیگر را نیز مورد بررسی قرار داد و نتایج حاصل را تحلیل نمود.
- در پژوهش جاری، از معماری‌های مختلف معرفی شده در شبکه‌های کانولوشن مانند MobileNet، AlexNet، LeNet و یا دیگر معماری-های موجود استفاده نشده است و می‌توان در کارهای آینده این معماری‌ها را نیز تست کرد و بهبود یا عدم بهبود را بعد از انجام آزمایشات مشاهده نمود. همچنین می‌توان از ترکیب راهکار پیشنهادی با معماری های عمیق دیگر استفاده نمود، یا از الگوریتم های فرا ابتکاری مانند الگوریتم بهینه سازی ازدحام ذرات(PSO) و موارد دیگر بهره گرفت و عملکرد مدل و راهکار پیشنهادی را به همراه استفاده از چنین الگوریتم ها و معماری هایی مورد تحلیل و بررسی قرار داد.

مراجع:

[۱] Heady, R., Luger, G., Maccabe, A., & Servilla, M. (۱۹۹۰). *The architecture of a network level intrusion detection system* (No. LA-SUB-۹۳-۲۱۹). Los Alamos National Lab., NM (United States); New Mexico Univ., Albuquerque, NM (United States). Dept. of Computer Science.

[۲] Panda, M., Abraham, A., & Patra, M. R. (۲۰۱۲). A hybrid intelligent approach for network intrusion detection. Procedia Engineering, ۳۰, ۱-۹.

[٢٤]Roy,S.S.,Mallik,A.,Gulati,R.,Obaidat,M.S.,Krishna,P.V.(٢٠١٧,Januar y).A deep learning based artificial neural network approach for intrusion detection.In International Conference on Mathematics and Computing(pp.٤٤-٥٣).Springer,Singapore.

[٢٥] Li, Z., Qin, Z., Huang, K., Yang, X., & Ye, S. (٢٠١٧, November). Intrusion detection using convolutional neural networks for representation learning. In International Conference on Neural Information Processing (pp. ٨٥٨-٨٦٦). Springer, Cham.

[٢٦] Liu,Y.Liu,S.Zhao,X.(٢٠١٧).Intrusion detection algorithm based on convolutional neural network.DEStech Transactions on Engineering and Technology Research,(iceta).

[٢٧] Niyaz, Q. (٢٠١٧). Design and Implementation of a Deep Learning based Intrusion Detection System in Software-Defined Networking Environment (Doctoral dissertation, University of Toledo).

[٢٨] Marir, N., Wang, H., Feng, G., Li, B., & Jia, M. (٢٠١٨). Distributed abnormal behavior detection approach based on deep belief network and ensemble svm using spark. IEEE Access, ٦, ٥٩٦٥٧-٥٩٦٧١.

[٢٩] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (٢٠١٨). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, ٢(١), ٤١-٥٠.

[٣٠] Jiang, F., Fu, Y., Gupta, B. B., Lou, F., Rho, S., Meng, F., & Tian, Z. (٢٠١٨). Deep learning based multi-channel intelligent attack detection for data security. IEEE transactions on Sustainable Computing.

[٣١]Tang,T.A.,Mhamdi,L.,McLernon,D.,Zaidi,S.A.R.,Ghogho,M.(٢٠١٨,J une).Deep recurrent neural network for intrusion detection in sdn-based networks. In ٢٠١٨ ٤th IEEE Conference on Network Softwarization and Workshops(NetSoft)(pp.٢٠٢-٢٠٦).IEEE.

[٣٢] Ponkarthika, M., & Saraswathy, V. R. (٢٠١٨). Network intrusion detection using deep neural networks. Asian J Appl Sci Technol, ٢(٢), ٦٦٥-٦٧٣.

[٣٣] Parvat, A., Dev, S., Kadam, S., & Chavan, J. (٢٠١٨, August). Network Intrusion Detection System Using Ensemble of Binary Deep Learning Classifiers. In International Conference on Smart Trends for Information Technology and Computer Communications (pp. ٣-١٠). Springer, Singapore.

[٣٤] Potluri, S., Ahmed, S., & Diedrich,C.(٢٠١٨,December).Convolutional Neural Networks for Multiclass Intrusion Detection System.In International Conference on Mining Intelligence and Knowledge Exploration(pp.٢٢٥-٢٣٨).Springer,Cham.

[٣٥] Farahnakian,F.,Heikkonen,J.(٢٠١٨,February).A deep auto-encoder based approach for intrusion detection system.In ٢٠١٨ ٢٠th International Conference on Advanced Communication Technology(ICACT)(pp.١٧٨-١٨٣).IEEE.

[٣٦] Nguyen, S. N., Nguyen, V. Q., Choi, J., & Kim, K. (٢٠١٨, February). Design and implementation of intrusion detection system using convolutional neural network for dos detection. In Proceedings of the ٢Nd International Conference on Machine Learning and Soft Computing (pp. ٣٤-٣٨). ACM.

