مقاله پژوهشی

استفاده از یادگیری انتقالی برای افزایش امنیت سایبری در شبکه‌های اینترنت اشیا

آرمان سمیعی، عرفان خدرصلح و هادی‌شهریار شاه‌حسینی

چکیده: سیستم‌های تشخیص نفوذ با شناسایی دسترسی غیرمجاز شبکه‌های کامپیوتری و بررسی نقض‌های امنیتی احتمالی، نقش اساسی در دفاع از شبکه‌های کامپیوتری ایفا می‌کنند. IDSهای سنتی برای مبارزه با حملات امنیتی پیچیده جدید ایجادشده با مشکلاتی مواجه می‌شوند. از این رو، نیاز روزافزونی به راه‌حل تشخیص نفوذ خودکار وجود دارد که می‌تواند فعالیت‌های مخرب را با دقت بیشتری شناسایی کند. در این مقاله، مدل جدید تشخیص نفوذ شبکه اینترنت اشیا با استفاده از یک شبکه عصبی بر اساس معماری VGG۱۶ از پیش آموزش دیده پیشنهاد شده است. مدل یک فرآیند دو مرحله‌ای است که در مرحله اول برخی از لایه‌های VGG۱۶ را از پیش بر روی مجموعه داده‌ی ImageNet آموزش داده شده و وزن‌های آن را انتقال می‌دهیم و در مرحله دوم به طور خاص برای تشخیص نفوذ در شبکه‌های اینترنت اشیا عمل تنظیم دقیق انجام می‌شود. زیرا این شبکه‌ها به دلیل محدودیت‌های منابع، پروتکل‌های منحصر به فرد و تنوع دستگاه‌ها، آسیب‌پذیری‌های خاصی دارند که نیازمند روش‌های تشخیص نفوذ مختص به خود هستند. مدل روی مجموعه داده‌های UNSW-NB۱۵ و NSL-KDD، اعمال شده است. نتایج نشان می‌دهد که روش پیشنهادشده می‌تواند به طور مؤثر با تولید عملکرد واقعی از نظر صحت، دقت، فراخوانی و امتیاز_F۱ یاد بگیرد.

***کلیدواژه:* اینترنت اشیا، سیستم‌های تشخیص نفوذ، یادگیری انتقالی، یادگیری عمیق.**

۱- مقدمه

با گسترش مداوم مقیاس شبکه، امنیت شبکه با تهدیدهای پیچیده‌تری نسبت به قبل مواجه می‌شود [۱]. از این رو، مسائل امنیتی شبکه توجه روزافزونی را به خود جلب می‌کنند. به خصوص در شبکه‌های اینترنت اشیا[1] (IoT) که به دلیل تنوع گسترده دستگاه‌ها و پروتکل‌های ارتباطی، محدودیت‌های منابع و معماری‌های پراکنده، امنیت آن‌ها با چالش‌های منحصر به فردی مواجه است [۲]. سیستم‌های متداول امنیت شبکه برای کشف حملات مشکوک، شامل فایروال‌ها، سیستم‌های تشخیص نفوذ[2] (IDS) وسیستم‌های پیشگیری از نفوذ می‌شوند [۳]. IDS به دلیل قابلیت تشخیص نفوذهای جدید و پیش‌بینی نفوذهای آتی، نسبت به دیواره‌های آتش[3] و سیستم‌های پیشگیری از نفوذ برتری دارند [۴]. این مسئله در شبکه‌های اینترنت اشیا اهمیت بیشتری پیدا می‌کند، زیرا این شبکه‌ها به دلیل ویژگی‌های که پیش‌تر گفته شد، هدف حملات پیچیده‌تری هستند و نیازمند روش‌های تشخیص نفوذ پیشرفته‌تری می‌باشند [۵]. به طور مشخص، وظیفه IDSها جمع‌آوری و شناسایی رفتارهای غیر عادی در شبکه است [۳]. با تجزیه و تحلیل بسته‌های داده‌های ضبط‌شده، IDSها می‌توانند رفتارهای مجاز شبکه را بررسی، حملات را شناسایی و برای مهار آن‌ها گزارش دهند [۶].

معمولاً عملکرد IDSهایی که در طراحی آن‌ها بر الگوریتم‌های ثابت، قوانین پیش‌فرض و الگوهای حملات شناخته‌شده تکیه شده است ضعیف بوده و دارای نرخ‌های تشخیص پایین و نرخ‌های مثبت کاذب بالا هستند [۷]. همچنین در میان IDSهای مبتنی بر الگوریتم‌های یادگیری ماشین پیشنهاد شده در پژوهش‌های مختلف، روش‌های سنتی در سناریوهایی که با حملات Flood (که در شبکه‌های اینترنت اشیا رایج هستند [۸]) روبه‌رو می‌شوند عملکرد ضعیفی دارند [۹]. به علاوه، بر خلاف بسیاری از شبکه‌ها که مجموعه‌ای بزرگ از داده‌های برچسب‌دار برای آموزش مدل‌های مبتنی بر یادگیری عمیق در دسترس بوده و امکان استخراج الگوهای پیچیده در فرایند یادگیری را فراهم می‌سازد [۱۰]. در شبکه‌های اینترنت اشیا چنین مجموعه‌ای از داده‌های برچسب‌گذاری شده برای حملات ناشناخته وجود ندارد [۱۱]. همچنین در این شبکه‌ها، جمع‌آوری داده‌های آموزشی جدید پرهزینه و زمان‌بر بوده [۱۲] و مجموعه داده‌های موجود نیز بسیار نامتقارن هستند [۱۳]. از این رو محققان برای رفع این مشکل به‌کارگیری الگوریتم‌های یادگیری عمیق درطراحی IDS را پیشنهاد نمودند.

دلایل این تصمیم را می‌توان در وابستگی IDSها به الگوریتم‌های طبقه‌بندی به کار رفته در طراحی آن‌ها [۱۴]، برتری روش‌های یادگیری عمیق نسبت به روش‌های یادگیری سنتی از دو جنبه‌ی یادگیری ویژگی‌های پیچیده و حذف (یا کاهش چشمگیر) هزینه‌های فرایند استخراج و آماده‌سازی ویژگی جست‌وجو نمود [۱۵]. در شبکه‌های اینترنت اشیا، این موضوع اهمیت بیشتری پیدا می‌کند زیرا تنوع دستگاه‌ها و پروتکل‌های مختلف مورد استفاده، به همراه محدودیت‌های منابع، نیازمند روش‌های پیشرفته‌تری برای تشخیص حملات است به‌علاوه، داده‌های برچسب‌دار کافی برای آموزش مدل‌های سنتی به‌ندرت در دسترس هستند، و جمع‌آوری داده‌های جدید نیز هزینه‌بر و زمان‌بر است [۱۶].

