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

Spring, 2022, 3 (1), 37-46
DOR: 20.1001.1.27832570.1400.2.4.7.4

Received: 21 Sep 2021
Accepted: 10 Nov 2021

Intrusions Detection System in The Cloud Computing Using Heterogeneity Detection Technique

Roozbeh Hoseinnezhad[1], Ali Ghaffari[2*]

1. Phd. Student, Department of Camputer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran.
2. Associate Professor, Department of Camputer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran. *(Corresponding Author)* A.ghaffari@iaut.ac.ir

Abstract

Introduction: The distributed structure of cloud computing makes it an attractive target for potential cyberattacks by intruders. In this paper, using the anomaly detection approach, a method for embedding an intrusion detection system for cloud computing is presented. Therefore, by studying how to check the parameters and the combined role of the parameters in the detection of penetration in the cloud, a method for detecting suspicious behavior in the cloud is provided. The most logical way to detect an intrusion is to use supervised methods to learn the parameters of normal customer behavior. Therefore, the detection of biased behavior in the form of suspicious behavior was implemented and discussed, investigated, and compared with an initial simulation in the form of identifying abnormal behavior in different behavioral areas by the neural network.

Method: In this article, the basis of abnormality detection in different aspects is to examine the behavior of users and use the capabilities of reproducing inputs in RNN neural networks. In these networks, during the training of the network, the weights are adjusted in such a way that they can minimize the average square of the error so that the network can produce common repeating patterns well. Therefore, after training, these networks cannot reproduce well the input patterns that are actually significantly different from the training samples. Hence, these networks are able to identify anomalies in the tested sets. Accordingly, RNN networks are used here to model normal behavior.

Findings: The simulation results show that the proposed method, which is based on the recurrent neural network, can improve the false positive, false negative, and detection accuracy compared to the classification method.

Discussion: In this article, the detection of biased behavior in the form of suspicious behavior was implemented and discussed, investigated, and compared with an initial simulation in the form of identifying abnormal behavior in different behavioral fields. The simulation results show that the proposed method, which is based on the iterative neural network, can improve the false positive, false negative, and detection accuracy compared to the classification method.

Keywords: Cloud computing, anomaly detection, normal behavior, behavioral parameters, biased behavior.

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

تشخیص نفوذ در ابر رایانشی توسط تکنیک تشخیص ناهمگونی

تاریخ دریافت: ۱۴۰۰/۰۷/۰۳
تاریخ پذیرش: ۱۴۰۰/۰۸/۱۹

سال سوم، بهار ۱۴۰۱
شمارهٔ اول، صص: ۳۷ – ۴۶

روزبه حسین‌نژاد[۱]، علی غفاری[۲*]

۱. دانشجوی دکتری، گروه مهندسی کامپیوتر، واحد تبریز، دانشگاه آزاد اسلامی، تبریز، ایران. Roozbehmaah@gmail.com
۲. دانشیار، گروه مهندسی کامپیوتر، واحد تبریز، دانشگاه آزاد اسلامی، تبریز، ایران. (نویسندهٔ مسئول)
A.ghaffari@iaut.ac.ir

چکیده: در سال‌های اخیر، ظهور و گسترش روزافزون استفاده از رایانش ابری، درک همه از معماری‌های زیرساخت، ارائه نرم‌افزار و مدل‌های توسعه را به‌شدت تغییرداده‌است. پس از انتقال از رایانه‌های مرکزی به مدل‌های سرویس گیرنده/سرویس دهنده، رایانش ابری عناصری از محاسبات گرید، محاسبات ابزار و محاسبات خودکار را دربرمی‌گیرد و به یک معماری استقرار نوآورانه تبدیل‌می‌شود. این انتقال سریع به سمت رایانش ابری، نگرانی‌هایی برای موفقیت سیستم‌های اطلاعاتی، ارتباطات و امنیت اطلاعات ایجادکرده‌است. ساختار توزیع شده رایانش ابری به‌عنوان هدفی جذاب برای حملات سایبری بالقوه توسط نفوذگران تبدیل‌می‌شود. در این مقاله با استفاده از رویکرد تشخیص ناهنجاری، روشی برای تعبیه یک سیستم تشخیص نفوذ برای رایانش ابری ارائه‌شده‌است. لذا با مطالعه بر روی چگونگی بررسی پارامترها و نقش ترکیبی پارامترها در تشخیص نفوذ در ابر، به بررسی و ارائه چهارچوب نظری به همراه شبیه‌سازی رفتار مشکوک در ابر پرداخته‌شده‌است. منطقی‌ترین روش برای شناسایی نفوذ، استفاده از روش‌های همراه با ناظر برای یادگیری پارامترهای رفتار عادی مشتریان است. لذا تشخیص رفتار مغرضانه در قالب رفتار مشکوک، با یک شبیه‌سازی اولیه در قالب شناسایی رفتار غیرعادی در حیطه‌های مختلف رفتاری توسط شبکه عصبی تکرارکننده پیاده‌سازی، بررسی و مقایسه شده‌است. نتایج حاصل از شبیه‌سازی روش پیشنهادی نشان‌می‌دهد که این تحقیق می‌تواند جنبه‌های جدیدی را برای بررسی مسأله تشخیص نفوذ در ابر ارائه‌کند و از روش دسته‌بندی نیز کارایی بهتری از خود نشان‌دهد.

واژه‌های کلیدی: ابر رایانشی، تشخیص ناهنجاری، پارامترهای رفتاری، رفتار نرمال، رفتار مغرضانه.

۱. مقدمه

مفهوم رایانش ابری از معماری نرم‌افزار توزیع‌شده پدیدآمده‌است. خدمات ابر محاسباتی از مراکز داده واقع‌شده، ارائه‌می‌شود در نقاط مختلف جهان مایکروسافت شیرپوینت و برنامه‌های گوگل نمونه‌هایی کلی از خدمات رایانش ابری هستند [4-1]. در حال حاضر، مدل‌های رایانش ابری منبع اصلی چالش‌ها و آسیب‌پذیری‌ها هستند. نفوذگران از ضعف مدل‌های ابری در دسترسی به داده‌های خصوصی کاربران با حمله به قدرت پردازش سیستم‌های کامپیوتری سوءاستفاده‌می‌کنند.[8-5] . جدا از شباهت و نقاط مشترک رایانش ابر و شبکه‌های کامپیوتری، مسئله امنیت در رایانش ابری چالش اساسی محسوب‌می‌شود[11-9] .

به‌طورکلی، دو نوع سیستم تشخیص نفوذ وجوددارد: سیستم‌های شناسایی سوءاستفاده و رفتارهای غیرعادی. در سیستم‌هایشناسایی سوءاستفاده، سیستم از ساختار کلی حملات اطلاع دارد و الگوی خاصی را برای اشکال مختلف حملات دراختیاردارد که توسط آن می‌تواند از نفوذ به سیستم جلوگیری‌کرده و یا اقدامات لازم را برای مقابله با نفوذ انجام‌دهد. اما، در سیستم‌های شناسایی رفتارهای غیرعادی، تنها رفتار درست و معمولی کاربر است که اطلاعات و مشخصات آن در اختیار سیستم قراردارد. از این رو، در این سیستم‌ها، هدف شناسایی رفتار غیرعادی است که احتمال‌دارد از نوع حمله و نفوذ باشد.

در این مقاله با استفاده از رویکرد تشخیص ناهنجاری، روشی برای تعبیهٔ یک سیستم تشخیص نفوذ برای رایانش ابری ارائه‌می‌شود. در روش پیشنهادی از شبکه عصبی استفاده‌شده‌است.

