Vol. 5, No. 14, Apr-Jun 2025,(71-82)
Journal of New Achievements in Electrical, Computer and Technology (JNAECT)
مجله دستاوردهای نوین در برق،کامپیوتر و فناوری
دوره ۵، شماره ۱۴، بهار ۱۴۰۴ (۸۲-۷۱)
journal homepage: https://jnaect.ir

استفاده از تکنیکهای یادگیری ماشین برای شناسایی و پیشگیری از تهدیدات انجام شده بر علیه سرورهای بانکی

حسین باغبان
دانشجوی دکترای هوش مصنوعی، دانشکده مهندسی کامپیوتر، دانشگاه آزاد واحد فردوس
hossein.baghban@iau.ac.ir

.

چکیده- صنعت بانکداری یکی از اصلی ترین اهداف حملات سایبری است. با توجه به حساسیت داده های مالی و پیامدهای نشت آنها، استفاده از روشهای سنتی امنیتی کافی نیست. یادگیری ماشین با توانایی تحلیل الگوهای پیچیده و شناسایی ناهنجاریها، راه حل مناسبی برای این چالش ارائه میدهد و استفاده از تکنیکهای یادگیری ماشین میتواند امنیت سرورهای بانکی را به طور چشمگیری بهبود بخشد. ترکیب چندین روش و به روزرسانی مداوم مدلها با داده های جدید، کلید موفقیت در مقابله با تهدیدات پیچیده سایبری است. با افزایش حملات سایبری به بانکها و مؤسسات مالی، نیاز به سیستمهای امنیتی پیشرفته بیش از پیش احساس میشود. لذا این مقاله به بررسی تکنیکهای یادگیری ماشین مورد استفاده توسط محققان مختلف برای شناسایی و پیشگیری از تهدیدات امنیتی در سرورهای بانکی میپردازد.

کلید واژه- تکنیکهای یادگیری ماشین، حملات و تهدیدات امنیتی، شناسایی و پیشگیری از تهدیدات، سرورهای بانکی.

.

1- مقدمه

یادگیری ماشین به سیستم‌ها این توانایی را می‌دهد که بدون برنامه‌نویسی مستقیم، الگوها و روابط را از داده‌ها بیاموزند. در حوزه امنیت سایبری، این تکنیک‌ها نقش مهمی در تحلیل داده‌های ورودی و شناسایی فعالیت‌های مشکوک ایفا می‌کنند [1] . . امروزه حملات سایبری تکامل یافته‌اند و پیش‌بینی و جلوگیری از وقوع آن‌ها دشوار شده است. پیچیدگی تهدیدات سایبری منجر به توسعه سیستم‌های امنیتی مبتنی بر فناوری پیشرفته شده است، اما این روش‌ها هنوز موفق به حذف مؤثر تهدیدات سایبری نشده‌اند. الگوریتم‌های یادگیری ماشین در کاربردهای امنیت سایبری برای سازمان‌ها بسیار مفید واقع شده‌اند. این الگوریتم‌ها فرصت بزرگی برای سازمان‌ها فراهم می‌کنند تا با تهدیدات رو به افزایش حملات سایبری مقابله کنند. استفاده از الگوریتم‌های یادگیری ماشین در امنیت سایبری برای سازمان‌ها مزایای زیادی دارد زیرا در تشخیص تهدیدات سایبری مانند بدافزارها، مؤثرتر، قابل گسترش و عملی‌تر از روش‌های معمول هستند که نیازمند دخالت انسانی‌اند (,2019Gupta).

این مقاله در پنج بخش تنظیم شده است. در بخش دوم به معرفی یادگیری ماشین و برخی از تکنیکها و کاربردهای آنها خواهیم پرداخت. در بخش سوم درباره حملات امنیتی انجام شده بر علیه سرورهای موسسات مالی و بانکها بحث خواهیم کرد. در بخش چهارم برخی از تحقیقات انجام شده توسط محققان مختلف در زمینه استفاده از تکنیکهای یادگیری ماشین برای شناسایی حملات انجام شده بر علیه سرورهای بانکی را مرورخواهیم کرد و در نهایت در فصل پنجم نتیجه گیری را آورده و برخی از چالشهای موجود در شناسایی تهدیدات امنیتی در سرورهای بانکی را بیان خواهیم کرد.

2- یادگیری ماشین

یادگیری ماشین (Machine Learning) یکی از شاخه‌های هوش مصنوعی است که به سیستم‌ها و کامپیوترها این امکان را می‌دهد که بدون برنامه‌ریزی مستقیم، الگوها و قوانین را از داده‌ها بیاموزند و وظایف مختلف را انجام دهند. یادگیری ماشین فرایندی است که در آن کامپیوترها از داده‌ها برای پیش‌بینی یا تصمیم‌گیری بدون دخالت انسان استفاده می‌کنند. در این تکنیک، الگوریتم‌ها برای تحلیل و پردازش داده‌ها و استخراج اطلاعات مفید از آن‌ها به کار می‌روند [2].