این مقاله در تاریخ ۳ مهر ماه ۱۴۰۳ دریافت و در تاریخ ۱۲ اسفند ماه ۱۴۰۴ بازنگری شد.

آرمان سمیعی، دانشکده مهندسی برق، دانشگاه علم و صنعت، تهران، ایران، (email: arman_samiee@elec.iust.ac.ir).

عرفان خدرصلح، دانشکده مهندسی برق، دانشگاه علم و صنعت، تهران، ایران، (email: erfan_khedersolh@elec.iust.ac.ir).

هادی‌شهریار شاه‌حسینی (نویسنده مسئول)، دانشکده مهندسی برق، دانشگاه علم و صنعت، تهران، ایران، (email: shahhoseini@iust.ac.ir).

1. Internet of Things
2. Intrusion Detection Systems
3. Firewalls

از سوی دیگر و به‌طور کلی نیز مدل‌های یادگیری عمیق (از جمله در کاربرد اینترنت اشیا) باید با داده‌های جدید از ابتدا آموزش داده شوند و این موضوع حجم زیادی از منابع محاسباتی، سخت‌افزاری و زمان را نیاز دارد [۱۷]. برای رفع این چالش محققان اخیراً به‌کارگیری یادگیری انتقالی در طراحی IDS را پیشنهاد نمودند.

یادگیری انتقالی یک پیشرفت اخیر یادگیری عمیق است که دانشی را که قبلاً در یک دامنه منبع آموخته بود در یک دیگر اعمال می‌کند [۱۸]. استفاده از یادگیری انتقالی از طریق انتقال مدل‌های از پیش‌آموزش‌دیده، نه تنها منجر به کاهش چشمگیر نیاز به منابع محاسباتی، سخت‌افزاری و زمان می‌شود، بلکه در IDSها تشخیص حملات شناخته‌شده به‌ویژه در دامنه‌هایی با داده‌های کمیاب مانند شبکه‌های اینترنت اشیا را بهبود می‌بخشد [۵]. به‌عبارت دیگر، یادگیری انتقالی به IDSهای مبتنی بر یادگیری عمیق کمک می‌کند تا بر محدودیت‌های خود در تشخیص حملات تهدیدات در حال تحول و در تشخیص مؤثر حملات سایبری در شبکه‌هایی با مجموعه داده‌های کمیاب و نامتعادل غلبه کنند [۱۹].

در این پژوهش پیاده‌سازی یک چارچوب تشخیص نفوذ کارآمد بر اساس یادگیری انتقالی را پیشنهاد می‌کنیم که میزان تشخیص و دقت را برای خانواده‌های شناخته شده و جدید حملات سایبری در شبکه‌های اینترنت اشیا با مجموعه‌داده‌های کمیاب و نامتعادل ارزیابی می‌کنیم.

مدل پیشنهادی این پژوهش بر روی دو مورد از پراستفاده‌ترین مجموعه‌های داده‌های حوزه‌ی تشخیص نفوذ، یعنی UNSW-NB۱۵ و NSL-KDD که شامل جریان‌های ترافیک عادی و حمله‌ی سایبری در حوزه‌ی اینترنت اشیاء هستند، مورد ارزیابی قرار گرفته و در مقایسه با تحقیقات اخیر، نتایج امیدوارکننده‌ای به دست آمده است.

نوآوری های این مقاله به شرح زیر است:

- ارائه یک IDS کارآمد با استفاده از آموزش انتقالی: این مقاله یک چارچوب تشخیص نفوذ نوآورانه را معرفی می‌کند در آن از یادگیری انتقالی استفاده شده است که به‌ویژه برای بهبود کارایی در شبکه‌های IoT که با مجموعه داده‌های پراکنده و نامتعادل مشخص می‌شود، مؤثر است.
- اثربخشی ثابت شده روی مجموعه داده‌های UNSW-NB۱۵ و NSL-KDD: در این مقاله نتایج امیدوارکننده‌ای از تعیین معیارها در مجموعه داده‌های UNSW-NB۱۵ و NSL-KDD را ارائه می‌کنیم، که معیارها مناسب حاوی جریان‌های ترافیک عادی و مخرب اینترنت اشیا هستند.
- برآورده کردن نیازهای روز در سیستم‌های تشخیص نفوذ شبکه اینترنت اشیا: این چارچوب به‌طور خاص برای رسیدگی به چالش‌های پیش روی شبکه‌های اینترنت اشیا ازجمله نیاز به دقت تشخیص بالا، طراحی شده است که آن را به یک راه‌حل هدفمند برای امنیت اینترنت اشیا تبدیل می‌کند.

در ادامه در بخش دوم این مقاله کارهای مرتبط معرفی می‌شود. بخش سوم به روش‌شناسی و فرایند پیاده‌سازی به‌تفصیل می‌پردازد. در بخش چهارم نتایج ارزیابی‌ها و تحلیل آن‌ها ارائه می‌شود و در بخش آخر به نتیجه‌گیری می‌پردازد.

۲- کارهای مرتبط

تشخیص نفوذ شبکه یک مسئله طبقه‌بندی که در سال‌ها اخیر بسیار مورد توجه پژوهشگران بوده است. در این پژوهش‌ها یکی از چالش‌های همیشگی استخراج الگوهای منحصر به فرد از نفوذهای حمله و تمیز دادن حملات از ترافیک عادی است. در پژوهش‌های متعدد انتشار یافته در سال‌های اخیر از روش‌های آماری سنتی تا روش‌های مبتنی بر یادگیری عمیق استفاده شده است؛ اما تنها چند مطالعه وجود دارد که کاربرد یادگیری انتقالی در امنیت اینترنت اشیا را بررسی می‌کند.

ویو و همکاران [۲۰] یک سیستم تشخیص حمله مبتنی بر یادگیری عمیق برای شبکه‌های اینترنت اشیا را پیشنهاد کرده‌اند. به دلیل کمبود داده‌های برچسب‌گذاری شده روز، آن‌ها یک رویکرد یادگیری انتقالی را پیشنهاد می‌کنند که در آن از یک خودکدکننده (اتوانکدر) آموزش دیده بر روی یک مجموعه داده‌ی برچسب‌گذاری شده به خودکدکننده دیگری که روی یک مجموعه داده‌ی بدون برچسب آموزش داده شده است، منتقل می‌شود. هدف آن شناسایی حملات عمومی مانند پویش[1] حملات سیلابی[2] مانند سیلاب TCP و سیلاب UDP است. هرچند تمرکز کار ایشان بر روی تشخیص حملات سایبری در محیط‌های IoT است، ولی استفاده از پروتکل‌های خاص IoT مورد نظر نیست. به این معنی که، رویکرد ارائه‌شده در مقاله به گونه‌ای طراحی شده است که فقط بر روی حملات عمومی ذکر شده در بالا قابل اجرا است، که این محدودیت‌ها ممکن است در شبکه‌های مختلف از جمله IoT رخ دهند اما به دلیل عدم تمرکز بر پروتکل‌های خاصIoT ، نمی‌توانند به‌طور موثر حملات ویژه و پیچیده‌تر این حوزه را شناسایی کنند.