ساختار مقاله به‌صورت زیر سازمان‌دهی شده‌است: بخش ۲ به روش‌های پیشین و روش‌های مرتبط با موضوع این مقاله می‌پردازد. بخش ۳، راه‌حل پیشنهادی را ارائه‌می‌دهد. بخش ۴، ارزیابی کارایی روش پیشنهادی را نشان‌می‌دهد. درنهایت، بخش ۵ به جمع‌بندی و اشاره به کارهای آینده می‌پردازد.

۲. پیشینه پژوهش

در [3]، نویسندگان یک سیستم تشخیص نفوذ کارآمد را برای محیط ابری با استفاده از تکنیک‌های انتخاب ویژگی و طبقه‌بندی مجموعه توسعه‌داده‌اند. این روش بر تکنیک انتخاب ویژگی مجموعه تک متغیره تکیه‌داشت که برای انتخاب مجموعه‌های ویژگی کاهش‌یافته ارزشمند از مجموعه داده‌های نفوذی داده‌شده استفاده‌می‌شود. درحالی‌که طبقه‌بندی‌کننده‌های گروهی که می‌توانند به‌خوبی طبقه‌بندی‌کننده‌های منفرد را با هم ترکیب‌کنند تا با استفاده از تکنیک رأی‌گیری، یک طبقه‌بندی قوی تولیدکنند. یک روش پیشنهادی مبتنی‌بر مجموعه به‌طور مؤثر طبقه‌بندی‌می‌کند که آیا رفتار ترافیک شبکه عادی است یا حمله. نتایج روش پیشنهادی به میزان قابل‌توجهی افزایش عملکرد در مقایسه با سایر روش‌های موجود دست‌یافت. علاوه‌براین، آن‌ها یک آزمون t زوجی را انجام‌داده و ثابت‌کردند که عملکرد روش پیشنهادی به‌طور معنی‌داری با سایر روش‌های موجود متفاوت است. درنهایت، نتیجه این بررسی با بهترین دقت و کمترین نرخ هشدار کاذب به‌دست‌آمد.

در [۱۲]، یک تکنیک برای تشخیص حملات DDoS با استفاده از یک مدل شبکه عصبی مصنوعی (ANN) پیشنهادشده‌است. این مدل با استفاده از الگوریتم رقابتی امپریالیستی آموزش داده‌شده‌است. مجموعه داده NSL KDD برای ارزیابی عملکرد تکنیک پیشنهادی استفاده‌می‌شود. روش پیشنهادی ما دقت تشخیص ۸۳٫۵٪ و ۶۵٪ را با مجموعه داده‌های KDDTest+ و KDDTest-21 به ترتیب می‌دهد. مقایسه عملکرد با برخی دیگر از تکنیک‌های مبتنی‌بر یادگیری ماشین و تکنیک‌های پیشرفته نیز ارائه‌شده‌است. در [۱۳]، روشی مبتنی‌بر تشخیص ناهنجاری ارائه‌شده‌است که در آن از شبکه‌های عصبی پیش‌خوردی به‌منظور مدل‌سازی رفتار کاربران استفاده‌شده‌است. در [۱۴] مدلی برای شناسایی حملاتی از نوع حملات سیل‌آسا به‌نام معماری جلوگیری از حملات سیل‌آسا در محیط ابرایانش ابری ارائه‌شده‌است. نکته خاصی که در این کار دیده‌می‌شود، ارائه ترافیک به سیستم تشخیص نفوذ پس از گذر از یک فیلتر انتخاب ویژگی است. بدین‌ترتیب، انتظارمی‌رود بتوان از طریق این امر سرعت و دقت تشخیص نفوذ را بالابرد.

در [۱۵]، مفهومی به‌نام سیستم تشخیص نفوذ مینی برای تشخیص حملات در ابر رایانشی ارائه‌شده‌است. ایده اصلی در معماری ارائه‌شده در این کار بر این مبنا بناشده‌است که بتوان از طریق تخصیص سیستم‌های تشخیص نفوذ مینی به هر کاربر از سربار سنگین تشخیص نفوذ، درنتیجه تخصیص سیستم تشخیص نفوذ کلی به ابر جلوگیری‌کرد. بدین‌ترتیب، عملیات تشخیص نفوذ در ابر می‌تواند با سرعت بالاتر و دقت بیشتر انجام شود، ترافیک سنگین درخواست‌ها و انتقال اطلاعات حتی در بهترین حالت نیاز به تعبیه سیستم‌های سنگین در ابر دارد و سیستم تشخیص نفوذ مرکزی کار دشواری در ارائه کیفیت مناسب در برابر این ترافیک و حجم حملات ورودی خواهدداشت.

در [۱۶] یک مدل تشخیص نفوذ یکپارچه برای شناسایی رفتار مشکوک در محیط رایانش ابری ارائه‌شده‌است. در این کار برای تشخیص رفتار مشکوک از مفاهیم شناسایی ناهنجاری و شناسایی امضا استفاده‌می‌شود. اساس کارکردی این کار بر پایه شناسایی نفوذها و ناهنجاری‌هایی است که موجب به‌وجودآمدن تهدید برای محیط ابر می‌شوند. بدین ترتیب، در این کار از شناسایی ناهنجاری به‌منظور شناسایی رفتار غیرمنتظره و از شناسایی امضا برای شناسایی رفتار مشکوک به نفوذ در نتیجه مشاهدات پیشین و از پیش تعریف‌شده، استفاده‌می‌شود.

در [۱۷] رویکردی برای شناسایی حملات از نوع انکار سرویس توزیع‌شده در وب سرویس‌های درون ابر رایانشی ارائه‌شده‌است. در این کار نوع جدیدی از آسیب‌پذیری در وب سرویس‌های مبتنی‌بر ابر بررسی‌شده‌است که در آن برای ایجاد مشکل حملات انکار سرویس در لایه برنامه کاربردی تلاش‌می‌شود. هدف این نوع حملات منابع پردازشی هستند که توسط

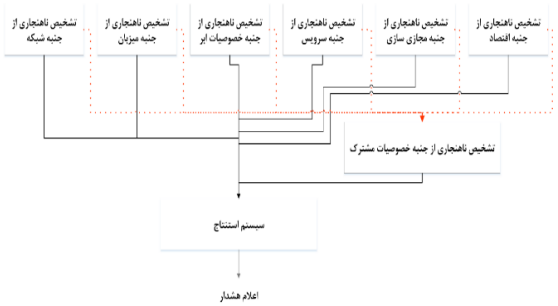
ارسال درخواست‌های پروتکل دسترسی شی ساده انجام‌می‌گیرد، به‌طوری‌که این درخواست‌ها حاوی محتوای XML مغرضانه هستند. این حملات قابل‌شناسایی در لایه شبکه یا انتقال نیستند زیرا به صورت بسته‌های مشروع ظاهرمی‌شوند.

۳. روش پیشنهادی

با توجه به این که معماری سرویس‌گرا از دیگر فناوری‌های برقراری ابر محسوب‌می‌شود، آسیب‌پذیری‌های مربوط به این معماری نیز، ابر را تحت‌تأثیر قرارمی‌دهند. هنگامی که حملاتی از نوع جلوگیری از سرویس توزیع‌شده، صورت‌بگیرد، منابع سیستم برای دسترسی توسط کاربر یا مشتری دچار اختلال‌می‌شوند. پارامترهای مورد استفاده برای حوزه سرویس عبارت‌اند از: میزان توقف موقت ارائه خدمت (TSU) و میزان ارزش توقف موقت ارائه خدمت (TSUV). میزان توقف موقت ارائه خدمت عبارت است از میزان زمانی که به هر دلیل سرویس در ابر در دسترس نیست.

