(تشخیص نفوذ مبتنی بر هوش مصنوعی در شبکه های کامپیوتری)

نسترن نبی یار
کارشناسی ارشد، گروه کامپیوتر، دانشگاه غیر انتفاعی آیین کمال، ارومیه، ایران

علی مصاحب طلب
مربی، گروه برق و کامپیوتر، دانشگاه فنی و حرفه ای، تهران، ایران

چکیده

تشخیص نفوذ(ID) یکی از عناصر کلیدی در تأمین امنیت شبکه های کامپیوتری در برابر حملات مخرب حائز اهمیت است. با پیشرفت های اخیر در زمینه های یادگیری عمیق(DL)، یادگیری هوش مصنوعی قابل توضیح(AXI)، یادگیری ماشین(ML) و یادگیری فدرال(FL)، این رویکرد ها به عنوان گزینه های جذابی برای بهبود تشخیص نفوذ مورد توجه قرار گرفته اند. رویکردهای مبتنی بر یادگیری عمیق با توجه به قابلیت‌های خود در یادگیری خودکار ویژگی‌های مرتبط از داده‌ها، عملکرد مؤثری در تشخیص نفوذ دارند. اما این روش‌ها به داده‌های برچسب‌گذاری شده و منابع محاسباتی قابل توجهی برای آموزش مدل‌های پیچیده نیاز دارند. در عوض، رویکردهای مبتنی بر یادگیری ماشین به منابع کمتری نیاز دارند، اما ممکن است در تعمیم به داده‌های جدید محدودیت‌هایی داشته باشند.

یادگیری هوش مصنوعی قابل توضیح با تمرکز بر شفافیت و تفسیرپذیری در تصمیم‌گیری مدل‌های هوش مصنوعی به کاربران این امکان را می‌دهد که بفهمند مدل‌ها چگونه به نتایج خاصی دست می‌یابند و این می‌تواند منجر به اعتماد بیشتر در استفاده از این سیستم‌ها شود. یادگیری فدرال، به عنوان یک رویکرد جدید، به چندین نهاد اجازه می‌دهد که بدون مبادله داده‌های خود، به طور مشترک یک مدل یادگیری کنند. این امر به حفظ حریم خصوصی و امنیت کمک می‌کند و آن را به گزینه‌ای مناسب برای تشخیص نفوذ تبدیل می‌سازد. این مقاله به شکاف‌های موجود در ادبیات پرداخته و سعی در ارائه یک مرور جامع از سناریوهای خاص کاربردی دارد. هدف آن کمک کردن به متخصصان و پژوهشگران است که تا با توجه به نیازهای خاصID ، به راحتی رویکرد مناسب را انتخاب کنند. عواملی نظیر اندازه شبکه، در دسترس بودن داده‌ها، و نگرانی‌های حفظ حریم خصوصی و امنیتی، همگی در انتخاب بهترین راهکار تأثیرگذار هستند. این تحلیل می‌تواند به افزایش آگاهی و بهبود تصمیم‌گیری در حوزه امنیت شبکه کمک کند و هدایت بهتری برای پیاده‌سازی سیستم‌های ID فراهم آورد.

واژگان کلیدی: شبکه های کامپیوتری، هوش مصنوعی، تشخیص نفوذ.

مقدمه

تشخیص نفوذ (IDS) بزاری حیاتی در امنیت سیستم‌ها و شبکه‌های کامپیوتری است که به هدف شناسایی فعالیت‌های مخرب، از جمله دسترسی‌های غیرمجاز و سوء استفاده از منابع، طراحی شده است. این سیستم‌ها توانایی آن را دارند که در زمان واقعی یا تقریباً واقعی،

اقداماتی را برای جلوگیری از خسارت‌های بیشتر یا سرقت اطلاعات انجام دهند. IDS با تجزیه و تحلیل الگوهای فعالیت در سیستم و شبکه، قادر به شناسایی رفتارهای مشکوک و حملات در حال انجام است. این سیستم‌ها می‌توانند به دو نوع مبتنی بر میزبان و مبتنی بر شبکه طبقه‌بندی شوند و با استفاده از روش‌های مختلفی مانند شناسایی مبتنی بر امضا یا رفتار می‌توانند تهدیدات را شناسایی کنند. پس از شناسایی نفوذ، IDS می‌تواند به پرسنل امنیتی یا سیستم‌های خودکار نظیر دیوار آتش هشدار دهد تا اقدامات لازم برای مهار یا کاهش حمله به سرعت انجام گیرد. به این ترتیب، ID به عنوان جزئی کلیدی از استراتژی‌های امنیتی جامع، کمک می‌کند تا سازمان‌ها به طور مؤثر، حوادث امنیتی را شناسایی و به آن‌ها پاسخ دهند (Muneer et al, 2024).

IDیکی از جنبه‌های حیاتی امنیت سایبری است که مدیریت و حفاظت مؤثر از آن می‌تواند به‌طور قابل توجهی خطرات امنیتی را کاهش دهد(Malik et al,2022) (Malik and Saleem, 2022).

ادغام فناوری و اینترنت در تمامی جنبه‌های زندگی، واقعاً نوار زندگی روزمره و فعالیت حرفه‌ای مردم را دگرگون کرده است. این تحولات نه‌تنها به ظهور روش‌های جدیدی برای کار از راه دور و آموزش آنلاین منجر شده بلکه امکان ارتباطات سریع و بی‌وقفه را نیز فراهم کرده‌اند. با این وجود، افزایش استفاده از فناوری و فضای مجازی با خود چالش‌های جدیدی به همراه آورده است، از جمله تهدیدات امنیتی نظیر هک، حملات سایبری و نشت اطلاعات حساس. لذا، حفاظت از اطلاعات شخصی و ایمنی در محیط آنلاین امری بسیار حیاتی و ضروری است. این امر شامل اتخاذ تدابیر احتیاطی در برابر کلاهبرداری‌های فیشینگ، استفاده از رمزهای عبور ایمن و به‌روز رسانی منظم نرم‌افزارها می‌شود. علاوه بر این، آموزش مستمر درباره ریسک‌های امنیت سایبری و شیوه‌های بهترین عمل، به عنوان عامل کلیدی در شناسایی و پیشگیری از تهدیدات، از اهمیت ویژه‌ای برخوردار است. در این راستا، آگاهی نسبت به آخرین خطرات امنیتی و توجه به نشانه‌های فعالیت‌های مشکوک می‌تواند به طور قابل توجهی به کاهش ریسک‌ها کمک کند(Muneer et al, 2024).

در مواجهه با حملات سایبری، شناسایی نشانه‌های اولیه اهمیت ویژه‌ای دارد. از جمله موارد رایج می‌توان به پاپ آپ‌ها یا پیام‌های خطای غیرمعمول، کاهش کارایی رایانه یا شبکه، ترافیک غیرمعمول در شبکه، تغییرات غیرمجاز در تنظیمات یا فرارها، و دریافت ایمیل‌ها یا پیوست‌های مشکوک اشاره کرد. آگاهی از این علائم می‌تواند در پیشگیری و کاهش خسارات ناشی از حملات سایبری مؤثر باشد(Mishra et al, 2017) (Wei et al, 2020).

ارزیابی‌ها و آزمایش‌های منظم امنیتی نقش حیاتی در شناسایی آسیب‌پذیری‌ها و تقویت امنیت شبکه‌ها ایفا می‌کنند. این اقدامات به حفاظت از اطلاعات حساس در برابر سرقت، تغییر و سوء استفاده کمک می‌کند. در دنیای دیجیتال امروز، تهدیداتی نظیر کلاهبرداری‌های فیشینگ، بدافزار، باج‌افزار و هک به‌طور فزاینده‌ای در حال رشد هستند. لذا ضروری است که افراد و سازمان‌ها به‌طور مستمر نرم‌افزارهای خود را به‌روزرسانی، از رمزهای عبور قوی استفاده کنند و اطلاعات خود را در زمینه تهدیدات امنیتی به‌روز نگه دارند تا از امنیت آنلاین خود محافظت نمایند(Muneer et al, 2024).

پیاده‌سازی احراز هویت چندعاملی، به‌عنوان یک لایه امنیتی اضافی، می‌تواند به‌طور قابل‌توجهی ریسک دسترسی غیرمجاز به سیستم‌ها را کاهش دهد. همچنین، ایجاد دیوارهای فرعی به تقسیم‌بندی شبکه و محدود کردن دسترسی به منابع حساس کمک می‌کند. علاوه بر این، پشتیبان‌گیری منظم از داده‌ها نه‌تنها در صورت بروز حملات سایبری، بلکه در مواقع نقص فنی نیز اطمینان از بازیابی اطلاعات را فراهم می‌آورد. این اقدامات به‌صورت جامع به تقویت امنیت سایبری و محافظت از دارایی‌های اطلاعاتی سازمان‌ها کمک می‌کند(Peng et al, 2018).

سیستم‌های تشخیص نفوذ (IDS) بخش ضروری یک قطعنامه امنیتی جامع محسوب می‌شوند، چرا که قابلیت شناسایی تهدیدات امنیتی در زمان واقعی و پاسخ سریع به آن‌ها را فراهم می‌آورند. این سیستم‌ها بسته به جایگاه خود در شبکه، می‌توانند مبتنی بر شبکه یا میزبان باشند. IDS مبتنی بر شبکه(NIDS) مسؤول نظارت بر ترافیک شبکه به دنبال نشانه‌های نفوذ است و در لایه شبکه فعالیت می‌کند، در حالی که IDS مبتنی بر میزبان (HIDS) به‌صورت محلی بر روی هاست‌های جداگانه نصب شده و رویدادهای مربوط به آن‌ها را برای شناسایی نشانه‌های خرابکاری تحت نظر دارد(Muneer et al, 2024).

سیستم‌های تشخیص نفوذ (IDS) می‌توانند در دو حالت اصلی فعالیت کنند: حالت تشخیص مبتنی بر امضا، که با استفاده از قوانین از پیش تعریف شده به شناسایی تهدیدات شناخته شده می‌پردازد، و حالت تشخیص مبتنی بر ناهنجاری، که از الگوریتم‌های یادگیری ماشین برای شناسایی انحرافات از رفتار عادی شبکه و نفوذهای احتمالی استفاده می‌کند. این روش‌ها به طور مشترک می‌توانند امنیت شبکه‌ها را افزایش دهند و تهدیدات را به صورت مؤثرتری شناسایی کنند(Peng et al, 2018).

در چند دهه اخیر، توجه به مسائل مرتبط با حملات سایبری به ویژه سیستم‌های تشخیص نفوذ (IDS) در سطح جهانی افزایش یافته است (Mishra et al, 2017).

الگوریتم‌های مختلف یادگیری ماشین (ML) به مسائل متعدد در این حوزه پاسخ داده‌اند(Mishra et al, 2017) (Modi et al 2012) از جمله این الگوریتم‌ها می‌توان به درخت‌های تصمیم، مدل‌های ماشین برداری پشتیبانی، k-means، k-نزدیک‌ترین همسایه، و رویکردهای هوش مصنوعی اشاره کرد. هر یک از این روش‌ها با رویکردهای خاص خود، توانایی‌ها و نقاط قوت منحصر به فردی را برای حل چالش‌های مختلف ارائه می‌دهند(Wei et al, 2020) (Schueller et al, 2018) (Sundararaman et al, 2023) (Dhanush et al. 2023).

با توجه به تحولات اخیر در علم داده و یادگیری ماشین، راه‌حل‌های مبتنی بر شبکه‌های عصبی عمیق به طور فزاینده‌ای مورد توجه پژوهشگران و متخصصان قرار گرفته‌اند. این تکنیک‌ها شامل انواع مختلفی از شبکه‌ها مانند شبکه عصبی کانولوشن ((CNN، شبکه عصبی تکراری ((RNN، ماشین بولتزمن محدود ((RBMو شبکه‌های عصبی ارسال پیام ((MPNNمی‌شوند که هر یک با قابلیت‌های منحصر به فرد خود به بهبود دقت و کارایی تحلیل داده‌ها کمک می‌کنند. این شبکه‌ها به طور خاص در زمینه‌های مختلفی از جمله بینایی کامپیوتری، پردازش زبان طبیعی و داده‌های زمانی به کار گرفته می‌شوند(Ghosh et al, 2015) (Liu and Lang, 2015).

مدل‌های Tese DL به عنوان ابزارهای پیشرفته در سیستم‌های تشخیص نفوذ (IDS) در محیط‌های مبتنی بر مه، ابر و اینترنت اشیاء شناخته می‌شوند(Pathmudi et al, 2023). استفاده از این مدل‌ها به منظور بهبود دقت و کارایی سیستم‌های امنیتی، فرصتی ارزشمند برای شناسایی به‌موقع تهدیدات و حملات سایبری فراهم می‌آورد(Almiani et al, 2020) (Alkadi et al, 2021).

مدل‌سازی سیستم‌های تشخیص نفوذ (IDS) به عنوان یک چالش در انتخاب ویژگی‌ها و به کارگیری طبقه‌بندهای سنتی مطرح است. در این راستا، استفاده از الگوریتم‌های بهینه‌سازی متا اکتشافی (MH) می‌تواند به عنوان راه‌حلی مؤثر برای غلبه بر مشکلات بهینه‌سازی پیچیده درIDS ها مدنظر قرار گیرد(Muneer et al, 2024).

