مجله‌بین المللی روندها و فناوری کامپیوتر
شابک:۲۲۳۱–۲۸۰۳/https://doi.org/10.14445/22312803/IJCTT-V73I3P107
جلد۷۳، شماره ۳، ۵۷-۶۳، مارس ۲۰۲۵ ©
۲۰۲۵گروه تحقیقاتی حس هفتم®

مقاله‌اصلی

ارزیابی‌ریسک و انطباق با قوانین مبتنی بر هوش مصنوعی در امنیت‌سایبری ابری

تیاگاراجان‌مانی چتیار۱ونکاتا آشوک کومار بوییناز۲، ساندیپ رنگیننی۳

۱محقق مستقل، ساوت ویندزور، کنتیکت، ایالات متحده.
۲محقق مستقل، کامینگ، جورجیا، ایالات متحده.
۳محقق مستقل، وست هیلز، کالیفرنیا، ایالات متحده.

۱نویسنده مسئول: thiyaga1980@gmail.com

دریافت:۱۴ ژانویه ۲۰۲۵ بازبینی شده:۱۹ فوریه ۲۰۲۵ پذیرفته‌شده: ۱۱ مارس ۲۰۲۵ منتشرشده: ۲۹ مارس ۲۰۲۵

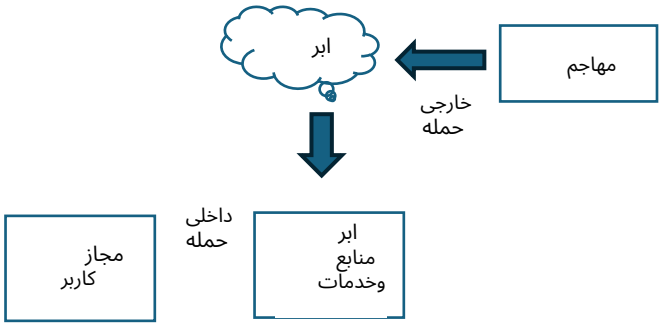
چکیده-رایانش ابری، انقلابی در زیرساخت های دیجیتال، می تواند به سازمان ها اجازه دهد تا در مقیاس وسیع فعالیت کنند. اگرچه رایانش ابری مزایای‌خود را دارد، اما با تهدیدات امنیتی جدیدی همراه است و بنابراین نیاز به فرآیندهای ارزیابی ریسک و انطباق دقیق دارد. با استفاده از یادگیری ماشینی‌و هوش مصنوعی برای بهبود تشخیص تهدید، خودکارسازی نظارت بر انطباق و کاهش آسیب پذیری ها، ما یک رویکرد ارزیابی ریسک امنیت سایبری‌ابری مبتنی بر هوش مصنوعی و انطباق با مقررات ارائه می دهیم. از تجزیه و تحلیل رفتاری، تشخیص ناهنجاری و تجزیه و تحلیل پیش بینی کننده‌برای شناسایی تهدیدات سایبری قبل از وقوع آنها استفاده می کنیم. سیستم های هوش مصنوعی با نظارت بر داده های جمع آوری شده‌از سیستم ابری برای الگوهای رفتاری تکراری که نشان دهنده تخلف هستند، تأخیر پاسخ را کاهش می دهند تا از نقض های امنیتی جلوگیری‌کنند. ارزیابی ریسک در زمان واقعی این چارچوب به سازمان ها اجازه می دهد تا اقدامات امنیتی را بر اساس اثرات و احتمالات بالقوه اولویت بندی‌کنند. هوش مصنوعی می تواند مجموعه داده های عظیمی را برای شناسایی شکاف های انطباق، توصیه راه حل ها و ارائه گزارش های آماده‌حسابرسی بررسی کند و در عین حال سربار عملیاتی و خطای انسانی را به حداقل برساند. معماری مقیاس پذیر و انعطاف پذیری برای پاسخگویی به‌خطرات جدید امنیت سایبری، آن را به یک سیستم ایده آل برای استفاده در محیط های چند ابری و ابر هیبریدی تبدیل می کند. این یک مزیت بزرگ برای‌شناسایی ریسک و نظارت بر انطباق است زیرا این سیستم پتانسیل یادگیری و سازگاری با گذشت زمان را دارد. این امر، دفاع در برابر تهدیدات APT، روز صفر و داخلی را تقویت می کند. ادغام هوش مصنوعی با سیستم های SIEM، پاسخ به حادثه و همبستگی تهدید در زمان واقعی را افزایش می دهد.برخی از مزایایی که سازمان ها می توانند با استفاده از هوش مصنوعی برای مدیریت انطباق از آن بهره مند شوند عبارتند از کاهش هزینه های‌حسابرسی، بهبود حاکمیت امنیتی و گزارش دهی سریع تر نظارتی. این یافته نشان دهنده ضرورت برنامه های هوش مصنوعی برای ایمن سازی‌محیط های ابری است و پذیرش بیشتر آن را در چارچوب های امنیت سایبری توصیه می کند. مطالعات آینده بر مدل های بهبود یافته مبتنی‌بر هوش مصنوعی در جهت امنیت سایبری، اولویت بندی قابلیت توضیح، استفاده اخلاقی از هوش مصنوعی و تطبیق مقررات تمرکز خواهد کرد.

کلمات‌کلیدی -اتوماسیون انطباق، امنیت ابری، هوش مصنوعی تشخیص ریسک، مدل سازی پیش بینی، تشخیص ناهنجاری.

۱.مقدمه

اکثرسازمان ها علاوه بر مدیریت داده ها، به سمت استفاده از پردازش‌نیز روی آوردند. با این حال، با توجه به اینکه فضای ابری یک مرز جدیداست، تهدیداتی برای امنیت فضای ابری وجود دارد که برای کاربران‌نهایی تازگی دارد، از جمله مسائل مربوط به انطباق، اگرچه فضای‌ابری مزایای متعددی مانند مقیاس پذیری، مقرون به صرفه بودن وانعطاف پذیری عملیاتی دارد.