خوا و همکاران در [۲۱] به بررسی و ارزیابی یک چارچوب یادگیری انتقالی برای تشخیص نفوذ در شبکه‌های اینترنت اشیا می‌پردازند. این مطالعه از ترکیب یادگیری انتقالی و یادگیری فدرال برای بهبود عملکرد تشخیص حملات سایبری در شبکه‌های IoT استفاده می‌کند. برای کاهش انتقال منفی، مقاله نیاز به نمونه‌های مشترک بین شبکه‌های منبع و هدف دارد. این نیاز می‌تواند در مواردی که چنین نمونه‌هایی به سختی قابل دسترسی هستند، محدودیت‌هایی ایجاد کند. نتایج ایشان نشان می‌دهد که رویکرد مبتنی بر یادگیری انتقالی پیشنهادی بهتر از روش‌های مبتنی بر یادگیری عمیق عمل می‌کند. مجموعه داده‌های هدف شامل حملاتی هستند که در مجموعه داده‌های منبع وجود ندارند و تأثیر رویکرد پیشنهادی بر تشخیص حملات جدید به خوبی در نتایج به دست آمده قابل مشاهده نیست. یوتائو و همکاران در [۲۲] مدلVGG-RED را معرفی می‌کنند. روشی مبتنی بر یادگیری انتقالی که داده‌های تشخیص نفوذ اینترنت را به طور مؤثری برای بهبود سیستم‌های تشخیص نفوذ IoT به کار می‌برد با استفاده از کاهش بعد شبکه عصبی برای کاهش نیازهای محاسباتی که این فرآیند منجر به از دست رفتن برخی ویژگی‌های مهم و باعث کاهش دقت مدل‌ها می‌شود.

مهدی و همکاران در [۲۳] یک سیستم تشخیص نفوذ برای IoT با استفاده از رویکرد یادگیری انتقالی عمیق ارائه کرده‌اند. این رویکرد شامل انتخاب ویژگی‌های مؤثر، طراحی مدل ResNet بر پایه یادگیری انتقالی، و ارزیابی با استفاده از داده‌های واقعی است. در این مقاله به طیف محدود از حملات سایبری در زمینه IOT پرداخته می‌شود. به عبارت دیگر آن‌ها بر روی تعداد محدودی از حملات سایبری خاص شامل حملات اخلال در خدمت ، اخلال در خدمت توزیع شده ، تزریق داده ، مردمیانی، درب پشتی می‌شود که در محیط‌های IoT تمرکز دارند. این امر بیان می‌کند که دامنه حملات سایبری مورد مطالعه و بررسی در کار ایشان محدود است، تنها شامل چند نوع حمله است و فقط بر حملاتی تمرکز دارد که در محیط‌های

1. Scanning
2. Flooding

IoT بسیار مرتبط یا شایع هستند. چوداری و همکاران در [۲۴] از مجموعه داده‌های UNSW-NB۱۵ و NSL-KDD در یک مدل شبکه عصبی عمیق با ۲۰ لایه پنهان برای شناسایی و تشخیص حملات در شبکه‌های اینترنت اشیا استفاده می‌کنند. این مدل بر اساس داده‌های آموزشی مختلفی تنظیم و ارزیابی شده است. عملکرد مدل شبکه عصبی عمیق (DNN) با استفاده از معیارهای معتبر مورد ارزیابی قرار گرفته است.

کوچر در [۲۵] به ارزیابی عملکرد الگوریتم‌های مختلف یادگیری ماشین شامل KNN، تقویت گرادیان ترکیبی، درخت تصمیم، جنگل تصادفی، رگرسیون لجستیک و دسته‌بندی‌کننده بیز در تشخیص نفوذ در شبکه‌های اینترنت اشیا پرداخته است. هدف اصلی این مطالعه بهبود دقت و کارایی سیستم‌های تشخیص نفوذ با استفاده از مجموعه داده UNSW-NB۱۵ است. لاریوا-نوو و همکاران در [۲۶] به ارزیابی یک سیستم تشخیص نفوذ برای شبکه‌های اینترنت اشیا می‌پردازند. هدف آن مطالعه بهبود دقت تشخیص نفوذ با استفاده از تکنیک‌های مختلف پیش‌پردازش داده‌ها و ارزیابی آن‌ها بر روی مجموعه داده‌های UNSW-NB۱۵ و NSL-KDD است.

دیشا در [۲۷] به تحلیل و ارزیابی سیستم‌های تشخیص نفوذ در شبکه‌های اینترنت اشیا با استفاده از مدل‌های مختلف یادگیری ماشین پرداخته است. چهار مدل یادگیری ماشین مختلف شامل درخت تصمیم، جنگل تصادفی، درخت تقویت‌شده و پرسپترون‌چندلایه برای تشخیص نفوذ استفاده شده‌اند. هدف این مطالعه بهبود دقت و کارایی سیستم‌های تشخیص نفوذ با استفاده از مجموعه داده UNSW-NB۱۵ است. سلمان و همکاران در [۲۸] به بررسی سیستم‌های تشخیص نفوذ غیرعادی در شبکه‌های با استفاده از الگوریتم‌های یادگیری عمیق می‌پردازند و از مجموعه داده UNSW-NB۱۵ استفاده می‌کنند. در آن مقاله دو مدل مختلف پیشنهاد شده است که یک مدل شبکه عصبی پیچشی ترکیب شده با شبکه‌های حافظه کوتاه-بلند مدت و یک مدل شبکه عصبی مصنوعی با لایه‌های کاملا متصل است. مدل‌های پیشنهادی برای انجام اسکن‌های امنیتی بر روی دستگاه‌های اینترنت اشیا و ارزیابی الگوهای ترافیک شبکه استفاده شده‌اند.

