سامانه‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)

**Winter, 4 (4), 57-65**
**DOR:**

**Received: 25 Oct 2023**
**Accepted: 4 Dec 2023**

**مقاله پژوهشی**

# Presenting A Hybrid Method of Deep Neural Networks to Prevent Intrusion in Computer Networks

**Mohsen Roknaldini [1], Erfaneh Noroozi[2*]**

1. Department of Computer Engineering, Qeshm branch, Islamic Azad university, Qeshm, Iran. Rokn.bmh@gmail.com
2. Department of Computer Engineering, Qeshm branch, Islamic Azad university, Qeshm, Iran. **Corresponding Author*, NoroozіErfaneh@gmail.com

**Abstract**

**Introduction**: Nowadays, computer networks have significant impacts on our daily lives, leading to cybersecurity becoming a crucial area of research. Cybersecurity techniques mainly encompass antivirus software, firewalls, and intrusion detection systems. Intrusion detection system is one of the fundamental security tools in the field of computer networks and systems. The primary goal of an intrusion detection system is to identify and alert about any unauthorized activities, threats, or attacks on a system or network. By analyzing the flow of data and network/system events, the intrusion detection system attempts to identify patterns and indicators related to various attacks and intrusions. Intrusion detection systems can operate based on rules or learning. In the rule-based approach, algorithms and rules created by security experts and analysts are used to detect patterns and identify attacks. However, in the machine learning approach, machine learning algorithms and deep neural networks are employed to extract patterns and features related to attacks from real data.

**Method:** This study focuses on the examination and presentation of a combined approach using deep neural networks to prevent intrusions in computer networks. The primary objective of this research is to enhance the efficiency of intrusion detection systems. To achieve this goal, a combined approach of deep learning and artificial neural networks is proposed. This approach utilizes deep neural networks to detect more complex features and improves the model's performance.

**Results:** Simulation results demonstrate that deep neural network methods such as MLP, CNN, LSTM, and GRU yield favorable outcomes compared to other single-layer machine learning techniques. In this study, two combined methods, CNN-GRU and CNN-LSTM, were introduced and tested on the KDD CUP'99 dataset for comprehensive analysis and evaluation. Both combined approaches exhibit high accuracy and lower classification errors compared to other introduced methods. Therefore, it can be concluded that the CNN-LSTM combined approach performs well on the KDD CUP'99 dataset.

**Discussion:** Based on the achieved results, the combined CNN-LSTM and CNN-GRU methods offer very good performance with accuracies of 99.95% and 99.92%, respectively, on the KDD CUP'99 dataset. Among these methods, minor differences in the performance of some parameters for classes may exist, yet both approaches remain acceptable. Hence, it can be concluded that the combined CNN-LSTM approach performs well on the KDD CUP'99 dataset.

**Keywords**: Deep learning, neural network, feature selection, intrusion detection system.

سامانه‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)
انجمن علمی تجارت الکترونیکی ایران
واحد زنجان

# ارائه یک روش ترکیبی شبکه‌های عصبی عمیق جهت جلوگیری از نفوذ در شبکه‌های کامپیوتری

تاریخ دریافت: ۰۳/ ۰۸/ ۱۴۰۲
تاریخ پذیرش: ۱۳/ ۰۹/ ۱۴۰۲

دورهٔ چهارم، زمستان ۱۴۰۲
شمارهٔ چهارم، صص: ۵۷-۶۵

**محسن رکن‌الدینی [۱]، عرفانه نوروزی [۲*]**

۱. گروه مهندسی کامپیوتر، واحد قشم، دانشگاه آزاد اسلامی، قشم، ایران. Rokn.bmh@gmail.com
۲. گروه مهندسی کامپیوتر، واحد قشم، دانشگاه آزاد اسلامی، قشم، ایران. (نویسندهٔ مسئول) NoroozíErfaneh@gmail.com

**چکیده:** در این پژوهش به بررسی و ارائه یک روش ترکیبی شبکه‌های عصبی عمیق جهت جلوگیری از نفوذ در شبکه‌های کامپیوتری پرداخته‌می‌شود. هدف اصلی این پژوهش، افزایش کارایی سیستم تشخیص نفوذ است. برای دستیابی به این هدف، یک روش ترکیبی از یادگیری عمیق و شبکه عصبی مصنوعی ارائه‌شده‌است. این روش با استفاده از شبکه‌های عصبی عمیق، ویژگی‌های پیچیده‌تر را تشخی‌ص داده و عملکرد مدل را بهبودمی‌بخشد. با استفاده از روش‌های ترکیبی شامل ترکیب معماری شبکه‌های عصبی، ویژگی‌ها، خروجی‌ها و ترکیب نتایج از شبکه‌های عصبی مختلف، تنوع و قدرت تشخیصی مدل افزایش می‌یابد و درستی و عملکرد آن بهبودمی‌یابد. نتایج شبیه‌سازی‌ها نشان‌می‌دهد که روش‌های شبکه‌های عصبی عمیق مانند MLP، CNN، LSTM و GRU نتایج خوبی نسبت به دیگر روش‌های تک‌لایه‌ای یادگیری ماشین دارند. در این پژوهش دو روش ترکیبی شبکه عصبی عمیق CNN-GRU و CNN-LSTM معرفی‌شدند که به‌منظور تحلیل و ارزیابی کلی بر روی مجموعه‌داده KDD CUP'99 آزمایش‌شد. دو رویکرد ترکیبی، صحت بالا و خطای دسته‌بندی کمتری نسبت به دیگر روش‌های معرفی‌شده، دارند؛ بنابراین، می‌توان نتیجه‌گرفت که در مجموعه داده KDD CUP'99 روش ترکیبی CNN-LSTM عملکرد مناسبی دارد.