اصول یادگیری ماشین عبارتند از [3]:

- داده‌ها (Data): داده‌ها قلب یادگیری ماشین هستند. برای ساخت مدل‌های دقیق، داده‌های با کیفیت بالا و متنوع ضروری است.
- الگوریتم‌ها (Algorithms): الگوریتم‌ها مانند شبکه‌های عصبی، ماشین‌های بردار پشتیبان (SVM)، جنگل‌های تصادفی و K-Means برای تحلیل داده‌ها و حل مسائل استفاده می‌شوند.
- ارزیابی مدل (Model Evaluation): معیارهایی مانند دقت، بازخوانی و نرخ خطا برای ارزیابی کیفیت مدل به کار می‌روند.
- پیش‌پردازش داده‌ها (Data Preprocessing): مرحله‌ای حیاتی برای تمیز کردن داده‌ها، حذف نویز و آماده‌سازی آن‌ها برای استفاده در مدل‌های یادگیری ماشین.

یادگیری ماشین به سرعت در حال تحول است و نقش مهمی در بهبود بسیاری از جنبه‌های زندگی ما ایفا می‌کند.

2-1- انواع تکنیکهای یادگیری ماشین

انواع تکنیکهای یادگیری ماشین عبارتند از [4]

- یادگیری نظارت‌شده (Supervised Learning): در این روش، مدل با داده‌های برچسب‌دار آموزش داده می‌شود. هدف این است که مدل بتواند رابطه بین ورودی‌ها و خروجی‌ها را بیاموزد. مثال: تشخیص ایمیل‌های اسپم.
- یادگیری بدون نظارت (Unsupervised Learning): در این روش، داده‌ها بدون برچسب هستند و الگوریتم‌ها سعی می‌کنند الگوها و ساختارهای مخفی در داده‌ها را پیدا کنند.- مثال: خوشه‌بندی داده‌ها برای تقسیم‌بندی مشتریان.
- یادگیری تقویتی (Reinforcement Learning): این روش بر اساس سیستم پاداش و تنبیه کار می‌کند. مدل برای انجام وظایف در محیط‌هایی که در آن تصمیم‌گیری اهمیت دارد، آموزش داده می‌شود.- مثال: آموزش ربات برای بازی کردن.
- یادگیری نیمه‌نظارت‌شده (Semi-Supervised Learning): ترکیبی از داده‌های برچسب‌دار و بدون برچسب برای آموزش مدل استفاده می‌شود.- مثال: کاربرد در پزشکی.

2-2- برخی از کاربردهای یادگیری ماشین

یادگیری ماشین در زمینه‌های مختلف کاربرد دارد و توانایی آن در تحلیل داده‌ها و پیش‌بینی دقیق نتایج باعث شده است که به یکی از ابزارهای پرکاربرد در فناوری مدرن تبدیل شود. برخی از کاربردهای یادگیری ماشین عبارت‌اند از [5]:

- امنیت سایبری

✓ شناسایی حملات سایبری: الگوریتم‌ها برای تشخیص فعالیت‌های مشکوک و مقابله با بدافزارها استفاده می‌شوند.

✓ پیشگیری از تقلب: شناسایی رفتارهای غیرعادی کاربران برای جلوگیری از کلاهبرداری.

- پزشکی و سلامت

✓ تشخیص بیماری‌ها: یادگیری ماشین به پزشکان کمک می‌کند بیماری‌ها را بر اساس داده‌های پزشکی شناسایی کنند.

✓ تحلیل تصاویر پزشکی: کمک به تشخیص بهتر با بررسی تصاویر رادیولوژی یا اسکن‌ها.

- مالی و بانکداری

✓ ارزیابی ریسک: تحلیل داده‌های مالی برای پیش‌بینی ریسک‌های اعتباری یا سرمایه‌گذاری

✓ تشخیص تقلب: شناسایی تراکنش‌های مشکوک در بانک‌ها.

- تجارت الکترونیک

✓ پیشنهاد محصولات: استفاده از داده‌های رفتار مشتریان برای پیشنهاد محصولاتی که ممکن است مورد علاقه آن‌ها باشد.

- ✓ مدیریت موجودی: پیش‌بینی میزان تقاضا برای محصولات و بهینه‌سازی ذخیره‌سازی.
- صنعت و تولید
- ✓ پیش‌بینی خرابی تجهیزات: تحلیل داده‌های دستگاه‌ها برای پیش‌بینی خرابی و کاهش هزینه‌ها.
- ✓ خودکارسازی فرآیندها: بهینه‌سازی خطوط تولید با کمک الگوریتم‌های یادگیری ماشین
- حمل و نقل
  - ✓ مسیریابی بهینه: استفاده در نرم‌افزارهای مسیریابی برای پیدا کردن بهترین مسیرها
  - ✓ خودروهای خودران: آموزش خودروها برای حرکت امن و تصمیم‌گیری بهتر در جاده.
- کشاورزی
- ✓ پیش‌بینی شرایط آب و هوایی: برای بهبود برنامه‌ریزی محصولات کشاورزی
- ✓ تشخیص بیماری‌های گیاهان: شناسایی مشکلات گیاهان با تحلیل تصاویر.