۱،۳. معماری سیستم تشخیص نفوذ پیشنهادی

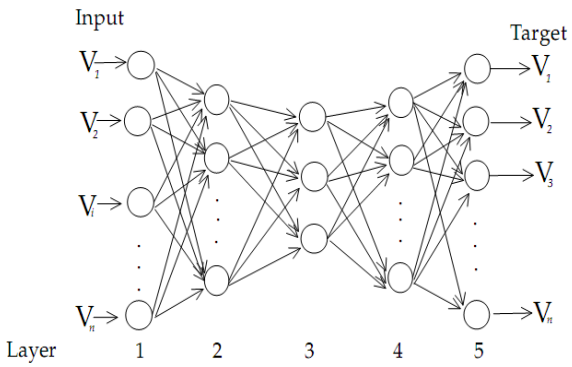
در سیستم‌های تشخیص ناهنجاری یک نوع ارتباط متقابل میان پارامترهای ورودی وجوددارد که علاوه‌بر این ارتباط متقابل میان ورودی‌ها، بر اساس نوع سیستم تشخیص نفوذ، ارتباط متقابلی میان برخی از خروجی‌ها و ارتباط متقابلی میان برخی از ورودی‌ها به‌وجودمی‌آید. این امر، مبنای برخی روش‌های مدل‌سازی محسوب‌می‌شود، اما چنانچه سیستم تشخیص نفوذ بر مبنای رویکرد یادگیری همراه با ناظر برای ساخت مدل نرمال از رفتار موردنظر ساخته‌شود، این امر بیشتر موردتوجه قرارمی‌گیرد. بارزترین نمونه از این نوع ارتباطات پارامتریک می‌تواند در گره‌های پنهان شبکه‌های عصبی مشاهده‌شود که خروجی را بر اساس اتصالات درونی میان لایه پنهان و لایه ورودی و همچنین معماری اتصالات گره‌ها و تابع انتقال گره‌ها تعیین‌می‌کند. همچنین، روش‌های یادگیری در شبکه‌های عصبی نیز به گونه‌های متفاوت رویکرد مدل‌سازی رفتار را به روش مذکور تحت تأثیر قرارمی‌دهند. این امر در شبکه‌های عصبی مبتنی‌بر نظریه تشدید تطبیقی ART بیشتر قابل‌رؤیت است که به‌صورت خام یک روش یادگیری غیرهمراه با ناظر است. اما با ترکیب نظریه‌های تکاملی مانند Fuzzy ART، به رویکردی همراه با ناظر تبدیل‌می‌شود. البته در اینجا، تمرکز کار روی همان یادگیری همراه با ناظر توسط شبکه‌های عصبی است که بدون جداسازی دسته‌های مختلف ورودی‌ها می‌تواند پیچیدگی محاسباتی قابل‌توجهی را به سیستم تشخیص نفوذ تحمیل‌کند. بنابراین، مدل رویکرد پیشنهادی به‌صورت شکل ۱ درمی‌آید. در رویکرد پیشنهادی، یک مؤلفه دیگر نیز با نام تشخیص ناهنجاری از جنبه خصوصیات مشترک نیز مشاهده‌می‌شود. این مؤلفه درواقع برخی پارامترها را مدّنظر قرارمی‌دهد که کلیت رفتار سیستم را نشان‌می‌دهند و درواقع ورودی‌های آن نوعی ارتباط متقابل را با یکدیگر برای تعیین رفتار خروجی سیستم از برخی جنبه‌ها دارامی‌باشند. این امر، برای جلوگیری از گرفتاری در رفتار محلی پارامترها در حوزه‌های خود در این معماری اضافه‌شده‌است.



شکل ۱: مدل روش پیشنهادی

۲،۳. تشخیص ناهنجاری

در این مقاله، مبنای تشخیص ناهنجاری در جنبه‌های مختلف، بررسی وضعیت رفتار کاربران و استفاده از قابلیت‌های تولید مجدد ورودی‌ها در شبکه‌های عصبی RNN است [18, 19]. در این شبکه‌ها طی آموزش شبکه، وزن‌ها به‌گونه‌ای تنظیم‌می‌شوند که بتوانند میزان متوسط مربع خطا را کمینه سازند به‌طوری‌که شبکه بتواند الگوهای تکراری مشترک را به‌خوبی تولیدکنند [20]. ازاین‌رو، این شبکه‌ها پس از آموزش نمی‌توانند الگوهای ورودی را که درواقع به‌صورت ناهنجاری تفاوت عمده‌ای به نمونه‌های آموزشی دارند، به‌خوبی بازتولید کنند. ازاین‌رو، این شبکه‌ها قادرند به شناسایی ناهنجاری در مجموعه‌های مورد آزمون بپردازند [21-24]. به‌این‌ترتیب، در اینجا از شبکه‌های RNN به‌منظور مدل‌سازی رفتار نرمال استفاده‌می‌شود. شکل ۲، معماری عمومی یک RNN را نشان‌می‌دهد.



شکل ۲: معماری عمومی یک شبکه RNN

در شکل 2 شبکه RNN دارای سه لایه پنهان (لایه ۲ و ۳ و ۴) است. تعداد نرون‌های داخل لایه ورودی و خروجی با یکدیگر و با تعداد ویژگی‌های ورودی با شبکه برابر است که باید توسط شبکه RNN موردنظر مدل‌سازی و بازتولید شوند. تعداد لایه‌های پنهان و همچنین تعداد نرون‌های درون هر لایه معمولاً به‌صورت تجربی انتخاب‌می‌شوند. در اینجا معیار جدیدی برای استنتاج میزان ناهنجاری معرفی‌می‌شود. این معیار که پس از نرمال‌سازی داده‌ها، محاسبه‌می‌شود، با نام فاکتور ناهنجاری معرفی‌می‌شود که توسط محاسبه میزان متوسط ناهنجاری در میان ویژگی‌های مورد استفاده در داده‌ها مقداردهی می‌شود:

$$OF = \frac{1}{N}\sum_{i=1}^{N}(x^i - t^i)^2 \qquad (1)$$

به‌طوری‌که مقدار خروجی ویژگی i ام بوده و مقدار واقعی این ویژگی است. اما، ممکن است در مواردی مقدار OF کوچک باشد اما از نظر یک یا چند ویژگی خاص این مقدار زیاد باشد، بنابراین نیاز است بیش‌ترین اختلاف نیز بررسی‌شود تا به‌عنوان یک متریک تکمیلی در کنار OF ارزیابی‌شود:

$$O_{max} = max\{ \quad (x^i - t^i)^2; i = 1, \dots, N\} \qquad (۲)$$

در این تحقیق به‌منظور آزمایش رویکرد پیشنهادی برای تشخیص نفوذ در ابر رایانشی، به‌دلیل عدم‌وجود پایگاه داده معتبر در ابر، به شبیه‌سازی و تولید پایگاه داده پرداخته‌می‌شود. به‌منظور برطرف‌شدن این مشکل، قیدشده‌است که نیاز شبکه‌ها بیش از آن که یادگیری همراه با ناظر باشد، یادگیری نظارت‌نشده است. به‌طور خلاصه این مشکل درنهایت با رویکردی به‌نام RBM بررسی‌شد. در شبکه‌های RBM، یادگیری غیرنظارتی توسط نوعی شبکه عصبی پیاده‌سازی‌می‌شود که امکان استخراج ویژگی‌های سطح بالاتر را از داده‌های خام ورودی فراهم‌می‌کند. اگرچه رویکردهایی مبتنی‌بر تابع گوسی برای مدل‌سازی توابع غیرخطی ارائه‌شده‌است، اما آموزش زنجیره‌ای برای مدل‌سازی کرنل‌های گوسی امری بسیار زمانبر است. ازاین‌رو، ادامه کار برای ساخت مدل رفتار نرمال در تشخیص نفوذ مبتنی‌بر ناهنجاری در این تحقیق نمی‌تواند مسیر RBM، و شبکه‌های عمیق را طی‌کند.