**واژه‌های کلیدی:** یادگیری عمیق، شبکه عصبی، انتخاب ویژگی، سیستم تشخیص نفوذ.

## ۱. مقدمه

امروزه شبکه‌های کامپیوتری تأثیرات زیادی بر زندگی روزمره ما دارند این امر باعث‌شده که امنیت سایبری به یک زمینه مهم تحقیقاتی تبدیل-شود. تکنیک‌های امنیت سایبری عمدتاً شامل نرم‌افزارهای ضدویروسی، فایروال‌ها و سیستم‌های تشخیص نفوذ[۱] هستند. این تکنیک‌ها شبکه‌ها را از حملات داخلی و خارجی محافظت‌می‌کنند. در میان آن‌ها، IDS نوعی سیستم تشخیص نفوذ هستند که با نظارت بر وضعیت نرم‌افزار و سخت‌افزار در حال اجرا در یک شبکه، نقش کلیدی در حفاظت از امنیت سایبری را ایفامی‌کنند. اولین سیستم تشخیص نفوذ در سال ۱۹۸۰ ارائه-شد [1]. از آن زمان، بسیاری از سیستم‌های تشخیص نفوذ معرفی‌شده-اند. بااین‌حال، بسیاری از سیستم‌های تشخیص نفوذ هنوز از نرخ هشدار نادرست بالایی رنج‌می‌برند و هشدارهای زیادی را برای موقعیت‌های غیرتهدیدکننده ایجادمی‌کنند که بار تحلیلگران امنیتی را بالامی‌برد و می‌تواند باعث نادیده‌گرفته‌شدن حملات خطرناک شود2]] . بنابراین، بسیاری از محققان بر روی توسعه سیستم‌های تشخیص نفوذ با نرخ تشخیص بالاتر و کاهش نرخ هشدار نادرست تمرکزکرده‌اند. مشکل دیگر سیستم‌های تشخیص نفوذ موجود این است که آن‌ها توانایی تشخیص حملات ناشناخته را ندارند. از آنجا که محیط‌های شبکه به سرعت تغییرمی‌کنند، انواع حملات و حملات جدید به‌طور مداوم ظاهرمی‌شوند. بنابراین، توسعه سیستم‌های تشخیص نفوذ می‌توانند حملات ناشناخته را شناسایی‌کنند امری ضروری است. برای حل مشکلات ذکرشده، محققان به تمرکز بر روی ساخت سیستم‌های تشخیص نفوذ با استفاده از روش‌های یادگیری ماشینی کرده‌اند. یادگیری ماشینی نوعی تکنیک هوش مصنوعی است که می‌تواند به‌طور خودکار اطلاعات مفید را از مجموعه‌داده‌های عظیم کشف‌کند 3]] .

## ۲. سیستم تشخیص نفوذ

سیستم تشخیص نفوذ یا (IDS)[۲]یکی از اصولی‌ترین ابزارهای امنیتی در حوزه شبکه و سیستم‌های کامپیوتری است. هدف اصلی یک سیستم تشخیص نفوذ، شناسایی و اعلام هرگونه فعالیت غیرمجاز، تهدید یا حمله به یک سیستم یا شبکه است. سیستم تشخیص نفوذ با تحلیل و بررسی جریان داده‌ها و رویدادهای شبکه و سیستم، سعی در شناسایی الگوها و نشانه‌های مربوط به حملات و نفوذهای مختلف دارد. سیستم تشخیص نفوذ می‌تواند به‌صورت مبتنی بر قوانین[۳] یا مبتنی بر یادگیری[۴] عمل‌کند. در رویکرد قوانین، الگوریتم‌ها و قوانینی که توسط امنیت‌گذاران و تحلیل‌گران تهیه‌شده‌اند، برای تشخیص الگوها و شناسایی حملات استفاده‌می‌شود. اما در رویکرد یادگیری، الگوریتم‌های یادگیری ماشینی و شبکه‌های عصبی عمیق به‌کارگرفته‌می‌شوند تا بتوانند الگوها و ویژگی‌های مربوط به حملات را از داده‌های واقعی استخراج‌کنند [4].

سیستم تشخیص نفوذ می‌تواند به‌صورت رویدادمحور[۵] و یا جریان محور[۶] عمل‌کند. در رویکرد رویدادمحور، سیستم بر اساس رویدادهای مشخصی که در شبکه رخ می‌دهند؛ مانند تلاش برای ورود غیرمجاز به سیستم یا ارسال پیام‌های ترافیک غیرعادی، تشخیص حملات را انجام می‌دهد. درحالی‌که در رویکرد جریان محور، سیستم بر اساس تحلیل جریان ترافیک شبکه و شناسایی الگوهای مشخص در جریان داده‌ها، حملات را تشخیص‌می‌دهد. استفاده از سیستم تشخیص نفوذ در سازمان‌ها و شبکه‌ها به‌طور گسترده‌ای افزایش‌یافته‌است، زیرا امنیت اطلاعات و سیستم‌ها در مقابل تهدیدات روزافزون حائز اهمیت است. با استفاده از سیستم تشخیص نفوذ، سازمان‌ها قادرخواهندبود تا به‌صورت سریع و مؤثر به حملات و تهدیدهای امنیتی پاسخ‌دهند و از آسیب‌های جدی به سیستم‌ها جلوگیری‌کنند [4].

## ۳. مروری بر کلیات پژوهش‌ها

ایده‌های تحقیقاتی زیادی دررابطه‌با سیستم‌های تشخیص نفوذ با استفاده از تکنیک‌های یادگیری ماشین، تکنیک‌های یادگیری عمیق[۷] و الگوریتم‌های گروهی و تکاملی ارائه‌شده‌اند. در این پژوهش تمرکز اصلی بر روی روش‌های یادگیری عمیق می‌باشد.

در مرجع 5]] یک تکنیک یادگیری عمیق به نام FFDNNs برای پیاده‌سازی سیستم تشخیص نفوذ طراحی‌کردند. برخلاف شبکه‌های عصبی مصنوعی[۸] ، شبکه‌های عصبی عمیق[۹] ممکن است حاوی صدها لایه پنهان باشند. آنان در پژوهش خود از مجموعه‌داده NSL-KDD استفاده نمودند. آن‌ها در مدل خود از استخراج ویژگی استفاده تا بعد ورودی را کاهش دهند. آن‌ها دسته‌بندی حملات خود را با مجموعه‌داده‌های دودویی و چند دسته‌ای انجام‌دادند. مدل آن‌ها در مقایسه با روش‌هایی مانند SVM، Decision Tree و KNN بهتر عمل می‌کنند.