الگوریتم‌های MH شامل روش‌هایی نظیر بهینه‌سازی ازدحام ذرات (PSO)(Gosh et al, 2019) ، الگوریتم جستجوی کلاغ (CSA)(SaiSindhuTeja et al, 2021)، الگوریتم ژنتیک(GA) ، الگوریتم جستجوی هارمونی تصادفی و الگوریتم بهینه‌ساز گرگ خاکستری (GWO)می‌باشند. این الگوریتم‌ها به منظور بهینه‌سازی مسائل پیچیده و multifaceted در زمینه‌های مختلف علمی و صنعتی مورد استفاده قرار می‌گیرند و توانایی بالایی در جستجو و اکتشاف راه‌حل‌های بهینه از خود نشان می‌دهند.(Nguyen and Kim, 2020) (Malhotra et al, 2017)

این الگوریتم‌ها به‌منظور افزایش حریم خصوصی و کارایی سیستم‌های تشخیص نفوذ (IDS) بهینه‌سازی انتخاب ویژگی‌های مورد استفاده برای پیش‌بینی‌ها را تسهیل می‌کنند. با بهبود فرآیند انتخاب ویژگی، این الگوریتم‌ها قادرند حجم داده‌های پردازش شده را کاهش دهند و در نتیجه بهبود عملکرد کلی IDS را تضمین کنند. این رویکرد نه تنها دقت پیش‌بینی‌ها را افزایش می‌دهد بلکه امنیت اطلاعات حساس را نیز بهبود می‌بخشد(Mayuranathan et al, 2019) (Rm et al, 2020).

توسعه سیستم‌های تشخیص نفوذ (IDS) چالش‌برانگیز و نیازمند تحلیل عمیق رفتار فعالیت‌های مخرب در محیط‌های شبکه است. آزمایش مدل‌های IDS در آزمایشگاه می‌تواند بینش‌های مفیدی در زمینه کارایی و دقت آن‌ها فراهم آورد، اما خطر بیش‌افزاری وجود دارد که ممکن است به عملکرد ضعیف در دنیای واقعی منجر شود. از این رو، ارزیابی معتبر مدل IDS در محیط واقعی حیاتی است تا از اثربخشی آن اطمینان حاصل شود. این ارزیابی می‌تواند از طریق استقرار مدل در یک شبکه زنده و نظارت بر عملکرد آن انجام شود که

تصویر دقیقی از شرایط واقعی شبکه را ارائه می‌دهد و کمک می‌کند تا نقاط ضعف شناسایی شود. همچنین، به‌روزرسانی مداوم مدل برای همگام‌سازی با تهدیدات جدید و تغییرات رفتار شبکه امری ضروری است(Muneer et al, 2024).

دانش عمیق (DL) در زمینه‌های متنوعی از جمله طبقه‌بندی تصویر، تشخیص اشیا و تقسیم‌بندی کاربردهای قابل توجهی یافته است. این تکنولوژی در حوزه‌هایی نظیر تشخیص چهره و صنایع خودروهای خودمختار پیشرفت‌های چشمگیری را به ارمغان آورده و در بخش‌های پزشکی، بینایی کامپیوتر، امور مالی، تبلیغات، پردازش زبان طبیعی (NLP)، امنیت سایبری و سیستم‌های تشخیص نفوذ (IDS)نیز تأثیرگذار بوده است(Dawoud et al, 2018) (Alkadi et al, 2021) (SaiSindhuTeja et al, 2021).

طرح‌های مختلف شبکه‌های عصبی کانولوشنی(CNN) برای کاربرد در سیستم‌های تشخیص نفوذ (DS) اُمورد بررسی قرار گرفته‌اند. این مدل‌ها از نظر عمق و وسعت، نوع عملکرد کانولوشن، تعداد و اندازه فیلترها، نوع و اندازه جمع‌بندی، و تعداد لایه‌های کاملاً متصل و پارامترهای محیطی که در آن‌ها به کار می‌روند، تفاوت‌های چشمگیری دارند. این تنوع در طراحی، انعطاف‌پذیری و کارایی بالای این شبکه‌ها را در شناسایی الگوهای نامعمول و پیش‌بینی تهدیدات امنیتی ارتقا می‌دهد(Muneer et al, 2024).

مدل‌های MobileNet، ResNet، NASNet، EfficientNet، MnasNet و AlexNet به عنوان نمونه‌هایی از تلاش‌های مستمر در جهت بهبود دقت و کارایی در شناسایی تصویر (ID) مطرح شده‌اند. این مدل‌ها به‌ویژه بر اساس نتایج حاصل از جستجوی مجدد طراحی شده‌اند و هر یک از آن‌ها ویژگی‌ها و قابلیت‌های منحصر به فردی را برای بهینه‌سازی عملکرد در زمینه‌های مختلف ارائه می‌دهند.(Nguyen and Kim, 2020) (Malhotra et al, 2017).

این مطالعه یک مدل جدید سیستم تشخیص نفوذ (IDS) را ارائه می‌دهد که با ترکیب تکنیک‌های بهینه‌سازی عمیق یادگیری (DL)و فراابتکاری، به کاهش پیچیدگی و افزایش دقت در استخراج ویژگی‌ها می‌پردازد. مدل مذکور با استفاده از شبکه‌های عصبی کانولوشن (CNN)، به استخراج کارآمد و ساده ویژگی‌ها از داده‌های خام می‌پردازد. این فرایند شامل بهره‌گیری از تعداد زیادی بلوک کانولوشن است که به استخراج ویژگی‌های مفید کمک می‌کند و در نهایت، داده‌ها به نمایش‌های با ابعاد پایین‌تر تبدیل می‌شوند تا CNN با استفاده از ساختارهای ساده و روش‌های آموزشی بهینه، یادگیری موثرتری را انجام دهد(Muneer et al, 2024).

لایه کاملاً متصل به شبکه‌های عصبی کانولوشنی (CNN)توانایی استخراج ویژگی‌های کلیدی از داده‌ها را دارد و می‌تواند فعالیت‌ها را به دسته‌های مخرب و غیر مخرب طبقه‌بندی کند. این تحقیق با هدف افزایش دقت و کارایی سیستم‌های تشخیص نفوذ (IDS)به بررسی ادغام نقاط قوت روش‌های بهینه‌سازی یادگیری عمیق و الگوریتم‌های فرا اکتشافی می‌پردازد. با این رویکرد نوآورانه، امید می‌رود که عملکرد سیستم‌های امنیتcy سایبری به طرز قابل توجهی بهبود یابد.(Deshpande et al, 2018) (Liu and Lang, 2019) (Pathmudi et al, 2023).

اخیراً، یادگیری ماشینی و یادگیری فدرال به عنوان عوامل کلیدی در سیستم‌های تشخیص نفوذ (IDS)معرفی شده‌اند. یادگیری ماشینی، به عنوان زیرمجموعه‌ای از هوش مصنوعی، به رایانه‌ها این امکان را می‌دهد که از داده‌ها یاد بگیرند و به‌طور خودکار عملکرد خود را بهبود بخشند. در حوزه تشخیص نفوذ، این فناوری می‌تواند برای طراحی الگوریتم‌هایی بهره‌برداری شود که به شناسایی خودکار فعالیت‌های مخرب و نفوذهای شبکه کمک می‌کنند. با آموزش مدل‌ها روی مجموعه‌های عظیم داده‌های تاریخی، این الگوریتم‌ها قادرند الگوهای رفتاری مرتبط با حملات سایبری را شناسایی کرده و در زمان واقعی نقاط داده جدید را طبقه‌بندی کنند تا نفوذهای احتمالی را شناسایی کنند.یادگیری فدرال یک تکنیک مبتنی بر یادگیری ماشین است که در شرایطی کاربرد دارد که داده‌ها بین چندین نهاد یا سازمان توزیع شده‌اند. در زمینه شناسایی نفوذ در شبکه، این روش به نهادهای مختلف امکان می‌دهد تا به طور مشترک یک مدل یادگیری ماشین را آموزش دهند، بدون اینکه نیاز به جمع‌آوری داده‌ها در یک سرور مرکزی باشد. هر نهاد با استفاده از داده‌های محلی خود، مدل‌های محلی را آموزش می‌دهد و سپس این مدل‌ها به یک سرور مرکزی ارسال می‌شوند تا در یک مدل جهانی ترکیب شوند. این فرآیند به طور مکرر تکرار می‌شود تا کارایی مدل افزایش یابد و امنیت اطلاعات حفظ شود. یادگیری فدرال در زمینه‌های مرتبط با شناسایی ((IDبه‌ویژه در حفظ حریم خصوصی و امنیت داده‌ها مؤثر است. این تکنیک با انجام آموزش مدل به‌صورت محلی، از ارسال

داده‌ها به سرور مرکزی جلوگیری می‌کند و به این ترتیب خطر نقض داده‌ها را کاهش می‌دهد و اطمینان از حریم خصوصی اطلاعات را افزایش می‌دهد. همچنین، با بهره‌گیری از داده‌های مشترک میان چندین دستگاه یا سازمان، یادگیری فدرال می‌تواند به بهبود دقت مدل‌های شناسایی کمک کند(Muneer et al, 2024).

سیستم‌های تشخیص نفوذ (IDS)به عنوان ابزارهایی حیاتی برای شناسایی و پیشگیری از فعالیت‌های مخرب در شبکه‌های کامپیوتری عمل می‌کنند(Muneer et al, 2024). در این راستا، تکنیک‌های یادگیری ماشینی و یادگیری فدرال به‌طور گسترده‌ای در IDS به‌کار گرفته می‌شوند(Zhao et al, 2020) تا دقت و کارایی این سیستم‌ها را بهبود بخشند. این فناوری‌ها با تحلیل الگوهای ترافیک شبکه و یادگیری از داده‌های توزیع‌شده، توانمندی تشخیص تهدیدات را افزایش می‌دهند و امکان واکنش سریع به حملات سایبری را فراهم می‌آورند. الگوریتم‌های یادگیری ماشینی قادرند تا حجم وسیعی از داده‌ها را تحلیل کرده و الگوها و ناهنجاری‌ها را در ترافیک شبکه شناسایی نمایند تا حملات احتمالی را شناسایی کنند. از سوی دیگر، یادگیری فدرال به چندین طرف این امکان را می‌دهد که بدون به اشتراک‌گذاری داده‌های خود، در ساخت یک مدل مشترک همکاری کنند و بدین ترتیب حریم خصوصی و امنیت داده‌ها را تقویت کنند. هر یک از این تکنیک‌ها نقاط قوت و ضعفی دارند و کارایی آن‌ها در سیستم‌های تشخیص نفوذ (IDS)به عوامل متعددی نظیر کیفیت و دسترسی به داده‌ها، منابع محاسباتی و نگرانی‌های امنیتی بستگی دارد. در حوزه ایمن‌سازی شبکه‌های کامپیوتری، سیستم تشخیص نفوذ (ID) نقشی اساسی در حفاظت از زیرساخت‌ها در برابر طیف گسترده‌ای از حملات مخرب ایفا می‌کند(Muneer et al, 2024).

در چشم‌انداز پیچیده و همیشه در حال تحول امنیت شبکه، پیشرفت‌های اخیر در تکنولوژی‌های یادگیری ماشینی، یادگیری عمیق(Ahmed et al, 2023) (Sajjad et al, 2023)، یادگیری فدرال و هوش مصنوعی قابل توضیح، به عنوان ابزارهای نوآورانه جهت تقویت شناسایی تهدیدات، مورد توجه قرار گرفته‌اند. این تکنولوژی‌ها نه تنها روش‌های جدیدی برای تقویت امنیت شبکه فراهم می‌آورند، بلکه چالش‌هایی را نیز به همراه دارند که نیازمند رویکردهای جدید در مدیریت و پیاده‌سازی است. به طور کلی، این تحول در زمینه امنیت شبکه، افق‌های جدیدی را برای حفاظت از اطلاعات ایجاد می‌کند و راهکارهایی مؤثر را در برابر تهدیدات پیشرفته ارائه می‌دهد. برای پیمایش مؤثر در این زمین پیچیده و پویا، پرسش‌های تحقیقاتی بنیادی ظهور کرده‌اند که با هدف روشن کردن نقاط قوت و محدودیت‌ها و تعیین زمینه‌های کاربردی مناسب طراحی شده‌اند. این سؤالات به ایجاد دانش و بینش‌های ضروری برای شاغلین شبکه کمک می‌کنند تا قادر به اتخاذ تصمیمات آگاهانه و استراتژیک باشند و در عین حال سیستم‌های خود را در برابر تهدیدات مخرب تقویت نمایند. در راستای تلاش پیوسته برای دنیای دیجیتال امن‌تر، این پرسش‌های پژوهشی به عنوان چراغ‌های راهنما عمل کرده و مسیر را به سوی شناسایی مؤثر و نوآورانه روشن می‌کنند. با توجه به پیشرفت‌های فناوری مدرن، به‌خصوص در زمینه‌های یادگیری ماشین (ML)، یادگیری عمیق (DL)، آموزش فدرال (FL)و هوش قابل توضیح (XAL)، پرسش‌های متعددی درباره بهبود امنیت و کارایی سیستم‌های شناسایی (ID)مطرح می‌شود. از یک سو، نقاط قوت و محدودیت‌های رویکردهای DL، به دلیل نیاز به داده‌های برچسب‌دار و منابع محاسباتی زیاد برای آموزش مدل‌های پیچیده، نیاز به تحلیل دقیق دارد. از سوی دیگر، رویکردهای ML به‌دلیل تمایز در الزامات محاسباتی و توانایی تعمیم به داده‌های جدید، جای خود را در این بحث باز می‌کنند. همچنین، آموزش فدرال(FL) امنیت و حفظ حریم خصوصی را بدون نیاز به انتقال داده‌های حساس بهبود می‌بخشد، اگرچه با چالش‌هایی چون هزینه‌های ارتباطی و محاسباتی مرتبط است. نقش XAI نیز در افزایش شفافیت و قابلیت تفسیر در ID امری حیاتی است. در نهایت، وجود شکاف‌هایی در ادبیات موجود پیرامون بررسی جامع‌تر این رویکردها و تعیین مناسب‌ترین استراتژی برای ID، بر اساس شرایط خاص، ضروری است(Muneer et al, 2024).

۱. بررسی ادبیات

پیش از این، چندین محقق در زمینه سیستم‌های تشخیص نفوذ (IDS) فعالیت کرده‌اند که نتایج و دستاوردهای آنها نقش بسزایی در پیشرفت این حوزه داشته است. برخی از آثار برجسته این پژوهشگران در این بخش معرفی و مورد بررسی قرار گرفته است(Muneer et al, 2024).