حملات‌سایبری به اندازه ای پیشرفته شده اند که مکانیسم های امنیتی‌موجود برای محافظت از زیرساخت های ابری کافی نیستند. به‌همین دلیل است که ارزیابی ریسک و راه حل های انطباق مبتنی برهوش مصنوعی در افزایش امنیت و تضمین انطباق، اهمیت فزاینده ای‌پیدا کرده اند. در نهایت، قابلیت تحویل منحصر به فرد، مقرون‌به صرفه بودن و انعطاف پذیری ارائه شده توسط رایانش ابری،نحوه عملکرد کسب وکارها را تغییر داده است. با گسترش زیرساخت های‌ابری ما، مکانیسم های امنیتی قدیمی که در محیط های‌فناوری اطلاعات سنتی مؤثر بودند، در محیط های ابری فاقدکارایی بودند.



شکل1 مدل تهدید برای محاسبات ابری

این‌گذار ناشی از آن است که هوش مصنوعی، ارزیابی ریسک و چارچوب های‌انطباق را به طور قابل توجهی پویاتر کرده و توانایی آنها را برای مقابله‌فعال تر با چالش های امنیت سایبری افزایش می دهد. پیشرفت های هوش‌مصنوعی، با نظارت بر سیستم های ابری شما، به صورت بلادرنگ (real-time)، امکان پیشگیری از آسیب پذیری ها را فراهم می کند.

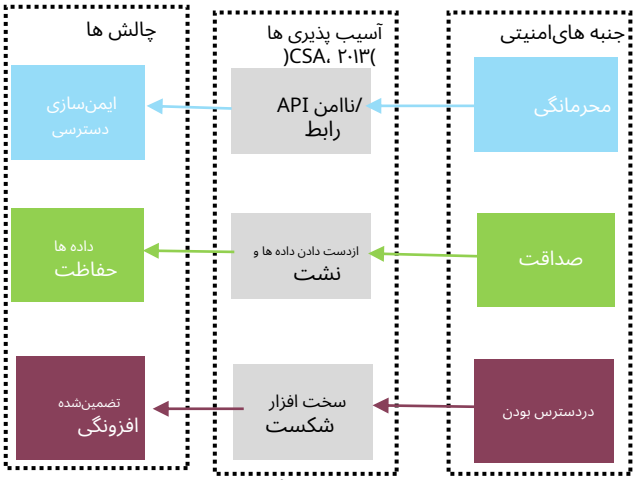
محیط هایی‌برای شناسایی تهدیدها از طریق تجزیه و تحلیل پیشرفته داده ها.چنین فناوری هوشمندی می تواند مقادیر زیادی از داده های شبکه‌را تجزیه و تحلیل کند تا الگوهایی را که می توانند نشان دهنده جرایم‌سایبری باشند، جستجو کند. این قابلیت پیشگیرانه، اثرات حادثه نقض‌امنیت را کاهش می دهد، دقت در تشخیص تهدیدها را بهبود می بخشدو زمان واکنش را کاهش می دهد. علاوه بر این، توسعه مدل های‌هوش مصنوعی، یادگیری مداوم را نیز ممکن می سازد که می تواندبرای مدل های ارزیابی ریسک که می توانند برای سازگاری با محیط‌ابری در حال تغییر و خطرات سایبری نوظهور پیکربندی شوند، مفیدباشد. این استانداردها ممکن است از نظر حفظ اعتماد کسانی که به‌جمع آوری و نگهداری ایمن داده های حساس توسط سازمان علاقه مندهستند، ضروری باشند.

بررسی های‌خودکار، نظارت بر رعایت استانداردهای نظارتی در زمان‌تقریباً بلادرنگ، ایجاد سوابق شکاف های انطباق در زمان واقعی‌و غیره، همگی از جمله راه حل های انطباق مبتنی بر هوش مصنوعی‌هستند. این سطوح از اتوماسیون نه تنها سربار اداری کارکنان‌امنیتی را کاهش می دهد و احتمال خطای انسانی را از بین می برد،بلکه به سازمان ها اجازه می دهد تا تمرکز خود را بر مدیریت ریسک‌استراتژیک تغییر دهند تا به سرعت یک تهدید را برطرف کنند. چارچوب‌امنیت سایبری ابری: چگونه هوش مصنوعی (AI) می تواند ارزیابی‌ریسک و انطباق با مقررات را متحول کند. این بحث می کند که‌چگونه هوش مصنوعی به خودکارسازی برخی از حوزه های بحث برانگیزدر حسابرسی کمک می کند و چگونه می توان با کاهش بارردیابی ریسک، بحث های انطباق را افزایش داد. راه حل های مبتنی‌بر هوش مصنوعی، سازمان ها را قادر می سازد تا یک معماری‌امنیت سایبری بسازند که نه تنها قادر به جلوگیری از حملات جدیداست، بلکه به اندازه کافی چابک است تا با الزامات نظارتی در حال‌تحول سازگار شود.

۲.مرور ادبیات

علاقه‌روزافزون به رایانش ابری منجر به افزایش حجم ادبیات در موردارزیابی ریسک امنیت سایبری ابری با استفاده از هوش مصنوعی‌با توجه به انطباق با قوانین شده است. با روی آوردن سازمان هابه فضای ابری، حملات سایبری پیشرفته در محیط های ابری‌پیچیده و در نهایت بسیار پویا عمیق تر شده اند و تکنیک های امنیتی‌ابتدایی و فلفلی مانند ممیزی ها و محافظت در برابر نفوذ مبتنی‌بر قانون را آشکار می کنند. دانشمندان در مورد روشی برای به کارگیری‌ترکیبی از روش های هوش مصنوعی و یادگیری ماشینی برای‌مدیریت تشخیص تهدید، مدیریت ارزیابی ریسک و نظارت بر انطباق‌در فضای ابری گمانه زنی کرده اند. مطالعات متعددی بر نیاز حیاتی‌به ارزیابی ریسک مبتنی بر هوش مصنوعی برای فعال کردن تشخیص‌آسیب پذیری و پیشگیری از تهدید در زمان واقعی تأکید دارند.