در مرجع [6] یک روش یادگیری عمیق مبتنی بر شبکه عصبی معرفی کردند که در این مدل شبکه عصبی پیچشی بهبودیافته‌ای [۱۰] برای سیستم تشخیص نفوذ طراحی‌کردند. مدل شبکه عصبی پیچشی بهبودیافته از پنج‌لایه کانولوشن، چهارلایه کاملاً یکپارچه، دولایه ادغام و یک‌لایه SoftMax تشکیل‌شده‌است. پژوهشگران در این مطالعه خود، از مجموعه‌داده NSL-KDD برای ارزیابی عملکرد مدل آن‌ها استفاده-کردند. آموزش مدل شبکه عصبی پیچشی بهبودیافته شامل فرآیند انتشار روبه‌جلو و انتشار به عقب است. روش پیشنهادی با مدل‌های دیگر مانند LeNet-5، شبکه باور عمیق[۱۱] و شبکه عصبی بازگشتی[۱۲] مقایسه-شدند که نرخ تشخیص نفوذ مدل پیشنهادی آن‌ها بیشتر از مدل‌های LeNet-5 و شبکه باور عمیق است؛ اما کمتر از شبکه عصبی بازگشتی است.

در مرجع 7]] یک روش شبکه عصبی بازگشتی مبتنی بر یادگیری عمیق برای پیاده‌سازی سیستم تشخیص نفوذ معرفی‌کرده‌اند. تفاوت اساسی بین روش شبکه عصبی بازگشتی‌ها و سایر شبکه عصبی روبه‌جلو [۱۳]، توانایی به‌خاطرسپردن اطلاعات قبلی و استفاده از آن در لایه فعلی است. مدل پیشنهادی آنان بر روی مجموعه‌داده NSL-KDD موردارزیابی‌قرارگرفت که نشان‌می‌دهد شبکه عصبی بازگشتی دارای نرخ سازگاری بالا و نرخ مثبت کاذب نسبتاً پایینی در مقایسه با سایر روش‌های مرسوم، از جمله Naïve Bayes و J48 است.

در مرجع 8]] یک معماری مبتنی بر هوش مصنوعی با استفاده از مدل شبکه عصبی پیچشی بهینه بر روی داده‌های زمان واقعی ارائه‌کردند. آن‌ها عملکرد مدل خود را با استفاده از پارامترهایی مانند F-Score، کارایی، دقت، ویژگی و فراخوانی بر روی دو مجموعه‌داده اندازه‌گیری‌کردند. مجموعه‌داده‌های CSIC-2010 و CICIDS-2017 آن‌ها گزارش‌دادند که سیستم تشخیص نفوذ مبتنی بر هوش مصنوعی می‌تواند بین ترافیک معمولی و غیرعادی تشخیص‌دهد؛ ولی نمی‌تواند از سیستم تشخیص نفوذ مبتنی بر امضا استفاده‌کند. علاوه بر این، آن‌ها ادعاکرده‌اند که مدل پیشنهادی می‌تواند قوانین Snort را برای سیستم تشخیص نفوذ که از امضا استفاده‌می‌کند، تقویت‌کند.

در مرجع 9]] از واحد بازگشتی گیتی (دروازه‌دار) [14] برای رمزگذاری و توسعه یک سیستم تشخیص نفوذ استفاده‌شد. واحد بازگشتی گیتی مکانیزم دروازه‌ای است که با شبکه‌های عصبی مکرر استفاده‌می‌شود. آنان از دو نوع واحد بازگشتی گیتی کدگذاری‌شده و واحد بازگشتی گیتی دودویی کدگذاری‌شده استفاده‌کردند. پژوهش آنان ادعامی‌کند که واحد بازگشتی گیتی رمزگذاری‌شده نمایش بهتری از ورودی‌ها را ارائه‌می‌دهد درحالی‌که واحد بازگشتی گیتی دودویی رمزگذاری‌شده، همراه با نمایش بهتر ورودی‌ها، زمان دسترسی و اندازه حافظه را نیز کاهش‌می‌دهد.

در مرجع10]] یک مدل تشخیص نفوذ جدید ترکیبی پیشنهاد‌کرده‌اند که شامل یک شبکه عصبی عمیق ویک رمزگذار خودکار شرطی بهبودیافته[15] است. روش پیشنهادی برای یادگیری و کشف و نمایش‌های پراکنده بین ویژگی‌های داده‌های شبکه و کلاس‌های حملات استفاده‌می‌شود. رمزگشای آموزش‌دیده نمونه‌های حمله جدیدی را باتوجه‌به دسته‌های نفوذ مشخص‌شده تولیدمی‌کند تا داده‌های آموزشی را متعادل‌کند و تنوع نمونه‌های آموزشی را افزایش‌دهد و در نتیجه نرخ تشخیص حملات نامتعادل را بهبودبخشد. آنان از مجموعه‌داده‌های NSL-KDD و UNSW-NB15 برای ارزیابی عملکرد روش پیشنهادی استفاده‌می‌کنند. روش پیشنهادی دقت کلی، نرخ تشخیص و نرخ مثبت کاذب بهتری را نسبت به ۹ روش تشخیص نفوذ دارد.