جدول ۱: بررسی انتقادی رویکردهای مبتنی بر یادگیری ماشین (ML) در ID (Muneer et al, 2024).

نویسنده	سال	رویکرد ML	دقت (٪)
Ahmed et al.	۲۰۲۲	جنگل تصادفی ((RF	۹۵/۱
Singh et al.	۲۰۲۲	بردار پشتیبان رگرسیون	۹۸
Pranto et al.	۲۰۲۲	استراتژی انتخاب ویژگی گروه مبتنی بر ML	۹۹/۵
Raghuvanshi et al.	۲۰۲۲	SVM	۹۸
Albulayhi et al.	۲۰۲۲	IDS مبتنی بر ML	۹۹/۹۸
Asif et al.	۲۰۲۱	روش مبتنی بر ML درهم آمیخته با مدل هوشمند مبتنی بر MapReduce برای ID (MR-IMID)	۹۷/۷
Çavus¸o˘glu	۲۰۱۹	IDS ترکیبی و لایه ای	۹۹/۷
Alqahtani et al	۲۰۲۰	RF	۹۴
Liu and Lang	۲۰۱۹	KNN	۹۹
Ren et al.	۲۰۱۹	IDS با استفاده از بهینه سازی داده های ترکیبی DO-IDS))	۹۲/۸
Bindra and Sood	۲۰۱۹	RF	۹۶
Sai Kiran et al.	۲۰۲۰	SVM	۹۸/۹۵
Saranya et al.	۲۰۲۰	RF	۹۹/۸۱
Logeswari et al.	۲۰۲۳	انتخاب ویژگی هیبریدی HFS Light GBM IDS))	۹۸/۷۲
Muhammad and Saleem	۲۰۲۲	Na¨ıve Bayes	۹۸/۶

جدول ۲: بررسی انتقادی رویکردهای مبتنی بر یادگیری عمیق در ID (Muneer et al, 2024).

نویسنده	سال	رویکرد DL	دقت (٪)
Yin et al.	۲۰۱۷	RNN-IDS	۹۷/۰۹
Vani	۲۰۱۷	روش گروهی مبتنی بر LSTM	۹۲/۳
Wang et al.	۲۰۱۷	IDS مبتنی بر ویژگی‌های مکانی-زمانی سلسله مراتبی ((HAST-IDSبا CNN	۹۹/۸۹
Loukas et al.	۲۰۱۷	RNN	۸۶/۹
Shone et al.	۲۰۱۸	NDAE	۹۷/۸۵
Lee et al.	۲۰۱۸	رمزگذار خودکار	۹۸/۹
Al-Qatf et al.	۲۰۱۸	یادگیری خودآموز IDS- (STL)	۹۹/۴۱
Ding and Zhai	۲۰۱۸	CNN	۸۰/۱۳
Parampottupadam and Moldovann	۲۰۱۸	یادگیری عمیق (H2Oمدل های دو جمله ای و چند جمله ای)	۹۹/۹۸
Xin et al.	۲۰۱۸	CNN	۹۹/۴۱
Faker and Dogdu	۲۰۱۹	DNN	۹۹/۱۶
Laqtib et al.	۲۰۱۹	CNN	۷۷
Ge et al.	۲۰۱۹	FFNN	۸۲
Khan et al.	۲۰۱۹	مدل یادگیری عمیق دو مرحله ای TSDL).)	۹۹/۳۱
Gurung et al	۲۰۱۹	رمزگذارهای خودکار	۸۷/۲
Su et al.	۲۰۲۰	مدل BAT	۸۴/۲۵
Gamage and Samarabandu	۲۰۲۰	ANN	۹۸/۲۵
Boukhalfa et al.	۲۰۲۰	LSTM	۹۹/۹۳
Shende and Torat	۲۰۲۰	LSTM	۹۶/۹۲
Kocher and Kumar	۲۰۲۱	ANN	۹۹/۴
Mighan and Kahani	۲۰۲۱	ANN	۹۸/۵۱

Ashiku and Dagli	۲۰۲۱	DNN	۹۵/۶
Salih et al	۲۰۲۱	Bayesian CNN	۹۹/۳۲۷۱
Imrana et al.	۲۰۲۱	دو جهته ((BiDLSTM	۹۴/۲۶
Otoum et al.	۲۰۲۲	DL-IDS	۹۹
Nasir et al.	۲۰۲۲	DF-IDS	۹۹/۹
Jasim	۲۰۲۲	شبکه های باور عمیق ((DBN	۹۹
Akshay Kumaar et al.	۲۰۲۲	چارچوب ترکیبی مبتنی بر DL "ImmuneNet"	۹۹/۲
Houda et al.	۲۰۲۲	چارچوب DL مبتنی بر هوش مصنوعی قابل توضیح (.XAI)	۹۹
Chaganti et al	۲۰۲۳	LSTM	۹۷/۱
Figueiredo et al.	۲۰۲۳	LSTM	۹۹
Rizvi et al	۲۰۲۳	شبکه عصبی علتی گشاد شده ۱ بعدی D-DCNN)۱)	۹۹/۹۸

جدول ۳: بررسی انتقادی رویکردهای مبتنی بر یادگیری فدرال (FL) در ID (Muneer et al, 2024).

نویسنده	سال	رویکرد FL	دقت (٪)
Supriya and Gadekallu	۲۰۲۳	بهینه سازی ازدحام ذرات مبتنی بر رویکرد FL (PSO)	۹۴/۴۷
Mu et al	۲۰۲۳	FedProc: نمونه اولیه متضاد FL	دقت را با ۱/۶٪ به ۷/۹ بهبود می بخشد
Yu et al.	۲۰۲۳	روش فورج آهن مبتنی بر FL	۹۷
Nguyen et al.	۲۰۲۰	IDS اینترنت اشیا مبتنی بر FL	۹۹/۹
Liu et al	۲۰۲۱	IDS مبتنی بر FL و Blockchain	۸۰<
Chen et al	۲۰۲۰	واحد بازگشتی مبتنی بر یادگیری مبتنی بر توجه ((FedAGRU	۹۸/۸۲
Rahman et al.	۲۰۲۰	طرح مبتنی بر FL	۸۳/۰۹
Mothukuri et al.	۲۰۲۱	رویکرد تشخیص ناهنجاری مبتنی بر FL	۹۰/۲۵۵
Zhao et al	۲۰۱۹	شبکه عصبی عمیق چند وظیفه ای در یادگیری فدرال ((MT-DNN-FL	۹۶/۵۴
Rey et al.	۲۰۲۲	چارچوب تشخیص بدافزار مبتنی بر FL	۹۸/۵۹
Belenguer et al.	۲۰۲۲	برنامه مبتنی بر FL	۹۲
Zhang et al.	۲۰۲۲	SecFedNIDS: دفاع قوی برای حمله مسمومیت در برابر IDS شبکه مبتنی بر یادگیری فدرال	۴۸ را بهبود می بخشد
Sarhan et al.	۲۰۲۳	طرح اشتراک اطلاعات تهدیدات سایبری	۹۲

در این مطالعه(Eskandari et al, 2020)، نویسندگان بر اهمیت روزافزون امنیت سایبری در عصر فناوری اطلاعات تأکید کرده‌اند. گسترش نیاز به سیستم‌های تشخیص نفوذ (IDS)و بهبود آن‌ها از طریق یادگیری ماشین (ML)توجهات بسیاری را جلب کرده است. هدف اصلی این تلاش‌ها ارائه ابزارهای کارآمدتر برای محافظت از شبکه‌ها و سیستم‌ها در برابر حملات سایبری است. این تحقیق به معرفی Passban، یک IDS مختص دستگاه‌های اینترنت اشیا، می‌پردازد که بر روی دروازه‌های ارزان‌قیمت این حوزه قابل استقرار است. با این حال، چالش‌های انطباق با تغییرات سریع در تهدیدات اینترنت اشیا و مسائل مقیاس‌پذیری در شبکه‌های متنوع دستگاه‌ها به‌طور کامل مورد بررسی قرار نگرفته است(Muneer et al, 2024).

در مقاله مذکور(Mirsky et al, 2018)، مجتبی و همکاران به پیش‌بینی یک سیستم تشخیص نفوذ (IDS)پرداخته‌اند که به‌طور خاص برای محیط‌های سخت‌افزاری محدود طراحی شده است. این IDS با استفاده از تکنیک‌های یادگیری بدون نظارت، قابلیت تشخیص ناهنجاری‌ها در داده‌های شبکه را داراست و به‌منظور بهبود عملکرد، از سرعت یادگیری و سازگاری با تغییرات در رفتار شبکه بهره می‌برد. هدف اصلی نویسندگان ارائه راه‌حلی مؤثر برای شناسایی تهدیدات امنیتی است که به‌طور ویژه برای شرایط محدود سخت‌افزاری بهینه شده باشد. اگرچه این مقاله Kitsune را به‌عنوان یک سیستم تشخیص نفوذ کارآمد معرفی می‌کند، اما چالش‌های مربوط به

مقیاس‌پذیری و تعمیم آن در موقعیت‌های واقعی و دنیای تهدیدات مختلف همچنان به‌طور کامل مشخص نشده است. همچنین نیاز به مداخله انسانی در فرآیند راه‌اندازی و نگهداری این سیستم نیز به وضوح تعیین نشده است(Muneer et al, 2024).

در مقاله مذکور (Zhao et al, 2019)، نویسندگان یک سیستم تشخیص نفوذ (IDS)معرفی کردند که از الگوریتم‌های AutoEncoder برای شناسایی آنلاین استفاده می‌کند. AutoEncoder، به عنوان یک الگوریتم یادگیری عمیق، قادر به تشخیص ناهنجاری‌ها در داده‌ها است. IDS مورد بحث در این مطالعه، الگوریتم‌های AutoEncoder را برای داده‌های شبکه بلادرنگ به کار می‌گیرد و به عنوان یک راه‌حل شناسایی آنلاین عمل می‌کند. هدف این سیستم، شناسایی تهدیدات امنیتی به طور سریع، کارآمد و دقیق است. با استفاده از الگوریتم‌های AutoEncoder، این IDS توانایی یادگیری از داده‌ها را دارد و می‌تواند با تغییرات رفتار شبکه سازگار شود(Muneer et al, 2024).

طبقه‌بندی‌کننده متوالی مبتنی بر شبکه‌های عصبی مصنوعی(ANN) به منظور متعادل‌سازی نرخ‌های مثبت و منفی کاذب در سیستم‌های شناسایی تهدیدات سایبری طراحی شده است. با این حال، چالش‌هایی نظیر سربار محاسباتی، افزایش تاخیر در تشخیص و نیاز به تنظیم دقیق عملکرد این مدل مطرح است. علاوه بر این، این مطالعه از ارزیابی جامع در مورد کارآمدی این روش در برابر تهدیدات سایبری پویا و در حال تحول ناتوان است(Muneer et al, 2024).

نویسندگان (Gharaee and Hosseinvand, 2016)به بررسی کاربرد شبکه‌های عصبی مصنوعی (ANN)و سایر روش‌های طبقه‌بندی در تشخیص شبکه‌های تروس پرداخته‌اند. در این مطالعه، کارایی ANN با دیگر الگوریتم‌های طبقه‌بندی مقایسه شده است تا بهترین راهکار برای مشکل خاص شناسایی شود. نتایج نشان می‌دهد استفاده از یک رویکرد مجموعه‌ای که ترکیبی از طبقه‌بندی‌کننده‌های متعدد را به کار می‌گیرد، می‌تواند کارایی بیشتری در تشخیص تهدیدات امنیتی ارائه دهد. این رویکرد با استفاده از نقاط قوت الگوریتم‌های مختلف، نقاط ضعف آنها را کاهش می‌دهد و دقت را افزایش می‌بخشد. به‌علاوه، روش IDS مبتنی بر ناهنجاری که از الگوریتم ژنتیک و ماشین بردار پشتیبان (SVM)بهره می‌برد، به بهبود دقت و کاهش مثبت کاذب کمک می‌کند. با این حال، ارزیابی جامع عملکرد آن در محیط‌های مختلف و در برابر حملات متغیر همچنان نیازمند تحقیق بیشتری است و مقیاس‌پذیری عملی مدل نیز برای مدیریت ترافیک شبکه‌های واقعی جای سوال دارد(Muneer et al, 2024).

نویسندگان(Belouch and Idhammad, 2017) یک مکانیسم امنیتی شبکه جدید مبتنی بر استخراج ویژگی را معرفی کردند که از ترکیب الگوریتم ژنتیک (GA)و ماشین‌های بردار پشتیبان (SVM)با حداقل مربعات برای شناسایی ناهنجاری‌ها در مسائل امنیتی استفاده می‌کند. ارزیابی‌ها نشان‌دهنده نرخ‌های مثبت کاذب پایین و نرخ‌های مثبت بالا در شناسایی تهدیدات است که مؤثر بودن این مدل در جلوگیری از هشدارهای کاذب را تأیید می‌نماید. اجرای SVM با الگوریتم ژنتیک اختصاصی و حداقل مربعات، بهبودهایی در کارایی و دقت مدل نسبت به تکنیک‌های پیشین ایجاد کرده است. همچنین، طبقه‌بندی‌کننده دو مرحله‌ای با الگوریتم RepTree به تقویت دقت شناسایی (ID)کمک می‌کند، هرچند که نتواند به‌طور مؤثر الگوهای حمله جدید را که در داده‌های آموزشی موجود نیستند، شناسایی کند. با این حال، این مقاله به تحلیل عمیق‌تری از استحکام مدل در برابر حملات متخاصم و مقیاس‌پذیری آن در محیط‌های پیچیده واقعی نمی‌پردازد(Muneer et al, 2024).