درواقع، هر دو مدل یادگیری تحت نظارت و بدون نظارت در یادگیری‌ماشینی (ML) می توانند حجم قابل توجهی از داده های ترافیک‌شبکه را تجزیه و تحلیل کنند تا چرخه ها و نشانه هایی از یک حمله‌سایبری احتمالی را کشف کنند (Gritti, C. et al., 2015). به همین‌ترتیب،)2017 ,He, D. et al توضیح می دهند که الگوریتم های‌یادگیری عمیق در مقایسه با مدل های رگرسیون سنتی،در کاهش مثبت های کاذب در تجزیه و تحلیل تشخیص مبتنی‌بر رفتار تهدید، بسیار مؤثر هستند. عوامل تجزیه و تحلیل پیش بینی‌نیز در ادبیات به عنوان یک جنبه کلیدی از امنیت سایبری پیشگیرانه‌مورد توجه قرار گرفته اند. یک روش شناسی ممکن برای ریسک‌هوش مصنوعی (AI) ارزیابی‌مبتنی بر سابقه حمله توسط وانگ سی و همکاران (۲۰۰۹) برای پیش بینی نقض های‌امنیتی آینده معرفی شده است. تحقیقات آنها نشان می دهد که چگونه‌هوش مصنوعی می تواند در تصمیم گیری برای اولویت بندی تهدیدها بر اساس‌احتمال و اثر، آگاهی بخش باشد و این برای کمک به شرکت ها جهت تمرکزمنابع امنیتی در جایی که بهترین عملکرد را دارند، بسیار مهم است. طبق مطالعه‌آنها، برای رعایت مقرراتی از جمله HIPAA، GDPR، ISO 27001 و NIST ،این برنامه خاطرنشان می کند که راه حل های مبتنی بر هوش مصنوعی می توانندبه طور مداوم سیاست های امنیتی را رصد کنند، نقض قوانین را شناسایی‌کرده و راه حل هایی را پیشنهاد دهند.



شکل2 جنبه های امنیتی ذخیره سازی ابری، آسیب پذیری ها و چالش ها

کاردیگری که با سیستم های امنیتی ابری ارتباط برقرار می کند و از هوش‌مصنوعی برای افزایش ممیزی های انطباق استفاده می کند، ارائه ی‌جانسن، واشینگتن (۲۰۱۱) است. این تحقیق می گوید راه حل های‌خودکار انطباق، با تولید گزارش های بلادرنگ و تضمین انطباق‌مداوم با مقررات امنیت سایبری، زندگی حسابرسان انسانی را ساده ترمی کنند. هوش مصنوعی برای نظارت بر مقررات می تواند به سازمان هادر کاهش خطرات قانونی و جریمه ها کمک کند. یکی از حوزه های‌جدایی ناپذیر چارچوب های امنیت سایبری مبتنی بر هوش مصنوعی،تشخیص پیشرفته ی تهدید است. جیا، آر. و همکاران (۲۰۲۱) نقش‌هوش مصنوعی در سیستم های SIEM. طبق یافته های آنها، سیستم های‌SIEM تقویت شده با هوش مصنوعی در شناسایی «تهدیدات‌داخلی، حملات روز صفر و حملات انکار سرویس توزیع شده (DDoS)» نسبت به همتایان سنتی خود بسیار مؤثرتر عمل کردند. همچنین،کن، اس جی و همکاران (۲۰۱۵) بینش هایی در مورد ادغام امنیت‌سایبری مبتنی بر ZTA و هوش مصنوعی ارائه می دهند.

آنهاکشف کردند که هوش مصنوعی می تواند احراز هویت کاربر را بهترانجام دهد، دسترسی ممتاز را رصد کند و قوانین امنیتی را بر اساس ارزیابی‌ریسک تعیین کند. این تکنیک امنیتی تطبیقی، زیرساخت ابری امن‌را در برابر حمله داخلی و دسترسی غیرمجاز کاهش می دهد. اگرچه مزایای‌زیادی دارد، محققان برخی از مشکلات بالقوه ارزیابی و انطباق ریسک‌مبتنی بر هوش مصنوعی را تشریح کرده اند. همانطور که لی، ای. وهمکاران (2019) و رن، وای. و همکاران (2019) عناصر غیرقابل توضیح‌بودن را برای مدل های هوش مصنوعی شناسایی می کنند. نگرانی‌عمده دیگر، حریم خصوصی داده ها است (شن، دبلیو. و همکاران 2017و وانگ، بی. و همکاران 2012). هوش مصنوعی باید در مورد داده های‌حساس به ابر هوشیار باشد تا نشت نکند. برای رفع این مانع، محققان‌قصد دارند مدل های هوش مصنوعی (XAI) قابل توضیح تری را توسعه‌دهند، ...

مدیریت‌امنیت سایبری با استفاده از هوش مصنوعی، و تطبیق هوش مصنوعی با تهدیدات‌سایبری جدید.

ادغام‌هوش مصنوعی و بلاکچین مختص امنیت ابری و نظارت برانطباق هنوز در حال انجام است. بررسی ادبیات به این نتیجه رسیدکه سازمان ها به طور قابل توجهی از ارزیابی ریسک مبتنی بر هوش‌مصنوعی و اتوماسیون انطباق بهره مند شده اند، که تشخیص تهدید،اولویت بندی ریسک و انطباق با مقررات را برای تقویت امنیت‌سایبری ابری بهبود می بخشد.