احمد و همکاران در [۲۹] به تحلیل و ارزیابی سیستم‌های تشخیص نفوذ (IDS) با استفاده از الگوریتم‌های مختلف یادگیری ماشین برای شبکه‌های اینترنت اشیا پرداخته‌اند. هدف اصلی ایشان بهبود دقت و کارایی سیستم‌های تشخیص نفوذ با استفاده از مجموعه داده UNSW-NB۱۵ است. ترک در [۳۰] به بررسی و ارزیابی کارایی الگوریتم‌های مختلف یادگیری ماشین شامل رگرسیون لجستیک ، KNN، جنگل تصادفی، درخت تصمیم، پرسپترون‌چندلایه و شبکه‌های حافظه کوتاه-بلند مدت در تشخیص نفوذ سیستم‌های اینترنت اشیا با استفاده از مجموعه داده‌های UNSW-NB۱۵ و NSL-KDD پرداخته است.

مغربی در [۳۱] از مجموعه داده UNSW-NB۱۵ برای بررسی سیستم‌های تشخیص نفوذ خودکار در محیط‌های اینترنت اشیا استفاده کرده است. هدف وی مطالعه ارائه یک مدل یادگیری ماشین به نام جنگل تصادفی برای بهبود دقت تشخیص نفوذ و کاهش هشدارهای نادرست در شبکه‌های IoT است. پرامیلارانی و همکارش در [۳۲] به توسعه یک سیستم تشخیص نفوذ در اینترنت اشیا با استفاده از یک طبقه‌بند جنگل تصادفی مبتنی بر هزینه پرداخته است. هدف ایشان از این مطالعه بهبود دقت و کاهش نرخ هشدار نادرست با استفاده از ماتریس هزینه است و از مجموعه داده‌های UNSW-NB۱۵ و NSL-KDD استفاده کرده‌اند.

جدول ۱: معماری VGG-16

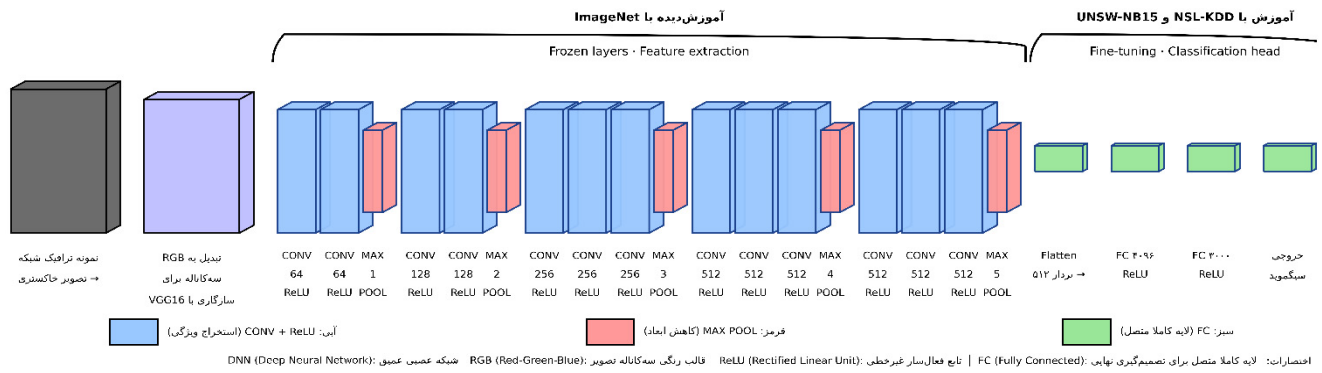
لایه	کرنل	اندازه خروجی	فعال‌ساز	تعداد پارامتر
Input	---	۲۲۴×۲۲۴×۳	---	۰
Convolutional۳-۶۴	۳×۳	۲۲۴×۲۲۴×۶۴	Relu	۱۷۹۲
Convolutional۳-۶۴	۳×۳	۲۲۴×۲۲۴×۶۴	Relu	۳۶۹۲۸
MAX POOLING	۲×۲	۱۱۲×۱۱۲×۶۴	×××	۰
Convolutional۳-۱۲۸	۳×۳	۱۱۲×۱۱۲×۱۲۸	Relu	۷۳۸۵۶
Convolutional۳-۱۲۸	۳×۳	۱۱۲×۱۱۲×۱۲۸	Relu	۱۴۷۵۸۴
MAX POOLING	۲×۲	۵۶×۵۶×۱۲۸	×××	۰
Convolutional۳-۲۵۶	۳×۳	۵۶×۵۶×۲۵۶	Relu	۲۹۵۱۶۸
Convolutional۳-۲۵۶	۳×۳	۵۶×۵۶×۲۵۶	Relu	۵۹۰۰۸۰
MAX POOLING	۲×۲	۲۸×۲۸×۲۵۶	×××	۰
Convolutional۳-۵۱۲	۳×۳	۲۸×۲۸×۵۱۲	Relu	۱۱۸۰۱۶۰
Convolutional۳-۵۱۲	۳×۳	۲۸×۲۸×۵۱۲	Relu	۲۳۵۹۸۰۸
Convolutional۳-۵۱۲	۳×۳	۲۸×۲۸×۵۱۲	Relu	۲۳۵۹۸۰۸
MAX POOLING	۲×۲	۱۴×۱۴×۵۱۲	×××	۰
Convolutional۳-۵۱۲	۳×۳	۱۴×۱۴×۵۱۲	Relu	۲۳۵۹۸۰۸
Convolutional۳-۵۱۲	۳×۳	۱۴×۱۴×۵۱۲	Relu	۲۳۵۹۸۰۸
Convolutional۳-۵۱۲	۳×۳	۱۴×۱۴×۵۱۲	Relu	۲۳۵۹۸۰۸
MAX POOLIN	۲×۲	۷×۷×۵۱۲	×××	۰
Fully Connected	×××	۴۰۹۶	Relu	۱۰۲۷۶۴۵۴۴
Fully Connected	×××	۴۰۹۶	Relu	۱۶۷۹۱۳۱۲
Output	---	۱۰۰۰	Soft-max	---

مور و همکاران در [۳۳] مدل‌های مختلف یادگیری ماشین شامل رگرسیون لجستیک، ماشین بردار پشتیبانی، درخت تصمیم و جنگل تصادفی را برای تشخیص نفوذ در شبکه‌های اینترنت اشیا با استفاده از مجموعه داده UNSW-NB۱۵ مورد استفاده قرار داده‌اند.