رویکردهای مبتنی‌بر تشخیص امضا درواقع می‌توانند با تولید نتایج مثبت اشتباه کمتر خودنمایی‌کنند. اما، مشکل عمده این روش این است که اساساً با این ابعاد وسیع در ابر و تعدد مؤلفه‌های دخیل درون محیط ابر، اطلاعات مبنی‌بر امضای نفوذها و حملات در عمل بسیار ناچیز است. ازاین‌رو، رویکرد تشخیص ناهنجاری برای تشخیص رفتار مغرضانه، در حال حاضر، راهکار مناسب برای تشخیص نفوذ محسوب‌خواهدشد. در این مقاله بیشتر به تشخیص رفتار مشکوک از طریق تشخیص ناهنجاری در رفتار کاربران می‌پردازیم. بنابراین، معیار ارزیابی در این تحقیق مبتنی‌بر سنجش‌های تشخیص ناهنجاری خواهدبود.

۳،۳. ایجاد پایگاه داده

در اینجا پایگاه داده ۵ دسته مختلف از داده‌ها را دربرمی‌گیرد: شبکه یا NIDS، ماشین مجازی یا VMIDS، حوزه تقاضا، حوزه ابر و حوزه سرویس. ازاین‌رو، این ۵ حوزه بررسی‌می‌شوند:

حوزه شبکه

پارامترهای منتخب برای حوزه شبکه شامل موارد زیر می‌شوند: پروتکل مورد استفاده (PID)، طول سرآیند بسته اطلاعاتی (PLEN)، Check Sum (CS)، پورت مبدأ و پورت مقصد.

در ابر ماشین مجازی بر اساس قوانین میزبان، بسته به ترافیک و مجموعه‌ای خاص از بسته‌ها می‌شود. نکته مهم اینجاست که این ترافیک با توجه به آزادی عمل کاربران برای استفاده از سیستم‌ها و مکان‌های مختلف برای برقراری ارتباط با ابر، و همچنین مشخص نبودن میزبان فیزیکی ماشین مجازی مشتری مشخص که با توجه به توزیع بار و متعادل‌سازی بار در ابر در هر لحظه می‌تواند تغییرکند، به‌طورقطع نمی‌تواند وابسته به نشانی IP مبدأ و نشانی مقصد باشد. البته در ادبیات موضوع نشانی مبدأ و نشانی مقصد تقریباً جزء لاینفک سیستم‌های تشخیص نفوذ مبتنی‌بر شناخت ناهنجاری در شبکه است. پارامترهای مشترک دیگر نیز، با توجه به نشانی مبدأ و مقصد می‌تواند شامل پورت ارتباطی مبدأ و مقصد باشد که دیگر نشانی مبدأ و مقصد را برخلاف نشانی IP، موقعیت جغرافیایی محدودنمی‌کند.

حوزه ماشین مجازی

حوزه ماشین مجازی شامل موارد زیر می‌شود: نام مالک ماشین مجازی (VMO)، نام فرآیند (PO)، تعداد نخ‌های فرآیند (TN)، درصد استفاده از ظرفیت پردازنده (CU) و درصد استفاده از ظرفیت RAM (RU).

حوزه تقاضا

حوزه تقاضا شامل موارد زیر می‌باشد: میزان تقاضا، میزان ردشدن درخواست، میزان دانه‌دانه‌ای بودن تقاضا. با توجه به این که تقاضا به ابر بیشتر تقاضا برای یک محصول تجاری محسوب‌شده و ماهیت ابر که مستقیماً ارائه خدمات پردازشی برخط را برای مشتریان در بازار فراهم‌می‌کند، قوانین بازارهای محصولات تجاری نیز بر ارائه تقاضا به ابر حاکم خواهدبود. این امر مانند تقاضا برای سهام محسوب‌می‌شود و تقاضا برای محصولات تجاری و سهام و به‌طورکلی پارامترهای وابسته اقتصادی به محصولات تجاری دارای دوره‌های تکرار الگو هستند. درواقع دوره‌های تکرار الگو شامل دوره‌های بلندمدت، میان‌مدت و کوتاه‌مدت می‌شوند که تکرار این‌ها طی زمان منجر به تولید رفتار خاص مربوط به یک پارامتر مدل‌سازی می‌شود. البته طول مدت زمان ممکن است یک الگو میزان پیوسته‌ای را از کوتاه‌مدت تا بلندمدت شامل‌شود و پارامترهای مدل‌سازی نیز در زمان پیوسته مدل‌سازی می‌شوند. این دوره‌های زمانی تکرار الگو، درحقیقت مبنای اصل پیش‌بینی برای سری‌های زمانی را تشکیل‌می‌دهد و این دوره‌های مشخص هستند که قابلیت پیش‌بینی را فراهم‌می‌سازند. بر این اساس، روند میزان تقاضا با توجه به دوره‌های تکراری رفتار مشتریان؛ میزان ردشدن درخواست با توجه به ظرفیت منابع در ابر و تعداد و میزان درخواست‌ها و میزان دانه‌دانه‌ای بودن تقاضا با توجه به نیازهای مشخص کاربران، در زمان‌های مشخص در روز می‌تواند بیان‌کننده تأثیر عامل اقتصادی تقاضا بر تشکیل رفتار نرمال میان کاربران در ابر محسوب‌شود. درواقع، در طراحی سیستم‌های تشخیص نفوذ مبتنی‌بر شبکه تحلیل خاصی را نمی‌توان برای توجیه رفتار نرمال مشتریان ارائه‌کرد، اما با اضافه‌شدن عامل اقتصادی تقاضا در ابر وجود رفتار نرمال کاملاً قابل‌توجیه بوده و مبنای قوی دارد. بنابراین، وجود رفتار نرمال بر اساس وجود عامل اقتصادی تقاضا در ابر و درنتیجه طراحی سیستم‌های تشخیص نفوذ مبتنی‌بر شناخت ناهنجاری در ابر مبنا و جامعیت بسیار قوی‌تری در ابر نسبت به سیستم مشابه در شبکه‌های کامپیوتری و دیگر حوزه‌های تشخیص نفوذ دارد.

دانه‌دانه‌ای بودن عبارت است از:

$$Granularity = \frac{\sum_{i=1}^{N} e^{CPU_i}}{e^{\sum_{i=1}^{N} CPU_i}} \qquad (۲)$$

البته برای مقادیری که در اینجا به‌عنوان دانه‌دانه‌ای بودن به‌دست‌می‌آید، سیستم شبکه عصبی به‌دلیل محدوده وسیع این متغیر کارایی کمی از خود نشان‌می‌دهد. ازاین‌رو، رابطه (۲) با رابطه (۳) جایگزین‌می‌شود.

$$Granularity_t = \frac{e^{N_t}}{N_t} \quad (۳)$$

به‌طوری‌که N تعداد درخواست‌ها در زمان t می‌باشد.

حوزه ابر

حوزه خصوصیات ابر شامل پارامترهای زیر می‌شود: روند بارکاری پردازنده (CW)، روند بارکاری RAM (RW). اگرچه عامل اقتصاد روند ورودی تقاضا به ابر را پوشش‌داد، اما بحث درونی ابر دارای برخی پارامترهای منحصربه‌فرد است که باید از دیدگاه پارامترهای درونی ابر به آن توجه‌شود. این پارامترها شامل میزان کلی بارکاری پردازنده‌ها و RAM های موجود در مجموعه منابع ابر است. مبنای این دو پارامتر این است که علاوه‌بر ماشین‌های مجازی، مکانیسم‌های مدیریتی میزبان‌های فیزیکی نیز مقادیری از منابع ابر را مصرف‌می‌کنند که مصارف کنترلی و مدیریت دارند. بنابراین، با توجه به عوامل بیرونی، بارکاری و روند تغییر آن در لحظات مختلف روز می‌تواند وابسته به این موارد نیز باشد. حال آن‌چه اهمیت این پارامترها را بیشتر می‌کند، حملاتی هستند که منابع ابر را مصرف‌کرده و خود ابر را تحت‌تأثیر قرارمی‌دهند. بدین‌ترتیب، با مشاهده و مانیتورینگ این رفتار از بارکاری پردازنده و RAM می‌توان ناهنجاری‌های قابل‌توجه را تشخیص‌داده و به سیستم تشخیص و یا سیستم جلوگیری از نفوذ ارجاع‌داد.