در مرجع 11]] یک مدل جدید تشخیص نفوذ شبکه با استفاده از شبکه‌های عصبی پیچشی ارائه‌کردند که برای انتخاب خودکار ویژگی‌ها از مجموعه‌داده خام استفاده‌کردند. ضریب وزن و تابع هزینه هر کلاس را بر اساس اعداد آن تنظیم‌کردند تا مشکل مجموعه‌داده نامتعادل حل‌شود. این مدل نرخ هشدار کاذب را کاهش‌می‌دهد و دقت کلاس را بهبود می‌بخشد. آنان از مجموعه‌داده استاندارد NSL-KDD برای ارزیابی عملکرد مدل CNN پیشنهادی استفاده‌کرده‌اند. نتایج شبیه‌سازی آنان نشان‌می‌دهد که دقت، نرخ هشدار کاذب و هزینه محاسبه مدل پیشنهادی بهتر از الگوریتم‌های استاندارد سنتی عمل‌کرده‌است.

در مرجع 12]] ، یک روش جدید تشخیص نفوذ مبتنی بر شبکه عصبی پیچشی پیشنهادشده‌است. در مرحله دوم، بر اساس رویکرد پیشنهادی، یک سیستم تشخیص نفوذ کارآمد، بلادرنگ و خودکار به نام IDS-CNNطراحی‌شده‌است. این سیستم توسط چندین ابزار منبع‌باز ساخته‌شده‌است. این سیستم از پیش‌پردازش داده‌ها، آموزش شبکه عصبی، تست شبکه و پاسخ نفوذ بر اساس پلتفرم لینوکس تشکیل‌شده‌است. در نهایت با مجموعه‌داده‌های NSL-KDD و آزمایش جریان واقعی شبکه، نشان‌دادند که سیستم پیشنهادی آنان دقت تشخیص بهتری نسبت به روش پیشرفته دارد.

نویسندگان یک سیستم تشخیص نفوذ مبتنی بر یادگیری عمیق برای شبکه‌های تعریف شده توسط نرم‌افزار[16] ارائه می‌دهند [13]. روش پیشنهادی در این مقاله شامل استفاده از معماری شبکه عصبی عمیق برای آموزش و دسته‌بندی بسته‌های شبکه است. معماری شبکه عصبی پیچشی و شبکه عصبی بازگشتی در این سیستم استفاده‌می‌شوند تا ویژگی‌های مختلف بسته‌های شبکه را استخراج‌کنند و به تشخیص نفوذ در شبکه کمک‌کنند. نتایج آزمایش‌ها نشان‌می‌دهد که سیستم پیشنهادی دقت بالا و عملکرد قابل‌قبولی در تشخیص نفوذ در شبکه‌های تعریف‌شده توسط نرم‌افزار دارد.

پژوهشگران در مرجع [15] از یک الگوریتم فراابتکاری رقابت امپریال برای آموزش شبکه‌های عصبی در زمینه تشخیص نفوذ استفاده‌کرده‌اند. نتایج روش پیشنهادی آنان عملکرد بسیار بهتری از جنبه سرعت و دقت نسبت به روش‌های آموزشی کلاسیک داشته‌است.

پژوهشگران در مرجع 16]] از رویکرد تشخیص ناهنجاری جهت تعبیه یک سیستم تشخیص نفوذ در رایانش ابری استفاده‌کرده‌اند. همچنین آنان با بررسی پارامترها و نقش ترکیبی پارامترها در تشخیص نفوذ در ابر، به بررسی و ارائه چهارچوب نظری به همراه شبیه‌سازی رفتار مشکوک در ابر پرداخته‌اند.

## ۴. سیستم تشخیص نفوذ مبتنی بر یادگیری عمیق

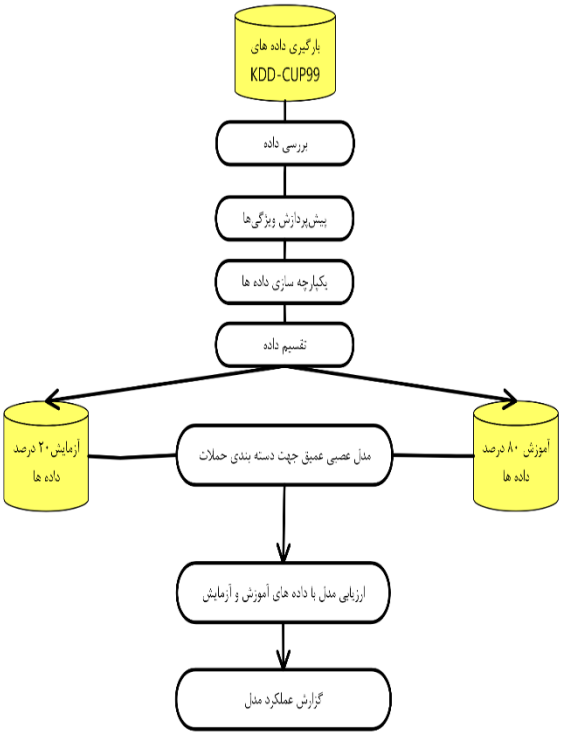
هدف اصلی این پژوهش، استفاده از روش‌ها و تکنیک‌های یادگیری عمیق در زمینه ساختن مدل‌های تشخیص نفوذ است. در زمینه تشخیص نفوذ، هدف ما این است که بتوانیم الگوهایی که نشان‌دهنده فعالیت‌های مشکوک و تهدیدات امنیتی هستند، را شناسایی‌کنیم. برای این منظور، از روش‌های پردازش استنتاجی استفاده‌می‌کنیم که ما را قادرمی‌سازند ویژگی‌های سیستم را به‌صورت خودکار استخراج و تحلیل کنیم. این ویژگی‌ها می‌توانند مشخصه‌هایی مانند الگوهای ترافیک شبکه، الگوهای استفاده از سیستم، الگوهای زمان‌بندی فعالیت‌ها و غیره باشند. سپس با استفاده از دسته‌بندی‌کننده‌های یادگیری عمیق، ما می‌توانیم این الگوها را تشخیص‌داده و رفتارهای غیرعادی و سناریوهای سوءاستفاده را شناسایی‌کنیم. با استفاده از روش‌های یادگیری عمیق، می‌توان مدل‌هایی را بسازیم که به‌طور خودکار و بادقت بالا، ویژگی‌های مفید و قابل‌توجه را از داده‌ها استخراج‌کنند. به‌عبارت‌دیگر، این مدل‌ها قادرند با تحلیل و تشخیص الگوهای پیچیده در داده‌ها، به‌طور خودکار تغییرات و تهدیدات امنیتی را تشخیص‌دهند. استفاده از روش‌ها و تکنیک‌های یادگیری عمیق در مدل‌سازی تشخیص نفوذ، امکان تشخیص بهتر و دقیق‌تر تهدیدات امنیتی را فراهم‌می‌کند و به ما کمک‌می‌کند تا بهترین راهکارهای امنیتی را برای حفاظت از سیستم‌ها و شبکه‌ها پیداکنیم.