۳- روش‌شناسی و فرایند پیاده‌سازی

آموزش انتقالی یکی از روش‌های پیشرو در یادگیری ماشین است که به طور گسترده‌ای در زمینه طبقه‌بندی تصویر استفاده می‌شود. مدل VGG یک شبکه عصبی کانولوشنی با معماری خاص است مدل VGG بر روی مجموعه داده‌ی ImageNet آموزش دیده شده است، که یک مجموعه داده مهم در زمینه پردازش تصویر است. این مجموعه داده شامل بیش از ۱۴ میلیون تصویر با کیفیت بالا از ۱۰۰۰ کلاس مختلف است. ImageNet به عنوان یک معیار مهم در زمینه تحقیقات بینایی ماشین شناخته می‌شود و برای آموزش و ارزیابی الگوریتم‌های یادگیری عمیق، شبکه‌های عصبی کانولوشنی مورد استفاده قرار می‌گیرد. مدل VGG دو معماری مختلف دارد یکی VGG-۱۶ که شامل ۱۶ لایه است و دیگری VGG-۱۹ که شامل ۱۹لایه است. در این مقاله، از VGG-۱۶ استفاده شده است که این مدل شامل ۱۶ لایه است که به دو بخش اصلی تقسیم می‌شود. ابتدا دو لایه کانولوشن، سپس لایه پولینگ و سپس دو لایه کانولوشن و لایه پولینگ و سپس تکراری از سه لایه کانولوشن و لایه‌های پولینگ و در نهایت سه‌لایه کاملا متصل است. این معماری شامل یک تعداد قابل توجه‌ای از وزن‌های قابل آموزش است. جدول ۱ خلاصه مدل VGG-۱۶ را نشان می‌دهد.

شکل ۱ ساختار کلی روش پیشنهادی مبتنی بر یادگیری انتقالی را نشان می‌دهد. در این روش، از مدل VGG-۱۶ از پیش‌آموزش‌دیده بر



شکل ۱: معماری روش پیشنهادی.

روی مجموعه‌داده‌ی ImageNet برای انتقال دانش و استخراج ویژگی‌های عمومی از ترافیک شبکه استفاده شده است. در مرحله‌ی پیش‌پردازش داده‌ها، نمونه‌های خام ترافیک شبکه از مجموعه‌داده‌های UNSW-NB۱۵ و NSL-KDD آماده‌سازی شدند تا با ساختار ورودی مدل VGG-۱۶ سازگار شوند. در این مرحله، داده‌های پرت و مقادیر گمشده حذف گردید و ویژگی‌های عددی با روش Min–Max Normalization در بازه‌ی [۰,۱] نرمال‌سازی شدند. سپس ویژگی‌های غیرعددی با استفاده از One-Hot Encoding به داده‌های عددی تبدیل شدند تا مدل بتواند آن‌ها را پردازش کند. در ادامه، هر نمونه‌ی داده به‌صورت ماتریس دوبعدی از ویژگی‌ها بازنمایی شد و با نگاشت مقادیر به شدت روشنایی، به تصویر سطح خاکستری تبدیل گردید. این تصاویر با تکرار سه‌باره در کانال‌های RGB (قرمز، سبز و آبی) ، به داده‌های سه‌کاناله‌ی سازگار با مدل‌های بینایی ماشین تبدیل شدند. این فرایند، زمینه‌ی بهره‌گیری از وزن‌های ازپیش‌آموزش‌دیده‌ی مدل VGG-۱۶ را بر پایه‌ی مجموعه‌داده‌ی ImageNet فراهم کرده و موجب انتقال دانش بینایی به حوزه‌ی ترافیک شبکه می‌شود. در پایان، داده‌ها به‌صورت تصادفی به دو مجموعه‌ی آموزش (۸۰٪) و آزمون (۲۰٪) تقسیم شدند. بخش نخست مدل شامل لایه‌های کانولوشنی و حداکثر تجمع (ماکس پولینگ) و است که وزن‌های آن‌ها در چارچوب یادگیری انتقالی تثبیت شده و در فرآیند جدید آموزش داده نمی‌شوند. این بخش مسئول انتقال دانش عمومی از دامنه‌ی تصویر به دامنه‌ی ترافیک شبکه و استخراج الگوهای پایه‌ای از داده‌های ورودی است.

در فرآیند آموزش، برای بهره‌گیری از دانش پیش‌آموخته در دامنه‌ی منبع و بهبود دقت در دامنه‌ی هدف، ۱۳ لایه‌ی ابتدایی مدل VGG-۱۶ ثابت نگه‌داشته شدند تا ویژگی‌های عمومی حاصل از آموزش بر روی مجموعه‌داده‌ی ImageNet به مسأله‌ی تشخیص نفوذ منتقل شوند. در مقابل، ۳ لایه‌ی انتهایی مدل که بخش کاملاً متصل را تشکیل می‌دهند، به‌صورت کامل آموزش داده شدند تا مدل بتواند با ویژگی‌های خاص مجموعه‌داده‌های UNSW-NB۱۵ و NSL-KDD تطبیق یابد و دقت خود را در تشخیص نفوذ افزایش دهد. در این میان، لایه‌ی Flatten خروجی بخش کانولوشنی را به برداری یک‌بعدی از ویژگی‌ها تبدیل می‌کند، دو لایه‌ی پنهان کاملاً متصل با تابع فعال‌ساز ReLU نگاشت غیرخطی لازم برای تفکیک داده‌ها را فراهم می‌کنند و لایه‌ی خروجی با تابع سیگموید احتمال هر نمونه را برای طبقه‌بندی در دو گروه «عادی» یا «حمله» محاسبه می‌کند. به این ترتیب، لایه‌های اولیه نقش حفظ و انتقال دانش عمومی را بر عهده دارند، در حالی که لایه‌های انتهایی وظیفه‌ی یادگیری دقیق الگوهای جدید و تصمیم‌گیری نهایی را ایفا می‌کنند. این ترکیب سبب می‌شود تا مدل از دانش گسترده‌ی دامنه‌ی تصویر بهره‌مند گردد و بتواند خود را با ویژگی‌های خاص داده‌های شبکه‌های اینترنت اشیا سازگار کند.

انتخاب این معماری با هدف دستیابی به تعادل میان دقت، کارایی و هزینه‌ی محاسباتی صورت گرفته است. ثابت نگه‌داشتن لایه‌های ابتدایی موجب کاهش قابل‌توجه بار محاسباتی و زمان آموزش می‌شود، در حالی که آموزش لایه‌های نهایی امکان تنظیم دقیق مرزهای تصمیم را فراهم می‌سازد. این رویکرد سبب می‌شود مدل در محیط‌های دارای منابع محدود نیز قابل‌استفاده باشد و در عین حال، توانایی بالایی در تشخیص حملات ناشناخته و داده‌های متنوع از خود نشان دهد. به بیان دیگر، ساختار پیشنهادی ضمن حفظ دانش عمومی، بهینه‌ترین مسیر یادگیری برای سازگاری با مجموعه‌داده‌های امنیتی جدید را فراهم می‌کند و دقت سیستم تشخیص نفوذ را در دامنه‌ی هدف افزایش می‌دهد. برای اجرای شبیه‌سازی، از زبان برنامه‌نویسی پایتون استفاده شد. کتابخانه‌های مختلفی برای پیش‌پردازش داده‌ها، ساخت و آموزش مدل‌های یادگیری عمیق به کار گرفته شدند. از Pandas برای پردازش داده، Scikit-Learn برای پیش‌پردازش و ارزیابی مدل، NumPy برای عملیات عددی، و TensorFlow و Keras برای ساخت و آموزش شبکه‌های عصبی استفاده گردید. نمونه‌برداری تصادفی با کتابخانه‌ی Random انجام شد و تمامی مراحل در محیط گوگل کولب مبتنی بر سیستم‌عامل لینوکس پیاده‌سازی گردید.

