25 th International Conference on
Information Technology, Computer and Telecommunication
Event Place: Tbilisi,Georgia
www.itctconf.ir
بیست و پنجمین کنفرانس بین المللی
فناوری اطلاعات، کامپیوتر و مخابرات | گرجستان
25th International Conference on Information Technology,Computer and Telecommunication
PUBLISH IN JOURNALS — INTERNATIONAL CERTIFICATION

امنیت محاسبات ابری و یادگیری عمیق: رویکرد ANN

و مقایسه با یادگیری ماشینی

عرشیا خان آرموپی دانشجوی کارشناسی مهندسی کامپیوتر دانشگاه رحمان رامسر **امیرعلی سعادت** دانشجوی

کارشناسی مهندسی کامپیوتر دانشگاه رحمان رامسر

محمد رستمی دانشجوی کارشناسی مهندسی کامپیوتر دانشگاه رحمان رامسر

چکیده:

تکنیکهای یادگیری عمیق تاثیر قابل توجهی در بهبود امنیت در حوزههای مختلف با استفاده از مدلهای شبکه عصبی مصنوعی نشان دادهاند. هنگامی که این تکنیکها در امنیت محاسبات ابری به کار میروند، راهحلهای مقرونبهصرفهای ارائه میدهند که از طریق اتوماسیون شناسایی تهدیدها، کاهش نظارت دستی و بهبود کلی کارایی امنیتی ممکن میشوند. مدلهای یادگیری عمیق با استفاده از شبکههای عصبی نقش اساسی در وظایفی مانند تشخیص نفوذ، تشخیص بدافزار ،تشخیص ناهنجاریها و تحلیل لاگها ایفا میکنند. ادغام یادگیری عمیق در امنیت ابری نیازمند ارزیابی دقیق سیستمهای موجود، تعریف اهداف، انتخاب و آمادهسازی مجموعه دادهها، تنظیم مدل و اصلاحات نهایی برای سازگاری است. علاوه بر این، پیادهسازی تکنیکهای یادگیری عمیق در امنیت ابری مستلزم در نظر گرفتن عواملی مانند منابع محاسباتی، هزینههای جمعآوری و آمادهسازی دادهها، توسعه مدل، تلاشهای ادغام و نظارت و نگهداری مداوم است. این مقاله مدلی از شبکه عصبی مصنوعی) (ANNبا انتشار پیشرونده را در امنیت ابری پیشنهاد میدهد و مراحل کلیدی برای ادغام چنین مدلهایی در استراتژیهای امنیت ابری را بررسی میکند. با توجه به اینکه کارایی مدل ANN به عواملی مانند کیفیت دادههای آموزشی، معماری شبکه و الگوریتمهای تنظیم وزن بستگی دارد، این مطالعه از مجموعه دادههای Kaggle.comبرای اعتبارسنجی استفاده میکند و مراحل آموزش و ارزیابی مدل ANN را نشان میدهد.

مقدمه:

تکنیکهای یادگیری عمیق) (DLبه عنوان ابزارهای موثری برای بهبود امنیت در حوزههای مختلف ظاهر شدهاند. این تکنیکها از قابلیتهای شبکههای عصبی مصنوعی برای یادگیری و شناسایی الگوها از حجمهای زیادی از دادهها استفاده میکنند، که منجر به راهحلهای امنیتی قویتر و کارآمدتر میشود]۱[]۲[. هنگامی که این تکنیکها در امنیت محاسبات ابری به کار میروند، مزایای زیادی دارند که تاثیر مستقیم بر هزینهاثر بخشی محصولات دارد .یکی از مزایای بزرگ پیادهسازی یادگیری عمیق در امنیت ابر، شناسایی تهدیدات به صورت خودکار است. الگوریتمهای DL میتوانند حجم زیادی از دادهها مانند لاگهای ترافیک شبکه، لاگهای سیستم و رفتار کاربر را تحلیل کنند تا به طور خودکار ناهنجاریها و تهدیدات احتمالی امنیتی را شناسایی کنند] ۲[]۳[. این به همراه سایر استفادهها، نیاز به نظارت و تحلیل دستی را کاهش میدهد، که منجر به شناسایی سریعتر حوادث امنیتی، پاسخ به موقع، کاهش خسارات و صرفهجویی در زمان و منابع میشود. به این ترتیب، با اتوماسیون وظایف مختلف امنیتی، یادگیری عمیق خطر خطای انسانی را که میتواند منجر به نقض امنیت و هزینههای مرتبط شود، به حداقل میرساند.

سیستمهای خودکار مبتنی بر یادگیری عمیق میتوانند وظایف را به طور مداوم و دقیق انجام دهند، که منجر به بهبود کلی اثر بخشی امنیت میشود]٤[]٥[. مدلهای DL الگوها و روابط در دادهها را یاد میگیرند، که اجازه میدهد شناسایی و طبقهبندی تهدیدات با دقت بیشتری انجام شود. از طریق شناسایی الگوها و ناهنجاریهایی که ممکن است توسط سیستمهای مبتنی بر قوانین سنتی نادیده گرفته شوند، پیادهسازی DL این امکان را برای سازمانها فراهم میکند تا تخصیص منابع را بهینه کنند و هزینههای غیرضروری را به حداقل برسانند.