در مقاله مذکور(Baig et al, 2017)، الگوریتم الگوی هرس درخت خطای کاهش یافته (RepTree)به عنوان یک راهکار نوین در امنیت شبکه ارائه شد. این مدل شامل چهار جزء اساسی است: لایه انتخاب ویژگی، گروه‌بندی پروتکل شبکه، لایه تشخیص ناهنجاری و لایه بازرسی ناهنجاری. لایه انتخاب ویژگی به کاربران این امکان را می‌دهد که ویژگی‌های مناسب برای نیازهای امنیتی خود را برگزینند. گروه‌بندی پروتکل، ترافیک شبکه را بر اساس پروتکل‌های مختلف (TCP، UDP و غیره) طبقه‌بندی می‌کند. لایه تشخیص ناهنجاری با بهره‌گیری از الگوریتم REPTree به شناسایی رفتارهای غیرعادی شبکه می‌پردازد و در نهایت، لایه بازرسی این ناهنجاری‌ها را ارزیابی می‌کند تا تهدیدات امنیتی بالقوه را شناسایی کند. در همین راستا، نویسندگان به تشریح CANID، یک شبکه عصبی مصنوعی مبتنی بر مجموعه‌های آبشاری، پرداخته و به چالش‌های آن در برابر حملات جدید و مقیاس‌پذیری در محیط‌های واقعی اشاره دارند(Muneer et al, 2024).

در مقاله مذکور(Al-Zewairi et al, 2017)، محققان روشی نوآورانه را معرفی کردند که به تغذیه شبکه با بردارهای ویژگی استخراج شده از داده‌های ترافیک شبکه و آموزش آن برای شناسایی الگوهای ترافیک عادی و غیرعادی می‌پردازد. در مرحله آزمایش، شبکه به تحلیل داده‌های جدید پرداخته و براساس آموزش خود، ترافیک را به دو دسته عادی و غیرعادی طبقه‌بندی می‌کند. این تحقیق با استفاده از مجموعه داده‌های NSL-KDD و UNSW-NB 15 انجام شده است و شامل بردارهای ویژگی مربوط به ترافیک شبکه است که به‌طور مشخص برچسب‌گذاری شده‌اند. نتایج نشان‌دهنده دقت بالای طبقه‌بندیدو جمله‌ای مبتنی بر یادگیری عمیق پیشنهادی در شناسایی ترافیک شبکه است. با این حال، نگرانی‌هایی درباره قابلیت تعمیم این روش به سناریوهای حمله جدید و ارزیابی عملکرد آن در برابر حملات خصمانه وجود دارد. به منظور استفاده بهینه از قابلیت‌های شبکه‌های عصبی کانولوشن (CNN)در پردازش داده‌های دو بعدی، ویژگی‌ها به تصاویر تبدیل شدند. این تبدیل شامل کدگذاری یکباره ویژگی‌های اسمی و تبدیل هر قطعه ۸ بایتی به یک پیکسل بود که در نهایت به تصاویر ۸ × ۸ پیکسل انجامید. محققان یک CNN سه لایه برای طبقه‌بندی حملات شبکه پیاده‌سازی کرده و کارایی آن را با سایر شبکه‌های یادگیری عمیق، نظیر ResNet 50 و GoogLeNet، مقایسه کردند. نتایج به دست آمده نشان از دقت ۹۱.۱۴ درصد برای مجموعه داده NSL-KDD و ۹۴.۹ درصد برای مجموعه داده UNSW-NB15 داشت. همچنین، نویسندگان یک سیستم تشخیص نفوذ (IDS)مبتنی بر شبکه عصبی مصنوعی (ANN)را پیشنهاد کردند که از یک رویکرد انتخاب ویژگی بهینه برای افزایش کارایی استفاده می‌کند. این روش بر روی مجموعه‌های داده UNSW-NB15 و NSL-KDD ارزیابی شده و دقت ۹۵.۴۵ درصد را نشان داد که با نتایج روش‌های مدرن موجود مقایسه می‌شود(Muneer et al, 2024).

نویسندگان به طور مؤثر یک مدل شناسایی ترکیبی را معرفی کرده‌اند که شامل ادغام شبکه‌های باور عمیق (DBN)و ماشین‌های بردار حمایت (SVM)است. این ترکیب به لحاظ ظرفیت یادگیری و دقت شناسایی، بهبود چشمگیری را در پردازش داده‌ها و تحلیل الگوها ارائه می‌دهد و می‌تواند به عنوان رویکردی نوآورانه در زمینه‌های مختلف کاربردی محسوب شود (Guha et al, 2016) (Moustafa et al, 2021).

نویسندگان(Tama and Rhee, 2019) یک سیستم تشخیص نفوذ (IDS)مبتنی بر ناهنجاری جدید ارائه کرده‌اند که در آن از ماشین‌های تقویت‌شده گرادیان(GBM) به عنوان موتور تشخیص اولیه بهره‌برداری می‌شود. این رویکرد نوآورانه می‌تواند به شناسایی تهدیدات امنیتی با دقت بالا و کاهش نرخ مثبت کاذب کمک کند، و بهبودهای قابل توجهی در عملکرد سیستم‌های امنیتی به ارمغان آورد. نویسندگان با بهره‌گیری از رویکرد جستجوی شبکه‌ای به بهینه‌سازی پارامترهای مدل GBM پرداخته و عملکرد سیستم تشخیص نفوذ (IDS)خود را بر اساس روش‌های اعتبارسنجی نگهدارنده و متقاطع در سه مجموعه داده جداگانه، شامل UNSW-NB15، NSL-KDD و GPRS، ارزیابی کردند. نتایج تجربی نشان‌دهنده عملکرد superior این IDS در مقایسه با چندین طبقه‌بندی‌کننده دیگر مانند طبقه‌بندی‌کننده فازی، جنگل GAR و مجموعه‌های مبتنی بر درخت در معیارهای مختلفی نظیر دقت، ویژگی، حساسیت و مساحت زیر منحنی (AUC)هستند. هرچند این مطالعه، عملکرد برتر GBM در شناسایی ناهنجاری‌ها را تأیید می‌کند، ولی به بررسی توانمندی مدل در انطباق با استراتژی‌های حمله در حال ظهور یا تکاملی نپرداخته است. لذا، تأیید یافته‌های این مطالعه نیازمند آزمایش‌های بیشتر در دنیای واقعی و استفاده از مجموعه‌های داده متنوع به منظور سنجش استحکام مدل خواهد بود(Muneer et al, 2024).

در مطالعه‌ای که توسط نویسندگان (Primartha and Tama, 2017) انجام شده است، عملکرد یک سیستم تشخیص نفوذ (IDS)مبتنی بر جنگل تصادفی (RF)از نظر دقت و نرخ هشدار نادرست مورد بررسی قرار گرفت. برای آموزش و آزمایش مدل، از مجموعه داده‌های NSL KDD، UNSW-NB15 و GPRS استفاده شده است. نتایج حاکی از آن است که گروهی متشکل از ۸۰۰ درخت بهترین عملکرد را ارائه داده و گروهی از ۲۰ درخت، بدترین نتیجه را داشته است. همچنین، عملکرد IDS مبتنی بر RF در مقایسه با دیگر طبقه‌بندی‌کننده‌ها، نظیر Random Tree و Naive Bayes، به‌طور قابل توجهی بهتر بوده است. با این حال، این مطالعه به روند بررسی سازگاری مدل با الگوهای حمله جدید و میزان استحکام آن در برابر حملات متخاصم نپرداخته است، و تمرکز آن بیشتر بر ارزیابی بر روی مجموعه داده‌های موجود و عدم بررسی کاربردهای عملی در محیط‌های شبکه پویاست(Muneer et al, 2024).

در این اثر، رویت و همکاران(Roy et al, 2019) یک چارچوب جدید یادگیری فدرال به نام BrainTorrent را معرفی کرده‌اند که به‌طور خاص برای محیط‌های همتا به همتا (P2P)طراحی شده است. از سوی دیگر، نویسندگان تحقیق دیگری با نام BAFFLE، چارچوب متفاوتی مبتنی بر BC را پیشنهاد می‌کنند که نیازی به جمع‌کننده ندارد و کارایی محاسباتی بالایی را در یک شبکه خصوصی Ethereum به نمایش می‌گذارد. هرچند این مطالعه BrainTorrent را به عنوان یک راهکار مناسب برای کاربردهای پزشکی معرفی می‌کند، اما به‌طور کامل چالش‌های مربوط به هماهنگی شبکه، امنیت و مقیاس‌پذیری در محیط‌های غیرمتمرکز و همتا به همتا را بررسی نمی‌کند. همچنین، نگرانی‌های مرتبط با حریم خصوصی و حفاظت از داده‌ها در زمینه پزشکی چند مرکزی همچنین از نظر پیچیدگی‌های دنیای واقعی به‌طور جامع مورد توجه قرار نگرفته است(Muneer et al, 2024).

این تحقیق (Alazab et al, 2021)، یک مرور جامع از کاربرد یادگیری فدرال (FL)در امنیت اطلاعات ارائه می‌دهد و به‌طور خاص بر روی شناسایی (ID)تأکید می‌کند. نویسندگان با ارائه بینش‌های شفاف، دامنه وسیع‌تری از ID را تحلیل می‌کنند. علاوه بر این، تمرکز بر روی سیستم‌های تشخیص نفوذ فدرال (FIDS)نیز وجود دارد، هرچند که روش‌شناسی آن‌ها از نویسندگان اصلی متفاوت است. این مطالعه پتانسیل FL را در بهبود امنیت سایبری به نمایش می‌گذارد، اما به بررسی عمیق چالش‌ها و پیچیدگی‌های پیاده‌سازی FL در محیط‌های پویا و زمان واقعی نمی‌پردازد و موانع عملی، مسایل هماهنگی شبکه و نیاز به اقدامات امنیتی قوی را نادیده می‌گیرد(Muneer et al, 2024).

این مقاله همچنین به جنبه‌های قانونی و اخلاقی مرتبط با استفاده از یادگیری فدرال (FL)در مدیریت داده‌های حساس در سیستم‌های بلادرنگ نمی‌پردازد. نویسندگان (Agrawal et al, 2021) به جمع‌آوری فهرستی از سیستم‌های شناسایی نفوذ فدرال (FIDS)موجود پرداخته و یک نمای کلی از روش‌های آنها ارائه می‌دهند، در حالی که مسائل حل نشده در این حوزه را نیز شناسایی می‌کنند. این مطالعه قادر به شناسایی بسته‌های رمزگذاری شده نیست، که این موضوع امکان انجام حملات را فراهم می‌آورد. به علاوه، توسعه یک مدل استاندارد برای داده‌های دینامیک و عظیم چالش‌های زیادی به همراه دارد و ممکن است به بروز هشدارهای نادرست منجر شود(Muneer et al, 2024).

۲. رویکردهای هوش مصنوعی مبتنی بر جعبه سیاه و جعبه سفید در سیستم‌های تشخیص نفوذ

در حوزه سیستم‌های تشخیص نفوذ (IDS)، دو رویکرد متضاد هوش مصنوعی، جعبه سیاه و جعبه سفید، به طور قابل توجهی توسعه یافته‌اند. روش‌های جعبه سیاه شامل IDS مبتنی بر یادگیری ماشین (ML)و یادگیری عمیق (DL)هستند که از الگوریتم‌ها و شبکه‌های عصبی برای شناسایی خودکار الگوها و ناهنجاری‌ها در داده‌ها استفاده می‌کنند. این روش‌ها به ویژه در شناسایی حملات پیچیده و جدید مؤثرند، اما به دلیل فقدان شفافیت در تصمیم‌گیری و آسیب‌پذیری در برابر حملات متخاصم، محدودیت‌هایی دارند. در مقابل، رویکردهای جعبه سفید مانند IDS مبتنی بر قانون و مهندسی ویژگی، بیشتر بر تفسیرپذیری و مشارکت دانش کارشناسان تأکید دارند و قابلیت درک بیشتری از فرایندهای خود را ارائه می‌دهند. سیستم‌های تشخیص نفوذ (IDS)مبتنی بر قانون، با تکیه بر الگوهای از پیش تعیین شده، شناسایی حملات شناخته شده را تسهیل می‌کنند، هرچند ممکن است در شناسایی تهدیدات جدید ناکام باشند. IDS مبتنی بر مهندسی ویژگی، با فراهم کردن امکان طراحی ویژگی‌ها بر مبنای دانش کارشناسان، قابلیت تفسیرپذیری را برای شناسایی انواع حملات بهبود می‌بخشد، اما نیاز به سرمایه‌گذاری در تخصص دامنه و خطر پوشش ناقص الگوها وجود دارد. در مقابل، IDS مبتنی بر یادگیری فدرال (FL)به عنوان یک رویکرد نوین، تضمینی برای حریم خصوصی به واسطه آموزش مدل‌ها بر روی دستگاه‌های مجزا ارائه می‌دهد. این تکنیک به طور همزمان به دغدغه‌های حریم خصوصی و همکاری می‌پردازد، اما چالش‌هایی مانند هزینه‌های ارتباطی و از دست رفتن اطلاعات دقیق را به دنبال دارد. در نهایت، درک مفاهیم جعبه سیاه و جعبه سفید برای انتخاب‌های هوشمندانه در توسعه و بهبود IDS ضروری است(Muneer et al, 2024). سیستم‌های تشخیص نفوذ (IDS)مبتنی بر رویکردهای یادگیری ماشین(ML)، یادگیری عمیق (DL)و یادگیری فدرال (FL)نتایج امیدوارکننده‌ای در شناسایی و کاهش تهدیدات امنیتی به نمایش گذاشته‌اند. یادگیری ماشین، به عنوان زیرشاخه‌ای از هوش مصنوعی(Yamin Siddiqui et al, 2022) (Khan et al, 2021)، به طور فزاینده‌ای در