٤- نتایج ارزیابی‌ها

٤-١ مجموعه داده

برای ارزیابی مدل پیشنهادی از دو مجموعه‌داده‌ی استاندارد UNSW-NB NB15۱۵ و NSL-KDD استفاده شد. مجموعه‌داده‌ی UNSW-NB۱۵ توسط مؤسسه‌ی مرکز استرالیایی امنیت سایبری[1] در سال ۲۰۱۵ ایجاد شده و شامل بیش از ۲٫۵ میلیون نمونه از ترافیک عادی و حملات سایبری متنوع مانند DoS، Fuzzers، Backdoors، Analysis، Reconnaissance است. این مجموعه دارای ۴۹ ویژگی رفتاری و آماری بوده و داده‌های آن برای شبیه‌سازی محیط‌های واقعی شبکه‌های IoT بسیار مناسب است. مجموعه‌داده‌ی NSL-KDD نسخه‌ی اصلاح‌شده‌ی KDD-Cup'۹۹ است که شامل ۱۲۵٬۹۷۳ نمونه آموزشی و ۲۲٬۵۴۴ نمونه آزمایشی می‌باشد. این داده‌ها با ۴۱ ویژگی در چهار گروه حمله‌ی اصلی DoS، Probe، R۲L[2] و U۲R[3] سازمان‌دهی

1. Australian Centre for Cyber Security
2. Remote to Local Attack
3. User to Root Attack

جدول ۲: نتایج اجرای مدل پیشنهادی.

شبکه	مجموعه‌داده	صحت	دقت	بازخوانی	امتیاز_F۱
ResNet۵۰	UNSW-NB۱۵	٪۹۸,۵۹	٪۹۸,۷۰	٪۹۸,۴۹	٪۹۸,۶۰
	NSL-KDD	٪۹۰,۳۱	٪۹۲,۵۹	٪۸۷,۷۶	٪۹۰,۱۱
InceptionV۳	UNSW-NB۱۵	٪۹۹,۶۵	٪۹۹,۳۶	٪۹۹,۹۵	٪۹۹,۶۵
	NSL-KDD	٪۹۸,۱۰	٪۹۷,۲۱	٪۹۹,۰۷	٪۹۸,۱۳
DenseNet۱۲۱	UNSW-NB۱۵	٪۹۹,۶۷	٪۹۹,۳۴	٪۱۰۰	٪۹۹,۶۷
	NSL-KDD	٪۹۷,۸۷	٪۹۷,۷۸	٪۹۷,۹۸	٪۹۷,۸۸
VGG-۱۶	**UNSW-NB۱۵**	**٪۹۹,۷۴**	**٪۹۹,۴۹**	**٪۱۰۰**	**٪۹۹,۷۴**
	NSL-KDD	**٪۹۸,۴۴**	**٪۹۷,۹۰**	**٪۹۹,۰۱**	**٪۹۸,۴۵**

شده‌اند. NSL-KDD با حذف داده‌های تکراری و ایجاد تعادل در کلاس‌ها، ارزیابی دقیق‌تر مدل‌های تشخیص نفوذ را ممکن می‌سازد. این دو مجموعه‌داده، به دلیل تنوع در نوع حملات و ساختار ویژگی‌ها، معیار مناسبی برای ارزیابی دقت و تعمیم‌پذیری مدل پیشنهادی مبتنی بر یادگیری انتقالی محسوب می‌شوند و می‌توان اطمینان حاصل کرد که مدل قادر است در مواجهه با حملات مختلف، به خوبی عمل کند و به طور مؤثری تهدیدات را تشخیص دهد.

٤-۲ معیارهای ارزیابی مدل

در این بخش که به ارزیابی عملکرد مدل اختصاص یافته است، با استفاده از معیارهای معتبر از جمله صحت[1]، دقت[2]، فراخوانی[3] و امتیاز_F۱[4] کارایی رویکرد یادگیری انتقالی را در شناسایی تهدیدات سایبری در شبکه‌های IOT مورد بررسی قرار گرفته است. صحت معیاری است که درصد پیش‌بینی‌های صحیح مدل بر روی داده‌های آزمون را نشان می‌دهد. دقت نسبت تعداد نمونه‌های مثبت واقعی شناسایی شده به کل نمونه‌هایی که به‌عنوان مثبت پیش‌بینی شده‌اند را نشان می‌دهد. فراخوانی نشان‌دهنده توانایی مدل در شناسایی تمام نمونه‌های مثبت واقعی است و امتیاز_F۱ تعادل بین دقت و فراخوانی را برای دستیابی به یک ارزیابی جامع‌تر از عملکرد مدل فراهم می‌کند. پارامترهای ذکرشده به صورت زیر محاسبه می‌شوند

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \quad (۱)$$

$$Precision = \frac{TP}{TP + FP} \quad (۲)$$

$$Recall = \frac{TP}{TP + FN} \quad (۳)$$

$$F۱_Score = \frac{۲ \times (Precision \times Recall)}{Precision + Recall} \quad (۴)$$

که در آنها TP، TN، FP و FN به ترتیب مثبت و منفی صادق و مثبت و منفی کاذب هستند.

1. Accuracy
2. Precision
3. Recall
4. F1-Score

جدول ۳: مقایسه با سایر روش‌ها.