با این حال، با روندها و تحولات جدید، شناسایی بلادرنگ باقی میماند مهمترین و چالشبرانگیزترین مسئله برای هر سیستم.
برای مقابله با این مشکل، لازم است که بتوان راهحلهایی را ارائه داد که بتواند دادهها را در زمان واقعی تحلیل کرده و شناسایی سریع تهدیدات احتمالی امنیتی را امکانپذیر کند] ٦[. با توجه به اینکه مدلهای DL قادر به تطبیق با تهدیدات در حال تحول و یادگیری از دادههای جدید در زمان واقعی هستند، چنین رویکردی تبدیل به موثرترین ابزار برای بهینهسازی میشود. با به حداقل رساندن زمانهای پاسخ، جلوگیری از مثبت کاذب و کاهش نیاز به بهروزرسانیها و تنظیمات مکرر دستی، سیستم امنیتی کارآمدتر و هزینهاثرتر میشود. علاوه بر این، تحلیل دادهها و الگوهای تاریخی، یادگیری عمیق بینشهای ارزشمندی را در مورد تهدیدات احتمالی آینده فراهم میکند. از طریق تحلیل پیشبینی، سازمانها میتوانند به طور پیشگیرانه منابع را تخصیص دهند و اقدامات پیشگیرانهای را انجام دهند، که منجر به کاهش حوادث امنیتی و هزینههای مرتبط میشود]۷[]۸[.

علاوه بر مزایای فنی ذکر شده، مزایای غیر فنی دیگری نیز باید در نظر گرفته شود. به طور خاص، عوامل کیفی مانند بهبود شهرت، اعتماد مشتری، مزیت رقابتی و غیره. این عوامل نیز باید بخشی از تصویر بزرگتر باشند، زیرا به ارزش کلی پذیرش تکنیکهای یادگیری عمیق کمک میکنند]۱[]۸[.

همانطور که از مزایای ذکر شده مشاهده میشود، تکنیکهای یادگیری عمیق راهحلهای مقرونبهصرفهای را برای امنیت محاسبات ابری ارائه میدهند. ادغام یادگیری عمیق میتواند تخصیص منابع را بهینه کند، اثر بخشی کلی امنیت را افزایش دهد و از خسارات مالی احتمالی جلوگیری کند.

ادغام رویکرد یادگیری عمیق در امنیت ابری: مدلها و الگوریتمهای یادگیری عمیق نقش مهمی در بهبود امنیت محاسبات ابری ایفا میکنند. این مدلها در کاربردهای مختلف امنیت ابری مانند تشخیص نفوذ، تشخیص بدافزار، تشخیص ناهنجاریها، تحلیل لاگ، کنترل دسترسی و غیره مورد استفاده قرار میگیرند]۲[]۳[]۹[. همانطور که قبلاً ذکر شد، بزرگترین ارزش مدلهای DL در توانایی یادگیری الگوهای پیچیده، شناسایی ناهنجاریها و تطبیق با تهدیدات در حال تحول نهفته است. با این حال، زمانی که نوبت به انتخاب مدلهای خاص برای امنیت ابری میرسد، این امر به طور کامل به ماهیت مشکل، در دسترس بودن منابع محاسباتی، دادهها، حساسیت و معماری سیستم موجود و سایر نیازهای خاص سازمان بستگی دارد. برخی از مدلها و الگوریتمهای یادگیری عمیق که به طور رایج در زمینه امنیت ابری استفاده میشوند شامل CNN، RNN، LSTM، GAN، DRL و غیره هستند.

سازمانها میتوانند تکنیکهای یادگیری عمیق را به چندین روش در استراتژیهای امنیت ابری خود ادغام کنند. همانطور که قبلاً بحث شد، سازمانها میتوانند از ادغام یادگیری عمیق در امنیت محاسبات ابری بهرهمند شوند[۱۰[. صرف نظر از کاربرد در وظایفی مانند تحلیل داده، تشخیص ناهنجاری، تشخیص و طبقهبندی بدافزار، تشخیص و پیشگیری از نفوذ، احراز هویت کاربر و کنترل دسترسی، اجرای موفق تکنیکهای یادگیری عمیق نیازمند استراتژیها و منابع کافی است] ۲[]۱۱[]۱۲[.

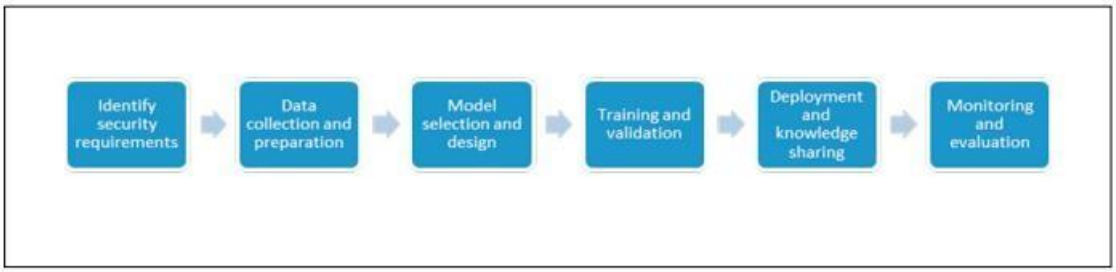

Fig. 1. Key steps to integrate deep learning into cloud security.