3- تهدیدات و حملات امنیتی در سرورهای بانکی

صنعت بانکداری به لحاظ ماهیت حساس کسب و کاری آن، همواره موضوع جذابی برای تهدیدات سایبری است تا جایی که تعداد حملاتی که این صنعت مهم را هدف قرار می دهند، تقریباً ۳ برابر حملات به سایر صنایع است. حملات سایبری که به بانک ها و مؤسسات مالی انجام می شوند بیشتر برای دسترسی به اطلاعات محرمانه مشتریان و سپرده گذاران بانکی به منظور سرقت پول آنها صورت می گیرند. نقش آگاهی بخشی در خصوص امنیت سایبری صنعت بانکداری به دلیل خودکار شدن بسیاری از فرایندها و همچنین فراگیری میزان استفاده روشمند از فناوری در انجام تراکنش ها میزان اهمیت محرمانگی اطلاعات و نیاز به اعتبارسنجی دسترسی ها را در این صنعت، بسیار برجسته تر از سایر مشاغل کرده است. ایجاد یک مدل امنیتی مناسب برای هر مؤسسه مالی و اعتباری، مستلزم شناخت دقیق تهدیدها و آسیب پذیری های امنیتی است که احتمال دارد بانک ها و مؤسسه های مالی را تحت تأثیر قرار دهد. تمام سیستم های بانکی اعم از ATMها، مراکز داده، دستگاه های کارتخوان فروشگاهی (POS) و حتی کارکنان شاغل در این مراکز می توانند به عنوان یک حفره امنیتی برای نفوذ و حمله سایبری محسوب شوند. از مهمترین آسیب هایی که به دلیل نداشتن یک مدل امنیتی کارا ممکن است به مؤسسات مالی و بانکی وارد شود می توان به مواردی همچون آسیب به اعتبار، افزایش هزینه ها و کاهش درآمد ناشی از سرقت مالی یا ریزش مشتریان و سرمایه گذاران اشاره کرد. بنابراین شناسایی تهدیدها و توجه کافی به اعمال تدابیر امنیتی جهت مقابله با آنها از جمله مهمترین وظایف مدیران امنیتی بانک ها و مؤسسات مالی و اعتباری به شمار می رود. بیشتر حملات سایبری انجام شده به بانک ها و مؤسسات مالی، ناشی از پیکربندی نادرست سیستم ها و سرویس ها و به روزرسانی مداوم آنها و همچنین عدم آگاهی کارکنان است. یکی از مهمترین حفره های امنیتی این صنعت همچون سایر مشاغل، خطای نیروی انسانی است. بسیاری از بانک های بزرگ دنیا این موضوع را عامل 93 درصد از آسیب پذیری ها در برابر تهدیدات سایبری می دانند.

حملات سایبری که هدف آنها کارمندان بانک ها، راهبران و مشتریان خدمات بانکی است عموماً به شکل یک ایمیل معتبر از طرف یکی از مدیران ارشد بانک یا کارمندی با رتبه بالا ارسال می شود تا بتواند سطوح امنیتی را در هم شکسته و به اطلاعات حساس مالی مشتریان و داده های بانکی دسترسی پیدا کند. در حملات پیشرفته تر همچون فیشینگ و تهدیدات پیشرفته از ایمیل های جعلی به همراه روش های پیچیده مهندسی اجتماعی استفاده می شود تا شخص خاصی را مورد هدف قرار داده و از وی به عنوان طعمه جهت ایجاد تهدید امنیتی سوءاستفاده شود. ایمیل ارسالی در چنین حملاتی می تواند شامل یک فایل پیوست آلوده یا لینک به وب سایت مخربی باشد که شخص گیرنده به محض باز کردن فایل پیوست یا کلیک بر روی آن لینک، سیستم خود را در معرض حمله قرار می دهد. پس از نصب و فعال شدن بدافزار بر روی سیستم، حمله شروع شده و فرایند جمع آوری و ارسال داده های حساس سازمانی آغاز می شود [6].