مرجع	صحت	دقت	بازخوانی	امتیاز_F۱
[۲۴]	٪۹۵,۴۳	٪۹۳,۱۲	٪۹۴,۲۱	٪۹۳,۶۶
[۲۵]	٪۹۵,۴۳	٪۹۶,۰۰	٪۹۷,۰۰	٪۹۷,۰۰
[۲۶]	٪۹۹,۲۰	٪۹۷,۳۰	٪۹۹,۰۰	٪۹۸,۱۰
[۲۷]	٪۹۲,۷۶	٪۹۰,۹۶	٪۹۶,۴۲	٪۹۳,۶۱
[۲۸]	٪۹۶,۰۸	٪۹۶,۰۸	٪۹۶,۰۸	٪۹۶,۰۸
[۲۹]	٪۹۹,۳۰	٪۹۹,۷۰	٪۹۸,۵۰	٪۹۹,۹۵
[۳۰]	٪۹۸,۶۰	٪۹۸,۰۰	٪۹۸,۰۰	٪۹۸,۰۰
[۳۱]	٪۹۰,۱۷	٪۹۰,۱۴	٪۹۰,۱۷	٪۹۰,۱۴
[۳۲]	٪۹۹,۶۰	٪۹۹,۴۸	٪۹۸,۷۳	٪۹۹,۵۴
[۳۳]	٪۹۸,۶۳	٪۹۹,۷۱	٪۹۹,۶۳	٪۹۹,۶۷
روش پیشنهادی	٪۹۹,۷۴	٪۹۹,۴۹	٪۱۰۰	٪۹۹,۷۴

٤-۳ نتایج مدل پیشنهادی

همان‌طور که در جدول ۲ ملاحظه می‌شود، عملکرد مدل‌ها بر اساس پارامترهای که در بخش قبل توضیح داده‌شده است، یعنی صحت، دقت، فراخوانی و امتیاز_F۱ بر روی دو مجموعه داده، UNSW-NB۱۵ و NSL-KDD ارزیابی شده است. داده‌های موجود نشان می‌دهند که مدل VGG-۱۶ بر روی مجموعه داده‌ی UNSW-NB۱۵ به مقادیر صحت ٪۹۹,۷۴، دقت برابر ٪۹۹,۴۹ و فراخوانی برابر ٪۱۰۰ امتیاز_F۱ برابر با ٪۹۹,۷۴ دست می‌یابد.

٤-٤ تحلیل پیچیدگی محاسباتی و زمان استنتاج

با توجه به محدودیت منابع محاسباتی در اینترنت اشیا، ارزیابی کارایی مدل از نظر پیچیدگی زمانی و حافظه‌ای اهمیت ویژه‌ای دارد. معماری VGG-۱۶ به‌دلیل تعداد بالای پارامترها، به‌صورت مستقیم برای محیط‌های سبک‌وزن مناسب نیست، اما استفاده از یادگیری انتقالی و ثابت نگه‌داشتن وزن‌های اولیه لایه‌های استخراج ویژگی باعث کاهش چشم‌گیر نیاز محاسباتی در فرآیند آموزش شده است. در مرحله‌ی استنتاج، مدل تنها از بخش انتقال‌یافته‌ی VGG-۱۶ برای استخراج ویژگی‌ها استفاده می‌کند و لایه‌های کاملاً متصل با ساختار سبک‌تر طراحی شده‌اند تا حجم محاسبات کاهش یابد. در آزمایش‌ها، زمان استنتاج برای هر نمونه کمتر از چند میلی‌ثانیه اندازه‌گیری شد که نشان می‌دهد مدل قابلیت پیاده‌سازی مؤثر در محیط‌های IoT با توان پردازشی محدود را دارد.

٤-۵ مقایسه با سایر روش‌ها

همانطور که در جدول ۳ مشاهده می‌شود، روش ذکر شده در مقایسه با سایر روش‌ها از نظر صحت، دقت، فراخوانی و امتیاز_F۱ عملکرد بهتری از خود نشان داده است. برتری روش به دلیل استفاده از مدل ازپیش‌آموزش‌دیده‌شده VGG-۱۶، برای تشخیص نفوذ در IoT است، که با تنظیمات بهینه مدل برای داده‌های UNSW-NB۱۵، به دقت بالایی در شناسایی نفوذ رسیده است.

۵- نتیجه‌گیری

حملات شبکه‌های کامپیوتری تهدیدی جدی برای امنیت هستند. توسعه یک راه حل خودکار تشخیص نفوذ شبکه برای کاهش خطرات فعالیت‌های مخرب ضروری است. روش‌های سنتی موجود و الگوریتم‌های

یادگیری ماشین به اندازه کافی برای مشکلات تشخیص نفوذ شبکه مؤثر نیستند. در این مقاله، روشی مبتنی بر یادگیری انتقالی برای تشخیص نفوذ شبکه‌های IoT پیشنهاد شده است. برخی از لایه‌ها VGG-۱۶ از پیش بر روی مجموعه داده ImageNet آموزش داده شده، که در اولین مرحله وزن‌های آن را انتقال می‌دهیم. در مرحله دوم، این وزن‌ها را برای تشخیص نفوذ در شبکه‌های اینترنت اشیا بهینه‌سازی شده است تا به خصوصیات این شبکه‌ها که شامل محدودیت‌های منابع، تنوع پروتکل‌ها و معماری‌های مختلف است، پاسخ دهد. عملکرد مدل بر روی مجموعه داده‌ی UNSW-NB۱۵ و NSL-KDD ارزیابی شده است. این مجموعه داده شامل نمونه‌هایی از حملات مختص به شبکه‌های اینترنت اشیا است که توانایی مدل در شناسایی تهدیدات خاص این حوزه را به خوبی نشان می‌دهد. نتایج اثربخشی مدل را با محاسبه صحت، دقت، فراخوانی و امتیاز_F۱ نشان داده شده است. دقت بالای مدل در تشخیص حملات مرتبط با اینترنت اشیا نشان‌دهنده قابلیت‌های برتر این رویکرد در مقابله با چالش‌های امنیتی این شبکه‌ها اینترنت اشیا است.

در ادامه این پژوهش در آینده، با وجود نتایج مناسب حاصل از روش پیشنهادی مبتنی بر یادگیری انتقالی در شناسایی نفوذ در شبکه‌های اینترنت اشیا، می‌توان به توسعه آن بر اساس رفع دو محدودیت آن پرداخت. نخست، کارآیی مدل ممکن است در مواجهه با مجموعه‌داده‌های جدید که شامل الگوهای ترافیکی ناشناخته یا حملات نوظهور هستند، کاهش یابد، زیرا وزن‌های انتقال‌یافته‌ی مدل VGG-۱۶ بر اساس داده‌های تصویری آموزش دیده‌اند و ممکن است در شرایطی با ساختار آماری متفاوت عملکرد ایده‌آل نداشته باشند. دوم، پیاده‌سازی مدل در محیط‌های واقعی IoT با منابع محدود که ممکن است با چالش‌هایی مانند توان پردازشی پایین و محدودیت حافظه روبه‌رو شود. برای بهبود این موارد، می‌توان در تحقیقات آینده از روش‌های فشرده‌سازی مدل و یادگیری انتقالی تطبیقی[1] بهره گرفت تا مدل به‌صورت مؤثرتری برای سناریوهای بلادرنگ به‌کار گرفته شود.