در شکل ۱، مراحل کلیدی برای ادغام یادگیری عمیق در امنیت ابری نشان داده شده است. با پیروی از این مراحل، سازمانها میتوانند به طور موفقیتآمیزی یادگیری عمیق را در استراتژیهای امنیت محاسبات ابری خود ادغام کنند. با این حال، برای سازمانهایی که میخواهند یادگیری عمیق را در راهحلها و معماریهای امنیت موجود ادغام کنند، این فرآیند نیازمند ارزیابی جامعتری خواهد بود)شکل ۳(. اولین مرحله برای پیادهسازی، ارزیابی نقاط قوت و ضعف سیستم موجود است. این امر شناسایی آسانتر مناطق و وظایفی که ممکن است نیاز به ادغام DL داشته باشند یا اجازه ادغام را بدهند، ممکن میسازد.

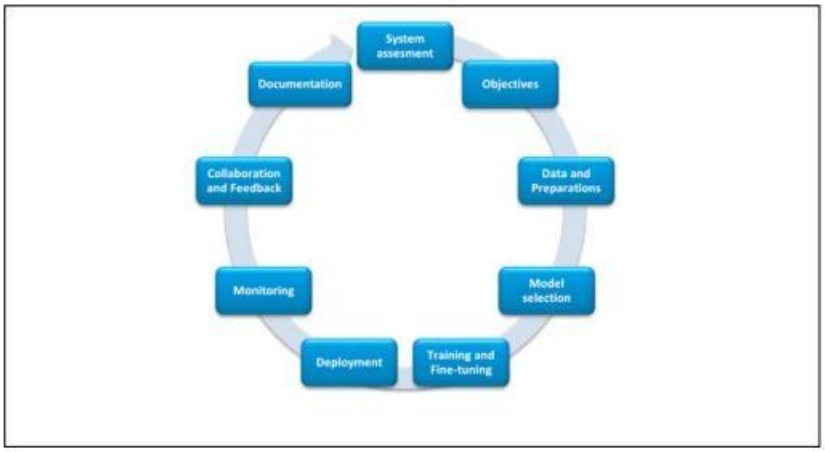

Fig. 2. Key phases for DL integration into existing security systems

مرحلهی یافتن حوزهها و وظایفی که میتوانند با استفاده از یادگیری عمیق بهبود یابند، به اهداف از پیش تعریفشده یا اهدافی که سازمان دارد، نزدیک است. داشتن اهدافی که به وضوح تعریف شدهاند، برای تعیین وظایف یا چالشهای خاصی که یادگیری عمیق میتواند در سیستم امنیت ابری آنها را برطرف کند، بسیار مهم است برای بهینهسازی استراتژیها. این امر به صورت مستقیم به انتخاب مدل مناسب برای وظایف و اهداف تعیینشده اشاره دارد. آموزش مدل نیازمند حجم زیادی از دادهها است که به دقت برای وظیفهی دادهشده انتخاب و پیشپردازش شدهاند]۱۳[. با توجه به اهمیت انتخاب مجموعه داده ،پردازش و آمادهسازی دادهها، این مرحله نیازمند تحقیق دقیق است. کل موفقیت مدل به مجموعه داده و آمادهسازی دادهها بستگی دارد] ۱٤[. پس از تصمیمگیری در مورد دادهها، برای تطبیق با زمینهی خاص امنیت ابری، لازم است تنظیمات مدل از جمله تنظیم ابرپارامترها، انجام اعتبارسنجی متقاطع، بهینهسازی و غیره در نظر گرفته شود. فرآیند نهایی ادغام ممکن است نیازمند اصلاحات نهایی برای اطمینان از سازگاری و ادغام با اجزای موجود باشد. نظارت و بازخورد بخشی از چرخهی ادغام موفق هستند، بنابراین داشتن مکانیسمهای درست برای این مرحله ضروری است.

۳. شبکه عصبی و مدل پیشنهادی

یک شبکه عصبی در سطح پیشرفته را می توان به عنوان یک مدل محاسباتی که بر روی آرایشی از لایه ها، ورودی ها به خروجی ها را با واحدهای پردازشی مرتبط به هم نشان می دهد، شناخته می شود] ۱۳[،]۱۵[. چنین مدلی داده هایی را که از روی شبکه عبور می کند فیلتر می کند تا سیگنال ورودی مربوطه را که به لایه بعدی ارسال می شود، تعیین کند. اساساً تصمیم میگیرد که آیا یک نورون خاص فعال شود یا خیر، و در غیاب نورونهای خاص، به عنوان یک مدل خطی ساده توسعه میابد]۱٦[.

با هدف تعیین تأثیر عوامل بر هزینههای امنیت ابر، ما یک رویکرد جدید با استفاده از یک مدل ANN انتشار پیشخور ارائه میکنیم. بر اساس فناوری رمزگذاری همگن، روش پیشنهادی ممکن است بلافاصله یک مدل ANN ساده برای داده های رمزگذاری شده آموزش داده و ایجاد کند]۱۳[. برای اجرای این رویکرد سه مرحله وجود دارد: مرحله آموزش، مرحله آزمایش و مرحله اعتبار سنجی، که در یک محیط ابری به هم مرتبط هستند.