## ۵. داده‌های تشخیص نفوذ

به‌طورکلی، بررسی و تحلیل خصوصیات و رفتار حمله‌ها و نفوذکنندگان در شبکه‌های کامپیوتری بسیار پیچیده است و نیاز به تخصص و تجربه کارشناسان دارد. با پیشرفت شبکه‌های کامپیوتری، تعداد حمله‌ها و نفوذکنندگان نیز روزبه‌روز بیشتر می‌شود. درواقع، دانشی که از تجربه و آموزش افراد خبره به‌دست‌می‌آید، با گذر زمان منسوخ و نیازمند به‌روزرسانی است. همچنین، به‌دلیل تعداد بیشتر حمله‌ها و تنوع روش‌های نفوذ، نیاز به شخص خبره در تشخیص و پیشگیری از این حملات همواره محسوس است. گروه IST [۱۷] در آزمایشگاه Lincoln MIT تحت نظارت سازمان پژوهشی پیشرفته پروژه‌های دفاعی [۱۸] و دفتر تحقیقاتی نیروی هوایی آمریکا و سازمان ملی بهداشت و امنیت، اولین مجموعه‌داده استاندارد برای بررسی و ارزیابی سیستم‌های تشخیص نفوذ جمع‌آوری‌کردند. این داده‌ها در طول چند هفته در یک شبیه‌سازی برای آزمایش سیستم تشخیص نفوذ DARPA استفاده‌شدند. این مجموعه‌داده‌ها بر اساس سال جمع‌آوری اطلاعات ۱۹۹۸، ۱۹۹۹ و ۲۰۰۰ طبقه‌بندی‌شده‌است. در این داده‌ها، علاوه بر داده‌های جمع‌آوری‌شده از شبکه، رویدادهای ثبت‌شده در ماشین‌های موجود در شبکه آزمایشی (مانند سیستم‌عامل‌های لینوکس، BSD، Solaris و ویندوز) نیز درنظرگرفته‌شده‌است. مجموعه‌داده‌های سال ۱۹۹۹ توسط یکی از اعضای گروه IST تحت نظارت لینکولن و در حین انجام پروژه دکتری جمع‌آوری‌شدند [14]. در مسابقه بین‌المللی سوم کشف دانش و داده‌کاوی KDD CUP'99 که در پنجمین کنفرانس مربوط به این حوزه برگزارشد، از این مجموعه‌داده‌ها استفاده‌شد. هدف از این مسابقه طراحی یک موتور تشخیص نفوذ با بهترین عملکرد بود. این بانک اطلاعاتی شامل رکوردهای استاندارد است که شبیه‌سازی حملات و نفوذهایی را در یک شبکه نظامی شبیه‌سازی می‌کند.

## ۶. روش پیشنهادی

در این پروژه، تمرکز ما بر روی نتایج آزمایش‌ها، پیش‌پردازش و الگوریتم‌های شبکه‌های عصبی عمیق و یک روش ترکیبی بر روی مجموعه‌داده KDDCUP99 است. داده‌های مطرح‌شده به ۵ کلاس تقسیم‌خواهیم‌کرد که ۴ کلاس حاوی حملات و یک کلاس حاوی ترافیک عادی است. برای این منظور، مراحل زیر انجام‌خواهندشد. شکل ۱ روش پیشنهادی را نمایش‌می‌دهد.




**شکل ۱: روش پیشنهادی**

- بارگیری داده‌ها: مجموعه‌داده KDD CUP'99 از سایت معتبر دریافت‌شده‌است.
- پیش‌پردازش داده: پیش‌پردازش داده‌ها جهت استفاده در مدل‌های شبکه عصبی موردنیاز است. این مرحله شامل تبدیل ویژگی‌ها، نرمال‌سازی داده و حذف داده‌های نامربوط است.
- الگوریتم‌های شبکه عصبی عمیق: مدل‌های شبکه عصبی عمیق را با استفاده از معماری‌هایی مانند شبکه‌های MLP، CNN، LSTM و GRU آموزش خواهنددید. این مدل‌ها می‌توانند ویژگی‌های مهم را از داده استخراج‌کرده و حملات را تشخیص‌دهند.
- تقسیم داده‌ها: نسبت تقسیم داده نیز ۸۰٪ آموزش و ۲۰٪ آزمایش درنظرگرفته‌شده‌اند.
- روش ترکیبی: در این مرحله، ترکیب شبکه‌های عصبی با یکدیگر انجام‌خواهدشد و ویژگی‌ها را از دو یا چند روش مختلف استخراج‌می‌کنند و آن‌ها را با یکدیگر ترکیب‌می‌کنند. این روش می‌تواند به‌دقت و عملکرد سیستم کمک‌کند.
- آزمایش و ارزیابی: مدل‌های خود را بر روی مجموعه‌داده KDD CUP'99 آزمایش خواهیم‌نمود و نتایج را در قسمت بعدی مورد تحلیل و ارزیابی خواهدشد. ما از معیارهایی مانند دقت، درستی (صحت) و فراخوانی، امتیاز F و AUC استفاده‌خواهدشد. درنهایت از زبان برنامه‌نویسی پایتون و ابزار

Google Colab برای شبیه‌سازی و ایجاد مدل‌های دسته‌بندی استفاده‌خواهیم‌کرد.