حوزه سرویس

پارامترهای مورد استفاده برای حوزه سرویس عبارت‌اند از: میزان توقف موقت ارائه خدمت (TSU) و میزان ارزش توقف موقت ارائه خدمت (TSUV). میزان توقف موقت ارائه خدمت عبارت است از میزان زمانی که به هر دلیل سرویس در ابر در دسترس نیست. این مورد نیز یکی دیگر از مواردی است که منحصراً در ابر موردتوجه است چون خدمات به‌عنوان شیء سرویس ارائه‌شده و مدت زمانی که دسترسی به این شیء امکان‌پذیر نیست یعنی توقف موقت در ارائه خدمت از سوی ابر به مشتری رخ‌داده‌است.

هنگامی که حملاتی از نوع DoS یا هر شکل مربوط به آن مانند DDoS و یا به‌صورت Flood صورت‌گیرد، منابع سیستم و شبکه برای دسترسی توسط کاربر یا مشتری دچار اختلال‌می‌شوند. هنگامی که ماشین‌های مجازی از یک ماشین فیزیکی میزبان به ماشین فیزیکی میزبان دیگر انتقال‌می‌یابند، این امر معمولاً به‌صورت فرآیند Pre-Copy انجام‌می‌شود. درنتیجه، یک ماشین مجازی دیگر به‌صورت موازی با ماشین مجازی موردنظر بر روی ماشین فیزیکی مقصد کارمی‌کند و تا زمانی که انتقال اطلاعات نیازمند کمترین زمان توقف موقت ارائه خدمت برای انتقال اطلاعات ضروری مجموعه کاری پردازنده شود، این امر ادامه‌خواهدیافت. بنابراین، در زمان‌های مختلف روز هنگامی که میزان تقاضا و بارکاری در مدت زمان‌های یکسان در روزهای مختلف میزان متفاوتی را نسبت به دیگر لحظات در روز شامل‌می‌شود، میزان توقف موقت ارائه خدمت نیز به نسبت متفاوت خواهدبود. اگرچه، این میزان می‌تواند تابعی از وضعیت ابر، وضعیت و تقاضای مشتریان و عوامل بیرونی باشد؛ اما، به هر حال تابعی از برخی متغیرها از قبیل روند رفتاری مشتریان، میزان بارکاری، تعمیر و نگهداری و موارد درون و برون سیستمی است.

درواقع، هرچقدر سرویس هزینه بالاتری داشته‌باشد، میزان توقف موقت ارائه خدمت نیز مهم‌تر خواهدبود. برای تأکید می‌توان به این امر اشاره‌کرد که انتظار می‌رود حملات بیشتر به ماشین‌های مجازی مهم‌تر صورت‌گیرند تا ماشین‌های مجازی ارزان‌تر و کوچک‌تر. هرچند، اهداف مختلف نفوذگران می‌تواند نتایج و نیت‌های متفاوتی داشته و به‌طورکلی خود ابر را هدف قراردهند، اما این امر می‌تواند برای تحت‌تأثیر قراردادن یک ماشین مجازی با تأثیر بر ماشین‌های مجازی دیگر رخ‌دهد.

۴،۳. مدل‌سازی سری‌های زمانی با استفاده از ابزار یادگیری ماشین

مدل‌سازی مذکور به معنی این است که سیستم یادگیرنده قابلیت بازتولید خروجی دریافتی را پس از دریافت ورودی مربوطه داراست. در این تحقیق البته ما با دو نوع یادگیری نظارتی روبرو هستیم. پارامترهای مربوط به حوزه شبکه و ماشین مجازی توسط تعبیه یک autoencoder (یا شبکه عصبی تکرارکننده) از طریق همان شکل (ورودی-خروجی) مربوط به یادگیری نظارتی اما با دریافت زوج مقادیر (ورودی-ورودی)، مدل‌سازی‌می‌شوند که همان شکل یادگیری نظارتی کلاسیک می‌باشد. اما، پارامترهای حوزه‌های تقاضا، ابر و سرویس به‌صورت سری زمانی مطرح‌می‌شوند و شکل ورودی-خروجی را برای سیستم یادگیرنده فراهم‌نمی‌کنند. چنانچه بخواهیم یک سری زمانی را توسط روش‌های یادگیری ماشین نظارتی مدل‌سازی‌کنیم، مسئله به‌طورکلی با نام مسئله یادگیری نظارتی ترتیبی شناخته‌خواهدشد. مدل‌سازی سری‌های زمانی می‌تواند دو جنبه متفاوت داشته‌باشد. جنبه اول رابطه محور پایه یا زمان را با مقدار پارامتر متغیر مورد مدل‌سازی قرارداده و به پیش‌بینی پارامتر اصلی سری زمانی توسط عامل زمان می‌پردازد. اما، این نوع مدل‌سازی نمی‌تواند انعطاف پذیری کافی را برای مسائل چندمتغیره فراهم‌آورد، زیرا پارامتر موردنظر ممکن است کاملاً به زمان وابسته نبوده و روند پیشین تغییر مقدار متغیر را دنبال‌کند. بنابراین، رویکرد جامعی که برای مدل‌سازی سری‌های زمانی استفاده‌می‌شود، معمولاً بیش از آن که عامل زمان را در محاسبه مقدار آتی متغیر دخیل‌کند، به پیش‌بینی مقدار آتی متغیر توسط بازبینی و مدل‌سازی چند مقدار اخیر آن می‌پردازد. البته، چگونگی این امر خود مباحث بازی را در استخراج الگو و داده‌کاوی بازمی‌کند، اما به‌طورکلی روش‌های شناخته‌شده‌ای مانند پنجره لغزان، بیش‌ترین کاربرد را در شناسایی الگوها و مدل‌سازی سری‌های زمانی توسط روش‌های یادگیری نظارتی داراست. بنابراین اینجا نیز از تکنیک پنجره لغزان استفاده‌می‌شود.

تکنیک پنجره لغزان، درحقیقت پنجره به طول N داده متوالی از سری زمانی را جدامی‌کند. از داده‌های درون این پنجره N-1 داده اول

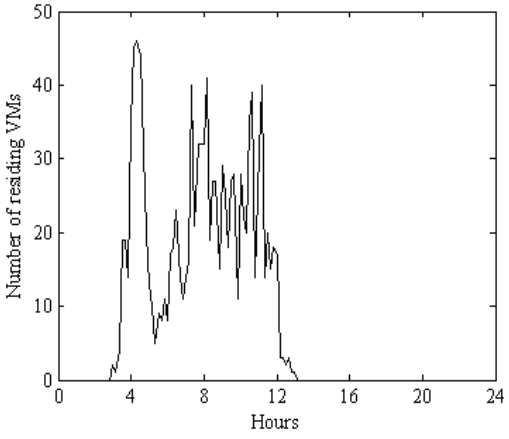
به‌عنوان ورودی درنظرگرفته‌شده و داده Nام به‌عنوان خروجی مطرح-می‌شود. بدین ترتیب، چنانچه از ابتدای سری زمانی با حرکت به اندازه یک واحد، تمام داده‌های متوالی را به این شکل درآوریم، مسئله به‌صورت دلخواه برای پذیرش توسط روش‌های یادگیری نظارتی از قبیل شبکه عصبی درمی‌آید. بدین ترتیب، می‌توان توسط شبکه‌های عصبی به مدل‌سازی پارامترهای رفتار نرمال کاربران در حوزه‌های تقاضا، ابر و سرویس پرداخت.