۳.۱.مجموعه داده

مجموعه داده مورد استفاده برای این مطالعه در Kaggle.com موجود است) مجموعه داده ای که برای بررسی اعتبار روش پیشنهادی استفاده می شود

https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iio در دسترس است:

مجموعه داده شامل ۵۲ فایل با ۱۶۳۸ ستون با ویژگی های مختلف است. مجموعه داده شامل ویژگیهای بهدستآمده از منابع مختلف، از جمله هشدارها، منابع سیستم، گزارشها، ترافیک شبکه، و ۶۱ ویژگی پیشنهادی جدید با همبستگی بالا از ۱۱۷۶ ویژگی است[۱۴]. مجموعه داده یک مدل ANN از دو جزء اصلی داده های ورودی و برچسب های خروجی تشکیل شده است.

مجموعه داده معمولاً به سه زیر مجموعه برای آموزش، اعتبار سنجی و آزمایش تقسیم می شود. زیر مجموعه آموزشی برای آموزش مدل ANN استفاده می شود. بخش بزرگی از مجموعه داده را شامل می شود و برای بهینه سازی وزن ها و سوگیری های شبکه از طریق فرآیند یادگیری استفاده می شود. نمودار آموزشی برای این کار با استفاده از MATLAB نشان داده شده در شکل ۳ تولید شده است. زیر مجموعه اعتبارسنجی برای تنظیم پارامترهای هایپر مدل ANN در طول فرآیند آموزش استفاده می شود. این به ارزیابی عملکرد مدل بر روی داده های دیده نشده و تصمیم گیری در مورد تنظیمات کمک می کند .
نمودار اعتبارسنجی با استفاده از MATLAB که در شکل ٤b نشان داده شده است، تولید شده است. زیر مجموعه آزمون برای ارزیابی عملکرد نهایی مدل ANN آموزش دیده استفاده می شود. این یک ارزیابی بیطرفانه از قابلیتهای تعمیم مدل بر روی دادههای دیده نشده ارائه میکند[۱۵]. نمودار تست با استفاده از MATLAB همانطور که در شکل ٤a نشان داده شده است تولید شده است.

۳.۲. پیش پردازش

پیش پردازش آماده سازی مجموعه داده برای آموزش یک مدل ANN ضروری است. این شامل تبدیل و دستکاری داده های ورودی خام به منظور ایجاد مناسب برای شبکه برای یادگیری از آن است[۱۷]. پیش پردازش به بهبود کیفیت داده ها، عادی سازی ویژگی ها و رسیدگی به هرگونه ناسازگاری یا مقادیر از دست رفته کمک می کند. برخی از رایج ترین تکنیک های پیش پردازش شامل پاکسازی داده ها، عادی سازی داده ها و افزایش داده ها می باشد. این تکنیکهای پیشپردازش به بهبود کیفیت و مناسب بودن مجموعه داده برای آموزش یک مدل ANN کمک میکنند، از نمایش منصفانه همه ویژگیها اطمینان میدهند، مقادیر از دست رفته را مدیریت میکنند، و چالشهای مربوط به دادهها را ویژه حوزه مشکل برطرف میکنند.[۱۸] در مجموعه داده ما، قبل از پردازش اولیه، دادههای نمونه و دادههای گروهی برای

ساختن راهاندازی مدل ANN فرمولبندی میشوند. پس از انتخاب مجموعه داده، سه موضوع اساسی بررسی می شود. داده های از دست رفته اولین مسئله است، و این داده ها با مقدار فوری معمولی مبادله می شوند، سپس داده ها نرمال و تصادفی می شوند .یک روش میانگین که برای محاسبه مقادیر از دست رفته استفاده می شود به صورت زیر فرموله می شود:

ANNلایه کاربردی در۳.۳.

در مدل ANN، لایه کاربردی به آخرین لایه نورون ها اشاره دارد، جایی که هر نورون مربوط به یک کلاس یا مقدار خروجی خاص است. هدف لایه کاربردی تبدیل اطلاعات آموخته شده توسط لایه های قبلی به فرمی مناسب برای مشکل است. این پیش بینی ها یا خروجی های نهایی مدل ANN را ارائه می دهد. در این تحلیل در حال انجام ،۱۹ نورون در لایه ورودی وجود دارد، در حالی که لایه خروجی شامل ۱٦ نورون پنهان است. مدل ANN برای نشان دادن تنها یک هدف طراحی شده است که تأثیر پارامترهای مختلف بر امنیت هزینه ابر را تعریف می کند. تابع Sigmoid (x) لایه با ورودی)۲(تعریف میشود که میتواند تابع فعالسازی)x(را درج کند، جایی که لایه پنهان با ورودی)۳(تعریف میشود.

$$S(x) = \frac{1}{1+e^{-\partial j}} \qquad (2)$$

$$\partial j = \sum_{i=1}^{m} \left(\alpha_i j + E_i \right) + b_1$$

به طور مشابه، تابع فعال سازی)x(با لایه خروجی)٤(و لایه مخفی خروجی مربوطه تعریف می شود.

$$A(x) = \frac{1}{1+e^{-\partial k}} \qquad (4)$$

$$\partial k = \sum_{j=1}^{n} (\beta_j k + E_i) + b_2 \qquad (5)$$

در معادلات بالا ،b۱ و b۲ ثابت دلخواه هستند و E_i نشان دهنده خطاهای مرتبط با مسئله است.