امنیت شبکه برای نظارت بر ترافیک و شناسایی فعالیت‌های غیرمجاز یا مخرب مورد استفاده قرار می‌گیرد. در حالی که IDSهای سنتی عمدتاً بر اساس قوانین و امضاهای از پیش تعریف شده عمل می‌کنند، الگوریتم‌های ML قادر به شناسایی ناهنجاری‌ها و انحرافات از الگوهای رفتاری عادی هستند که ممکن است نشان‌دهنده نفوذ باشد. این رویکردها امکان تشخیص حملات ناشناخته را به وجود می‌آورند و به تقویت امنیت شبکه کمک می‌کنند. برخی از رویکردهای ML در جدول ۱ نشان داده شده است. در جدول ۱ نشان داده شده است یادگیری ماشین (ML)به‌عنوان یک تکنیک مؤثر در شناسایی (ID)به‌تدریج مورد توجه قرار گرفته و الگوریتم‌های متنوعی در این حوزه توسعه یافته‌اند. از بین این الگوریتم‌ها، K-Nearest Neighbor (KNN) و ماشین‌های بردار پشتیبان (SVM)به‌عنوان راهکارهای پرکاربرد شناخته شده‌اند. همچنین شبکه‌های عصبی مصنوعی (ANN)قادر به یادگیری الگوها و پیش‌بینی بر اساس داده‌های ورودی هستند، در حالی که SVM به‌خوبی داده‌ها را به کلاس‌های مختلف تفکیک می‌کند. درختان تصمیم (DT)و جنگل‌های تصادفی (RF)به دلیل قابلیت مدیریت داده‌های طبقه‌بندی شده و پیوسته، از محبوبیت بالایی برخوردارند. به‌علاوه، روش‌های یادگیری عمیق (DL)مانند شبکه‌های عصبی کانولوشن (CNN)و شبکه‌های عصبی بازگشتی (RNN)نتایج قابل توجهی در ID ارائه کرده‌اند. با این حال، انتخاب مناسب‌ترین الگوریتم ML بستگی به عوامل متعددی از جمله نوع داده‌ها، مشکل خاص و منابع آموزشی دارد. رویکردهای مبتنی بر یادگیری عمیق، نظیر شبکه‌های عصبی کانولوشنی (CNN)و شبکه‌های عصبی بازگشتی (RNN)، به طور قابل توجهی در شناسایی تروسیون‌ها از طریق استخراج الگوهای یادگیری از داده‌های خام ترافیک شبکه پیشرفت کرده‌اند. به‌علاوه، روش‌های یادگیری ماشین مانند ماشین‌های بردار پشتیبان (SVM)و درختان تصمیم (DT)به طبقه‌بندی مؤثر این داده‌ها کمک می‌کنند و قابلیت شناسایی نفوذها بر اساس الگوهای آموخته شده را فراهم می‌آورند. همچنین، یادگیری فدرال (FL)امکان همکاری میان چندین طرف را برای آموزش مدل‌های جهانی بدون تبادل داده‌های خصوصی میسر می‌سازد؛ امکانی که آن را برای محیط‌های حساس ایده‌آل می‌کند. انتخاب بهترین رویکرد بستگی به عواملی نظیر اندازه و پیچیدگی مجموعه داده، نیاز به امنیت و حریم خصوصی، و منابع محاسباتی در دسترس دارد. به‌طور کلی، این رویکردها به‌طور مؤثر تهدیدات امنیتی را در شبکه‌های پیچیده و پویا شناسایی و کاهش می‌دهند. جدول ۲ نمای کلی از انواع مختلف سیستم‌های تشخیص نفوذ (IDS)مبتنی بر یادگیری عمیق (DL)در حوزه امنیت سایبری ارائه می‌دهد. این روش‌ها شامل شبکه‌های عصبی عمیق، شبکه‌های عصبی پیش‌خور، شبکه‌های عصبی بازگشتی، و مدل‌های دیگر مانند LSTM و خود-آموزش هستند. هر یک از این تکنیک‌ها با ویژگی‌های خاص خود طراحی شده‌اند تا به نیازهای متنوع کاربردها در امنیت سایبری پاسخ دهند. به‌ویژه، RNN به دلیل توانایی‌اش در پردازش داده‌های متوالی، برای تشخیص نفوذ بسیار مناسب است. انتخاب بهترین روش IDS به نیازهای خاص هر محیط وابسته است(Muneer et al, 2024).

شبکه‌های عصبی بازگشتی (RNN)قابلیت تجزیه و تحلیل ترافیک شبکه را در زمان واقعی دارند و می‌توانند ناهنجاری‌ها و تهدیدات بالقوه را شناسایی کنند. این کار با بهره‌گیری از حافظه ورودی‌های گذشته و ایجاد حلقه‌های بازخوردی در خروجی شبکه صورت می‌گیرد. به این ترتیب، RNN ها با تحلیل داده‌های تاریخی قادر به شناسایی الگوهای غیرمعمول در ترافیک شبکه می‌شوند و به تقویت امنیت سایبری کمک می‌کنند (Ali et al, 2021) (Said et al, 2022) (Houda et al, 2022) (Akshay Kumaar et al, 2022) (Nasir et al, 2022) (Otoum et al, 2022) (Muhammad and Saleem, 2022) (Logeswari et al, 2023) (Ren et al, 2019) (Liu and Lang, 2019).

شبکه‌های عصبی می‌توانند با استفاده از ورودی‌های قبلی، مانند الگوهای ترافیک گذشته، در شناسایی رفتار غیرعادی در ترافیک فعلی کمک کنند. به‌طور خاص، شبکه‌های عصبی بازگشتی (RNN)به‌عنوان ابزارهای قدرتمند در شناسایی ناهنجاری‌ها در زمان واقعی شناخته می‌شوند، زیرا قادر به یادگیری وابستگی‌های پیچیده در داده‌های متوالی هستند. همچنین، شبکه‌های عصبی عمیق (DNN)که شامل چندین لایه برای یادگیری ویژگی‌ها از داده‌های ورودی می‌باشند، می‌توانند در تحلیل ترافیک شبکه و شناسایی ناهنجاری‌ها و تهدیدات ممکن مؤثر باشند. به علاوه، شبکه‌های عصبی پیشخوران (FDDNN)به‌عنوان شکلی خاص از DNN، می‌توانند برای یادگیری ویژگی‌های پیچیده در داده‌ها در فرآیند شناسایی ناهنجاری‌ها به کار گرفته شوند. شبکه‌های عصبی کانولوشن (CNN)به عنوان یک معماری یادگیری عمیق، به طور خاص برای پردازش داده‌های ساختار یافته شبکه، نظیر تصاویر، طراحی شده‌اند. این شبکه‌ها قابلیت استخراج ویژگی‌های معنادار از داده‌های ترافیک شبکه را دارند، که می‌تواند به شناسایی الگوهای مرتبط با انواع خاصی از نفوذ کمک

کند. از سوی دیگر، شبکه‌های عصبی مصنوعی (ANN)به الهام از عملکرد مغز انسان و محدوده‌های گسترده‌تری از کاربردهای یادگیری ماشین، قادر به شناسایی الگوهای پیچیده در داده‌های ترافیک شبکه هستند. این قابلیت‌ها به آن‌ها اجازه می‌دهد تا ناهنجاری‌هایی را که ممکن است نشان‌دهنده نفوذ احتمالی باشند، شناسایی کنند. شبکه‌های عصبی کانولوشنال بیزی (BCNN)نوعی از CNN هستند که قابلیت‌های بیزی را با هدف مدیریت عدم قطعیت در پیش‌بینی‌های مدل ترکیب می‌کنند. در شناسایی نفوذ (ID)، BCNN ها با مدلسازی عدم قطعیت مرتبط با پرسش‌های شناسایی، می‌توانند پیش‌بینی‌های قابل اعتمادتری ارائه دهند. از سوی دیگر، شبکه باور عمیق (DBN)به عنوان یک معماری یادگیری عمیق، با استفاده از روش‌های پیش نظارت نشده، ناهنجاری‌ها را در داده‌های ترافیک شبکه شناسایی می‌کند. همچنین، Autoencoder به یادگیری یک تصویر فشرده از شبکه می‌پردازد تا ناهنجاری‌ها و نفوذهای احتمالی را در ID شناسایی کند. این دو روش، به‌ویژه DBN و Autoencoder، ابزارهای مؤثری برای شناسایی رفتارهای غیرعادی در داده‌های ترافیکی محسوب می‌شوند. در تشخیص نفوذ(ID) ، الگوریتم‌های هوش مصنوعی (AE)می‌توانند با تحلیل ویژگی‌های داده‌های ترافیک شبکه، رفتار عادی را شناسایی کرده و به این ترتیب ناهنجاری‌ها و نفوذهای احتمالی را شناسایی کنند. نوعی از شبکه‌های عصبی بازگشتی (RNN)به نام LSTM از مکانیسم‌های گیتینگ بهره می‌برد تا اطلاعات را به‌صورت انتخابی ذخیره یا فراموش کند. این شبکه‌ها قادرند برای تجزیه و تحلیل بلادرنگ داده‌های ترافیک شبکه، با در نظر گرفتن الگوهای کوتاه‌مدت و بلندمدت، از LSTM استفاده کنند. یادگیری خودآموخته که نوعی یادگیری بدون نظارت است، بدون نیاز به داده‌های برچسب‌دار ویژگی‌ها را از داده‌ها استخراج کرده و امکان شناسایی ناهنجاری‌ها را فراهم می‌آورد. همچنین، HAST-ID به‌عنوان یک شناسه یادگیری عمیق، از ویژگی‌های زمانی مکانی سلسله مراتبی برای شناسایی نفوذ در شبکه استفاده می‌کند و از شبکه‌های کانولوشنی (CNN)برای استخراج ویژگی‌ها و از LSTM برای مدل‌سازی وابستگی‌های زمانی بهره می‌برد(Muneer et al, 2024).

از سوی دیگر، یک AutoEncoder عمیق غیر متقارن (NDAE)به‌منظور یادگیری اعمال عادی یک سیستم و شناسایی انحرافات به‌عنوان تداخل بالقوه، از یک رمزگذار خودکار عمیق غیر متقارن بهره می‌برد. پلتفرم Deep Learning H2O برای ساخت، آموزش و استقرار مدل‌های یادگیری عمیق در سیستم‌های تشخیص نفوذ (IDS)طراحی شده و از مدل‌های دوجمله‌ای و چندجمله‌ای برای طبقه‌بندی ترافیک شبکه به‌عنوان عادی یا نفوذی پشتیبانی می‌کند. همچنین، TSDL از یک رویکرد یادگیری دو مرحله‌ای در IDS مبتنی بر یادگیری عمیق خود استفاده می‌کند (Yin et al, 2017) (Jasim and Ammar, 2022) (Chowdhury et al, 2017). (Albulayhi et al, 2022) (Raghuvanshi et al, 2022)

استفاده از ترکیبی از شبکه‌های عصبی عمیق (DNN)و شبکه‌های عصبی بازگشتی (RNN)در مدل BAT برای شناسایی هویت، به‌عنوان یک رویکرد رایج در حوزه امنیت محسوب می‌شود. DNN به استخراج ویژگی‌ها کمک کرده و باعث کاهش ابعاد و انتزاع داده‌های خام به شکل قابل مدیریت می‌گردد. به ویژه، استفاده از RNN، به‌ویژه مدل BLSTM، به ثبت روابط و وابستگی‌های زمانی در داده‌ها کمک می‌کند که برای شناسایی دقیق ناهنجاری‌ها و نفوذها حیاتی است. علاوه بر این، مکانیسم توجه در مدل BAT این امکان را فراهم می‌کند که شبکه بر روی بخش‌های مرتبط‌تر داده تمرکز کند و در نتیجه پیش‌بینی‌هایی دقیق‌تر ارائه دهد(Muneer et al, 2024).

به طور کلی، استفاده از رویکردهای یادگیری عمیق (DL)در فرآیندهای شناسایی (ID)، نتایج امیدوارکننده‌ای را به همراه داشته و به عنوان یک حوزه فعال تحقیقاتی شناخته می‌شود. این رویکردها به ارائه راهکارهای نوآورانه و بهبود دقت در شناسایی الگوها کمک کرده و به تقویت پایه‌های علمی در این حوزه می‌انجامد(Otoum et al, 2022) (Ren et al, 2019) (Singh et al, 2022)

ID معمولاً برای تجزیه و تحلیل داده‌های سری زمانی، نظیر گزارش‌های ترافیک شبکه، مورد استفاده قرار می‌گیرد. D DCNN[1] نوعی شبکه عصبی کانولوشنی است که به ویژه برای پردازش توالی‌های داده طراحی شده است. این ساختار علّی متسع به شبکه این امکان را می‌دهد تا توالی‌های طولانی‌تری را پردازش کند و همچنین رابطه علی میان نقاط داده را حفظ نماید. ImmuneNet به عنوان یک چارچوب ترکیبی برای ID، تکنیک‌های یادگیری عمیق و الگوریتم‌های الهام گرفته از سیستم ایمنی را با یکدیگر ادغام می‌کند(Logeswari et al, 2023)