تحقیقات‌نشان می دهد که محافظت مبتنی بر هوش مصنوعی از طریق ممیزی ها،تجزیه و تحلیل های پیش بینی کننده و یادگیری ماشینی می تواند زیرساخت های‌ابری را ایمن کند.

بازبودن مدل های هوش مصنوعی، حریم خصوصی داده ها و مقیاس پذیری‌همچنان مسائل مزمنی هستند که نیاز به بررسی بیشتر دارند.با تکامل مداوم تهدیدات سایبری، سرویس های مبتنی بر هوش مصنوعی،جهت گیری امنیت ابری و مدیریت انطباق را شکل خواهند داد.

۲.۱مطالعه اهداف

۱.بررسی عملکرد هوش مصنوعی در امنیت سایبری ابری.
۲.ایجاد چارچوبی برای ارزیابی ریسک مبتنی بر هوش مصنوعی.

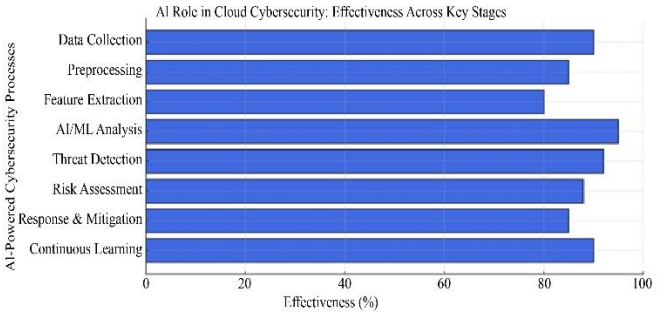
۳.برای افزایش شناسایی و پاسخ به تهدید در زمان واقعی.
۴.ارزیابی قابلیت و انعطاف پذیری هوش مصنوعی در مجموعه های ابری‌همزمان و ترکیبی.

۳.تحقیق و روش شناسی

خروجی‌مدل به شما نشان می دهد که مشکلات یا نگرانی ها چه می توانندباشند. اثربخشی ارزیابی های ریسک مبتنی بر هوش مصنوعی‌را با رویکردهای سنتی تر امنیت سایبری برای تشخیص و مبارزه‌با حملات مقایسه کنید.

استراتژی هایی‌را برای ادغام مدل های هوش مصنوعی در زیرساخت های‌امنیت سایبری ابری موجود تدوین کنید. حلقه های بازخوردرا می توان برای بهبود و تطبیق مکرر مدل در برابر تهدیدات جدیددر نظر گرفت.

بررسی‌عملکرد هوش مصنوعی در امنیت سایبری ابری با رویکردسازمان یافته ی این روش تحقیق آسان تر می شود. این تحقیق‌با جمع آوری داده ها و ادغام مدل ها، امیدوار است نشان دهدکه چگونه هوش مصنوعی (AI) می تواند تشخیص تهدیدات ابری‌را بهبود بخشد.



ایمپورت‌کردن numpy به عنوان np
ایمپورت‌کردن pandas به عنوان pd
ازsklearn.ensemble، IsolationForest را وارد کنید از
sklearn.metrics، classification_report را وارد کنید

np.random.seed)42(

np.random.normal)loc=0, scale=1, size=)1000, 2((= normal_data

np.random.normal)loc=3, scale=1, size=)20, 2((= ناهنجاری ها

= np.array)]0[*1000 +]1[*20(
data = np.vstack)]normal_data, abnormalities[(labels

برچسب ها
df = pd.DataFrame)data, columns=]'feature1', 'feature2'[(df]'label'[=

مدل= جنگل ایزوله (آلودگی = 0.05، حالت تصادفی= 42)
model.fit_predict)df]]'feature1', 'feature2'[[(df]'anomaly_score'[=

df]'predicted_label'[= df]'anomaly_score'[.map)}-1: 1, 1: 0{(

گزارش= گزارش طبقه بندی (df]'label'[، df]'predicted_label'[)
چاپ("گزارش طبقه بندی:\n", گزارش)

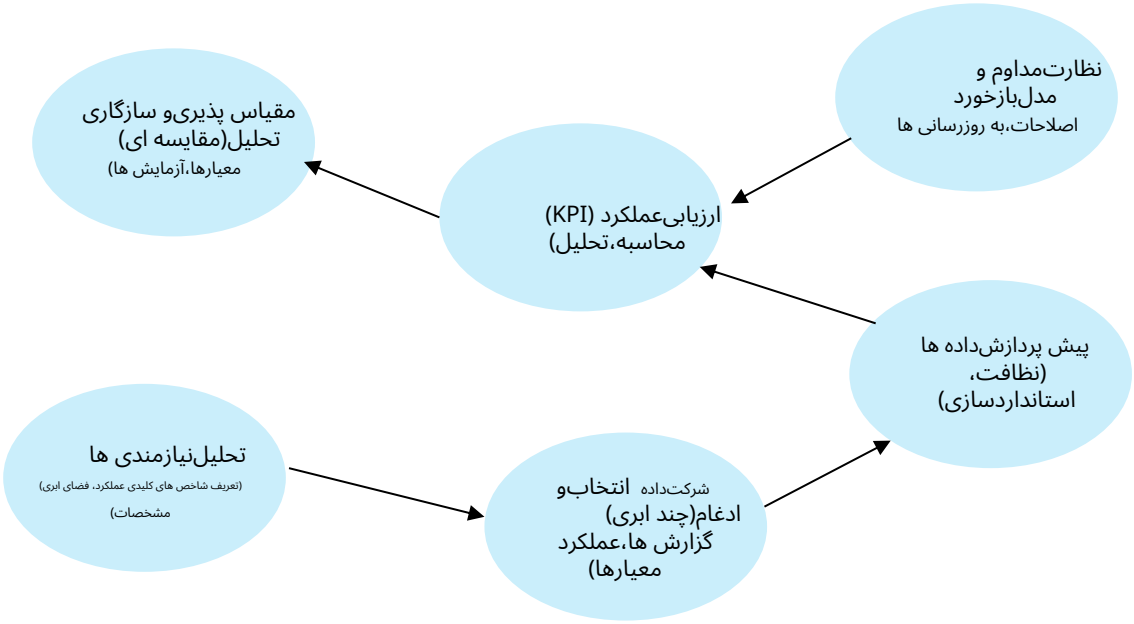
تشخیص‌ناهنجاری مبتنی بر هوش مصنوعی - به کارگیری مفاهیم دراینجا، خواهیم دید که چگونه می توان با استفاده از نمودار جریان زیر و نمونه‌کد پایتون، تشخیص ناهنجاری مبتنی بر هوش مصنوعی را پیاده سازی‌کرد، که به دستیابی به هدف ما که بهبود امنیت ابری است، کمک‌خواهد کرد. با متخصص بودن در این زمینه، می توانید نشانه های خطری‌مانند انتقال داده آهسته غیرطبیعی یا زمان طولانی غیرطبیعی برای‌ورود به سیستم را تشخیص دهید. در ارزیابی هوش مصنوعی، سه مدل‌اصلی یادگیری موجود را در نظر بگیرید: نظارت شده، بدون نظارت ونیمه نظارت شده.