در حالی که αij و βij به ترتیب درجه ارتباطی مستقیم لایه ورودی و لایه خروجی را تعریف می کنند ،و ∂j و ∂k مقادیر اندازه گیری شده لایه های پنهان ورودی و خروجی هستند.

$$T(c) = \begin{cases} mean\ (c)\ ,\ if \quad c = null \\ c,\ otherwise \end{cases}$$

۳.٤. لایه اعتبار سنجی در ANN

در طول مرحله آموزش یک شبکه عصبی مصنوعی، زیرمجموعه ای از داده های برچسب گذاری شده موجود برای اهداف اعتبار سنجی باق می ماند. این زیرمجموعه، که به عنوان مجموعه اعتبار سنجی شناخته می شود، برای آموزش شبکه استفاده نمی شود، بلکه به عنوان یک مجموعه داده مستقل عمل می کند.

ارزیابی عملکرد مدل در طول فرآیند آموزش] ۲۰[. مجموعه اعتبارسنجی برای نظارت بر مدل استفاده می شود تعمیم و تنظیم پارامترهای فوق یا تصمیم گیری در مورد بهینه سازی مدل]۲۱[. در طول فرآیند آموزشی، مدل به

صورت دورهای بر روی مجموعه اعتبارسنجی برای اندازهگیری عملکرد آن با استفاده از دقت و رگرسیون مورد ارزیابی قرار گرفت.در شکل ٤، نتیجه اعتبارسنجی مجموعه داده با استفاده از شبکه عصبی نشان داده شده است. ما این را برای تأیید اعتبار اعمال کردیم.

عملکرد شبکه با آموزش و آزمایش مجموعه داده های مربوط به اهداف، نمودارهای رگرسیون خروجی ها را نشان می دهند

٤. شبیه سازی و نتایج

مجموعه دادهها تحت یک تکنیک یادگیری ماشین قرار گرفتند و شبیهسازیها با استفاده ازمتلب انجام شد. مجموعه داده ٧٠٪ برای آموزش استفاده می شود، در حالی که ٣٠٪ باقی مانده برای آزمایش و اعتبار سنجی استفاده می شود. داده ها رمزگذاری شده و در فضای ابری ذخیره می شود. برای ارزیابی عملکرد مدل پیشنهادی، آن را در دورههای مختلف آموزش دادیم و از برنامه متلب برای اعمال سه الگوریتم ای ان ان مجزا استفاده میکنیم:

Levenberg-Marquardt (LM), Bayesian Regularization (BR), and Scale Conjugate Gradient (SCG

یافته های شبیه سازی در شکل ٣ و شکل ٤ نشان می دهد: مدل مجموعه داده آموزش دیده بر روی ابر با استفاده از نمودار ای ان ان به دست اورد. رگرسیون حالت و تکامل آموزش و نتایج

.

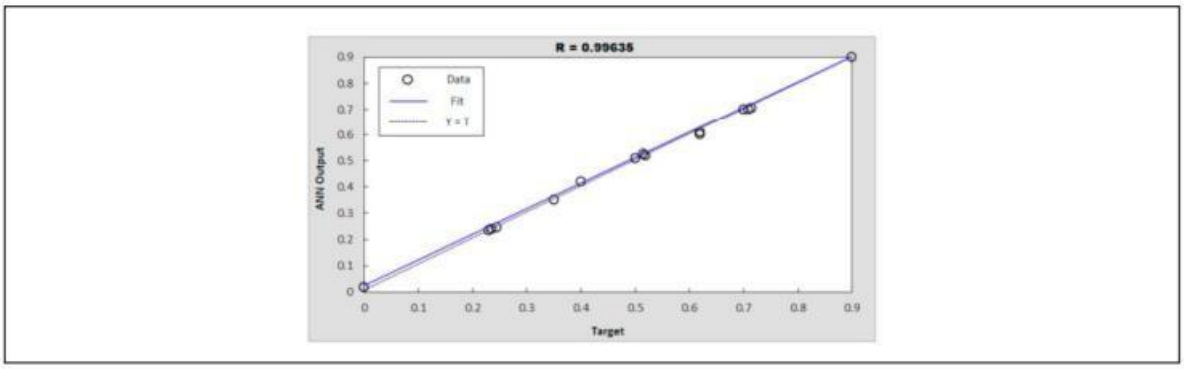

Fig. 3. Regression plot for training

شکل ٤ نتایج آزمایش اعتبارسنجی ابر مجموعه داده را با استفاده از تکنیک ان ان را نشان میدهد. این برای اعتبار سنجی عملکرد شبکه استفاده شد. نمودارهای رگرسیون خروجی های شبکه را پس از آموزش و آزمایش با استفاده از مجموعه داده های هدف نشان می دهند. داده ها در امتداد یک خط ٤٥ درجه قرار می گیرند، یک تناسب کامل، با اهداف برابر با خروجی های شبکه. با در نظر گرفتن بار اولیه و ترجیحات، خروجی شبکه پس از آموزش مجدد تغییر می کند و بربهبود بیشتر نتایج کمک میکند.