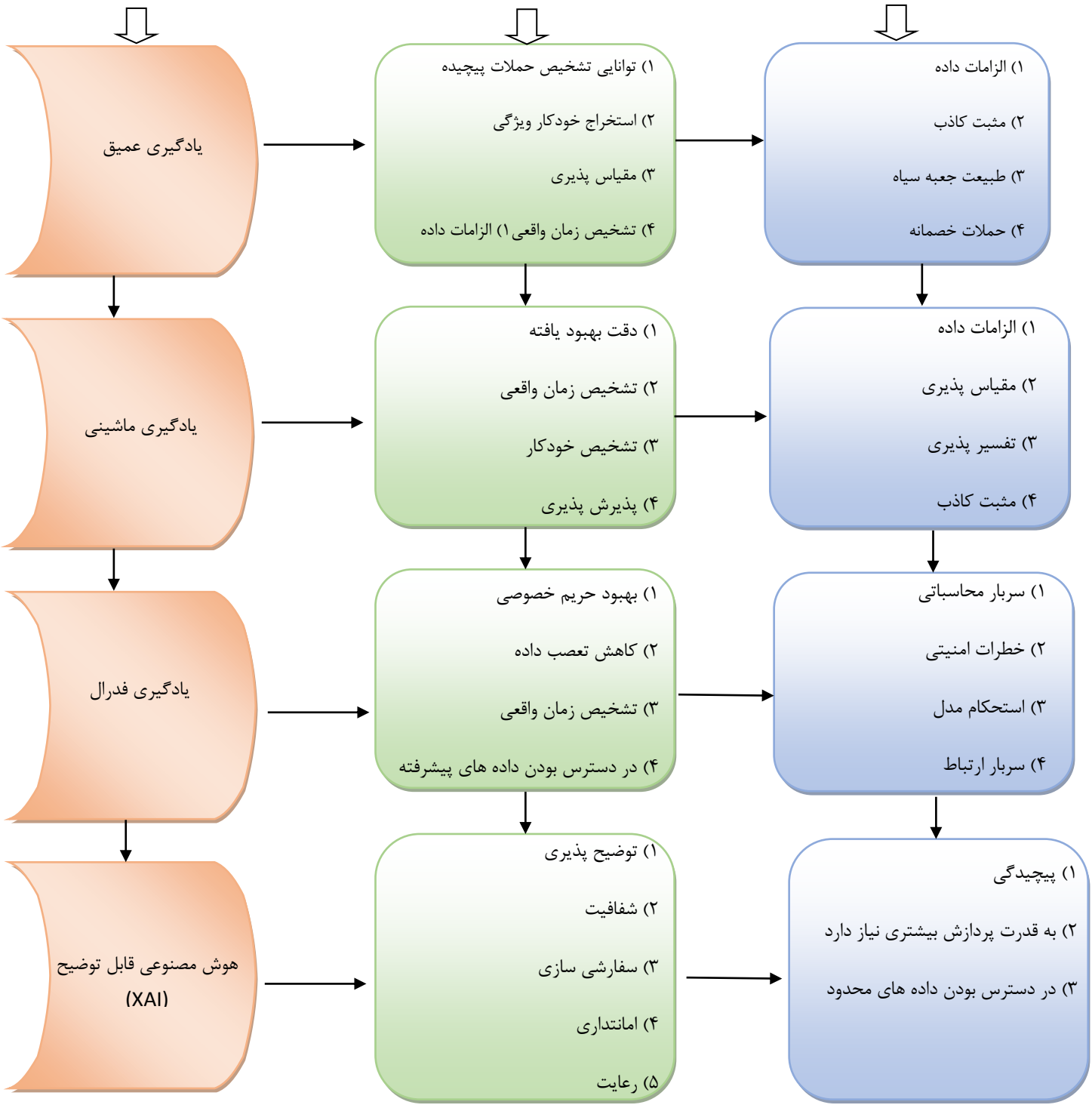
یک شبکه عصبی عمیق (DNN)به منظور استخراج ویژگی‌ها از داده‌های ترافیک شبکه به کار گرفته می‌شود، و به دنبال آن یک الگوریتم الهام گرفته از سیستم ایمنی برای تشخیص نفوذ بر اساس این ویژگی‌ها توسعه یافته است. هوش مصنوعی تبیین‌پذیر (XAI)در این زمینه بر طراحی الگوریتم‌هایی متمرکز است که توانایی ارائه توضیحات واضح و شفاف در مورد دلایل دسته‌بندی داده‌های ترافیکی به عنوان عادی یا نفوذ را دارند. این رویکرد مبتنی بر یادگیری عمیق، علاوه بر دقت در شناسایی تهدیدات، به تحلیلگران امنیتی امکان می‌دهد تا درک بهتری از فرآیند تصمیم‌گیری الگوریتم داشته باشند. جدول ۲ یک ارزیابی جامع از روش‌های مختلف یادگیری عمیق (DL)برای شناسایی تهدیدات (ID)ارائه می‌دهد و دقت هر یک از این رویکردها را مورد بررسی قرار می‌دهد. نتایج به‌دست‌آمده نشان می‌دهد که این روش‌ها قادر به پیش‌بینی تهدیدات امنیت سایبری به‌طور دقیق هستند و می‌توانند به بهبود فرایندهای دفاعی در مقابل حملات سایبری کمک کنند. تکنیک‌های یادگیری عمیق (DL) (Said et al, 2022)به علت قابلیت‌های ویژه خود در تحلیل روابط پیچیده و استخراج ویژگی‌های کلیدی از داده‌های خام، به طور گسترده‌ای در شناسایی نفوذ (ID)مورد استفاده قرار گرفته‌اند. مدل‌هایی همچون HAST-ID و رمزگذاری خودکار عمیق غیر متقارن (NDAE)به خوبی توانایی DL را در استخراج ویژگی‌های مکانی و زمانی و یادگیری تجسمی با ابعاد کوچک نشان می‌دهند. همچنین، چارچوب یادگیری عمیق H2O با تکیه بر مدل‌های دو جمله‌ای و چند جمله‌ای، رویکردی سریع و دقیق را در شناسایی نفوذ ارائه می‌دهد. به علاوه، شبکه‌های عصبی پیش‌خور (FFNN)و یادگیری عمیق دو مرحله‌ای (TSDL)از این ظرفیت به منظور پیش‌بینی نفوذ استفاده می‌کنند(Muneer et al, 2024).

حافظه کوتاه‌مدت دو جهته(BiDLSTM)، شبکه عصبی علت و معلولی ۱ بعدی (D-DCNN1)، چارچوب هیبریدی مبتنی بر یادگیری عمیق "ImmuneNet"و چارچوب یادگیری عمیق مبتنی بر هوش مصنوعی قابل توضیح (XAI)همگی به عنوان تکنیک‌های نوآورانه در تشخیص و شناسایی هویت (ID)نتایج امیدوارکننده‌ای را ارائه داده‌اند. این روش‌ها با تمرکز بر شبکه‌های حافظه کوتاه‌مدت دو طرفه و شبکه‌های عصبی علت و معلولی متسع، به همراه استفاده از دستگاه‌های مبتنی بر اینترنت اشیا(Raza et al, 2022) و دیگر چارچوب‌های مبتنی بر یادگیری ماشین(Naz et al, 2020) (Ali et al, 2021)، توانسته‌اند عملکرد بهتری را در این حوزه به نمایش بگذارند. در جدول ۳، FL به عنوان یک رویکرد نویدبخش برای شناسایی نفوذ (ID)معرفی شده است که به تعدادی از طرفین اجازه می‌دهد بدون نیاز به تبادل اطلاعات خصوصی خود، در آموزش یک مدل جهانی مشارکت کنند. این روش با محافظت از داده‌های حساس و کاهش ریسک نقض داده‌ها، مزایای قابل توجهی نسبت به روش‌های یادگیری ماشین متمرکز سنتی دارد. در حوزه ID، روش‌های مختلفی نظیر SVM فدرال (FedSVM)، ماشین یادگیری شدید فدرال (FedELM)، تشخیص ناهنجاری مبتنی بر گروه (FedEAD) و رمزگذار خودکار فدرال (FedAE)پیشنهاد شده‌اند. انتخاب بهینه‌ترین رویکرد FL برای ID به عواملی مانند تعداد ابزارهای مشارکت‌کننده، پیچیدگی داده‌ها، منابع ارتباطی و محاسباتی در دسترس، و سطح امنیت و حریم خصوصی مورد نیاز بستگی دارد. برای بهینه‌سازی عملکرد FL در سناریوهای واقعی، به تحقیقات بیشتری در این زمینه نیاز است. رویکردهای شامل یادگیری عمیق (DL)، یادگیری ماشین (ML)و یادگیری فدرال (FL)در سیستم‌های شناسایی نفوذ (IDS)عملکردهای برجسته‌ای را نشان داده‌اند، هرچند که هر یک نقاط قوت و ضعفی نیز دارند.IDS های مبتنی بر هوش مصنوعی قابل توضیح به وضوح مزایای قابل توجهی نسبت به روش‌های یادگیری عمیق و ماشین و همچنین IDS های فدرال ارائه می‌دهند. این سیستم‌ها شفافیت بالایی را از طریق توضیحات واضح از فرایند تصمیم‌گیری فراهم می‌کنند که فهم آن را تسهیل می‌کند. علاوه بر این، توانایی شناسایی سوگیری‌های موجود در سیستم، به بهبود انصاف و دقت کمک می‌کند. همچنین، این IDS ها به راحتی با شرایط مختلف سازگار شده و قابلیت تغییر قوانین تصمیم‌گیری را دارند. توانایی ارائه بینش‌های عمیق درباره تهدیدات و آسیب‌پذیری‌های امنیتی نیز از دیگر مزایای این سیستم‌ها است، که می‌تواند به پیشگیری از مسائل امنیتی کمک کند. در نهایت، سازمان‌ها با استفاده از IDS های هوش مصنوعی قابل توضیح می‌توانند الزامات قانونی را که نیازمند شفافیت در تصمیم‌گیری هستند، برآورده کنند و به این ترتیب، این نوع IDS در بسیاری از سناریوها گزینه‌ای مطلوب به شمار می‌آید(Muneer et al, 2024).

نقاط ضعف

نقاط قوت

رویکرد



شکل ۱: نقاط قوت و ضعف رویکرد DL، ML، FL و XAI (Muneer et al, 2024).

۳. نتیجه گیری

تشخیص نفوذ به عنوان یک ابزار کلیدی در امنیت اطلاعات در برابر حملات پیشرفته سایبری مطرح است. تکنولوژی‌های یادگیری عمیق و یادگیری ماشین هر کدام مزایا و چالش‌های خاص خود را دارند. در حالی که DL در شناسایی الگوهای پیچیده موثر است، به منابع زیادی نیاز دارد. از طرفی، ML در شناسایی حملات شناخته شده کارایی خوبی دارد، اما در برابر حملات ناشناخته دچار محدودیت است. همچنین، یادگیری فدرال می‌تواند گزینه‌ای مناسب برای سازمان‌ها با نگرانی‌های حریم خصوصی باشد. ارزیابی دقیق نیازها و منابع برای انتخاب بهترین تکنیک IDS امری ضروری است.

۴. جهت گیری های تحقیقاتی آینده و توصیه ها

با افزایش حملات پیشرفته سایبری، تشخیص نفوذ به عنوان یک عامل حیاتی در امنیت اطلاعات سازمان‌ها مطرح شده است. فناوری‌های نوین مانند یادگیری عمیق (DL)، یادگیری ماشین (ML)و یادگیری فدرال (FL)در این زمینه نقشی کلیدی ایفا می‌کنند. رویکردهای مبتنی بر DL با یادگیری الگوهای پیچیده داده‌های ترافیک شبکه، دقت بالایی در شناسایی حملات شناخته شده و ناشناخته ارائه می‌دهند، اما نیاز به منابع محاسباتی و داده‌های قابل توجهی دارند که ممکن است برای برخی سازمان‌ها چالش‌برانگیز باشد. از سوی دیگر، رویکردهای ML ساده‌تر و کم‌مصرف‌تر از DL هستند و در شناسایی حملات شناخته شده موفق عمل می‌کنند، اما در تشخیص حملات ناشناخته محدودیت‌هایی دارند. تکنیک‌های مبتنی بر FL نیز راه‌حلی امیدوارکننده برای سازمان‌ها با نگرانی‌های حریم خصوصی هستند، زیرا امکان آموزش مدل‌ها بر روی داده‌های توزیع‌شده را بدون نیاز به اشتراک‌گذاری آن فراهم می‌آورند. بنابراین، سازمان‌ها باید با دقت نیازها و منابع خود را برای انتخاب مناسب‌ترین تکنیک IDS مورد ارزیابی قرار دهند(Muneer et al, 2024).

این تحلیل به خوبی پتانسیل‌های پژوهشی آینده در حوزه شناسایی دیجیتال را روشن می‌کند. ادغام بلاک‌چین و هوش مصنوعی تبیین‌پذیر به‌عنوان دو فناوری نوین، می‌تواند بهبود قابل توجهی در امنیت و شفافیت سیستم‌های شناسایی دیجیتال ایجاد کند. بررسی قابلیت‌های بلاک‌چین در حفاظت از داده‌ها و امنیت سیستم‌های یادگیری فدرال، به‌خصوص در زمینه تشخیص نفوذ، موضوعی بسیار حائز اهمیت است که می‌تواند به ارتقاء دفاع در برابر تهدیدات سایبری منجر شود.

منابع

R. Malik, H. Raza, and M. Saleem, “Towards A Blockchain enabled integrated library managment system using hyperledger fabric: using hyperledger fabric,” International Journal of Computational and Innovative Sciences, vol. 1, no. 3, pp. 17–24, 2022.

J. A. Malik and M. Saleem, “Blockchain and cyber-physical system for security engineering in the smart industry,” in Security Engineering for Embedded and Cyber-Physical Sys tems, pp. 51–70, CRC Press, Boca Raton, FL, USA, 2022.

P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, “Intrusion detection techniques in cloud environment: a survey,” Journal of Network and Computer Applications, vol. 77, pp. 18–47, 2017.

J. Wei, C. Long, J. Li, and J. Zhao, “An intrusion detection algorithm based on bag representation with ensemble sup port vector machine in cloud computing,” Concurrency and Computation: Practice and Experience, vol. 32, no. 24, p. 14, 2020.

K. Peng, V. C. M. Leung, L. Zheng, S. Wang, C. Huang, and T. Lin, “Intrusion detection system based on decision tree over big data in fog environment,” Wireless Communications and Mobile Computing, vol. 2018, Article ID 4680867, 10 pages, 2018.

Q. Schueller, K. Basu, M. Younas, M. Patel, and F. Ball, “A hierarchical intrusion detection system using support vector machine for sdn network in cloud data center,” in Pro ceedings of the 28th International Telecommunication Net works and Applications Conference (ITNAC), p. 6, Sydney, Australia, June 2018.

C. Modi, D. Patel, B. Borisanya, A. Patel, and M. Rajarajan, “A novel framework for intrusion detection in cloud,” in Proceedings of the Fifth International Conference on Security of Information and Networks, pp. 67–74, Jaipur, India, April 2012.