ماداده های پرت را شناسایی می کنیم و تکنیک هایی را برای تشخیص‌ناهنجاری مانند جنگل های ایزوله و رمزگذارهای خودکار بررسی می کنیم.به عنوان مثال، مدل های انتخاب شده را می توان با استفاده ازداده های تاریخی با الگوهای تهدید شناخته شده آموزش داد. این بخش‌در مورد یک فرآیند سیستماتیک ارزیابی تأثیر هوش مصنوعی بر امنیت‌سایبری ابری صحبت می کند. این تحقیق نشان می دهد که فناوری های‌هوش مصنوعی ممکن است تصمیم گیری ابری، شناسایی آسیب پذیری‌و تشخیص ناهنجاری را بهبود بخشند. مراحل به شرح زیر است:استخراج گزارش های فعالیت های ابری، گزارش های جریان و هشدارها،مانند گزارش های هشدار امنیتی ابری و ترافیک شبکه ایجاد شده‌با یک ارائه‌ دهنده خدمات ابری (CSP). مجموعه داده های مختلف (دنیای واقعی و شبیه سازی شده) پوشش خوبی از هر دو جهت را تضمین‌می کنند.

پیش پردازش‌داده های جمع آوری شده: اطلاعات ناقص را پر کنید، مواردتکراری را حذف کنید و ویژگی ها را استانداردسازی کنید. انتخاب ویژگی‌به داده هایی مانند گزارش های سیستم، الگوهای دسترسی و حجم‌ترافیک اجازه می دهد تا با داده های بالقوه تأثیرگذار بهبود یابند.

بینش ها.به دنبال شاخص های آماری (و رفتاری) باشید که ممکن است‌نشان دهنده ی رفتارهای مشکوک باشند. می توان با استفاده ازیک رویکرد سیستماتیک مبتنی بر روش های داده محور، انتخاب مدل‌و ارزیابی مستمر، یک نقشه راه برای ساخت یک چارچوب ارزیابی‌ریسک مبتنی بر هوش مصنوعی برای امنیت سایبری ابری ایجادکرد. روش شناسی هدایت کننده ی فرآیند توسعه می تواند به شرح‌زیر باشد:

فرض‌کنید سیستم های هوش مصنوعی نیاز به رشد و انعطاف پذیری‌در تنظیمات چند ابری و ترکیبی دارند. در این صورت، یک‌فرآیند سیستماتیک برای جمع آوری داده ها، معیارهای عملکرد و تحقق‌بینش های عملی به ما کمک می کند تا مقیاس پذیری و انعطاف پذیری‌سیستم هوش مصنوعی را به درستی ارزیابی کنیم. در این‌تحقیق، بر پاسخگویی، استفاده از منابع و سازگاری بار کاری سیستم های‌هوش مصنوعی توزیع شده در زیرساخت های ابری مختلف‌تأکید شده است.




```
واردکردن weka.core.Instances؛
فایلDataSource weka.core.converters.ConverterUtils را وارد کنید؛ فایل
weka.classifiers.bayes.NaiveBayes را وارد کنید؛
واردکردن weka.classifiers.Evaluation;

واردکردن java.util.Random؛

کلاس‌عمومی RiskAssessmentFramework { public static
void main(String[] args) { try {

منبع‌داده
= DataSource("cloud_security_data.arff"); new
نمونه های‌مجموعه داده = source.getDataSet();

dataset.setClassIndex(dataset.numAttributes() - 1);

naiveBayes = new تابع NaiveBayes تابع NaiveBayes();

ارزیابی‌کننده = ارزیابی جدید (مجموعه داده)؛
evaluator.crossValidateModel(naiveBayes، مجموعه داده،
10،تصادفی جدید (1))؛

"=== ارزیابی ریسک مبتنی بر هوش مصنوعی ===");
System.out.println("
خلاصه ===", false));
System.out.println(evaluator.toSummaryString() + "
نتایج اعتبارسنجی متقابل ===");
ماتریس درهم ریختگی ===");
System.out.println(evaluator.toMatrixString() + "
System.out.println(evaluator.toClassDetailsString());

مجموعه داده(naiveBayes.buildClassifier)؛

برای(عدد صحیح i = 0; i < 5; i++) {
پیش بینی‌دوگانه =
naiveBayes.classifyInstance(dataset.instance(i));
System.out.println("نمونه " + i + " ریسک
احتمال:" + پیش بینی)؛
{

} گرفتن (استثنا e) {
e.printStackTrace();
{
}
{
```