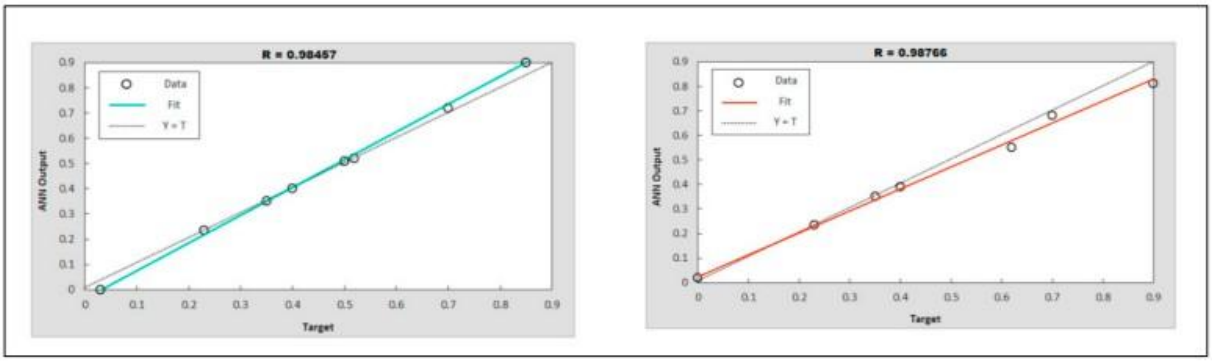

Fig. 4. (a) Regression for testing; (b) regression for validation.

یادگیری ماشین:(Machine Learning)

یادگیری ماشین شاخهای از هوش مصنوعی است که به کامپیوترها اجازه میدهد بدون برنامهریزی صریح یاد بگیرند . الگوریتمهای یادگیری ماشین از دادهها استفاده میکنند تا مدلهایی بسازند که بتوانند پیشبینیها و تصمیمگیریها را انجام دهند. الگوریتمهای یادگیری ماشین به دستههای زیر تقسیم میشوند:

- **یادگیری نظارتشده :(Supervised Learning)** مدلها با استفاده از دادههای آموزشی با برچسب آموزش میبینند. مثالها: رگرسیون خطی، درخت تصمیمگیری.
- **یادگیری بدون نظارت :(Unsupervised Learning)** مدلها با استفاده از دادههای آموزشی بدون برچسب آموزش میبینند. مثالها: خوشهبندیK-Means ، کاهش ابعاد.PCA
- **یادگیری تقویتی :(Reinforcement Learning)** مدلها با تعامل با محیط و دریافت پاداش یا تنبیه آموزش میبینند. مثالها: الگوریتم.Q-Learning **تفاوتهای یادگیری عمیق و یادگیری ماشین:**
- **میزان دادههای مورد نیاز** :یادگیری عمیق به دادههای بیشتری برای آموزش نیاز دارد تا از پتانسیل کامل خود استفاده کند، در حالی که یادگیری ماشین میتواند با دادههای کمتری عملکرد خوبی داشته باشد.
- **زمان و منابع محاسباتی** :الگوریتمهای یادگیری عمیق به قدرت پردازشی بالاتری نیاز دارند و زمان بیشتری برای آموزش مدلها لازم دارند.
- **پیچیدگی مدلها** :مدلهای یادگیری عمیق دارای معماریهای پیچیدهتری هستند و میتوانند الگوهای پیچیدهتری را در دادهها یاد بگیرند.

۵.نتیجه گیری

ادغام تکنیک های یادگیری عمیق در امنیت رایانش ابری مزایای بی شماری را ارائه می دهد. با تجزیه و تحلیل حجم زیادی از داده ها، الگوریتم های یادگیری عمیق می توانند تهدیدات امنیتی را در زمان واقعی شناسایی کرده و خطرات مختلف را به

حداقل برسانند. با این حال، پیاده سازی یادگیری عمیق در امنیت ابری نیاز به ارزیابی دقیق هزینه ها و منابع دارد. برای مثال سازمان ها در هنگام تنظیم راه حل با منابع محاسباتی، اکتساب داده ها و هزینه های آماده سازی، تخصص پرسنل و نظارت و نگهداری مداوم میشود اشاره کرد. ادغام تکنیک های یادگیری عمیق در امنیت ابری شامل چند مرحله برای یک نتیجه