[٣٧] Papamartzivanos,D.Mármol,F.G.Kambourakis,G.(٢٠١٩).Introducing deep learning self-adaptive misuse network intrusion detection systems.IEEE Access,٧,١٣٥٤٦.

[٣٨] Abusitta, A., Bellaiche, M., Dagenais, M., & Halabi, T. (٢٠١٩). A deep learning approach for proactive multi-cloud cooperative intrusion detection system. Future Generation Computer Systems, ٩٨, ٣٠٨-٣١٨.

[٣٩] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (٢٠١٩). A Comparative Analysis of Deep Learning Approaches for Network Intrusion Detection Systems (N-IDSs): Deep Learning for N-IDSs. International Journal of Digital Crime and Forensics (IJDCF), ١١(٣), ٦٥-٨٩.

[٤٠] Khan, M. A., Karim, M., & Kim, Y. (٢٠١٩). A Scalable and Hybrid Intrusion Detection System Based on the Convolutional-LSTM Network. Symmetry, ١١(٤), ٥٨٣.

[٤١] Chawla,A.,Lee,B.,Fallon,S.,Jacob,P.(٢٠١٩,September).Host based intrusion detection system with combined CNN/RNN model.In Joint European Conference on Machine Learning and Knowledge Discovery in Databases(pp.١٤٩-١٥٨).Springer,Cham.

[٤٢] Chockwanich,N.,Visoottiviseth,V.(٢٠١٩,February).Intrusion Detection by Deep Learning with TensorFlow.In ٢٠١٩ ٢١st International Conference on Advanced Communication Technology(ICACT)(pp.٦٥٤-٦٥٩).IEEE.

[٤٣] Ustebay, S., Turgut, Z., Aydin,M.A.(٢٠١٩,June).Cyber Attack Detection by Using Neural Network Approaches:Shallow Neural Network,Deep Neural Network and AutoEncoder.In International Conference on Computer Networks(pp.١٤٤-١٥٥).Springer,Cham.

[٤٤] Vigneswaran, K. R., Vinayakumar, R., Soman, K. P., & Poornachandran, P. (٢٠١٨, July). Evaluating shallow and deep neural

[٣] Sheikhan, M., & Bostani, H. (٢٠١٦). A hybrid intrusion detection architecture for internet of things. In ٢٠١٦ ٨th International Symposium on Telecommunications (IST) (pp. ٦٠١-٦٠٦). IEEE.

[٤] Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., ... & Kudlur, M. (٢٠١٦). Tensorflow: A system for large-scale machine learning. In *12th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 16)* (pp. ٢٦٥-٢٨٣).

[٥] He, D., Chen, X., Zou, D., Pei, L., & Jiang, L. (٢٠١٨, May). An Improved Kernel Clustering Algorithm Used in Computer Network Intrusion Detection. In Circuits and Systems (ISCAS), ٢٠١٨ IEEE International Symposium on (pp. ١-٥). IEEE.

[٦] Song, J., Takakura, H., Okabe, Y., & Kwon, Y. (٢٠٠٩). Unsupervised anomaly detection based on clustering and multiple one-class SVM. *IEICE transactions on communications*, *92*(٦), ١٩٨١-١٩٩٠.

[٧] Revathi, S., & Malathi, A. (٢٠١٣). A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection. *International Journal of Engineering Research & Technology (IJERT)*, *2*(١٢), ١٨٤٨-١٨٥٣.

[٨] Powers, D. M. (٢٠١١). Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation.

[٩] Chiba, Z., Abghour, N., Moussaid, K., El Omri, A., & Rida, M. (٢٠١٩, March). Smart Approach to Build A Deep Neural Network Based IDS for Cloud Environment Using an Optimized Genetic Algorithm. In Proceedings of the ٢nd International Conference on Networking, Information Systems & Security (p. ٦٠). ACM.

[١٠] Wang, G., Hao, J., Ma, J., & Huang, L. (٢٠١٠). A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering. *Expert systems with applications*, *37*(٩), ٦٢٢٥-٦٢٣٢.

[١١] Lin, S. W., Ying, K. C., Lee, C. Y., & Lee, Z. J. (٢٠١٢). An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection. *Applied Soft Computing*, *12*(١٠), ٣٢٨٥-٣٢٩٠.

[١٢] Aburomman, A. A., & Reaz, M. B. I. (٢٠١٦). A novel SVM-kNN-PSO ensemble method for intrusion detection system. *Applied Soft Computing*, *38*, ٣٦٠-٣٧٢.

[١٣] Yin, C., Zhu, Y., Fei, J., & He, X. (٢٠١٧). A deep learning approach for intrusion detection using recurrent neural networks. Ieee Access, ٥, ٢١٩٥٤-٢١٩٦١.

