

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

Mohsen Roknaldini¹, Erfaneh Noroozi^{*1}

1. Department of Computer Engineering, Qeshm branch, Islamic Azad university, Qeshm, Iran.
Rokn.bmh@gmail.com
2. Assistant Professor, Department of Computer Engineering, Sepidan branch, Islamic Azad university, Fars, Iran.
**Corresponding Author, Erfaneh.Noroozi@iau.ir*

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.



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

دوره چهارم، زمستان ۱۴۰۲
شماره چهارم، صص: ۵۷-۶۵

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

محسن رکن‌الدینی^۱، عرفانه نوروزی^{۲*}

۱. گروه مهندسی کامپیوتر، واحد قشم، دانشگاه آزاد اسلامی، قشم، ایران. Rokn.bmh@gmail.com
۲. استادیار، گروه مهندسی کامپیوتر، واحد سپیدان، دانشگاه آزاد اسلامی، فارس، ایران. (نویسنده مسئول)
Erfaneh.Noroozi@iaui.ac.ir

چکیده: در این پژوهش به بررسی و ارائه یک روش ترکیبی شبکه‌های عصبی عمیق جهت جلوگیری از نفوذ در شبکه‌های کامپیوتری پرداخته می‌شود. 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 ارائه شده است. این روش با استفاده از شبکه‌های عصبی عمیق، ویژگی‌های پیچیده‌تر را تشخیص می‌دهد و عملکرد مدل را بهبود می‌بخشد. 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 بهبود می‌یابد. نتایج شبیه‌سازی‌ها نشان می‌دهد 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 معرفی شدند که به منظور تحلیل و ارزیابی کلی بر روی مجموعه داده KDD CUP'99 آزمایش شد. دو رویکرد ترکیبی، صحت بالا و خطای دسته‌بندی کمتری نسبت به دیگر روش‌های معرفی شده، دارند؛ بنابراین، می‌توان نتیجه گرفت 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

می‌دهد. درحالی‌که در رویکرد جریان محور، سیستم بر اساس تحلیل جریان ترافیک شبکه و شناسایی الگوهای مشخص در جریان داده‌ها، حملات را تشخیص می‌دهد. استفاده از سیستم تشخیص نفوذ در سازمان‌ها و شبکه‌ها به‌طور گسترده‌ای افزایش یافته‌است، زیرا امنیت اطلاعات و سیستم‌ها در مقابل تهدیدات روزافزون حائز اهمیت است. با استفاده از سیستم تشخیص نفوذ، سازمان‌ها قادر خواهند بود تا به‌صورت سریع و مؤثر به حملات و تهدیدهای امنیتی پاسخ‌دهند و از آسیب‌های جدی به سیستم‌ها جلوگیری کنند [4].

۳. مروری بر کلیات پژوهش‌ها

ایده‌های تحقیقاتی زیادی در رابطه با سیستم‌های تشخیص نفوذ با استفاده از تکنیک‌های یادگیری ماشین، تکنیک‌های یادگیری عمیق^۷ و الگوریتم‌های گروهی و تکاملی ارائه شده‌اند. 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 طراحی کردند. برخلاف شبکه‌های عصبی مصنوعی^۸، شبکه‌های عصبی عمیق^۹ ممکن است حاوی صدها لایه پنهان باشند. آنان در پژوهش خود از مجموعه داده NSL-KDD استفاده نمودند. آن‌ها در مدل خود از استخراج ویژگی استفاده تا بعد ورودی را کاهش دهند. آن‌ها دسته‌بندی حملات خود را با مجموعه داده‌های دودویی و چند دسته‌ای انجام دادند. مدل آن‌ها در مقایسه با روش‌هایی مانند SVM، Decision Tree و KNN بهتر عمل می‌کند.

در مرجع [6] یک روش یادگیری عمیق مبتنی بر شبکه عصبی معرفی کردند که در این مدل شبکه عصبی پیچشی بهبود یافته‌ای^{۱۰} برای سیستم تشخیص نفوذ طراحی کردند. مدل شبکه عصبی پیچشی بهبود یافته از پنج لایه کانولوشن، چهار لایه کاملاً یکپارچه، دو لایه ادغام و یک لایه SoftMax تشکیل شده‌است. پژوهشگران در این مطالعه خود، از مجموعه داده NSL-KDD برای ارزیابی عملکرد مدل آن‌ها استفاده کردند. آموزش مدل شبکه عصبی پیچشی بهبود یافته 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 معرفی کرده‌اند. تفاوت اساسی بین روش شبکه عصبی بازگشتی‌ها و سایر شبکه عصبی روبه‌جلو^{۱۳}، توانایی به‌خاطر سپردن اطلاعات قبلی و استفاده از آن در لایه فعلی است. مدل پیشنهادی آنان بر روی مجموعه داده NSL-KDD مورد ارزیابی قرار گرفت که نشان می‌دهد 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.