3-1- لایه های امنیتی

لایه های امنیتی مورد نیاز برای بانک ها عبارتند از [3] :

- احراز هویت کاربران : در این گام، از راهکارهای احراز هویت چندعاملی استفاده می شود. این لایه، پایه و اساسی برای ایجاد دیگر لایه های امنیتی بانکداری اینترنتی به شمار می رود. رویکرد درست در مورد معماری این لایه آن است که احراز هویت کاربران، ترکیبی از دانسته های آنها همچون کلمات عبور، داشته های کاربران که می تواند فارغ از دستگاه های هوشمند آنها همچون تلفن همراه، توکن ها و ... باشد و نیز موجودیت کاربران همچون مشخصه های زیست سنجی و ویژگی های رفتاری آنها باشد.
- احراز اصالت دستگاه ها : به محض آنکه تأیید و احراز هویت کاربر انجام شد می بایست احراز اصالت دستگاه هایی که کاربران از آنها برای برقراری ارتباط با سامانه های بانکی استفاده می کنند، صورت گیرد. چنین احراز اصالت هایی بیشتر وابسته به شناسایی دستگاه های هوشمند و پروفایل های کاربران، شناسایی پروکسی ها و همچنین شناسایی و تشخیص موقعیت های مکانی کاربران مجاز در هنگام اتصال و درخواست سرویس آنلاین از بانک است.
- حفاظت از کاربران: در این مرحله از معماری امنیتی، دو چیز مشخص شده است: یکی کاربری که قصد دریافت خدمات آنلاین را از بانک دارد و دیگری هم دستگاهی که کاربر از آن برای ایجاد تعاملات و انجام تراکنش های بانکی خود استفاده می کند. در این گام می بایست از امنیت کانال های ارتباطی کاربران با بانک اطمینان حاصل کرد. لایه حفاظت از کاربران باید گستره ای از راهکارهای امنیتی همچون سیستم های شناسایی بدافزارهایی که نیاز به نصب توسط مشتریان ندارند تا استفاده از مرورگرهایی که اتصال دولایه سوکت امن را به سامانه بانکی برقرار می سازند، شامل شود.
- احراز اصالت تراکنش ها/هوش الگومحور: تمرکز این لایه، بیشتر بر روی تراکنش های حساسی می باشد که ممکن است شامل امضای قراردادها یا نقل و انتقال مبالغ زیاد باشند. اهمیت این لایه به عنوان یک لایه امنیتی اضافی، به خصوص در مواردی که ایجاد امنیت سطح بالا از اولویت های راهبردی بانک است، بیشتر می شود.

این لایه دربرگیرنده مواردی همچون تأییدیه های تراکنشی ثانویه ای که از سایر روش های احراز هویت دیگر علاوه بر کلمه عبور و شناسه کاربری استفاده می کنند و شامل امضای تراکنش ها برای مواردی که انجام تراکنش نیاز به تأیید اعتبار دارد و نیز تحلیل و پایش تراکنش ها و رفتارهای کاربران می شود، است.

- امنیت برنامه های کاربردی: با افزایش بانکداری مبتنی بر تلفن همراه، نیازمند آن هستیم که از امن بودن برنامه هایی که اجراکننده و همچنین بستر دریافت و ارسال داده های حساس بر روی دستگاه های تلفن همراه هستند، مطمئن شویم. این لایه شامل ایجاد ساختار و معماری امن برای برنامه های کاربردی و نیز احراز هویت های متقابل است. با ایجاد این لایه امنیتی در بانکداری اینترنتی می توان کلاهبرداری های برخط و سرقت داده ها توسط هکرها و مجرمان سایبری را بیش از پیش پیچیده و سخت تر کرد.

2-3- انواع حملات انجام شده بر علیه سرورهای بانکی

انواع حملات به سیستم های بانکی را می توان به سه دسته کلی زیر تقسیم بندی کرد [8] [7]

- حملات راه دور که تغییراتی را بر روی سیستم کاربر ایجاد نکرده و تنها از راه دور، ترافیک ماشین را شنود نموده یا ترافیک یک نشست را به سمت سرور دلخواه مهاجم هدایت می کنند. برخی از این حملات عبارتند از:

✓ فیشینگ (Phishing) : یشینگ، متداول ترین حمله راه دوری است که بانکداری آنلاین با آن مواجه است. در این روش، مهاجم با ایجاد یک نمونه کپی کاملاً مشابه با وب سایت اصلی و ارسال پیام برای مشتریان آن بانک سعی می کند آنها را متقاعد کرده تا ضمن مراجعه به وب سایت جعلی، اطلاعات کاربری خود را در آن وارد کنند. مهاجم با این روش می تواند تمامی داده های مورد نیاز برای دسترسی به حساب کاربری مشتریان بانک را جمع آوری کرده و از آنها برای انجام کلاهبرداری سایبری سوءاستفاده کند. حملات فیشینگ، بیشتر با ارسال ایمیل و هدایت مشتریان بانک ها به وب سایت های جعلی که گاهاً با SSL هم به منظور معتبر نشان دادن خود نمایش داده می شوند، همراه است؛ به طوری که کاربر به جعلی بودن ایمیل دریافتی و فرایند کلاهبرداری نتواند شک نکند. یکی از روش های مقابله با این حمله، استفاده از ابزارکی در مرورگرها است که ابتدا هویت نام دامنه درخواستی کاربر را بررسی کرده و در صورت جعلی بودن دامنه، علاوه بر ارایه هشدار لازم به کاربر از نمایش محتویات آن سایت نیز جلوگیری می کند.