ایجادجدول BY DEFAULT ON NULL AS IDENTITY
NUMBER GENERATED
metric_id(ai_performance_metrics,
نوع‌ابر)30(VARCHAR2، نام متریک
)30(VARCHAR2، مقدار متریک
شماره،
تاریخ‌پیش فرض سیستم را وارد کنید
محدودیتpk_ai_performance_metrics کلید اصلی
(metric_id))؛

واردکردن در معیارهای عملکرد ai (نوع_ابر، نام_متریک، مقدار_متریک)
مقادیر('چندکلاود'،'زمان_پاسخ'،12.5)؛

واردکردن در معیارهای عملکرد ai (نوع_ابر، نام_متریک، مقدار_متریک)
مقادیر('ترکیبی'، 'زمان_پاسخ'، 10)؛

واردکردن در معیارهای عملکرد ai (نوع_ابر، نام_متریک، مقدار_متریک)
مقادیر('OnPrem'، 'زمان_پاسخ'، ۱۵.۷۵)؛

واردکردن در معیارهای عملکرد ai (نوع_ابر، نام_متریک، مقدار_متریک)
مقادیر('لبه'، 'زمان_پاسخ'، 8.25)؛

واردکردن در معیارهای عملکرد ai (نوع_ابر، نام_متریک، مقدار_متریک)
مقادیر('چند ابری'، 'مقیاس پذیری'، ۷.۰)؛

واردکردن در معیارهای عملکرد ai (نوع_ابر، نام_متریک، مقدار_متریک)
مقادیر('ترکیبی'، 'مقیاس پذیری'، 8)؛

واردکردن در معیارهای عملکرد ai (نوع_ابر، نام_متریک، مقدار_متریک)
مقادیر('OnPrem'، 'مقیاس پذیری'، 6)؛

واردکردن در معیارهای عملکرد ai (نوع_ابر، نام_متریک، مقدار_متریک)
مقادیر('لبه'، 'مقیاس پذیری'، 9)؛

واردکردن در معیارهای عملکرد ai (نوع_ابر، نام_متریک، مقدار_متریک)
مقادیر('چند ابری'،'سازگاری'،8.5)؛

واردکردن در معیارهای عملکرد ai (نوع_ابر، نام_متریک، مقدار_متریک)
ارزش ها(«ترکیبی»، «سازگاری»، ۷.۷۵)؛

واردکردن در معیارهای عملکرد ai (نوع_ابر، نام_متریک، مقدار_متریک)
ارزش ها('OnPrem'، 'سازگاری'، ۷.۰)؛

واردکردن در معیارهای عملکرد ai (نوع_ابر، نام_متریک، مقدار_متریک)
ارزش ها('برتری'، 'سازگاری'، ۹.۲۵)؛

ایجادیا جایگزینی رویه تابع
print_avg_response_time()
عدد؛v_multi_avg
عددv_hybrid_avg;
شروع
انتخاب‌میانگین (مقدار متریک)
بهv_multi_avg
ازai_performance_metrics که در
آنcloud_type = 'چند ابری'
وmetric_name = 'زمان_پاسخ';

انتخاب‌میانگین (مقدار متریک)
بهv_hybrid_avg
ازai_performance_metrics که
درآن cloud_type = 'ترکیبی'
وmetric_name = 'زمان_پاسخ';

DBMS_OUTPUT.PUT_LINE('Hybrid: و MultiCloud میانگین زمان پاسخگویی برای
چندابر: ' || v_multi_avg);
DBMS_OUTPUT.PUT_LINE('هیبرید: ' || v_hybrid_avg);
پایان؛

شروع
زمان‌پاسخ میانگین چاپ؛
پایان؛

بااستفاده از این مطالعه و چارچوب روش شناختی، می توان مقیاس پذیری‌و انعطاف پذیری هوش مصنوعی در سیستم های چندابری و ترکیبی‌را به صورت سیستماتیک اندازه گیری کرد. با جمع آوری و پاکسازی داده هااز منابع ابری متعدد، ارزیابی شاخص های کلیدی عملکرد و نظارت بر عملکردسیستم به صورت بلادرنگ، سازمان ها می توانند اطمینان حاصل کنندکه راه حل های مبتنی بر هوش مصنوعی آنها در سناریوهای عملیاتی متنوع،انعطاف پذیر و سازگار باقی می مانند. این مثال واقع گرایانه از کد PL/SQL نشان می دهد که چگونه می توان چنین شاخص های عملکردی را دریک سیستم پایگاه داده واحد جمع آوری و تجزیه و تحلیل کرد و از تصمیمات‌مبتنی بر داده برای تنظیم هوش مصنوعی در یک محیط امنیت سایبری‌ابری پشتیبانی کرد.

۴.یافته ها

1.ارزیابی ریسک مبتنی بر هوش مصنوعی، تشخیص کلی ناهنجاری هاو فعالیت های مشکوک در محیط های ابری را بهبودمی بخشد و امکان تشخیص تهدید در زمان واقعی را فراهم‌می کند[14]. مدل های یادگیری ماشین می توانند در میان‌انبوهی از سوابق امنیتی، حملات احتمالی را سریع تر و دقیق تراز روش های مبتنی بر قانون قبلی جستجو کنند.
۲.حسابرسی امنیتی اتوماسیون که توسط هوش مصنوعی (AI) پشتیبانی‌می شود، انطباق با الزامات انطباق اجباری (مانند HIPAA، GDPR، ISO 27001 و NIST) را تضمین می کند. کاهش‌تلاش های دستی نه تنها ...

راهی‌برای محدود کردن نقض انطباق و همچنین افزایش کارایی حسابرسی.

۳.اکنون، آنها می توانند از ارزیابی ریسک مبتنی بر هوش مصنوعی برای رتبه بندی‌تهدیدات امنیتی بر اساس شدت استفاده کنند. تمرکز بر بزرگترین آسیب پذیری ها،تیم های امنیتی را قادر می سازد تا قبل از شروع حملات داده ها،از آنها جلوگیری کنند.