## ۷. ابزار پیاده‌سازی

در این پژوهش از Google Colab استفاده‌می‌شود که یک سرویس ابری است که توسط گوگل ارائه‌می‌شود و امکان‌می‌دهد کدهای پایتون را در محیط آنلاین اجراکرد. این سرویس بر پایه Jupyter Notebook بناشده‌است و از زبان برنامه‌نویسی پایتون به‌صورت مستقیم پشتیبانی‌می‌کند. Google Colab یک محیط توسعه محاسباتی قدرتمند است که بر روی سرورهای گوگل اجرامی‌شود و به شما امکان‌می‌دهد بدون نیاز به نصب هیچ نرم‌افزاری، کدهای پایتون را نوشته و اجراکرد. این محیط شامل ابزارهایی مانند بسته‌های محبوب پایتون، دستورالعمل‌های سیستمی و امکان استفاده از منابع محاسباتی قوی مانند واحدهای پردازش گرافیکی می‌باشد. این سرویس امکاناتی مانند دسترسی به سرویس‌های ابری، اشتراک‌گذاری کدها و همکاری چندنفره را فراهم‌می‌کند. همچنین، امکاناتی مانند ذخیره و بازیابی نوت‌بوک‌ها، دسترسی به دیتاست‌های محبوب مانند TensorFlow و PyTorch، و قابلیت اجرای کدهای پایتون در سرورهای گوگل نیز در این سرویس وجوددارد.

## ۸ .ارزیابی روش‌های یادگیری عمیق

در جدول ۱ نتایج ارزیابی روش‌های یادگیری عمیق با مجموعه‌داده KDD CUP'99 نشان‌داده‌شده‌است. در این پژوهش پارامترهای مختلفی آزمایش و با یکدیگر مقایسه‌شده‌اند.

**جدول ۱: ارزیابی روش یادگیری عمیق با مجموعه‌داده** KDD CUP'99

| Method | Class | Precision | Recall | F-Measure | AUC | Accuracy | Error |
|---|---|---|---|---|---|---|---|
| MLP | DoS | ۹۹,۸۶ | ۹۹,۹۹ | ۹۹,۹۲ | ۹۹,۹۹ | ۹۹,۷۷ | ۰,۲۳ |
| | Normal | ۹۹,۶۷ | ۹۹,۲۶ | ۹۹,۴۷ | ۹۹,۹۹ | | |
| | Probe | ۹۹,۵۰ | ۹۶,۲۶ | ۹۷,۸۵ | ۹۹,۹۹ | | |
| | R2L | ۷۹,۴۵ | ۸۵,۰۶ | ۸۲,۱۶ | ۹۹,۹۴ | | |
| | U2R | ۱۰۰ | ۰ | ۰ | ۹۹,۷۳ | | |
| | Average | ۹۵,۶۹ | ۷۶,۱۱ | ۷۵,۸۸ | ۹۹,۹۳ | | |
| CNN | DoS | ۹۹,۹۷ | ۹۹,۹۹ | ۹۹,۹۸ | ۹۹,۹۹ | ۹۹,۸۲ | ۰,۱۸ |
| | Normal | ۹۹,۷۰ | ۹۹,۴۵ | ۹۹,۵۸ | ۹۹,۹۹ | | |
| | Probe | ۹۱,۴۷ | ۹۸,۱۹ | ۹۴,۷۱ | ۹۹,۹۹ | | |
| | R2L | ۹۰,۸۶ | ۸۲,۵۷ | ۸۶,۵۲ | ۹۹,۹۱ | | |
| | U2R | ۳۳,۳۳ | ۹۰,۹۰ | ۱۴,۲۸ | ۹۹,۳۶ | | |
| | Average | ۸۳,۰۷ | ۷۷,۸۶ | ۷۹,۰۱ | ۹۹,۸۵ | | |
| LSTM | DoS | ۹۹,۹۹ | ۹۹,۹۷ | ۹۹,۹۸ | ۹۹,۹۹ | ۹۹,۸۸ | ۰,۱۲ |
| | Normal | ۹۹,۵۹ | ۹۹,۸۴ | ۹۹,۷۲ | ۹۹,۹۹ | | |
| | Probe | ۹۸,۷۷ | ۹۷,۴۶ | ۹۸,۱۲ | ۹۹,۹۹ | | |
| | R2L | ۹۱,۲۰ | ۸۱,۷۴ | ۸۶,۲۱ | ۹۹,۹۱ | | |
| | U2R | ۴۲,۸۵ | ۲۷,۲۷ | ۳۳,۳۳ | ۹۹,۲۶ | | |
| | Average | ۸۶,۴۸ | ۸۱,۲۶ | ۸۳,۴۷ | ۹۹,۸۳ | | |
| GRU | DoS | ۹۹,۹۴ | ۹۹,۹۸ | ۹۹,۹۶ | ۹۹,۹۹ | ۹۹,۸۴ | ۰,۱۶ |
| | Normal | ۹۹,۶۴ | ۹۹,۶۵ | ۹۹,۶۵ | ۹۹,۹۹ | | |
| | Probe | ۹۹,۵۰ | ۹۶,۷۴ | ۹۸,۱۰ | ۹۹,۹۸ | | |
| | R2L | ۸۳,۱۹ | ۸۲,۱۵ | ۸۲,۶۷ | ۹۹,۸۷ | | |
| | U2R | ۵۰,۰۰ | ۲۷,۲۷ | ۳۵,۲۹ | ۹۸,۲۰ | | |
| | Average | ۸۶,۴۵ | ۸۱,۱۶ | ۸۳,۱۴ | ۹۹,۶۱ | | |

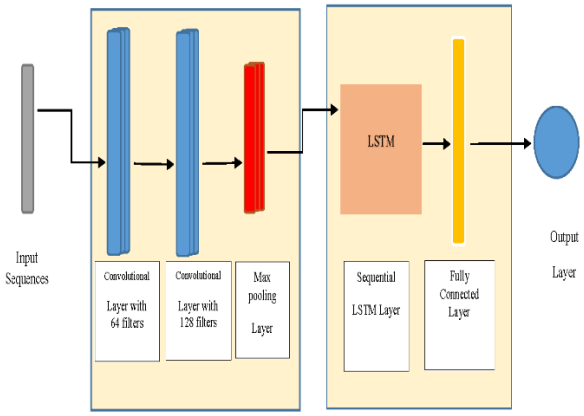
باتوجه‌به جدول ارزیابی جدول ۱ بالاترین کارایی برای روش LSTM با مجموعه‌داده KDD CUP'99 مقایسه‌شد و پارامترهای Precision، Recall، F-Measure، AUC، Accuracy و Error برای هر کلاس ارزیابی‌شد.