امروزه شبکه‌های کامپیوتری تأثیرات زیادی بر زندگی روزمره ما دارند این امر باعث شده که امنیت سایبری به یک زمینه مهم تحقیقاتی تبدیل شود. تکنیک‌های امنیت سایبری عمدتاً شامل نرم‌افزارهای ضد ویروس، فایروال‌ها و سیستم‌های تشخیص نفوذ^۱ هستند. این تکنیک‌ها شبکه‌ها را از حملات داخلی و خارجی محافظت می‌کنند. 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 ایفا می‌کنند. اولین سیستم تشخیص نفوذ در سال ۱۹۸۰ ارائه شد [1]. از آن زمان، بسیاری از سیستم‌های تشخیص نفوذ معرفی شده‌اند. با این حال، بسیاری از سیستم‌های تشخیص نفوذ هنوز از نرخ هشدار نادرست بالایی رنج می‌برند و هشدارهای زیادی را برای موقعیت‌های غیرتهدیدکننده ایجاد می‌کنند که بار تحلیلگران امنیتی را بالای برد و می‌تواند باعث نادیده گرفته شدن حملات خطرناک شود [2]. بنابراین، بسیاری از محققان بر روی توسعه سیستم‌های تشخیص نفوذ با نرخ تشخیص بالاتر و کاهش نرخ هشدار نادرست تمرکز کرده‌اند. مشکل دیگر سیستم‌های تشخیص نفوذ موجود این است که آن‌ها توانایی تشخیص حملات ناشناخته را ندارند. از آنجا که محیط‌های شبکه به سرعت تغییر می‌کنند، انواع حملات و حملات جدید به‌طور مداوم ظاهر می‌شوند. بنابراین، توسعه سیستم‌های تشخیص نفوذ می‌تواند حملات ناشناخته را شناسایی کند امری ضروری است. برای حل مشکلات ذکر شده، 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 مجموعه داده‌های عظیم کشف کند [3].

۲. سیستم تشخیص نفوذ

سیستم تشخیص نفوذ یا (IDS) 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^۲ یا مبتنی بر یادگیری^۳ عمل کند. در رویکرد قوانین، الگوریتم‌ها و قوانینی که توسط امنیت‌گذاران و تحلیل‌گران تهیه شده‌اند، برای تشخیص الگوها و شناسایی حملات استفاده می‌شود. اما در رویکرد یادگیری، الگوریتم‌های یادگیری ماشینی و شبکه‌های عصبی عمیق به‌کار گرفته می‌شوند تا بتوانند الگوها و ویژگی‌های مربوط به حملات را از داده‌های واقعی استخراج کنند [4].

سیستم تشخیص نفوذ می‌تواند به‌صورت رویدادمحور^۵ و یا جریان محور^۶ عمل کند. 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

ساخته شده است. این سیستم از پیش‌پردازش داده‌ها، آموزش شبکه عصبی، تست شبکه و پاسخ نفوذ بر اساس پلتفرم لینوکس تشکیل شده است. در نهایت با مجموعه داده‌های NSL-KDD و آزمایش جریان واقعی شبکه، نشان دادند 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^{۱۶} 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 استفاده می‌شوند تا ویژگی‌های مختلف بسته‌های شبکه را استخراج کنند و به تشخیص نفوذ در شبکه کمک کنند. نتایج آزمایش‌ها نشان می‌دهد که سیستم پیشنهادی دقت بالا و عملکرد قابل قبولی در تشخیص نفوذ در شبکه‌های تعریف شده توسط نرم‌افزار دارد.