[١٤] Baek, S., Kwon, D., Kim, J., Suh, S. C., Kim, H., & Kim, I. (٢٠١٧, June). Unsupervised labeling for supervised anomaly detection in enterprise and cloud networks. In ٢٠١٧ IEEE ٤th International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. ٢٠٥-٢١٠). IEEE.

[١٥] Wang, H., Gu, J., & Wang, S. (٢٠١٧). An effective intrusion detection framework based on SVM with feature augmentation. Knowledge-Based Systems, ١٣٦,١٣٠-١٣٩.

[١٦] Zhu, M., Ye, K., & Xu, C. Z. (٢٠١٨, June). Network anomaly detection and identification based on deep learning methods. In International Conference on Cloud Computing (pp. ٢١٩-٢٣٤). Springer, Cham.

[١٧]Hsu,C.M.,Hsieh,H.Y.,Prakosa,S.W.,Azhari,M.Z.,Leu,J.S.(٢٠١٨,Octo ber).Using Long-Short-Term Memory Based Convolutional Neural Networks for Network Intrusion Detection.In International Wireless Internet Conference(pp.٨٦-٩٤).Springer,Cham.

[١٨] Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (٢٠١٨). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. Journal of Computational Science, ٢٥, ١٥٢-١٦٠.

[١٩] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (٢٠١٩). Deep Learning Approach for Intelligent Intrusion Detection System. IEEE Access, ٧, ٤١٥٢٥-٤١٥٥٠.

[٢٠] Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A. R., & Ghogho, M. (٢٠١٦, October). Deep learning approach for network intrusion detection in software defined networking. In ٢٠١٦ International Conference on Wireless Networks and Mobile Communications (WINCOM) (pp. ٢٥٨-٢٦٣). IEEE.

[٢١] Wang, W., Sheng, Y., Wang, J., Zeng, X., Ye, X., Huang,Y.,&Zhu,M.(٢٠١٧).HAST-IDS:Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection.IEEE Access,٦,١٧٩٢-١٨٠٦.

[٢٢] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (٢٠١٧, September). Applying convolutional neural network for network intrusion detection. In ٢٠١٧ International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. ١٢٢٢-١٢٢٨). IEEE.

[٢٣] Mohammadi, S., & Namadchian, A. (٢٠١٧). A New Deep Learning Approach for Anomaly Base IDS using Memetic Classifier. International Journal of Computers, Communications & Control, ١٢(٥).

networks for network intrusion detection systems in cyber security. In ٢٠١٨ ٩th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. ١-٦). IEEE.
[٤٥]Pham,N.T.,Foo,E.,Suriadi,S.,Jeffrey,H.,Lahza,H.F.M.(٢٠١٨,January). Improving performance of intrusion detection system using ensemble methods and feature selection.In Proceedings of the Australasian Computer Science Week Multiconference(p.٢).ACM.
[٤٦] Sharma, J., Giri, C., Granmo, O. C., & Goodwin, M.(٢٠١٩).Multi-layer intrusion detection system with ExtraTrees feature selection,extreme learning machine ensemble,and softmax aggregation.*EURASIP Journal on Information Security*,*2019*(١), ١٥.
[٤٧] Ludwig, S. A.(٢٠١٧).Intrusion detection of multiple attack classes using a deep neural net ensemble.In ٢٠١٧ IEEE Symposium Series on Computational Intelligence (SSCI) (pp. ١-٧). IEEE.
[٤٨]Faker,O,&Dogdu,E.(٢٠١٩,April).Intrusion Detection Using Big Data and Deep Learning Techniques.In Proceedings of the ٢٠١٩ ACM Southeast Conference(pp٨٦-٩٣).ACM.
[٤٩] Ma, T., Wang, F., Cheng, J., Yu, Y., & Chen, X. (٢٠١٦). A hybrid spectral clustering and deep neural network ensemble algorithm for intrusion detection in sensor networks. Sensors, ١٦(١٠), ١٧٠١.
[٥٠] Barushka,A.,Hájek,P.(٢٠١٨,May).Spam filtering in social networks using regularized deep neural networks with ensemble learning.In IFIP International Conference on Artificial Intelligence Applications and Innovations(pp.٣٨-٤٩).Springer,Cham.
[٥١] Rawat, S., & Srinivasan, A. (٢٠١٩). Intrusion detection systems using classical machine learning techniques versus integrated unsupervised feature learning and deep neural network. arXiv preprint arXiv:١٩١٠,٠١١١٤.

---

[١] Intrusion Detection System

[٢] Deep Learning

[٣] Software Defined Network

[٤] https://www.unb.ca/cic/datasets/nsl.html

[٥] Deep Neural Network

[٦] Loss Function

[٧] Accuracy

[٨] Precision

[٩] Recall

[١٠] F-measure

[١١] True Positive

[١٢] True Negative

[١٣] False Positive

[١٤] False Negative

[١٥] https://colab.research.google.com