۴. ارزیابی شبکه عصبی در مدل‌سازی داده‌های ورودی

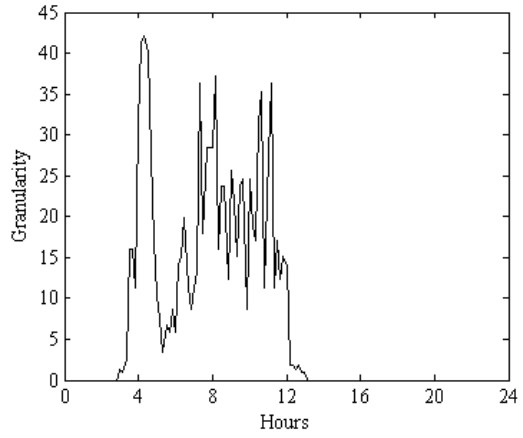
در این تحقیق، به‌طورکلی یادگیری نظارتی برای دو حوزه شبکه و ماشین مجازی به‌صورت یادگیری نظارتی کلاسیک و برای سه حوزه تقاضا ، ابر و سرویس به‌صورت ترتیبی استفاده‌می‌شود. در ادامه به شرح نحوه ارزیابی هریک از این حوزه‌ها می‌پردازیم.

۱،۴. مدل‌سازی سری زمانی حوزه تقاضا

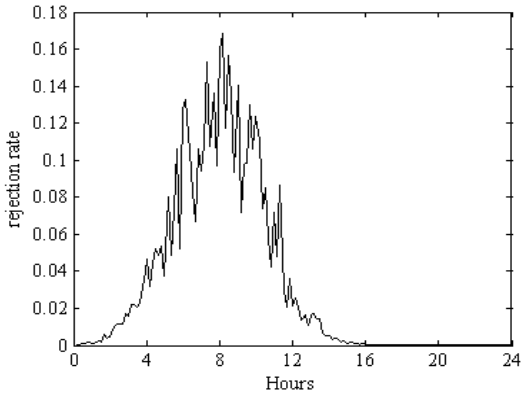
پارامترهای حوزه تقاضا نقطه اتکای این مقاله برای توجیه قابل‌پیش‌بینی بودن و دارای الگوهای معین بودن مشتریان در ابر است. بنابراین، باید بتوان پیش از هرچیز این جنبه را بررسی‌کرد. درواقع این پارامترها چنانچه لازم‌باشد به‌صورت زوج مقادیر «ورودی-خروجی» یا همان یادگیری نظارتی مدل‌سازی‌شوند، مسئله را به شکل یادگیری نظارتی ترتیبی مطرح‌می‌کنند که به‌شکل خام توسط شبکه‌های عصبی قابل مدل‌سازی نیست. ازاین‌رو، با استفاده از تکنیک پنجره لغزان این پارامترها به شکل مسئله یادگیری نظارتی کلاسیک درخواهندآمد. بدین ترتیب، توسط انتخاب پنجره‌ای با اندازه ۴ واحد، مدل‌سازی را برای این پارامترها انجام‌می‌دهیم. شکل ۳ نمودار توزیع تعداد تقاضا، میزان دانه‌دانه‌ای بودن تقاضا و نرخ ردشدن درخواست را نشان‌می‌دهد.



(الف)



(ب)



(ج)

شکل ۳: نمودار مشخصه پارامترهای حوزه تقاضا

برای تعیین معماری شبکه عصبی، ابتدا لازم است شکل ورودی و خروجی به‌صورت رابطه (۴) تعیین‌شود.

$$\begin{cases} input: \{x_{t-2}, x_{t-1}, x_t\} \\ output: x_{t+1} \end{cases} \quad (۴)$$

اما، برای تعیین معماری شبکه عصبی موردنظر، نکته مبهم تعداد گره‌های لایه پنهان است؛ البته تابع انتقال گره‌های لایه میانی و گره‌های خروجی نیز بسیار مهم هستند. اما با توجه به این که شبکه عصبی به‌عنوان تقریب‌زننده عمومی برای توابع غیرخطی پیوسته معمولاً دارای تابع انتقال Sigmoid در گره‌های لایه پنهان و تابع انتقال خطی در گره‌های لایه خروجی است، لذا، این توابع را برای شبکه عصبی یادشده درنظر-می‌گیریم. اما، تعداد گره‌های لایه پنهان موضوع بسیار مهمی است که نقش قابل‌توجهی در کارایی شبکه عصبی در مدل‌سازی داده‌های موردنظر دارد. درواقع با تغییر تعداد گره‌ها، کارایی شبکه عصبی را در مدل‌سازی سری‌های زمانی رفتار نرمال کاربران بررسی‌کرده و بهترین گزینه را انتخاب‌می‌کنیم. برای هر سه پارامتر Dem، Gran و Rej معماری شبکه‌های عصبی استفاده‌شده به‌صورت ۳)۸(۱، به معنی سه ورودی، ۸ گره در لایه پنهان و یک خروجی می‌باشد. جدول (۱) تحلیل حساسیت را برای پارامترهای Dem، Gran و Rej نشان‌می‌دهد:

جدول۱: تحلیل حساسیت را برای پارامترهای Dem، Gran و Rej

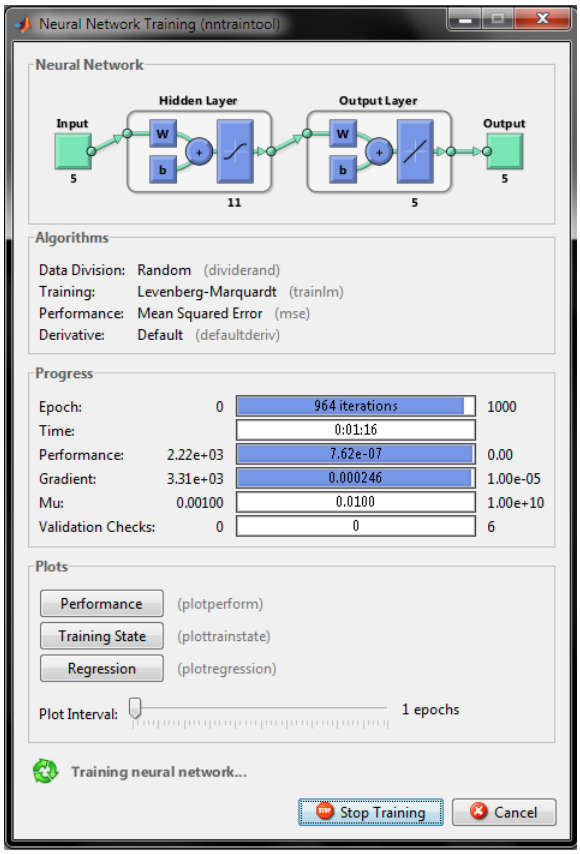
میزان نویز %	Dem		Gran		Rej	
	NMSE	R	NMSE	R	NMSE	R
0	۰,۰۰۵۲	۰,۹۷	۰,۰۰۴۴	۰,۹۸	۰,۰۰۳۳	0.97
۵	۰,۰۰۶۸	۰,۹۶	۰,۰۰۴۹	۰,۹۷	۰,۰۰۴۸	۰,۹۷
10	۰,۰۰۹۳	۰,۹۵	۰,۰۰۵۸	۰,۹۵	۰,۰۰۶۱	۰,۹۶
15	۰,۰۱۳	۰,۹۳	۰,۰۰۸۸	۰,۹۴	۰,۰۰۷۹	۰,۹۴

۲,۴. مدل‌سازی NIDS

برای مدل‌سازی رفتار نرمال کاربران در حوزه شبکه باید پارامترهای زیر را مدل‌سازی کند: شناسه کاربری، پروتکل مورداستفاده، طول سرآیند بسته اطلاعاتی، Check Sum، پورت مبدأ و پورت مقصد. شبکه عصبی مورداستفاده برای مدل‌سازی رفتار نرمال کاربران در حوزه شبکه همان‌طور که پیش تر عنوان شد یک شبکه عصبی تکرارکننده یا به‌صورت فنی‌تر یک autoencoder است. معماری این شبکه نیز به‌صورت سعی و خطا انتخاب‌شده و درنهایت به شکل ۶(۹)۶(۶) درآمده‌است.