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

پژوهشگران در مرجع [16] از رویکرد تشخیص ناهنجاری جهت تعبیه یک سیستم تشخیص نفوذ در رایانش ابری استفاده کرده‌اند. 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 شناسایی کنیم. برای این منظور، از روش‌های پردازش استنتاجی استفاده می‌کنیم که ما را قادر می‌سازند ویژگی‌های سیستم را به صورت 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 تشخیص داده و رفتارهای غیرعادی و سناریوهای سوءاستفاده را شناسایی کنیم. با استفاده از روش‌های یادگیری عمیق، می‌توان مدل‌هایی را بسازیم که به طور خودکار و با دقت بالا، ویژگی‌های مفید و قابل توجه را از داده‌ها استخراج کنند. به عبارت دیگر، این مدل‌ها قادرند با تحلیل و تشخیص الگوهای پیچیده در داده‌ها، به طور خودکار تغییرات و تهدیدات امنیتی را تشخیص دهند. استفاده از روش‌ها و تکنیک‌های یادگیری عمیق در مدل‌سازی تشخیص نفوذ، امکان تشخیص بهتر و دقیق‌تر تهدیدات امنیتی را فراهم می‌کند و به ما کمک می‌کند تا بهترین راهکارهای امنیتی را برای حفاظت از سیستم‌ها و شبکه‌ها پیدا کنیم.

در مرجع [8] یک معماری مبتنی بر هوش مصنوعی با استفاده از مدل شبکه عصبی پیچشی بهینه بر روی داده‌های زمان واقعی ارائه کردند. آن‌ها عملکرد مدل خود را با استفاده از پارامترهایی مانند F-Score، کارایی، دقت، ویژگی و فراخوانی بر روی دو مجموعه داده اندازه‌گیری کردند. مجموعه داده‌های CSIC-2010 و CICIDS-2017 آن‌ها گزارش دادند که سیستم تشخیص نفوذ مبتنی بر هوش مصنوعی می‌تواند بین ترافیک معمولی و غیرعادی تشخیص دهد؛ ولی نمی‌تواند از سیستم تشخیص نفوذ مبتنی بر امضا استفاده کند. علاوه بر این، آن‌ها ادعا کرده‌اند که مدل پیشنهادی می‌تواند قوانین Snort را برای سیستم تشخیص نفوذ که از امضا استفاده می‌کند، تقویت کند.

در مرجع [9] از واحد بازگشتی گیتی (دروازه‌دار)^{۱۴} برای رمزگذاری و توسعه یک سیستم تشخیص نفوذ استفاده شد. واحد بازگشتی گیتی مکانیزم دروازه‌ای است که با شبکه‌های عصبی مکرر استفاده می‌شود. آنان از دو نوع واحد بازگشتی گیتی کدگذاری شده و واحد بازگشتی گیتی دودویی کدگذاری شده استفاده کردند. پژوهش آنان ادعا می‌کند که واحد بازگشتی گیتی رمزگذاری شده نمایش بهتری از ورودی‌ها را ارائه می‌دهد در حالی که واحد بازگشتی گیتی دودویی رمزگذاری شده، همراه با نمایش بهتر ورودی‌ها، زمان دسترسی و اندازه حافظه را نیز کاهش می‌دهد.

در مرجع [10] یک مدل تشخیص نفوذ جدید ترکیبی پیشنهاد کرده‌اند که شامل یک شبکه عصبی عمیق و یک رمزگذار خودکار شرطی بهبودیافته^{۱۵} است. روش پیشنهادی برای یادگیری و کشف و نمایش‌های پراکنده بین ویژگی‌های داده‌های شبکه و کلاس‌های حملات استفاده می‌شود. رمزگشای آموزش دیده نمونه‌های حمله جدیدی را با توجه به دسته‌های نفوذ مشخص شده تولید می‌کند تا داده‌های آموزشی را متعادل کند و تنوع نمونه‌های آموزشی را افزایش دهد و در نتیجه نرخ تشخیص حملات نامتعادل را بهبود بخشد. آنان از مجموعه داده‌های NSL-KDD و UNSW-NB15 برای ارزیابی عملکرد روش پیشنهادی استفاده می‌کنند. 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 ارائه کردند که برای انتخاب خودکار ویژگی‌ها از مجموعه داده خام استفاده کردند. ضریب وزن و تابع هزینه هر کلاس را بر اساس اعداد آن تنظیم کردند تا مشکل مجموعه داده نامتعادل حل شود. این مدل نرخ هشدار کاذب را کاهش می‌دهد و دقت کلاس را بهبود می‌بخشد. آنان از مجموعه داده استاندارد NSL-KDD برای ارزیابی عملکرد مدل CNN پیشنهادی استفاده کرده‌اند. نتایج شبیه‌سازی آنان نشان می‌دهد که دقت، نرخ هشدار کاذب و هزینه محاسبه مدل پیشنهادی بهتر از الگوریتم‌های استاندارد سنتی عمل کرده است.