✓ حمله فارمینگ (Pharming): این نوع حمله از طریق آلوده کردن سرویس نام دامنه (DNS) می تواند کاربران را به آدرس اینترنتی (IP) جعلی که به جای آدرس صحیح، درون جدول نام دامنه ها آمده است هدایت کند. در واقع این حمله با هدایت افراد به سمت دامنه های غیرمعتبر، اقدام به سرقت مجوزهای دسترسی یا هویت آنها در هنگام ورود به سیستم می کند. تنها راه مقابله با این نوع از حملات، افزایش آگاهی مدیران سیستم و پیکربندی امن سرورهای سرویس نام دامنه است.

✓ شنود (Sniffing): این حمله، یکی دیگر از حملات راه دور است که در آن مهاجم اقدام به شنود داده هایی می کند که کاربر آن را دریافت یا ارسال می کند. راه مقابله با این نوع از حملات، استفاده از پروتکل های SSL/TLS برای رمزنگاری ترافیک تبادلی است. با این حملات می توان از طریق به روز نگهداشتن برنامه های کاربردی

سمت سرور و پیکربندی صحیح سرورها نیز تا حدود زیادی مقابله کرد.

- حملات محلی که بر روی سیستم کاربر، فعالیت های مخربی را انجام می دهند. حملاتی هستند که امکان شنود اطلاعات حساس کاربران را تا قبل از رمز شدن آنها با پروتکل SSL برای مهاجمان فراهم می کنند. این کار اغلب توسط بدافزاری انجام می شود که علاوه بر دسترسی به دایرکتوری های سیستم کاربر و حذف فایل های مورد نظر مهاجم، فرایند شنود را بر روی مرورگر وی آغاز می کند. در روش دیگر، حمله با استفاده از نمایش یک وب سایت جعلی مشابه سایت اصلی و با هدف سرقت داده های کاربران صورت می پذیرد. در این حالت، کاربر به وب سایت جعلی هدایت شده و اطلاعات ورودی خود به سیستم را در آن وارد می کند. یکی دیگر از روش های انجام این نوع از حملات، صفحات کلید (کیبردهای) سیستم کاربران است. اگرچه استفاده از صفحه کلید مجازی روشی برای مقابله با این مخاطره است ولی راهکار اصلی نیست.
- حملات چندگانه که ترکیبی از حملات راه دور و حملات محلی هستند. مهاجم در این نوع از حملات، روش های موجود در حملات محلی را با حملات راه دور ادغام کرده و حمله را بر روی سیستم کاربر شروع می کند. عمده فعالیت مهاجم در این نوع از حملات، جایگزین کردن یک آدرس جعلی با آدرسی معتبر و شناخته شده است. یکی دیگر از روش هایی که در این حملات زیاد از آن استفاده می شود، تغییر آدرس یا اصل فایل های موجود بر روی سیستم کاربر است. در روش های دیگر نیز حمله با تغییر مسیر درخواست های HTTP یا تغییر و انحراف جریان ترافیک انجام می شود. چنین حملاتی پیچیدگی بالایی داشته و برای مقابله با آنها نیاز به استفاده از روش های ترکیبی مقابله با حملات راه دور و حملات محلی است. یکی از راه حل های مقابله با حملات چندگانه، استفاده از نوار ابزارهای ضدفیشینگ و احراز هویت های متقابل میان سیستم کاربر و سرور است.

4- پیشینه تحقیق

Aaron و همکارانش [9] به بررسی پتانسیل یادگیری ماشین در ارتقای امنیت فناوری مالی با تمرکز بر چالش‌های کلیدی مانند تشخیص ناهنجاری، شناسایی تقلب، سیستم‌های تشخیص نفوذ (IDS) و مدیریت ریسک پرداختند. مروری بر الگوریتم‌های رایج یادگیری ماشین مانند درخت‌های تصمیم، شبکه‌های عصبی، ماشین‌های بردار پشتیبان (SVM) و روش‌های خوشه‌بندی، که در این وظایف امنیتی به‌کار می‌روند، ارائه نمودند. علاوه بر این، معیارهای ارزیابی مورد استفاده برای سنجش دقت، صحت، بازیابی و اثربخشی کلی این مدل‌ها را مورد بحث قرار دادند. با استفاده از مطالعات موردی واقعی، نمونه‌های موفق پیاده‌سازی یادگیری ماشین در امنیت فین‌تک را برجسته کرده و بینش‌هایی درباره بهترین روش‌ها و درس‌های آموخته‌شده ارائه کردند. Chhabra Roy و همکارانش [7] با هدف مرور انواع تقلب‌های سایبری داخلی تحقیقی انجام دادند که در رویدادهای کلان تقلب اخیر بانک‌های سرشناس هندی مورد توجه گسترده قرار گرفته‌اند. این محققان تلاش کرده‌اند تا تقلب‌های سایبری و عوامل محرک آن را شناسایی و دسته‌بندی کنند و سپس این موارد را برای برنامه‌ریزی بهینه کاهش ریسک، به یکدیگر مرتبط سازند. این تحقیق به بررسی انواع کلاهبرداری‌های سایبری که با همکاری داخلی (کارکنان یا نهادهای