۳,۴. مدل‌سازی VMIDS

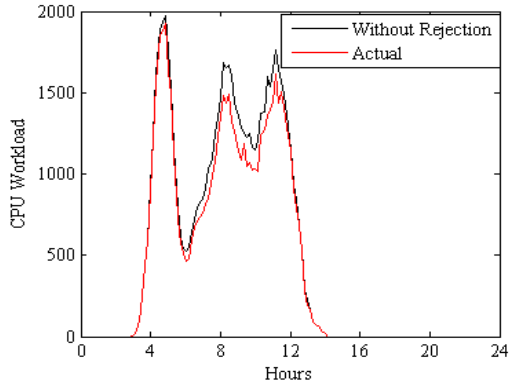
مانند مدل‌سازی در حوزه شبکه، حوزه رفتار ماشین مجازی نیز باید به‌صورت مدل‌سازی رفتار نرمال ماشین‌های مجازی توسط شبکه عصبی تکرارکننده یا autoencoder برای پارامترهای زیر صورت‌گیرد: نام مالک ماشین مجازی، نام فرآیند، تعداد نخ‌های فرآیند، درصد استفاده از ظرفیت پردازنده و درصد استفاده از ظرفیت RAM. مانند حوزه شبکه، سعی و خطا معیار تعیین مدل RNN برای مدل‌سازی رفتار نرمال ماشین مجازی خواهدبود. مدل این شبکه به صورت ۵(۵(۱۱(۵ درنظرگرفته‌شده‌است. این مدل در شکل ۴ آمده‌است.



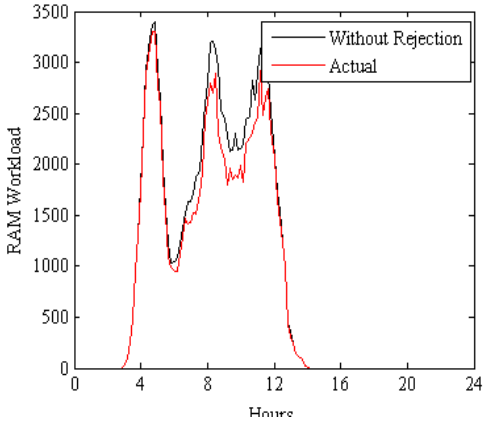
شکل ۴: مدل RNN مربوط به سیستم تشخیص نفوذ حوزه شبکه

۴,۴. مدل‌سازی سیستم حوزه ابر

حوزه ابر نیز برای مدل‌سازی رفتار عمومی ابر شامل پارامترهایی در قالب سری‌های زمانی برای بارکاری کلی پردازنده و RAM می‌باشد. این پارامترها نیز با استفاده از تکنیک پنجره لغزان، با پنجره‌ای به اندازه ۴ واحد، از مسئله یادگیری نظارتی ترتیبی به شکل مسئله نظارتی کلاسیک درمی‌آیند. شبکه‌های عصبی مورداستفاده برای مدل‌سازی بارکاری پردازنده و RAM به‌صورت ۱(۷(۳ می‌باشد. در شکل ۵ در الف و ب به‌ترتیب نمودار رفتار عمومی ابر برای بارکاری پردازنده و RAM را در زمان‌های یک روز نشان‌داده‌می‌شوند.



(الف)



(ب)

شکل ۵: نمودار رفتار عمومی ابر برای بارکاری پردازنده و RAM

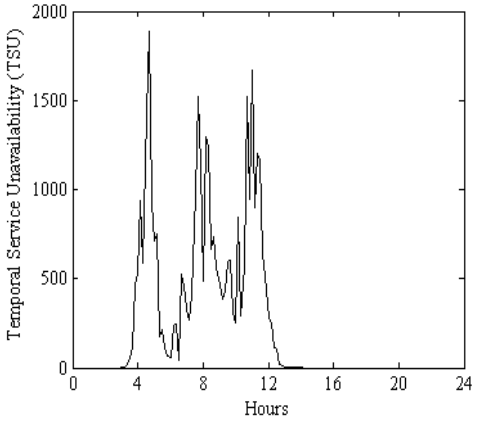
جدول ۲ تحلیل حساسیت برای کارایی این شبکه‌ها را در حضور نویز نشان‌می‌دهد.

جدول ۲: کارایی شبکه عصبی برای مدل‌سازی TSU و TSUV

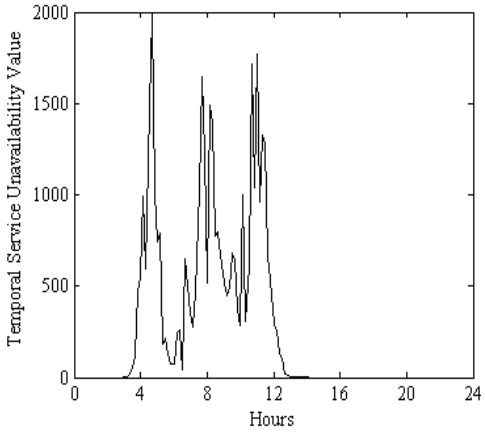
میزان نویز	بارکاری CPU		بارکاری RAM	
	NMSE	R	NMSE	R
٪۰	۰,۰۱۶	۰,۹۴	۰,۰۱۲	۰,۹۵
٪۵	۰,۰۱۹	۰,۹۳	۰,۰۱۶	۰,۹۵
٪۱۰	۰,۰۲۷	۰,۹۳	۰,۰۲۲	۰,۹۴
٪۱۵	۰,۰۳۲	۰,۹۰	۰,۰۳۵	۰,۹۲

۵,۴. مدل‌سازی سیستم حوزه سرویس

حوزه سرویس مانند حوزه تقاضا و حوزه ابر دارای پارامترهایی از نوع سری زمانی است که همانند این دو حوزه توسط تکنیک پنجره لغزان با پنجره‌هایی با اندازه ۴ به مسئله یادگیری نظارتی کلاسیک تبدیل-می‌شود. شکل ۴ نمودار TSU و TSUV را نشان‌می‌دهد.



(الف)



(ب)

شکل ۶: نمودار توقف موقت ارائه خدمت. الف) TSU، ب) TSUV

معماری‌های شبکه‌های عصبی تعبیه‌شده برای پارامترهای این حوزه شامل روند میزان توقف موقت ارائه خدمت و ارزش توقف موقت ارائه خدمت به‌ترتیب به‌صورت ۱(۷(۳، ۱(۷(۳ و ۱(۸(۳ می‌باشد. جدول ۳ تحلیل حساسیت را برای شبکه‌های عصبی این حوزه نشان‌می‌دهد.