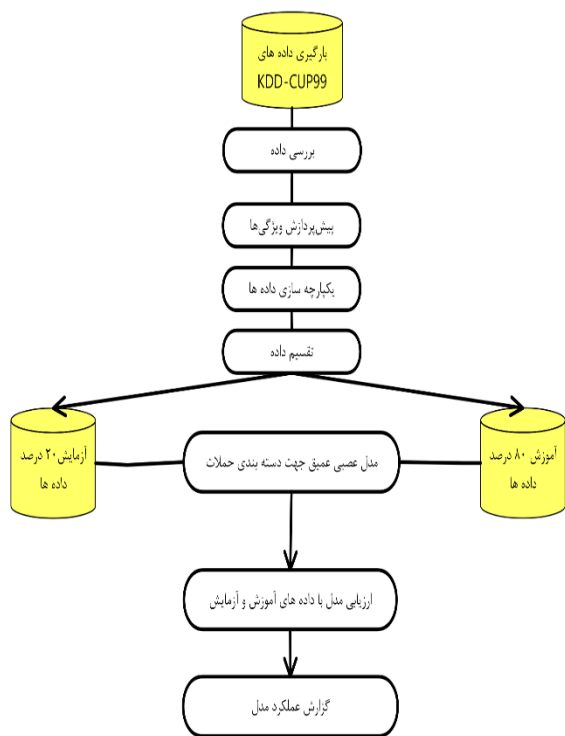
در مرجع [12]، یک روش جدید تشخیص نفوذ مبتنی بر شبکه عصبی پیچشی پیشنهاد شده است. در مرحله دوم، بر اساس رویکرد پیشنهادی، یک سیستم تشخیص نفوذ کارآمد، بلادرنگ و خودکار به نام IDS-CNN طراحی شده است. این سیستم توسط چندین ابزار منبع باز

۵. داده‌های تشخیص نفوذ

به‌طور کلی، 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. در واقع، دانشی که از تجربه و آموزش افراد خبره به‌دست می‌آید، 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 مجموعه داده استاندارد برای بررسی و ارزیابی سیستم‌های تشخیص نفوذ جمع‌آوری کردند. این داده‌ها در طول چند هفته در یک شبیه‌سازی برای آزمایش سیستم تشخیص نفوذ DARPA استفاده شدند. این مجموعه داده‌ها بر اساس سال جمع‌آوری اطلاعات ۱۹۹۸، ۱۹۹۹ و ۲۰۰۰ طبقه‌بندی شده‌است. در این داده‌ها، علاوه بر داده‌های جمع‌آوری شده از شبکه، رویدادهای ثبت شده در ماشین‌های موجود در شبکه آزمایشی (مانند سیستم‌عامل‌های لینوکس، BSD، Solaris، و ویندوز) نیز در نظر گرفته شده‌است. مجموعه داده‌های سال ۱۹۹۹ توسط یکی از اعضای گروه IST تحت نظارت لینکلن و در حین انجام پروژه دکتری جمع‌آوری شدند [14]. در مسابقه بین‌المللی سوم کشف دانش و داده‌کاوی KDD CUP'99 که در پنجمین کنفرانس مربوط به این حوزه برگزار شد، از این مجموعه داده‌ها استفاده شد. 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 مجموعه داده KDD CUP'99 است. داده‌های مطرح شده به ۵ کلاس تقسیم خواهیم کرد که ۴ کلاس حاوی حملات و یک کلاس حاوی ترافیک عادی است. برای این منظور، مراحل زیر انجام خواهند شد. شکل ۱ روش پیشنهادی را نمایش می‌دهد.