۴.حتی با وجود تفاوت در پلتفرم ها، مدل های هوش مصنوعی در پلتفرم های‌زیرساخت چند ابری و ترکیبی انعطاف پذیر هستند و نظارت‌امنیتی مداوم را در نقاط کنترل یادگیری ماشینی تضمین می کنند.

۵.اگرچه این امر باید ادغام موفقیت آمیز داده ها را در روزهای اولیه تضمین کند،واقعیت این است که مدیریت داده ها به اندازه کافی استاندارد نشده‌است تا اطمینان حاصل شود که مسائل ادغام داده ها در هوش مصنوعی‌مزمن نمی شوند.

۶.مشکل قابلیت توضیح مرتبط با راه حل های امنیت سایبری مبتنی‌بر هوش مصنوعی، درک ارزیابی های ریسک تولید شده توسط‌هوش مصنوعی را برای متخصصان امنیت چالش برانگیزمی کند.

۷.بهبود شفافیت مدل برای ایجاد اعتماد و بهبود مهارت های تصمیم گیری‌حیاتی است.

۸.از آنجایی که تهدیدهای سایبری دائماً در حال تغییر هستند، مدل های هوش مصنوعی‌امنیتی باید مرتباً بر روی مجموعه داده های جدید امنیت سایبری بازآموزی‌شوند. چارچوب های هوش مصنوعی تطبیقی که هوش تهدید در زمان‌واقعی را در خود جای می دهند تا دقت تشخیص را به میزان قابل توجهی‌بهبود بخشند.

۴.۱ پیشنهادات

۱.از رویکردهای هوش مصنوعی قابل توضیح (XAI) برای افزایش قابلیت تفسیرارزیابی های ریسک استفاده کنید. توضیحات مفصلی از فرآیندهای‌تصمیم گیری هوش مصنوعی را در اختیار تحلیلگران امنیتی‌قرار دهید.

۲.ایجاد راهکارهای هوش مصنوعی مستقل از فضای ابری که برای ممیزی‌انطباق در سراسر ابرها کار می کنند. از یکپارچه سازی های‌مبتنی بر API برای خودکارسازی ممیزی های‌امنیتی و پشتیبانی از اتوماسیون انطباق در لحظه استفاده‌کنید.

۳.از سیستم های امتیازدهی ریسک مبتنی بر هوش مصنوعی برای اولویت بندی‌و اولویت بندی منابع استفاده کنید. فرآیندهای پاسخگویی خودکاررا برای تهدیدهای پرخطر ایجاد کنید و در عین حال وقفه در تلاش های‌کم خطر را به حداقل برسانید.

۴.از داده های جدید که به طور مداوم در مدل های سیستم های هوش مصنوعی برای‌هوش تهدیدات سایبری به روزرسانی می شوند، استفاده کنید. روش های‌یادگیری فدرال را برای بهبود سازگاری مدل در عین حفظ حریم خصوصی‌داده ها بررسی کنید.

۵.سیاست های یکپارچه ی مدیریت داده ها را پیاده سازی کنید که انسجام را درنظارت امنیتی مقیاس پذیر و مبتنی بر هوش مصنوعی فراهم می کندو ابرهای عمومی، خصوصی و ترکیبی را در بر می گیرد. برای بهبودمدل هوش مصنوعی، بر عادی سازی و غنی سازی داده ها تمرکز کنید.

۶.از ابزارهای اصلاح خودکار مبتنی بر هوش مصنوعی برای خنثی کردن تهدیدهای امنیتی‌قبل از تبدیل شدن به بحران استفاده کنید.

۷.یکی دیگر از اقدامات پیشگیرانه ای که سرویس های امنیت سایبری از آن استفاده می کنند،تجزیه و تحلیل های پیش بینی کننده برای شناسایی و از بین بردن خطرات امنیتی‌قبل از تبدیل شدن آنها به یک مشکل است.

۸.بینش های هوش تهدید و بینش های هوش تهدید اعمال شده توسط هوش مصنوعی‌و بینش های هوش تهدید اعمال شده توسط شخصیت را برای غلبه‌بر تهدیدهای سایبری در حال تحول به اشتراک بگذارید.

۵.نتیجه گیری

هوش‌مصنوعی که ارزیابی ریسک و اتوماسیون انطباق را اطلاع رسانی‌می کند، پتانسیل امنیت سایبری ابری را ارائه می دهد وتوانایی سازمان ها را در شناسایی، نظارت و کاهش خطرات سایبری‌به طور قابل توجهی افزایش می دهد. رویکرد هوش مصنوعی‌به دلیل الگوریتم های پیشرفته یادگیری ماشین، تهدیدات رابسیار کارآمدتر از روش های سنتی ارزیابی و تفکیک می کند. اولویت بندی‌مبتنی بر ریسک و تهدیدات کلیدی می تواند به تیم های امنیتی‌در بهینه سازی تخصیص منابع و زمان واکنش کمک کند. علاوه‌بر این، اتوماسیون انطباق با هوش مصنوعی تضمین می کند که‌استانداردهای نظارتی مانند HIPAA، GDPR، ISO 27001 و NIST به طور مداوم رعایت می شوند و خطر عدم انطباق و جریمه های‌مرتبط را به حداقل می رسانند. با این حال، این مزایا با تعدادی‌موانع همراه است که باید برطرف شوند.