درون سازمانی) انجام می‌شوند، می‌پردازد. روش تحقیق استفاده شده در مقاله عبارتست از: شناسایی و طبقه‌بندی انواع کلاهبرداری‌های سایبری و عوامل ایجادکننده آنها (مانند ضعف‌های امنیتی، انگیزه‌های مالی، یا سوءاستفاده از دسترسی‌های داخلی)، برقراری ارتباط بین این عوامل و روش‌های کلاهبرداری، تا بتوان بر اساس آن برنامه‌های کاهش ریسک مؤثرتری طراحی کرد. Ejiofor و همکارانش [10] یک چارچوب جامع برای تقویت امنیت سایبری مالی ایالات متحده ارائه دادند که با ادغام تکنیک‌های یادگیری ماشین (ML) و هوش مصنوعی (AI) در سیستم‌های تشخیص تقلب طراحی شده است. چارچوب پیشنهادی با بررسی مفاهیم بنیادین امنیت سایبری مالی آغاز می‌شود و تهدیدات کلیدی و ملاحظات نظارتی را برجسته می‌سازد. سپس به مبانی یادگیری ماشین و هوش مصنوعی می‌پردازد و کاربردهای آن‌ها در تشخیص تقلب همراه با مزایا و محدودیت‌های مرتبط را مورد بحث قرار می‌دهد. این مقاله از طریق مطالعات موردی و بهترین شیوه‌ها، پیاده‌سازی‌های موفق ML/AI در امنیت سایبری مالی را نشان می‌دهد و درس‌هایی از کاربردهای واقعی استخراج می‌کند. Kuttiyappan و همکارانش [11] پژوهشی مبتنی بر طراحی کاربر-محور انجام دادند که از اطلاعات خصوصی افراد در عملیات بانکی محافظت می‌کند. این روش شامل مراحل زیر است: تولید داده‌های حمله از تراکنش‌های بانکی، پیکربندی گره‌های شبکه و مسیریابی بهینه، پیش‌پردازش داده‌ها برای حذف نویز و خطاها، استخراج ویژگی‌های سلسله‌مراتبی شبکه برای شناسایی الگوهای غیرعادی، محافظت از داده‌های کاربر و شناسایی حملات با استفاده از طبقه‌بند پیشرفته ResNet پلکانی. Narsimha و همکارانش [8] مکانیزم دفاعی امنیت سایبری را با استفاده از تکنیک‌های هوش مصنوعی (AI) و یادگیری ماشین (ML) همراه با مدل امنیتی فعلی Feedzai برای شناسایی تراکنش‌های بانکی متقلبانه معرفی کردند. آنها مقدمه‌ای بر مدل‌های محبوب ML و AI با الگوریتم جنگل تصادفی و ابزار نرم‌افزاری تشخیص تقلب Feedzai's Open ML ارائه داده‌اند که قابلیت تشخیص خودکار تقلب را برای چارچوب هوشمند فعلی در حل مشکل تشخیص تقلب مالی فراهم می‌کند. این سیستم با ترکیب الگوریتم‌های پیشرفته یادگیری ماشین و رویکردهای هوشمند امنیتی، توانایی مقابله مؤثر با انواع جدید تهدیدات سایبری در حوزه مالی را دارد. نتایج نشان داد این رویکرد می‌تواند دقت تشخیص تقلب را به میزان قابل توجهی افزایش دهد و از دارایی‌های مالی مشتریان محافظت کند. Obeng و همکارانش [12] به بررسی کاربرد تکنیک‌های یادگیری ماشین (شامل تکنیکهای یادگیری نظارت شده و نظارت نشده، شبکه های عصبی، تشخیص ناهنجاری ها) در افزایش امنیت تراکنش‌ها و مبارزه با تقلب مالی پرداختند. همچنین کاربرد هر روش را در شناسایی و پیشگیری از فعالیت‌های متقلبانه، همراه با مزایا و محدودیت‌های آن‌ها بررسی کردند. Gill و همکارانش [13] با استفاده از مجموعه داده‌های بانکی، به بررسی شاخص‌های حملات سایبری به مؤسسات مالی پرداختند. در این تحقیق، با ترکیب تکنیک‌های طبقه‌بندی و افزایش پیچیدگی معماری مدل‌های پایه، عملکرد سیستم پیش‌بینی حملات بهبود داده شده است. روش‌های مورد استفاده شامل: ماشین بردار پشتیبان (SVM)، روش همسایگان نزدیک (KNN) و جنگل تصادفی (RF) می باشد. خدمات مالی یکی از آسیب‌پذیرترین سرویس‌ها در محیط‌های رایانش ابری محسوب می‌شوند. Kathirkamanathan و همکارانش [14] با هدف مقابله با حملات DDoS علیه نقاط پایانی تراکنش‌های مالی در