شکل ۱: روش پیشنهادی

- بارگیری داده‌ها: مجموعه داده KDD CUP'99 از سایت معتبر دریافت شده‌است.
- پیش‌پردازش داده: پیش‌پردازش داده‌ها جهت استفاده در مدل‌های شبکه عصبی مورد نیاز 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 خواهند دید. این مدل‌ها می‌توانند ویژگی‌های مهم را از داده استخراج کرده و حملات را تشخیص دهند.
- تقسیم داده‌ها: نسبت تقسیم داده نیز ۸۰٪ آموزش و ۲۰٪ آزمایش در نظر گرفته شده‌اند.
- روش ترکیبی: در این مرحله، ترکیب شبکه‌های عصبی با یکدیگر انجام خواهد شد و ویژگی‌ها را از دو یا چند روش مختلف استخراج می‌کنند و آن‌ها را با یکدیگر ترکیب می‌کنند. این روش می‌تواند به دقت و عملکرد سیستم کمک کند.
- آزمایش و ارزیابی: مدل‌های خود را بر روی مجموعه داده KDD CUP'99 آزمایش خواهیم نمود و نتایج را در قسمت بعدی مورد تحلیل و ارزیابی خواهیم داشت. ما از معیارهایی مانند دقت، درستی (صحت) و فراخوانی، امتیاز F و AUC استفاده خواهیم داشت. در نهایت از زبان برنامه‌نویسی پایتون و ابزار

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 چند نفره را فراهم می‌کند. 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 وجود دارد.

۸. ارزیابی روش‌های یادگیری عمیق

در جدول ۱ نتایج ارزیابی روش‌های یادگیری عمیق با مجموعه داده KDD CUP'99 نشان داده شده است. در این پژوهش پارامترهای مختلفی آزمایش و با یکدیگر مقایسه شده‌اند.

جدول ۱: ارزیابی روش یادگیری عمیق با مجموعه داده 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 | . | . | 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 | | |

Google Colab برای شبیه‌سازی و ایجاد مدل‌های دسته‌بندی استفاده خواهیم کرد.

۷. ابزار پیاده‌سازی

در این پژوهش از Google Colab استفاده می‌شود که یک سرویس ابری است که توسط گوگل ارائه می‌شود و امکان می‌دهد کدهای پایتون را در محیط آنلاین اجرا کرد. این سرویس بر پایه Jupyter Notebook بنا شده است و از زبان برنامه‌نویسی پایتون به صورت مستقیم پشتیبانی می‌کند. Google Colab یک محیط توسعه محاسباتی قدرتمند است که بر روی سرورهای گوگل اجرا می‌شود و به شما امکان می‌دهد بدون نیاز به نصب هیچ نرم‌افزاری، کدهای پایتون را نوشته و اجرا کرد. این محیط شامل ابزارهایی مانند بسته‌های محبوب پایتون، دستورالعمل‌های

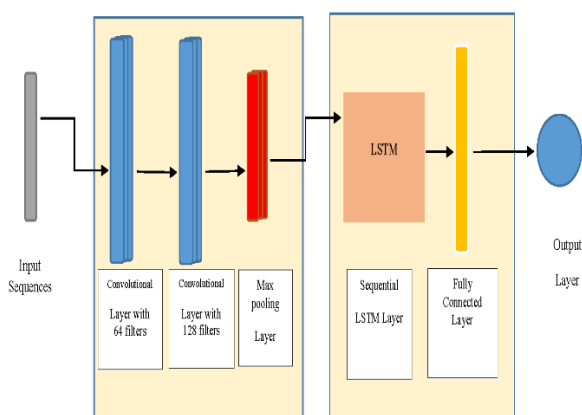
- بالاترین مقدار F-Measure برای کلاس DoS برابر ۹۹٫۹۸٪ مشاهده شده است.
 - ارزیابی درستی (صحت) کلی مدل برابر ۹۹٫۸۸٪ و خطای دسته‌بندی ۰٫۱۲٪ است.
 - ارزیابی میانگین AUC در روش LSTM و MLP بالاترین مقدار را داراست.
- با بررسی این مقادیر، می‌توان نتیجه گرفت که روش LSTM در مجموعه داده KDD CUP'99 عملکرد بهتری داشته است و همچنین روش GRU نیز بعد از LSTM کارایی بهتری دارد.

باتوجه به جدول ارزیابی جدول ۱ بالاترین کارایی برای روش LSTM با مجموعه داده KDD CUP'99 مقایسه شد و پارامترهای Precision، Recall، AUC، F-Measure، Accuracy و Error برای هر کلاس ارزیابی شد.