شفافیت‌مدل هوش مصنوعی یک چالش کلیدی است زیرا متخصصان‌امنیت برای ایجاد اعتماد و اصلاح استراتژی های پاسخ به حوادث،به قابلیت توضیح برای تصمیمات مبتنی بر هوش مصنوعی نیازدارند. در موقعیت های چند ابری و ترکیبی، مقیاس پذیری و چابکی نیزنیازمند مدیریت داده های استاندارد و ادغام یکپارچه هوش مصنوعی درپلتفرم های ابری عمومی و خصوصی هستند. از آنجایی که سازمان ها بایددر مورد امنیت سایبری پیشگیرانه عمل کنند، باید با ایجاد چارچوب های‌قابل توضیح هوش مصنوعی (XAI)، به اشتراک گذاری اطلاعات‌تهدید و توسعه مدل های هوش مصنوعی که به طور مداوم در حال‌یادگیری هستند، از هوش مصنوعی به طور کامل بهره ببرند. به روزرسانی‌منظم مدل های هوش مصنوعی با اطلاعات تهدید می تواند به‌تقویت دفاع امنیتی ابری کمک کند و به سیستم های امنیتی اجازه دهدتا به تهدیدات سایبری جدید پاسخ دهند. در نهایت، یک رویکرد هوشمند،مقیاس پذیر و بسیار مؤثر برای امنیت سایبری ابری، ارزیابی ریسک‌و راه حل های انطباق مبتنی بر هوش مصنوعی است. به طور خلاصه،هوش مصنوعی در امنیت سایبری به سازمان ها کمک می کند تاا‌ز طریق اتوماسیون مبتنی بر هوش مصنوعی، ارزیابی ریسک در زمان واقعی‌و قابلیت های پیش بینی، با چشم انداز در حال تحول تهدیدات سایبری‌سازگار شوند - سازمان ها را قادر می سازد تا تاب آوری امنیتی خودرا افزایش دهند، خطرات را به حداقل برسانند و از انطباق با مقررات اطمینان‌حاصل کنند.

بیانیه‌تأمین مالی

نویسندگان‌این تحقیق را به طور کامل تأمین مالی کردند.

منابع

[1] کلمنتاین گریتی، ویلی سوسیلو، و توماس پلانارد، «مالکیت داده های پویا و قابل اثبات کارآمد با قابلیت تأیید عمومی و حریم خصوصی داده ها»،*امنیت اطلاعات و حریم خصوصی: 20هفتمکنفرانس استرالیا*، بریزبن، کوئینزلند، استرالیا،صفحات ۳۹۵-۴۱۲، ۲۰۱۵. [کراس رف] [گوگل اسکالر] [لینک ناشر]

[2] دبیائو هی و همکاران، «ناامنی یک پروتکل حسابرسی عمومی مبتنی بر هویت برای داده های برون سپاری شده در ذخیره سازی ابری»،*علوم اطلاعات*، جلد ۳۷۵،صفحات ۴۸-۵۳، ۲۰۱۷. [کراس رف] [گوگل اسکالر] [لینک ناشر]

[3] وین ای. جانسن، «قلاب های ابری: مسائل امنیتی و حریم خصوصی در رایانش ابری»،*۴۴هفتمکنفرانس بین المللی علوم سیستم هاوایی*[.2011 Kauai, HI, USA, pp. 1-10,کراس رف] [گوگل اسکالر] [لینک ناشر]

[4] رو جیا و همکاران، «مروری سیستماتیک بر رویکردهای زمان بندی در پلتفرم های ابری چند-مستاجره ای»،*فناوری اطلاعات و نرم افزار*، جلد ۱۳۲، ۲۰۲۱. [کراس رف] [گوگل اسکالر] [لینک ناشر]

[5] اسنهال جی. کین و دیپتی پی. تنگ، «مروری بر تکنیک های تشخیص نفوذ برای محاسبات ابری و چالش های امنیتی»،*۲۰و کنفرانس‌بین المللی الکترونیک و سیستم های ارتباطی*، کویمباتور، هند، صفحات ۲۲۷-۲۳۲، ۲۰۱۵. [کراس رف] [گوگل اسکالر] [لینک ناشر]

[6] آیپینگ لی، شوانگ تان، و یان جیا، «روشی برای دستیابی به یکپارچگی داده های قابل اثبات در محاسبات ابری»،*مجله ابررایانه ها*، جلد ۷۵، صفحات ۹۲-۱۰۸،۲۰۱۹. [کراس رف] [گوگل اسکالر] [لینک ناشر]

[7] یونگجون رن و همکاران، «مالکیت داده های قابل اثبات مبتنی بر انتساب در ذخیره سازی ابری عمومی»،*دهمین کنفرانس بین المللی پنهان سازی هوشمنداطلاعات و پردازش سیگنال چندرسانه ای*، کیتاکیوشو، ژاپن، صفحات ۷۱۰-۷۱۳، ۲۰۱۴. [کراس رف] [گوگل اسکالر] [لینک ناشر]

[8] ونتینگ شن و همکاران، «طرح حسابرسی ابری امن با وزن کم و حفظ حریم خصوصی برای کاربران گروهی از طریق واسطه شخص ثالث»، *مجله کاربردهای شبکه‌و کامپیوتر*، جلد ۸۲، صفحات ۵۶-۶۴، ۲۰۱۷. [کراس رف] [گوگل اسکالر] [لینک ناشر]

[9] بویانگ وانگ، بائوچون لی، و هوی لی، «ناکس: حسابرسی با حفظ حریم خصوصی برای داده های مشترک با گروه های بزرگ در فضای ابری»، *مجموعه مقالات‌کنفرانس بین المللی رمزنگاری کاربردی و امنیت شبکه*، برلین، هایدلبرگ، جلد ۷۳۴۱، صفحات ۵۰۷-۵۲۵، ۲۰۱۲. [کراس رف] [گوگل اسکالر] [لینک ناشر]

[10] کانگ وانگ و همکاران، «تضمین امنیت ذخیره سازی داده ها در محاسبات ابری در کیفیت خدمات»،*مجموعه مقالات WQOS IEEE 17هفتم کارگاه‌بین المللی*، جلد ۱، صفحات ۱-۹، ۲۰۰۹. [گوگل اسکالر] [لینک ناشر]