- بالاترین مقدار Precision برای کلاس DoS برابر ۹۹,۹۹٪ مشاهده شده است.
- بالاترین مقدار Recall برای کلاس DoS برابر ۹۹,۹۷٪ مشاهده‌شده‌است.
- بالاترین مقدار F-Measure برای کلاس DoS برابر ۹۹,۹۸٪ مشاهده‌شده‌است.
- ارزیابی درستی (صحت) کلی مدل برابر ۹۹,۸۸٪ و خطای دسته‌بندی ۰,۱۲٪ است.
- ارزیابی میانگین AUC در روشLSTM وMLP بالاترین مقدار را داراست.

با بررسی این مقادیر، می‌توان‌نتیجه‌گرفت که روش LSTM در مجموعه‌داده KDD CUP'99 عملکرد بهتری داشته‌است و همچنین روش GRU نیز بعد از LSTM کارایی بهتری دارد.

## ۹. ارزیابی روش‌های یادگیری عمیق ترکیبی

در زیر شکل شماره ۲ نمایی از یادگیری عمیق ترکیبی پیشنهادی CNN- LSTM را نشان‌می‌دهد. در روش پیشنهادی از دو لایه تشکیل‌شده‌است یکی CNN و دیگریLSTM است و همچنین جدول ۲ نتایج ارزیابی روش‌های یادگیری عمیق ترکیبی GRU -CNN و CNN- LSTM با مجموعه‌داده KDD CUP'99 نشان‌داده‌شده‌است. در این پژوهش پارامترهای مختلفی آزمایش و با یکدیگر مقایسه‌شده‌اند.




**شکل ۲: روش یادگیری عمیق ترکیبی CNN- LSTM**

**جدول ۲: ارزیابی روش یادگیری عمیق ترکیبی با مجموعه‌داده KDD CUP'99**

| Method | Class | Precision | Recall | F-Measure | AUC | Accuracy | Error |
|---|---|---|---|---|---|---|---|
| CNN- GRU | DoS | ۹۹,۹۸ | ۹۹,۹۹ | ۹۹,۹۹ | ۹۹,۹۹ | ۹۹,۹۲ | ۰,۰۸ |
| | Normal | ۹۹,۸۲ | ۹۹,۸۱ | ۹۹,۸۲ | ۹۹,۹۹ | | |
| | Probe | ۹۹,۷۵ | ۹۸,۰۷ | ۹۸,۹۰ | ۹۹,۹۹ | | |
| | R2L | ۸۹,۹۷ | ۹۳,۷۷ | ۹۱,۳۱ | ۹۹,۹۵ | | |
| | U2R | ۶۲,۵۰ | ۴۵,۴۵ | ۵۲,۶۳ | ۹۹,۹۳ | | |
| | Average | ۹۰,۲۱ | ۸۷,۴۲ | ۸۸,۵۳ | ۹۹,۹۷ | | |
| CNN- LSTM | DoS | ۹۹,۹۹ | ۹۹,۹۹ | ۹۹,۹۹ | ۹۹,۹۹ | ۹۹,۹۵ | ۰,۰۵ |
| | Normal | ۹۹,۸۲ | ۹۹,۹۶ | ۹۹,۸۹ | ۹۹,۹۹ | | |
| | Probe | ۹۹,۷۵ | ۹۸,۶۷ | ۹۹,۲۱ | ۹۹,۹۷ | | |
| | R2L | ۹۷,۳۶ | ۹۲,۱۱ | ۹۴,۶۶ | ۹۹,۲۳ | | |
| | U2R | ۸۳,۳۳ | ۴۵,۴۵ | ۵۸,۸۲ | ۹۹,۴۴ | | |
| | Average | ۹۶,۰۵ | ۸۷,۲۴ | ۹۰,۵۲ | ۹۹,۸۶ | | |

باتوجه‌به جدول ارزیابی جدول ۲ بالاترین کارایی برای روش ترکیبی CNN-LSTM با مجموعه‌داده KDD CUP'99 مقایسه شد و پارامترهای Precision، Recall، F-Measure، Accuracy و Error برای هر کلاس ارزیابی‌شد.

- بالاترین مقدار Precision برای کلاس DoS برابر ۹۹,۹۹٪، برای کلاس Normal برابر ۹۹,۸۲٪ و برای کلاس Probe برابر ۹۹,۷۵٪ مشاهده‌شده‌است.
- بالاترین مقدار Recall برای کلاس DoS برابر ۹۹,۹۹٪ و برای کلاس Normal برابر ۹۹,۹۶٪ مشاهده‌شده‌است.
- بالاترین مقدار F-Measure برای کلاس DoS برابر ۹۹,۹۹٪، برای کلاس Normal برابر ۹۹,۸۹٪ و برای کلاس Probe برابر ۹۹,۲۱٪ مشاهده‌شده‌است.
- درستی مدل برای مجموعه‌داده KDD CUP'99 برابر ۹۹,۹۵٪ و خطای دسته‌بندی برابر ۰,۰۵٪ است.