- بالاترین مقدار Precision برای کلاس DoS برابر ۹۹٫۹۹٪ مشاهده شده است.
- بالاترین مقدار Recall برای کلاس DoS برابر ۹۹٫۹۷٪ مشاهده شده است.

۹. ارزیابی روش‌های یادگیری عمیق ترکیبی

در زیر شکل شماره ۲ نمایی از یادگیری عمیق ترکیبی پیشنهادی در روش پیشنهادی از دو لایه تشکیل شده است یکی CNN و دیگری LSTM است و همچنین جدول ۲ نتایج ارزیابی روش‌های یادگیری عمیق ترکیبی GRU و CNN- LSTM با مجموعه داده KDD CUP'99 نشان داده شده است. در این پژوهش پارامترهای مختلفی آزمایش و یکدیگر مقایسه شده‌اند.



شکل ۲: روش یادگیری عمیق ترکیبی CNN- LSTM

جدول ۲: ارزیابی روش یادگیری عمیق ترکیبی با مجموعه داده 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 | | |

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

- بالاترین مقدار Precision برای کلاس DoS برابر ۹۹٫۹۹٪، برای کلاس Normal برابر ۹۹٫۸۲٪ و برای کلاس Probe برابر ۹۹٫۷۵٪ مشاهده شده است.
- بالاترین مقدار Recall برای کلاس DoS برابر ۹۹٫۹۹٪ و برای کلاس Normal برابر ۹۹٫۹۶٪ مشاهده شده است.
- بالاترین مقدار F-Measure برای کلاس DoS برابر ۹۹٫۹۹٪، برای کلاس Normal برابر ۹۹٫۸۹٪ و برای کلاس Probe برابر ۹۹٫۲۱٪ مشاهده شده است.
- درستی مدل برای مجموعه داده KDD CUP'99 برابر ۹۹٫۹۵٪ و خطای دسته بندی برابر ۰٫۰۵٪ است.

۱۰. نتیجه گیری

روش های شبکه های عصبی عمیق MLP، CNN، LSTM، GRU، CNN-GRU در این پژوهش استفاده شده اند که قابلیت تشخیص و استخراج ویژگی های پیچیده تر را دارند. با استفاده از این شبکه ها، می توان الگوهای پنهان و پیچیده تر را در داده ها شناسایی کرد و به عنوان ویژگی های مهم در دسته بندی استفاده کرد؛ بنابراین، با استفاده از روش های ترکیبی شبکه های عصبی عمیق، می توان نتایج بهتری در تشخیص ویژگی ها و پیش بینی داده ها کسب کرد. این روش ها از قدرت استخراج و تشخیص ویژگی ها در شبکه های عصبی عمیق بهره می برند و با ترکیب نتایج و ویژگی های مختلف، دقت و عملکرد مدل را بهبود می بخشند. باتوجه به نتایج حاصل، دو روش ترکیبی CNN-LSTM و LSTM به ترتیب ۹۹٫۹۵٪ و ۹۹٫۹۲٪ بر روی مجموعه داده KDD CUP'99 کارایی بسیار خوبی را ارائه داده اند. در بین این روش ها، ممکن است به تفاوت های کوچک در عملکرد برخی از پارامترها برای کلاس ها دست یافت، اما همچنان هر دو روش قابل قبول هستند؛ بنابراین، می توان نتیجه گرفت که در مجموعه داده KDD CUP'99 روش ترکیبی CNN-LSTM عملکرد مناسبی دارد. انتخاب روش به عوامل دیگری مانند مقدار داده ها، زمان اجرا، پیچیدگی مدل و دیگر محدودیت ها 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 روش CNN-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٪ مشاهده شده است.
- بالاترین مقدار Recall برای کلاس DoS برابر ۹۹٫۹۹٪ و کلاس Normal برابر ۹۹٫۸۱٪ مشاهده شده است.
- بالاترین مقدار F-Measure برای کلاس DoS برابر ۹۹٫۹۹٪ و کلاس Normal برابر ۹۹٫۸۲٪ مشاهده شده است.
- ارزیابی درستی کلی مدل برابر ۹۹٫۹۲٪ و خطای دسته بندی ۰٫۰۸٪ است.
- ارزیابی میانگین AUC در روش CNN-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.

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.

[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

پی‌نوشت

- 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

- 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