برنامه‌های تحت وب، با بهره‌گیری از معماری حافظه طولانی-کوتاه مدت انباشته (Stacked LSTM) پژوهشی انجام دادند. این مطالعه بر سه مدل شبکه عصبی عمیق (شامل: حافظه طولانی-کوتاه مدت (LSTM) واحدهای بازگشتی دروازه‌دار (GRU) و شبکه عصبی مصنوعی ساده (ANN)) متمرکز است. این مدل قادر به تشخیص و طبقه‌بندی انواع حملات DDoS در لایه HTTP سرور می‌باشد. Noor و همکارانش [15] چارچوبی را برای خودکارسازی اسناد تهدید سایبری پیشنهاد کردند. به طور خاص، آنها بازیگران تهدید سایبری (CTA) را بر اساس الگوهای حمله آنها استخراج شده از گزارش‌های CTI، با استفاده از تکنیک معنایی توزیعی پردازش زبان طبیعی، نمایه کردند.

5- نتیجه‌گیری و چالشهای موجود

در این تحقیق به بررسی اجمالی یادگیری ماشین، تکنیکهای مورد استفاده در آن و برخی از کاربردهای آن پرداختیم. در ادامه درباره حملات و تهدیدات امنیتی بر علیه سرورهای بانکی بحث نموده و برخی از تحقیقات انجام شده توسط محققان دیگر را مرور نمودیم. برخی از چالشهای کشف شده در این تحقیق در زمینه شناسایی تهدیدات و حملات امنیتی در سرورهای بانکی عبارتند از [17] [16] :

- چالش در زمینه کیفیت و حجم داده‌ها

✓ مدل‌های یادگیری ماشین به داده‌های با کیفیت بالا و حجم زیاد برای آموزش نیاز دارند. داده‌های ناکامل یا دارای نویز ممکن است باعث کاهش دقت مدل‌ها شوند.

✓ فراهم کردن داده‌های مناسب در حوزه امنیت سایبری می‌تواند به دلیل حساسیت اطلاعات بانکی بسیار چالش‌برانگیز باشد.

- پیچیدگی الگوریتم‌ها

✓ الگوریتم‌های یادگیری ماشین معمولاً پیچیدگی بالایی دارند که نیازمند منابع محاسباتی قدرتمند هستند.

✓ برای پیاده‌سازی و مدیریت این الگوریتم‌ها، نیاز به تخصص بالا و تیم حرفه‌ای است.

- تهدیدات علیه الگوریتم‌های یادگیری ماشین

✓ حملات خصمانه می‌توانند الگوریتم‌های یادگیری ماشین را فریب دهند و امنیت سیستم را کاهش دهند.

✓ مهاجمان ممکن است داده‌های ورودی مدل را دستکاری کنند تا مدل نتواند تهدیدات را به درستی تشخیص دهد.

- محدودیت در پیش‌بینی تهدیدات جدید

✓ برخی از مدل‌های یادگیری ماشین فقط توانایی شناسایی تهدیدات شناخته‌شده را دارند و ممکن است در تشخیص تهدیدات جدید و پیچیده ناتوان باشند.

- ✓ به‌روزرسانی مداوم مدل‌ها برای انطباق با تهدیدات جدید نیازمند زمان و منابع است.
  - هزینه‌های اجرایی
- ✓ پیاده‌سازی، آموزش، و مدیریت سیستم‌های یادگیری ماشین معمولاً هزینه‌بر است. این امر می‌تواند برای برخی از موسسات مالی، به ویژه بانک‌های کوچک، چالش‌زا باشد.

نتایج این مطالعه می‌تواند به بانک‌ها و مؤسسات مالی کمک کند تا با درک بهتر ریشه‌های تقلب‌های سایبری داخلی، راهکارهای هدفمندتری برای پیشگیری و پاسخ به این تهدیدات توسعه دهند.