موفقیت آمیز است. اینها شامل ارزیابی نقاط قوت و ضعف سیستم موجود، شناسایی وظایف خاص که یادگیری عمیق است که می تواند شامل آدرس دهی، انتخاب مدل ها و الگوریتم های مناسب، آموزش مدل ها با داده های برچسب دار. سازگاری و یکپارچگی با اجزای موجود را تضمین میکند. حفظ کارایی و اثربخشی سیستم یکپارچه برای نظارت مستمر و بازخورد نیز مراحل بسیار مهمی هستند . برای ارائه یک نمای کلی از کار ساده اجرای یک تکنیک یادگیری عمیق، ما یک فید فوروارد پیشنهاد کردیم: مدل انتشار شبکه عصبی مصنوعی در امنیت ابر. این مدل برای آموزش و توسعه داده شد تا داده های رمزگذاری شده، امکان تجزیه و تحلیل کارآمد را برای ارزیابی کارایی در امنیت ابری فراهم می کند. اثربخشی مدل به عواملی مانند کیفیت و کمیت داده های آموزشی، طراحی معماری شبکه و الگوریتم های بهینه سازی بستگی دارد. راه حل های مقرون به صرفه ای برای افزایش امنیت رایانش ابری، بهبود شخصیت تهدید و بهینه سازی منابع ارائه می دهد **ANN** ادامه این کار بیشتر بر روی برخی عناصر موثر در هزینه های کلی تمرکز خواهد کرد. امنیت در ابر، به طور جداگانه و به عنوان بخشی از یک طبقه بندی گروه بزرگتر تجزیه و تحلیل می شود. تحقیقات آینده باید بررسی شود. توسعه معماری های

یادگیری عمیق کارآمد به طور خاص برای امنیت محاسبات ابری بهینه شده است. این مستلزم طراحی معماری هایی است که می توانند پردازش داده در مقیاس بزرگ را انجام دهند، محاسباتی را کاهش داده و به حداقل برسانند. با پرداختن به چنین اهداف و جهت گیری های تحقیقاتی، تکنیک های یادگیری عمیق می توانند ادامه پیدا کنند و سبب پیشبرد و ارائه راه حل های مقرون به صرفه و افزایش امنیت در رایانش ابری شوند.

منابع:

[۱] E. K. Subramanian and L. Tamilselvan, ‘A focus on future cloud: machine learning-based cloud security’, *SOCA*, vol. ۱۳, no. ۳, pp. ۲۳۷–۲۴۹, Sep. ۲۰۱۹, doi: ۱۰,۱۰۰۷/s۱۱۷۶۱-۰۱۹-۰۰۲۷۰-۰.

[۲] N. Srikanth and T. Prem Jacob, ‘An Real Time Cloud Security System and Issues comparison using Machine and Deep Learning’, in *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India: IEEE, Nov. ۲۰۲۱, pp. ۵۲۳–۵۲۹. doi: ۱۰,۱۱۰۹/ISMAC۵۲۳۳۰,۲۰۲۱,۹٦٤۰٦۵۰.

[۳] S. Badri *et al.*, ‘An Efficient and Secure Model Using Adaptive Optimal Deep Learning for Task Scheduling in Cloud Computing’, *Electronics*, vol. ۱۲, no. ٦, p. ۱٤٤۱, Mar. ۲۰۲۳, doi: ۱۰,۳۳۹۰/electronics۱۲۰٦۱٤٤۱.

[٤] K. Gulen, ‘Artificial Intelligence And Automation: Examples, Benefits And More’, Dec. ۰۹, ۲۰۲۲. https://dataconomy.com/۲۰۲۲/۱۲/۰۹/artificial-intelligence-and-automation/ (accessed May ۳۰, ۲۰۲۳).

[۵] K. W. Ullah, A. S. Ahmed, and J. Ylitalo, 'Towards Building an Automated Security Compliance Tool for the Cloud', in *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Melbourne, Australia: IEEE, Jul. ۲۰۱۳, pp. ۱۵۸۷–۱۵۹۳. doi: ۱۰,۱۱۰۹/TrustCom.۲۰۱۳,۱۹۵.

[۶] H. Xu, 'Cybersecurity and Data Quality in Cloud Computing: A Research Framework', in *Information Systems*, M. Papadaki, P. Rupino da Cunha, M. Themistocleous, and K. Christodoulou, Eds., in Lecture Notes in Business Information Processing. Cham: Springer Nature Switzerland, ۲۰۲۳, pp. ۲۰۱–۲۰۸. doi: ۱۰,۱۰۰۷/۹۷۸-۳۰۳۱-۳۰۶۹٤-٥_۱٥.

[۷] S. Moisset, 'How Security Analysts Can Use AI in Cybersecurity', *freeCodeCamp.org*, May ۲٤, ۲۰۲۳. https://www.freecodecamp.org/news/how-to-use-artificial-intelligence-in-cybersecurity/ (accessed Jun. ۲۷, ۲۰۲۳).

[۸] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani, and F. M. Dakalbab, 'Machine Learning for Cloud Security: A Systematic Review', *IEEE Access*, vol. ۹, pp. ۲۰۷۱۷–۲۰۷۳٥, ۲۰۲۱, doi: ۱۰,۱۱۰۹/ACCESS.۲۰۲۱,۳۰٥٤۱۲۹.

[۹] D. Chauhan, A. Kumar, P. Bedi, V. A. Athavale, D. Veeraiah, and B. R. Pratap, 'An effective face recognition system based on Cloud based IoT with a deep learning model', *MICROPROCESSORS AND MICROSYSTEMS*, vol. ۸۱, Mar. ۲۰۲۱, doi: ۱۰,۱۰۱٦/j.micpro.۲۰۲۰,۱۰۳۷۲٦.