B. Sundararaman, S. Jagdev, and N. Khatri, “Transformative role of artifcial intelligence in advancing sustainable tomato (Solanum lycopersicum) disease management for global food security: a comprehensive review,” Sustainability, vol. 15, no. 15, Article ID 11681, 2023.

G. Dhanush, N. Khatri, S. Kumar, and P. K. Shukla, “A comprehensive review of machine vision systems and arti fcial intelligence algorithms for the detection and harvesting of agricultural produce,” Scientifc African, vol. 21, Article ID e01798, 2023.

P. Ghosh, A. K. Mandal, and R. Kumar, “An efcient cloud network intrusion detection system,” Information Systems Design and Intelligent Applications, Springer, New York, NY, USA, 2015.

P. Deshpande, S. C. Sharma, S. K. Peddoju, and S. Junaid, “HIDS: a host based intrusion detection system for cloud computing environment,” International Journal of System Assurance Engineering and Management, vol. 9, no. 3, pp. 567–576, 2018.

C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, “A survey of intrusion detection techniques in cloud,” Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42–57, 2013.

T. Mohamed, A. Ibrahim, T. Faiz et al., “Intelligent hand gesture recognition system empowered with CNN,” in Proceedings of the 2022 International Conference on Cyber Resilience (ICCR), IEEE, Dubai, United Arab Emirates, July 2022.

H. Liu and B. Lang, “Machine learning and deep learning methods for intrusion detection systems: a survey,” Applied Sciences, vol. 9, no. 20, p. 4396, 2019.

V. R. Pathmudi, N. Khatri, S. Kumar, A. S. Abdul-Qawy, and A. K. Vyas, “A systematic review of IoT technologies and their constituents for smart and sustainable agriculture applications,” Scientifc African, vol. 19, Article ID e01577, 2023.

M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, “Deep recurrent neural network for iot intrusion detection system,” Simulation Modelling Practice and Teory, vol. 101, Article ID 102031, 2020.

A. Dawoud, S. Shahristani, and C. Raun, “Deep learning and software-defned networks: towards secure iot architecture,” Internet of Tings, vol. 34, pp. 82–89, 2018.

R. Zhao, Y. Yin, Y. Shi, and Z. Xue, “Intelligent intrusion detection based on federated learning aided long short-term memory,” Physical Communication, vol. 42, Article ID 101157, 2020.

O. Alkadi, N. Moustafa, B. Turnbull, and K. K. R. Choo, “A deep Blockchain framework-enabled collaborative intrusion detection for protecting iot and cloud networks,” IEEE In ternet of Tings Journal, vol. 8, no. 12, pp. 9463–9472, 2021.

P. Ghosh, A. Karmakar, J. Sharma, and S. Phadikar, “Cs-pso based intrusion detection system in cloud environment,” in Emerging Technologies in Data Mining and Information Security, pp. 261–269, Springer, New York, NY, USA, 2019.

R. SaiSindhuTeja and G. K. Shyam, “An efcient meta heuristic algorithm based feature selection and recurrent neural network for dos attack detection in cloud computing environment,” Applied Soft Computing, vol. 100, Article ID 106997, 2021.

M. T. Nguyen and K. Kim, “Genetic convolutional neural network for intrusion detection systems,” Future Generation Computer Systems, vol. 113, pp. 418–427, 2020.

M. Gauthama Raman, N. Somu, K. Kirthivasan, R. Liscano, and V. Shankar Sriram, “An efcient intrusion detection system based on hypergraph-genetic algorithm for param eter optimization and feature selection in support vector machine,” Knowledge-Based Systems, vol. 134, pp. 1–12, 2017.

S. Malhotra, V. Bali, and K. Paliwal, “Genetic programming and k-nearest neighbour classifer based intrusion detection model,” in Proceedings of the 2017 7th International Con ference on Cloud Computing, Data Science & Engineering Confuence, pp. 42–46, IEEE, Noida, India, June 2017.

M. Mayuranathan, M. Murugan, and V. Dhanakoti, “Retracted article: best features based intrusion detection system by RBM model for detecting DDoS in cloud envi ronment,” Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 3, pp. 3609–3619, 2019.

J. Kumar Seth and S. Chandra, “Mids: metaheuristic based intrusion detection system for cloud using k-nn and mgwo,” in Proceedings of the International Conference on Advances in Computing and Data Sciences, pp. 411–420, Springer, Dehradun, India, June 2018.

S. P. Rm, P. K. Maddikunta, M. Parimala et al., “An efective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture,” Computer Com munications, vol. 160, pp. 139–149, 2020.

F. Ahmed, M. Asif, and M. Saleem, “Identifcation and prediction of brain tumor using VGG-16 empowered with explainable artifcial intelligence,” International Journal of Computational and Innovative Sciences, vol. 2, no. 2, pp. 24–33, 2023.

M. Saleem, M. S. Khan, G. F. Issa et al., “Smart spaces: occupancy detection using adaptive back-propagation neural network,” in Proceedings of the 2023 International Confer ence on Business Analytics for Technology and Security (ICBATS), pp. 1–6, Dubai, United Arab Emirates, June 2023.

A. Athar, R. N. Asif, M. Saleem, S. Munir, M. R. Al Nasar, and A. M. Momani, “Improving pneumonia detection in chest X-rays using transfer learning approach (AlexNet) and adversarial training,” in Proceedings of the 2023 International Conference on Business Analytics for Technology and Security (ICBATS), pp. 1–7, Dubai, United Arab Emirates, July 2023.

A. Abualkishik, M. Saleem, U. Farooq, M. Asif, M. Hassan, and J. A. Malik, “Genetic algorithm based adaptive FSO communication link,” in Proceedings of the 2023 In ternational Conference on Business Analytics for Technology and Security (ICBATS), pp. 1–4, Dubai, United Arab Emirates, June 2023.

G. Sajjad, M. B. Shoaib Khan, T. M. Ghazal, M. Saleem, M. F. Khan, and M. Wannous, “An early diagnosis of brain tumor using fused transfer learning,” in Proceedings of the 2023 International Conference on Business Analytics for Technology and Security (ICBATS), pp. 1–5, Dubai, United Arab Emirates, June 2023. [33] H. A. Ahmed, A. Hameed, and N. Z. Bawany, “Network intrusion detection using oversampling technique and machine learning algorithms,” Peer Journal Computer Sci ence, vol. 8, p. e820, 2022.

A. Singh, J. Amutha, J. Nagar, S. Sharma, and C. C. Lee, “Lt fs-id: log-transformed feature learning and feature-scaling based machine learning algorithms to predict the k-barriers for intrusion detection using wireless sensor network,” Sensors, vol. 22, no. 3, p. 1070, 2022.

M. B. Pranto, M. H. Ratul, M. M. Rahman, I. J. Diya, and Z. B. Zahir, “Performance of machine learning techniques in anomaly detection with basic feature selection strategy a network intrusion detection system,” Journal of Ad vances in Information Technology, vol. 13, no. 1, 2022.

A. Raghuvanshi, U. K. Singh, G. S. Sajja et al., “Intrusion detection using machine learning for risk mitigation in IoT enabled smart irrigation in smart farming,” Journal of Food Quality, vol. 2022, Article ID 3955514, 8 pages, 2022.

K. Albulayhi, Q. Abu Al-Haija, S. A. Alsuhibany, A. A. Jillepalli, M. Ashrafuzzaman, and F. T. Sheldon, “IoT intrusion detection using machine learning with a novel high performing feature selection method,” Applied Sciences, vol. 12, no. 10, p. 5015, 2022.

M. Asif, S. Abbas, M. A. Khan, A. Fatima, M. A. Khan, and S. W. Lee, “MapReduce based intelligent model for intrusion detection using machine learning technique,” Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 10, pp. 9723–9731, 2022.

U Çavus¸o ¨ ˘glu, “A new hybrid approach for intrusion de tection using machine learning methods,” Applied In telligence, vol. 49, no. 7, pp. 2735–2761, 2019.

H. Alqahtani, I. H. Sarker, A. Kalim, S. M. Minhaz Hossain, S. Ikhlaq, and S. Hossain, “Cyber intrusion detection using machine learning classifcation techniques,” in Proceedings of the InComputing Science, Communication and Security: First International Conference, COMS2 2020.

H. Liu and B. Lang, “Machine learning and deep learning methods for intrusion detection systems: a survey,” Applied Sciences, vol. 9, no. 20, p. 4396, 2019.

J. Ren, J. Guo, W. Qian, H. Yuan, X. Hao, and H. Jingjing, “Building an efective intrusion detection system by using hybrid data optimization based on machine learning algo rithms,” Security and Communication Networks, vol. 2019, Article ID 7130868, 11 pages, 2019.

N. Bindra and M. Sood, “Detecting DDoS attacks using machine learning techniques and contemporary intrusion detection dataset,” Automatic Control and Computer Sci ences, vol. 53, no. 5, pp. 419–428, 2019. [44] K. Sai Kiran, R. K. Devisetty, N. P. Kalyan, K. Mukundini, and R. Karthi, “Building a intrusion detection system for IoT environment using machine learning techniques,” Procedia Computer Science, vol. 171, pp. 2372–2379, 2020.

T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. A. Khan, “Performance analysis of machine learning algorithms in intrusion detection system: a review,” Procedia Computer Science, vol. 171, pp. 1251–1260, 2020.

G. Logeswari, S. Bose, and T. Anitha, “An intrusion detection system for SDN using machine learning,” Intelligent Auto mation & Soft Computing, vol. 35, no. 1, pp. 867–880, 2023.

M. U. Muhammad and A. M. Saleem, “Intelligent intrusion detection system for Apache web server empowered with machine learning approaches,” International Journal of Computational and Innovative Sciences, vol. 1, no. 1, pp. 1–8, 2022.

C. Yin, Y. Zhu, J. Fei, and X. He, “A deep learning approach for intrusion detection using recurrent neural networks,” IEEE Access, vol. 5, pp. 21954–21961, 2017.

R. Vani, “Towards efcient intrusion detection using deep learning techniques: a review,” International Journal of In novative Research in Computer and Communication Engi neering, vol. 3297, p. 2007, 2017. [50] W. Wang, Y. Sheng, J. Wang et al., “HAST-IDS: learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection,” IEEE Access, vol. 6, pp. 1792–1806, 2018.

G. Loukas, T. Vuong, R. Heartfeld, G. Sakellari, Y. Yoon, and D. Gan, “Cloud-based cyber-physical intrusion detection for vehicles using deep learning,” IEEE Access, vol. 6, pp. 3491–3508, 2018.

N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, “A deep learning approach to network intrusion detection,” IEEE transactions on emerging topics in computational intelligence, vol. 2, no. 1, pp. 41–50, 2018.

B. Lee, S. Amaresh, C. Green, and D. Engels, “Comparative study of deep learning models for network intrusion de tection,” SMU Data Science Review, vol. 1, no. 1, p. 8, 2018.

M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, “Deep learning approach combining sparse autoencoder with SVM for network intrusion detection,” IEEE Access, vol. 6, pp. 52843–52856, 2018.

Y. Ding and Y. Zhai, “Intrusion detection system for NSL-KDD dataset using convolutional neural networks,” Proceedings of the 2018 2nd International Conference on Computer Science and Artifcial Intelligence, vol. 8, pp. 81–85, 2018.

S. Parampottupadam and A. N. Moldovann, “Cloud-based real-time network intrusion detection using deep learning,” in Proceedings of the 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), pp. 1–8, London, UK, May 2018.

Y. Xin, L. Kong, Z. Liu et al., “Machine learning and deep learning methods for cybersecurity,” IEEE Access, vol. 6, pp. 35365–35381, 2018.

O. Faker and E. Dogdu, “Intrusion detection using big data and deep learning techniques,” in Proceedings of the 2019 ACM Southeast Conference, pp. 86–93, New York, NY, USA, July 2019.

S. Laqtib, K. E. Yassini, and M. L. Hasnaoui, “A deep learning methods for intrusion detection systems based machine learning in manet,” Proceedings of the 4th International Conference on Smart City Applications, vol. 2, pp. 1–8, 2019.

M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, “Deep learning-based intrusion detection for IoT networks,” in Proceedings of the 2019 IEEE 24th Pacifc Rim In ternational Symposium on Dependable Computing (PRDC), pp. 256–25609, Kyoto, Japan, June 2019.

F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, “TSDL: a two-stage deep learning model for efcient network in trusion detection,” IEEE Access, vol. 7, pp. 30373–30385, 2019.

S. Gurung, M. Kanti Ghose, and A. Subedi, “Deep learning approach on network intrusion detection system using NSL-KDD dataset,” International Journal of Computer Network and Information Security, vol. 11, no. 3, pp. 8–14, 2019.

T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, “BAT: deep learning methods on network intrusion detection using NSL-KDD dataset,” IEEE Access, vol. 8, no. 8, pp. 29575–29585, 2020.

S. Gamage and J. Samarabandu, “Deep learning methods in network intrusion detection: a survey and an objective comparison,” Journal of Network and Computer Applica tions, vol. 169, Article ID 102767, 2020.

A. Boukhalfa, A. Abdellaoui, N. Hmina, and H. Chaoui, “LSTM deep learning method for network intrusion de tection system,” International Journal of Electrical and Computer Engineering, vol. 10, no. 3, p. 3315, 2020.

S. Shende and S. Torat, “Long short-term memory (LSTM) deep learning method for intrusion detection in network security,” International Journal of Engineering Research, vol. 9, no. 06, 2020.

G. Kocher and G. Kumar, “Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges,” Soft Computing, vol. 25, no. 15, pp. 9731–9763, 2021.

S. N. Mighan and M. Kahani, “A novel scalable intrusion detection system based on deep learning,” International Journal of Information Security, vol. 20, no. 3, pp. 387–403, 2021.

L. Ashiku and C. Dagli, “Network intrusion detection system using deep learning,” Procedia Computer Science, vol. 185, pp. 239–247, 2021.

A. A. Salih, S. Y. Ameen, S. R. Zeebaree et al., “Deep learning approaches for intrusion detection,” Asian Journal of Re search in Computer Science, pp. 50–64, 2021.

Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, “A bi directional LSTM deep learning approach for intrusion detection,” Expert Systems with Applications, vol. 185, Article ID 115524, 2021.

Y. Otoum, D. Liu, and A. Nayak, “DL-IDS: a deep lear ning–based intrusion detection framework for securing IoT,” Transactions on Emerging Telecommunications Tech nologies, vol. 33, no. 3, 2022.

M. Nasir, A. R. Javed, M. A. Tariq, M. Asim, and T. Baker, “Feature engineering and deep learning-based intrusion detection framework for securing edge IoT,” Te Journal of Supercomputing, vol. 78, no. 6, pp. 8852–8866, 2022.

A. D. Jasim and Ammar D.Jasim, “A survey of intrusion detection using deep learning in internet of things,” Iraqi Journal For Computer Science and Mathematics, vol. 3, no. 1, pp. 83–93, 2022.

M. Akshay Kumaar, D. Samiayya, P. M. Vincent, K. Srinivasan, C. Y. Chang, and H. Ganesh, “A hybrid framework for intrusion detection in healthcare systems using deep learning,” Frontiers in Public Health, vol. 9, p. 2295, 2022.

Z. A. E. Houda, B. Brik, and L. Khoukhi, “Why should i trust your ids? An explainable deep learning framework for in trusion detection systems in Internet of Tings networks,” IEEE Open Journal of the Communications Society, vol. 3, pp. 1164–1176, 2022.

R. Chaganti, W. Suliman, V. Ravi, and A. Dua, “Deep learning approach for SDN-enabled intrusion detection system in IoT networks,” Information, vol. 14, no. 1, p. 41, 2023.

J. Figueiredo, C. Serrão, and A. M. de Almeida, “Deep learning model transposition for network intrusion de tection systems,” Electronics, vol. 12, no. 2, p. 293, 2023.

S. Rizvi, M. Scanlon, J. McGibney, and J. Sheppard, Deep Learning Based Network Intrusion Detection System for Re source-Constrained Environments, Springer, Berlin, Ger many, 2023.

Y. Supriya and T. R. Gadekallu, “Particle swarm-based federated learning approach for early detection of forest fres,” Sustainability, vol. 15, no. 2, p. 964, 2023.

X. Mu, Y. Shen, K. Cheng et al., “Fedproc: prototypical contrastive federated learning on non-iid data,” Future Generation Computer Systems, vol. 143, pp. 93–104, 2023.

G. Yu, X. Wang, C. Sun et al., “IronForge: an open, secure, fair, decentralized federated learning,” IEEE Transactions on Neural Networks and Learning Systems, vol. 52, 2023.

T. D. Nguyen, P. Rieger, M. Miettinen, and A. R. Sadeghi, “Poisoning attacks on federated learning-based IoTintrusion detection system,” Proceedings 2020 Workshop on Decen tralized IoT Systems and Security, vol. 23, pp. 1–7, 2020.

H. Liu, S. Zhang, P. Zhang et al., “Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing,” IEEE Transactions on Vehicular Technol ogy, vol. 70, no. 6, pp. 6073–6084, 2021.

Z. Chen, N. Lv, P. Liu, Y. Fang, K. Chen, and W. Pan, “Intrusion detection for wireless edge networks based on federated learning,” IEEE Access, vol. 8, pp. 217463–217472, 2020.

S. A. Rahman, H. Tout, C. Talhi, and A. Mourad, “Internet of things intrusion detection: centralized, on-device, or fed erated learning?” IEEE Network, vol. 34, no. 6, pp. 310–317, 2020.

V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, “Federated-learning based anomaly detection for iot security attacks,” IEEE In ternet of Tings Journal, vol. 9, no. 4, pp. 2545–2554, 2022.

Y. Zhao, J. Chen, D. Wu, J. Teng, and S. Yu, “Multi-task network anomaly detection using federated learning,” Pro ceedings of the Tenth International Symposium on In formation and Communication Technology- SoICT 2019, vol. 4, pp. 273–279, 2019.

V. Rey, P. M. S´anchez S´anchez, A. Huertas Celdr´an, and G. Bovet, “Federated learning for malware detection in iot devices,” Computer Networks, vol. 204, Article ID 108693, 2022.

A. Belenguer, J. Navaridas, and J. A. Pascual, “A review of federated learning in intrusion detection systems for iot,” 2022, https://arxiv.org/abs/2204.12443.

Z. Zhang, Y. Zhang, D. Guo, L. Yao, and Z. Li, “SecFedNIDS: robust defense for poisoning attack against federated learning-based network intrusion detection system,” Future Generation Computer Systems, vol. 134, pp. 154–169, 2022.

M. Sarhan, S. Layeghy, N. Moustafa, and M. Portmann, “Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection,” Journal of Net work and Systems Management, vol. 31, no. 1, p. 3, 2023.

M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, “Passban IDS: an intelligent anomaly-based intrusion de tection system for IoT edge devices,” IEEE Internet of Tings Journal, vol. 7, no. 8, pp. 6882–6897, 2020.

Y. Mirsky, T. Doitshman, Y. Elovici, and A. K. Shabtai, “An ensemble of autoencoders for online network intrusion detection,” 2018, https://arxiv.org/abs/1802.09089.

H. Zhao, Y. Feng, H. Koide, and K. Sakurai, “An ANN based sequential detection method for balancing performance indicators of IDS,” 2019 Seventh International Symposium on Computing and Networking (CANDAR), vol. 56, pp. 239– 244, 2019.

H. Gharaee and H. Hosseinvand, “A new feature selection IDS based on genetic algorithm and SVM,” in Proceedings of the 2016 8th International Symposium on Telecommunica tions (IST), pp. 139–144, Tehran, Iran, August 2016.

M. Belouch, S. El, and M. Idhammad, “A two-stage classifer approach using reptree algorithm for network intrusion detection,” International Journal of Advanced Computer Science and Applications, vol. 8, no. 6, pp. 389–394, 2017.

M. M. Baig, M. M. Awais, and E. S. M. El-Alfy, “A multiclass cascade of artifcial neural network for network intrusion detection,” Journal of Intelligent and Fuzzy Systems, vol. 32, no. 4, pp. 2875–2883, 2017. [99] M. Al-Zewairi, S. Almajali, and A. Awajan, “Experimental evaluation of a multi-layer feed-forward artifcial neural network classifer for network intrusion detection system,” in Proceedings of the 2017 International Conference on New Trends in Computing Sciences (ICTCS), pp. 167–172, Amman, Jordan, May 2017.

S. Guha, S. S. Yau, and A. B. Buduru, “Attack detection in cloud infrastructures using artifcial neural network with genetic feature selection,” in Proceedings of the 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress, pp. 414–419, Auckland, New Zealand, June 2016.

K. K. Nguyen, D. T. Hoang, D. Niyato, P. Wang, D. Nguyen, and E. Dutkiewicz, “Cyberattack detection in mobile cloud computing: a deep learning approach,” in Proceedings of the 2018 IEEE Wireless Communications and Networking Con ference (WCNC), pp. 1–6, Barcelona, Spain, July 2018.

N. Moustafa, G. Misra, and J. Slay, “Generalized outlier Gaussian mixture technique based on automated association features for simulating and detecting web application at tacks,” IEEE Trans. Sustain. Comput, vol. 6, no. 2, pp. 245– 256, 2021.

B. A. Tama and K. H. Rhee, “An in-depth experimental study of anomaly detection using gradient boosted machine,” Neural Computing & Applications, vol. 31, no. 4, pp. 955– 965, 2019.

R. Primartha and B. A. Tama, “Anomaly detection using random forest: a performance revisited,” in Proceedings of the 2017 International Conference on Data and Software Engi neering (ICoDSE), pp. 1–6, Palembang, Indonesia, June 2017.

A. G. Roy, S. Siddiqui, S. Polsterl, N. Navab, and C. Wachinger, “Braintorrent: A peer-to-peer environment for decentralized federated learning,” 2019, https://arxiv.org/ abs/1905.06731.

M. Alazab, S. P. R M, P. M, P. Reddy, T. R. Gadekallu, and Q.-V. Pham, “Federated learning for cybersecurity: concepts, challenges and future directions,” IEEE Transactions on Industrial Informatics, vol. 58, 2021.

S. Agrawal, S. Sarkar, O. Aouedi et al., “Federated learning for intrusion detection system: concepts,” Challenges and Future Directions, vol. 16, 2021.

S. Yamin Siddiqui, M. Adnan Khan, S. Abbas, and F. Khan, “Smart occupancy detection for road trafc parking using deep extreme learning machine,” Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 3, pp. 727–733, 2022.

A. H. Khan, S. Abbas, M. A. Khan et al., “Intelligent model for brain tumor identifcation using deep learning,” Applied Computational Intelligence and Soft Computing, vol. 2022, Article ID 8104054, 10 pages, 2022.

M. F. Khan, T. M. Ghazal, R. A. Said et al., “An iomt-enabled smart healthcare model to monitor elderly people using machine learning technique,” Computational Intelligence and Neuroscience, vol. 2021, Article ID 2487759, 10 pages, 2021.

R. A. Said, H. Raza, S. Muneer et al., “Skin cancer detection and classifcation based on deep learning,” in Proceedings of the 2022 International Conference on Cyber Resilience (ICCR), pp. 1–11, Dubai, United Arab Emirates, August 2022.

A. Raheem, S. Muneer, M. Amjad, and H. Raza, “Role of artifcial neural networks in breast cancer detection,” In ternational Journal of Computational and Innovative Sci ences, vol. 1, no. 4, pp. 9–19, 2022. [113] H. Raza, M. Amjad, and S. Muneer, “IoT based cyber physical system in automobile devices with dew comput ing architecture,” Journal of NCBAE, vol. 1, no. 1, 2022.

N. S. Naz, M. A. Khan, S. Abbas, A. Ather, and S. Saqib, “Intelligent routing between capsules empowered with deep extreme machine learning technique,” SN Applied Sciences , vol. 2, no. 1, p. 108, 2020.

M. A. Khan, S. Abbas, A. Atta et al., “Intelligent cloud based heart disease prediction system empowered with supervised machine learning,” 2020, https://www.techscience.com/cmc/ v65n1/39558. [116] N. Ali, A. Ahmed, L. Anum et al., “Modelling supply chain information collaboration empowered with machine learn ing technique,” Intelligent Automation & Soft Computing, vol. 30, no. 1, 2021.

M. M. Chowdhury, F. Hammond, G. Konowicz, C. Xin, H. Wu, and J. Li, “A few-shot deep learning approach for improved intrusion detection,” in Proceeedings of the 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), pp. 456– 462, New York, NY, USA, June 2017.

Muneer, Salman, Farooq, Umer, Athar, Atifa, Ahsan Raza, Muhammad, Ghazal, Taher M., Sakib, Shadman, A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis, *Journal of Engineering*, 2024, 3909173, 16 pages, 2024. https://doi.org/10.1155/2024/3909173

S. Muneer and M. A. Rasool, “AA systematic review: ex plainable Artifcial Intelligence (XAI) based disease pre diction,” International Journal of Advanced Sciences and Computing, vol. 1, no. 1, pp. 1–6, 2022. [119] A. Howard, M. Sandler, G. Chu et al., “Searching for mobilenetv3,” in Proceedings of the IEEE/CVF International Conference on Computer Vision, Venice, Italy, July 2019.

M. Tan and Q. Le, “Efcientnet: rethinking model scaling for convolutional neural networks,” in Proceedings of the In ternational Conference on Machine Learning, pp. 6105–6114, Himachal Pradesh, India, June 2019.

M. Tan, B. Chen, R. Pang et al., “Mnasnet: platform-aware neural architecture search for mobile,” in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Washington, DC, USA, August 2019.

J. Liu, N. Inkawhich, O. Nina et al., “Ntire 2021 multimodal aerial view object classifcation challenge,” in Proceedings of the 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 588–595, Nashville, TN, USA, July 2021.

A. Ignatov, A. Romero, H. Kim, and T. Radu, “Real-time video super-resolution on smartphones with deep learning, mobile ai 2021 challenge: report,” in Proceedings of the IEEE/ CVF Conference on Computer Vision and Pattern Recogni tion, pp. 2535–2544, Nashville, TN, USA, May 2021.

S. E. Quincozes, C. Albuquerque, D. Passos, and D. Mosse, ´ “A survey on intrusion detection and prevention systems in digital substations,” Computer Networks, vol. 184, Article ID 107679, 2021.

Detection of intrusion based on artificial intelligence in computer networks

Nastaran Nabiyar
Master of Computer Engineering (Computer Networks), Non-profit AeenKamal University, Urmia, Iran
Ali MosahebTalab
Instructor, Electrical and Computer Engineering Department, Technical and Vocational University, Tehran, Iran.

Abstract

Intrusion Detection (ID) is a key element in securing computer networks against malicious attacks. With recent advancements in deep learning (DL), explainable artificial intelligence (AXI), machine learning (ML), and federated learning (FL), these approaches have gained attention as attractive options for enhancing intrusion detection. Deep learning-based methods demonstrate effective performance in intrusion detection due to their capabilities in automatically learning relevant features from data. However, these methods require labeled data and significant computational resources to train complex models. In contrast, machine learning-based approaches require fewer resources but may have limitations in generalizing to new data.

Explainable artificial intelligence focuses on transparency and interpretability in the decision-making of AI models, allowing users to understand how models arrive at specific outcomes, which can lead to greater trust in the use of these systems. Federated learning, as a new approach, enables multiple entities to collaboratively learn a model without exchanging their data. This contributes to privacy and security, making it a suitable option for intrusion detection. This paper addresses the gaps in the literature and aims to provide a comprehensive review of specific application scenarios. Its goal is to assist professionals and researchers in easily selecting the appropriate approach based on the specific needs of ID. Factors such as network size, data availability, and privacy and security concerns all influence the choice of the best solution. This analysis can help raise awareness and improve decision-making in the field of network security, providing better guidance for the implementation of ID systems.

Keywords: “Computer networks, artificial intelligence, Intrusion detection”.