6- منابع

[1] E. a. R. J. O. Rivandi"‏ ,A Novel Approach for Developing Intrusion Detection Systems in Mobile Social Networks ",".*Available at SSRN* .2024 ,*5174811*

[2] M. e. a. Wazid"‏ ,Uniting cyber security and machine learning: Advantages, challenges and future research ",". *ICT express* ,*8.3*pp. 313-321., .2022

[3] I. F. F. E. a. A. S. Kilincer"‏ ,Machine learning methods for cyber security intrusion detection: Datasets and comparative study ",". *Computer Networks* ,*188* p. 107840., .2021

[4] E. Rivandi"‏ ,FinTech and the Level of Its Adoption in Different Countries Around the World ",".*Available at SSRN* .2024 ,*5049827*

[5] J. C. I. C. a. P. J. G.-N. Martínez Torres"‏ ,Machine learning techniques applied to cybersecurity ",".*International Journal of Machine Learning and Cybernetics* ,*10.10*pp. 2823-2836., .2019

[6] B. B. a. M. S. ,. Gupta‏ ,Machine Learning for Computer and Cyber Security ",. *CRC Press: Boca Raton, FL, USA* .2019 , ,

[7] N. a. S. P. Chhabra Roy"‏ ,Internal-led cyber frauds in Indian banks: an effective machine learning–based defense system to fraud detection, prioritization and prevention ",. "*Aslib Journal of Information Management* ,*75.2*pp ,246-296 . .2023

[8] B. e. a. ,. Narsimha"‏ ,Cyber defense in the age of artificial intelligence and machine learning for financial fraud detection application ",. "*International Journal of Electrical and Electronics Research* ,*10.2*pp. 87-92., .2022

[9] W. C. e. a. Aaron" ‏ ,Ma-chine learning techniques for enhancing security in financial technology systems ",".*IEEE* .2024 ,

[10] O. E. ,. Ejiofor"‏ ,A comprehensive framework for strengthening USA financial cybersecurity: integrating machine learning and AI in fraud detection systems ". ",*European Journal of Computer Science and Information Technology* ,*11.6*pp . .2023 ,62-83

[11] D. a. V. R. Kuttiyappan"‏ ,Improving the Cyber Security over Banking Sector by

Detecting the Malicious Attacks Using the Wrapper Stepwise Resnet Classifier ",". *KSII Transactions on Internet and Information Systems (TIIS) ,,17.6*pp. 1657-1673, .2023

[12] S. e. a. Obeng"‏ ,Utilizing machine learning algorithms to prevent financial fraud and ensure transaction security ",, ".*World Journal of Advanced Research and Reviews ,,23.1*pp. 1972-1980., .2024

[13] M. A. e. a. Gill"‏ ,Cyber attacks detection through machine learning in banking ". ",*Bulletin of Business and Economics (BBE) ,,12.2*pp .2023 ,34-45 .

[14] N. e. a. Kathirkamanathan" ‏ ,Prevention of DDoS attacks targeting financial services using supervised machine learning and stacked LSTM *2022"*,"*IEEE 7th International conference for Convergence in Technology (I2CT). IEEE* ..2022 , ,

[15] U. e. a. Noor"‏ ,A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise ",".*Future Generation Computer Systems ,,96*pp .2019 ,227-242 .

[16] E. e. a. Bertino ‏ ,Machine Learning Techniques for Cybersecurity ",*Springer ,,* ..2023

[17] S. M. O. H. A. M. E. D. E.-D. a. S. K. Sur"‏ ,MACHINE LEARNING TECHNIQUES FOR CYBER SECURITY ",".*Journal of Theoretical and Applied Information Technology* .2024 *,. 102.7*

[18] A. E. Mohamed"‏ ,Comparative study of four supervised machine learning techniques for classification ",, ".*International Journal of Applied ,,7.2*pp. 1-15., .2017

[19] M. M. F. Y. a. A. O. O. WILLIAMS" ‏ ,Machine learning for proactive cybersecurity risk analysis and fraud prevention in digital finance ecosystems ",". *ecosystems 20(2021):* .2021 *,.21*

Using Machine Learning Techniques for Detecting and Preventing Threats against Banking Servers

Hossein Baghban
Ph.D. Student in Artificial Intelligence, Faculty of Computer Engineering,
Islamic Azad University, Ferdowsi Branch
Baghbanhossein1986@gmail.com

Abstract— The banking industry is one of the primary targets of cyberattacks. Given the sensitivity of financial data and the consequences of its leakage, traditional security methods are insufficient. Machine learning, with its capability to analyze complex patterns and identify anomalies, offers a suitable solution to this challenge. The application of machine learning techniques can significantly enhance the security of banking servers. Combining multiple methods and continuously updating models with new data is the key to success in addressing complex cyber threats. With the increase in cyberattacks targeting banks and financial institutions, the need for advanced security systems is more critical than ever. Therefore, this paper examines machine learning techniques employed by various researchers to detect and prevent security threats on banking servers.

Keywords: Machine learning techniques, cyberattacks and security threats, threat detection and prevention, banking servers