[۱۰] N. Kryvinska and L. Bickel, 'Scenario-Based Analysis of IT Enterprises Servitization as a Part of Digital Transformation of Modern Economy', *Applied Sciences*, vol. ۱۰, no. ۳, Art. no. ۳, Jan. ۲۰۲۰, doi: ۱۰,۳۳۹۰/app۱۰۰۳۱۰۷٦.

[۱۱] R. Zarai, M. Kachout, M. A. G. Hazber, and M. A. Mahdi, 'Recurrent Neural Networks and Deep Neural Networks Based on Intrusion Detection System', *OALib*, vol. ۰۷, no. ۰۳, pp. ۱–۱۱, ۲۰۲۰, doi: ۱۰,٤۲۳٦/oalib.۱۱۰٦۱٥۱.

[۱۲] M. Kawai, K. Ota, and M. Dong, 'Improved MalGAN: Avoiding Malware Detector by Leaning Cleanware Features', in *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, Okinawa, Japan: IEEE, Feb. ۲۰۱۹, pp. ۰٤۰–۰٤٥. doi: ۱۰,۱۱۰۹/ICAIIC.۲۰۱۹,۸٦٦۹۰۷۹.

[۱۳] M. U. Sana, Z. Li, F. Javaid, H. B. Liaqat, and M. U. Ali, 'Enhanced Security in Cloud Computing Using Neural Network and Encryption', *IEEE Access*, vol. ۹, pp. ۱٤٥۷۸٥–۱٤٥۷۹۹, ۲۰۲۱, doi:۱۰,۱۱۰۹/ACCESS.۲۰۲۱,۳۱۲۲۹۳۸.

[۱٤] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, 'Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning'. TechRxiv, Jan. ۲۷, ۲۰۲۲. doi: ۱۰,۳٦۲۲۷/techrxiv.۱۸۸٥۷۳۳٦.v۱.

[۱٥] M. M. Taye, 'Theoretical Understanding of Convolutional Neural Network: Concepts, Architectures, Applications, Future Directions', *Computation*, vol. ۱۱, no. ۳, Art. no. ۳, Mar. ۲۰۲۳, doi: ۱۰,۳۳۹۰/computation۱۱۰۳۰۰٥۲.

[۱٦] A. Gupta and M. Kalra, 'Intrusion Detection and Prevention system using Cuckoo search algorithm with ANN in Cloud Computing', in *2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Nov. ۲۰۲۰, pp. ٦٦–۷۲. doi: ۱۰,۱۱۰۹/PDGC٥۰۳۱۳,۲۰۲۰,۹۳۱٥۷۷۱.

[۱۷] W. Etaiwi and G. Naymat, 'The Impact of applying Different Preprocessing Steps on Review Spam Detection', presented at the ۸TH INTERNATIONAL CONFERENCE ON EMERGING UBIQUITOUS SYSTEMS AND PERVASIVE NETWORKS (EUSPN ۲۰۱۷) / ۷TH INTERNATIONAL CONFERENCE ON CURRENT AND FUTURE TRENDS OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN HEALTHCARE (ICTH-۲۰۱۷) / AFFILIATED WORKSHOPS, E. Shakshuki, Ed., ۲۰۱۷, pp. ۲۷۳–۲۷۹. doi: ۱۰,۱۰۱٦/j.procs.۲۰۱۷,۰۸,۳٦۸.

[۱۸] C. Fan, M. Chen, X. Wang, J. Wang, and B. Huang, 'A Review on Data Preprocessing Techniques Toward Efficient and Reliable Knowledge Discovery From Building Operational Data', *Frontiers in Energy Research*, vol. ۹, ۲۰۲۱, Accessed: Jun. ۲۷, ۲۰۲۳. [Online]. Available: https://www.frontiersin.org/articles/۱۰,۳۳۸۹/fenrg.۲۰۲۱,٦٥۲۸۰۱ .

[۱۹] P. E. Rauber, S. G. Fadel, A. X. Falcão, and A. C. Telea, 'Visualizing the Hidden Activity of Artificial Neural Networks', *IEEE Transactions on Visualization and Computer Graphics*, vol. ۲۳, no. ۱, pp. ۱۰۱–۱۱۰, Jan. ۲۰۱۷, doi: ۱۰,۱۱۰۹/TVCG.۲۰۱٦,۲٥۹۸۸۳۸.

[۲۰] G. B. Humphrey *et al.*, 'Improved validation framework and R-package for artificial neural network models', *Environmental Modelling & Software*, vol. ۹۲, pp. ۸۲–۱۰٦, Jun. ۲۰۱۷, doi: ۱۰,۱۰۱٦/j.envsoft.۲۰۱۷,۰۱,۰۲۳.

[۲۱] R. Pramoditha, 'Why Do We Need a Validation Set in Addition to Training and Test Sets?', *Medium*, Apr. ۱۲, . https://towardsdatascience.com/why-do-we-need-a-validation-set-in-addition-totraining-and-test-sets- ٥cf٤a٦٥٥٥٠e٠ (accessed Jun. ۲۷, ۲۰۲۳).