## ۱۰. نتیجه‌گیری

روش‌های شبکه‌های عصبی عمیق MLP، CNN، LSTM، GRU، CNN-GRU و CNN-LSTM در این پژوهش استفاده شده‌اند که قابلیت تشخیص و استخراج ویژگی‌های پیچیده‌تر را دارند. با استفاده از این شبکه‌ها، می‌توان الگوهای پنهان و پیچیده‌تر را در داده‌ها شناسایی کرد و به‌عنوان ویژگی‌های مهم در دسته‌بندی استفاده‌کرد؛ بنابراین، با استفاده از روش‌های ترکیبی شبکه‌های عصبی عمیق، می‌توان نتایج بهتری در تشخیص ویژگی‌ها و پیش‌بینی داده‌ها کسب‌کرد. این روش‌ها از قدرت استخراج و تشخیص ویژگی‌ها در شبکه‌های عصبی عمیق بهره‌می‌برند و با ترکیب نتایج و ویژگی‌های مختلف، دقت و عملکرد مدل را بهبودمی‌بخشند. باتوجه‌به نتایج حاصل، دو روش ترکیبی CNN-LSTM و CNN-GRU به‌ترتیب ۹۹,۹۵٪ و ۹۹,۹۲٪ بر روی مجموعه‌داده KDD CUP'99 کارایی بسیار خوبی را ارائه داده‌اند. در بین این روش‌ها، ممکن است به تفاوت‌های کوچک در عملکرد برخی از پارامترها برای کلاس‌ها دست‌یافت، اما همچنان هر دو روش قابل‌قبول هستند؛ بنابراین، می‌توان‌نتیجه‌گرفت که در مجموعه‌داده KDD CUP'99 روش ترکیبی CNN-LSTM عملکرد مناسبی دارد. انتخاب روش به عوامل دیگری مانند مقدار داده‌ها، زمان اجرا، پیچیدگی مدل و دیگر محدودیت‌ها بستگی دارد.

## References


[1] Anderson, J. P. (1980). Computer security threat monitoring and surveillance. Technical Report, James P. Anderson Company.

[2] Ashoor, A. S., & Gore, S. (2011). Importance of intrusion detection system (IDS). International Journal of Scientific and Engineering Research, 2(1), 1-4.


- ارزیابی میانگین AUC در روشCNN-LS برابر ۹۹,۸۶٪ است.

همچنین روش CNN-GRU نیز بعد از CNN-LSTM کارایی بهتری دارد.

- بالاترین مقدار Precision برای کلاس DoS برابر ۹۹,۹۸٪ و کلاس Normal برابر ۹۹,۸۲٪ مشاهده‌شده‌است.
- بالاترین مقدار Recall برای کلاس DoS برابر ۹۹,۹۹٪ و کلاس Normal برابر ۹۹,۸۱٪ مشاهده‌شده‌است.
- بالاترین مقدار F-Measure برای کلاس DoS برابر ۹۹,۹۹٪ و کلاس Normal برابر ۹۹,۸۲٪ مشاهده‌شده‌است.
- ارزیابی درستی کلی مدل برابر ۹۹,۹۲٪ و خطای دسته‌بندی ۰,۰۸٪ است.
- ارزیابی میانگین AUC در روشCNN-GRU برابر ۹۹,۹۷٪ است.


[3] Michie, D., Spiegelhalter, D. J., Taylor, C. C., & Campbell, J. (Eds.). (1995). Machine learning, neural and statistical classification. Ellis Horwood.

[4] Depren, O., Topallar, M., Anarim, E., & Ciliz, M. K. (2005). An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. Expert systems with Applications, 29(4), 713-722.

[5] Kasongo, S. M., & Sun, Y. (2020). A deep long short-term memory based classifier for wireless intrusion detection system. ICT Express, 6(2), 98-103.

[6] Yang, H., & Wang, F. (2019). Wireless network intrusion detection based on improved convolutional neural network. Ieee Access, 7, 64366-64374 .

[7] 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.

[8] 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.

[9] Hao, Y., Sheng, Y., & Wang, J. (2019). Variant gated recurrent units with encoders to preprocess packets for payload-aware intrusion detection. IEEE Access, 7, 49985-49998.

[10] 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, 19(11), 2528.

[11] Wu, K., Chen, Z., & Li, W. (2018). A novel intrusion detection model for a massive network using convolutional neural networks. Ieee Access, 6, 50850-50859.

[12] Wang, H., Cao, Z., & Hong, B. (2020). A network intrusion detection system based on convolutional neural network. Journal of Intelligent & Fuzzy Systems, 38(6), 7623-7637.

[13] Bui, N. T., Jung, J. H., & Kim, S. (2022). DeepLearningIDS: A deep learning-based intrusion detection system for software-defined networks.
[14] Stolfo, S. J., Fan, W., Lee, W., Prodromidis, A., & Chan, P. K. (2000). Cost-based Modeling and Evaluation for Data Mining with Application to Fraud and Intrusion Detection: Results from the JAM Project. Data Mining and Knowledge Discovery, 4(3), 225-243.
[15] Nazarpour, M., Nezafati, N., & Shokouhyar, S. (2023). Using the Modified Colonial Competition Algorithm to Increase the Speed and Accuracy of the Intelligent Intrusion Detection System.Intelligent Multimedia Processing and Communication Systems (IMPCS), 4(1) ,1-10.
[16] Ghaffari, A., & Hossinnezhad, R. (2022).Intrusions detection system in the cloud computing using heterogeneity detection technique.Intelligent Multimedia Processing and Communication Systems (IMPCS),3(1),37-46.

## پی‌نوشت

[1] intrusion detection systems
[2] Intrusion Detection System
[3] rule-based
[4] machine learning
[5] event-based
[6] flow-based
[7] Deep Learning
[8] Artificial Neural Networks
[9] Deep neural networks
[10] Improved Convolution neural networks (ICNN)
[11] Deep Belief Network
[12] Recurrent Neural Network
[13] Feed Forward Neural Network
[14] Gated Recurrent Units( GRU)
[15] improved conditional Variational Auto Encoder
[16] Software-Defined Networks
[17] Intelligent Systems and Technology
[18] DARPA