جدول ۳: کارایی شبکه عصبی برای مدل‌سازی TSU و TSUV

میزان نویز	TSU		TSUV	
	NMSE	R	NMSE	R
0%	۰,۰۱۱	۰,۹۵	۰,۰۱۲	۰,۹۷
5%	۰,۰۱۴	۰,۹۳	۰,۰۱۵	۰,۹۶
٪۱۰	۰,۰۱۸	۰,۹۲	۰,۰۱۷	۰,۹۴
15%	۰,۰۲۳	۰,۹۲	۰,۰۲	۰,۹۳

۵. نتیجه‌گیری

درواقع رویکردهای پیشین با تعداد ارجاعات بسیار زیاد معمولاً شبکه عصبی مدل‌ساز را به‌صورت یک دسته‌بندی‌کننده با یک گره در لایه خروجی به‌کارمی‌بردند تا بتوانند با یک مقدار صفر و یا یک نفوذ یا عادی-بودن رفتار را دسته‌بندی‌کنند. برای این امر، لازم است رفتار حمله همراه رفتار عادی با تعداد داده‌های برابر یعنی ٪۵۰ رفتار عادی و ٪۵۰ رفتار مربوط به نفوذ به شبکه به‌عنوان ورودی واردشود و یک برچسب تفاوت این دو رفتار متفاوت را به شبکه اطلاع‌دهد. مشکلی که دربارهٔ این رویکرد در ادبیات موضوع نیز به آن اشاره‌شده، همان مشکل معروف پیش برازش است که البته با مکانیسم‌های Cross-validation در قالب Early Stopping توسط شبکه‌های عصبی به آن پرداخته‌شده و مشکل برطرف‌خواهدشد. در این مقاله مدل‌سازی رفتار نرمال انجام‌شده و در روش موردمقایسه مدل‌سازی نفوذ صورت‌می‌گیرد. اما از طرفی، برای روش پیشنهادی داده‌های نفوذ دردسترس نیست و برای رویکرد موردمقایسه داده‌های عادی به این صورت، معیارهای ارزیابی منطقاً تقابل برعکس نتایج مثبت اشتباه و نتایج منفی اشتباه را درپی‌خواهندداشت. بنابراین، اگرچه حوزه معیارهای ارزیابی را در تقابل یکدیگر قرارمی‌دهد، اما رویکرد و دیدگاه مدل‌سازی یکسان بوده و کاملاً تطبیق‌می‌کند. روش پیشنهادی و روش موردمقایسه هر دو در تلاشند تا آنچه دراختیاردارند

را مدل‌سازی‌کنند و آنچه در اختیار نیست را به‌صورت تصادفی تولیدمی‌کنند. بنابراین چنانچه هر دو برای داده یکسان پیاده‌سازی‌شوند ولی اهمیت حوزه روش موردمقایسه به مدل‌سازی داده‌های رفتار نرمال تغییرکند، مسأله مقایسه به تقابل کارایی دو روش یادگیری ماشین در مدل‌سازی داده‌های موجود تبدیل‌می‌شود. نوع متغیرهای موردارزیابی در جدول ۴ دیده‌می‌شود:

مراجع

[1] Jaber, A. N., & Rehman, S. U. (2020). FCM–SVM based intrusion detection system for cloud computing environment. Cluster Computing, 1-11.

[2] Shamshirband, S., Fathi, M., Chronopoulos, A. T., Montieri, A., Palumbo, F., & Pescapè, A. (2020). Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. Journal of Information Security and Applications, 55, 102582.

[3] Krishnaveni, S., Sivamohan, S., Sridhar, S. S., & Prabakaran, S. (2021). Efficient feature selection and classification through ensemble method for network intrusion detection on cloud computing. Cluster Computing, 1-19.

[4] Zhang, Z., Wen, J., Zhang, J., Cai, X., & Xie, L. (2020). A many objective-based feature selection model for anomaly detection in cloud environment. IEEE Access, 8, 60218-60231.

[5] Wei, J., Long, C., Li, J., & Zhao, J. (2020). An intrusion detection algorithm based on bag representation with ensemble support vector machine in cloud computing. Concurrency and Computation: Practice and Experience, 32(24), e5922.

[6] Krishnaveni, S., Vigneshwar, P., Kishore, S., Jothi, B., & Sivamohan, S. (2020). Anomaly-based intrusion detection system using support vector machine. In Artificial Intelligence and Evolutionary Computations in Engineering Systems (pp. 723-731). Springer, Singapore.

[7] Aldribi, A., Traore, I., Moa, B., & Nwamuo, O. (2020). Hypervisor-based cloud intrusion detection through online multivariate statistical change tracking. Computers & Security, 88, 101646.

[8] Abdulqadder, I. H., Zhou, S., Zou, D., Aziz, I. T., & Akber, S. M. A. (2020). Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5G networks using AI-based defense mechanisms. Computer Networks, 179, 107364.

[9] Alkadi, O., Moustafa, N., Turnbull, B., & Choo, K. K. R. (2020). A deep blockchain framework-enabled collaborative intrusion detection for protecting iot and cloud networks. IEEE Internet of Things Journal.

[10] Mugabo, E., & Zhang, Q. Y. (2020). Intrusion Detection Method Based on Support Vector Machine and Information Gain for Mobile Cloud Computing. IJ Network Security, 22(2), 231-241.

[11] Kushwah, G. S., & Ranga, V. (2020). Voting extreme learning machine based distributed denial of service attack detection in cloud computing. Journal of Information Security and Applications, 53, 102532.

[12] Kushwah, G.S. and Ranga, V., 2022. DDoS Attacks Detection in Cloud Computing Using ANN and Imperialistic Competitive Algorithm. In Artificial Intelligence and Sustainable Computing (pp. 253-263). Springer, Singapore.

[13] R. Sondhiya, M .Shreevastav, and M. Mishra, "To Improve Security in Cloud Computing with Intrusion detection system using Neural Network," *International Journal of Soft Computing and Engineering (IJSCE)* vol. 3, 2013.

[14] K. Zunnurhain, "FAPA: a model to prevent flooding attacks in clouds," in *Proceedings of the 50th Annual Southeast Regional Conference*, 2012, pp. 395-396.

[15] S. N. Dhage and B. Meshram, "Intrusion detection system in cloud computing environment," *International Journal of Cloud Computing*, 2012, vol. 1, pp.282-61.

[16] H. M. Alsafi, W. M. Abduallah, and A.-S. K. Pathan, "IDPS: an integrated intrusion handling model for cloud computing environment," *International Journal of Computing & Information Technology (IJCIT)*, vol. 4, pp. 1-16, 2012.

[17] T. Vissers, T. S. Somasundaram, L. Pieters, K. Govindarajan, and P. Hellinckx, "DDoS defense system for web services in a cloud environment," *Future Generation Computer Systems*, vol. 37, pp. 37-45, 2014.

[18] Kim, M., Ou, E., Loh, P. L., Allen, T., Agasie, R., & Liu, K. (2020). RNN-Based online anomaly detection in nuclear reactors for highly imbalanced datasets with uncertainty. Nuclear Engineering and Design, 364, 110699.

[19] Wei, G., & Wang, Z. (2021). Adoption and realization of deep learning in network traffic anomaly detection device design. Soft Computing, 25(2), 1147-1158.

[20] Chaibi, N., Atmani, B., & Mokaddem, M. (2020, October). Deep Learning Approaches to Intrusion Detection: A new Performance of ANN and RNN on NSL-KDD. In Proceedings of the 1st International Conference on Intelligent Systems and Pattern Recognition (pp. 45-49).

[21] Murugesan, M., & Thilagamani, S. (2020). Efficient anomaly detection in surveillance videos based on multi layer perception recurrent neural network. Microprocessors and Microsystems, 79, 103303.

[22] Wu, D., Zhu, H., Zhu, Y., Chang, V., He, C., Hsu, C. H., ... & Huang, Z. (2020). Anomaly Detection Based on RBM-LSTM Neural Network for CPS in Advanced Driver Assistance System. ACM Transactions on Cyber-Physical Systems, 4(3), 1-17.

[23] Yin, C., Zhang, S., Wang, J., & Xiong, N. N. (2020). Anomaly detection based on convolutional recurrent autoencoder for IoT time series. IEEE Transactions on Systems, Man, and Cybernetics: Systems.

[24] Luo, D., Lu, J., & Guo, G. (2020). Road Anomaly Detection Through Deep Learning Approaches. IEEE Access, 8, 117390-117404.