مراجع

[1] X. Wu, *et al.*, "Threat analysis for space information network based on network security attributes: A review," *Complex & Intelligent Systems,* vol. 9, pp. 3429-3468, 2023.

[2] M. Lombardi, F. Pascale, and D. Santaniello, "Internet of things: A general overview between architectures, protocols and applications," *Information,* vol. 12, no. 2, Article ID: 87, 2021.

[3] M. Alkasassbeh and S. Al-Haj Baddar, "Intrusion detection systems: A state-of-the-art taxonomy and survey," *Arabian Journal for Science and Engineering,* vol. 48, pp. 10021-10064, 2023.

[4] M. Pradhan, C. K. Nayak, and S. K. Pradhan, "Intrusion detection system (IDS) and their types," In *Securing the internet of things: Concepts, methodologies, tools, and applications*: IGI Global, pp. 481-497, 2020.

[5] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cybersecurity,* vol. 4, Article ID:18, 2021.

[6] M. R. Ahmed, S. Shatabda, A. M. Islam, and M. T. I. Robin, *Intrusion Detection System in Software-Defined Networks Using Machine Learning and Deep Learning Techniques: A Comprehensive Survey*, Authorea Preprints, 2023.

[7] G. Kumar, K. Thakur, and M. R. Ayyagari, "MLEsIDSs: Machine learning-based ensembles for intrusion detection systems—A review," *The Journal of Supercomputing,* vol. 76, no. 11, pp. 8938-8971, Nov. 2020.

[8] A. Hkiri, *et al.* "Performance evaluation of mobile RPL-Based IoT networks under hello flood attack," *Electronics,* vol. 13, no. 11, Article ID: 2226, 2024.

[9] N. Gupta, V. Jindal, and P. Bedi, "CSE-IDS: Using cost-sensitive deep learning and ensemble algorithms to handle class imbalance in network-based intrusion detection systems," *Computers & Security,* vol. 112, pp. 102-499, Article ID: 102499, Jan. 2022.

[10] L. Alzubaidi, *et al.*, "Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions," *Journal of big Data,* vol. 8, Article ID: 53, 2021.

[11] I. Ullah, A. Ullah, and M. Sajjad, "Towards a hybrid deep learning model for anomalous activities detection in internet of things networks," *IoT,* vol. 2, no. 3, pp. 428-448, 2021.

[12] L. Santos, C. Rabadao, and R. Gonçalves, "Intrusion detection systems in Internet of Things: A literature review," in *Proc. 2018 13th Iberian Conf on Information Systems and Technologies*, 7 pp., Plasencia, Spain, 13-16 Jun. 2018.

[13] H. Jmila, G. Blanc, M. R. Shahid, and M. Lazrag, "A survey of smart home iot device classification using machine learning-based network traffic analysis," *IEEE Access,* vol. 10, pp. 97117-97141, 2022.

[14] A. Thakkar and R. Lohiya, "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions," *Artificial Intelligence Review,* vol. 55, pp. 453-563, 2022.

[15] S. Dargan, M. Kumar, M. R. Ayyagari, and G. Kumar, "A survey of deep learning and its applications: a new paradigm to machine learning," *Archives of Computational Methods in Engineering,* vol. 27, pp. 1071-1092, 2020.

[16] D. Swessi and H. Idoudi, "A survey on internet-of-things security: threats and emerging countermeasures," *Wireless Personal Communications,* vol. 124, no. 2, pp. 1557-1592, 2022.

[17] Z. Wang, Y. Lai, Z. Liu, and J. Liu, "Explaining the attributes of a deep learning based intrusion detection system for industrial control networks," *Sensors,* vol. 20, no. 14, Article ID: 3817, 2020.

[18] A. Hosna, *et al*., "Transfer learning: a friendly introduction," *Journal of Big Data,* vol. 9, no. 1, Article ID: 102, 2022.

[19] K. Kim, *et al*., "Deep Learning-Based IDSs," *Network Intrusion Detection using Deep Learning: A Feature Learning Approach,* pp. 35-45, 2018.

[20] L. Vu, Q. U. Nguyen, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, "Deep transfer learning for IoT attack detection," *IEEE Access,* vol. 8, pp. 107335-107344, 2020.

[21] T. V. Khoa, *et al*., "Deep transfer learning: A novel collaborative learning model for cyberattack detection systems in IoT networks," *IEEE Internet of Things Journal,* vol. 10, no. 10, pp. 8578-8589, 15 May 2023.

[22] W. Yutao, L. Zhongtian, B. Yi, L. Jie, X. Fangzheng, and B. Yu, "Internet of Things Intrusion Detection System based on Transfer Learning," in *Proc. IEEE 2nd Int. Conf. on Electronic Technology, Communication and Information*, pp. 25-30, Changchun, China, 27-29 May 2022.

[23] S. T. Mehedi, A. Anwar, Z. Rahman, K. Ahmed, and R. Islam, "Dependable intrusion detection system for IoT: A deep transfer learning based approach," *IEEE Trans. on Industrial Informatics,* vol. 19, no. 1, pp. 1006-1017, Jan. 2023.

[24] S. Choudhary and N. Kesswani, "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT," *Procedia Computer Science,* vol. 167, pp. 1561-1573, 2020.

[25] G. Kocher and G. Kumar, "Performance analysis of machine learning classifiers for intrusion detection using UNSW-NB15 dataset," *Comput. Sci. Inf. Technol,* vol. 10, no. 20, pp. 31-40, 2020.

[26] X. Larriva-Novo, V. A. Villagrá, M. Vega-Barbas, D. Rivera, and M. Sanz Rodrigo, "An IoT-focused intrusion detection system approach based on preprocessing characterization for cybersecurity datasets," *Sensors,* vol. 21, no. 2, Article ID: 656, 2021.

[27] R. A. Disha and S. Waheed, "A Comparative study of machine learning models for Network Intrusion Detection System using UNSW-NB15 dataset," in *Proc. Int. Conf. on Electronics, Communications and Information Technology*, 5 pp., Khulna, Bangladesh, 14-16 Sept. 2021.

[28] E. H. Salman, *et al.*, "An anomaly intrusion detection for high-density internet of things wireless communication network based deep learning algorithms," *Sensors,* vol. 23, no. 1, Article ID: 206, 2022.

[29] I. Ahmad, Q. E. Ul Haq, M. Imran, M. O. Alassafi, and R. A. AlGhamdi, "An efficient network intrusion detection and classification system," *Mathematics,* vol. 10, no. 3, Article ID: 530, 2022.

1. Adaptive Transfer Learning

[30] F. Türk, "Analysis of intrusion detection systems in UNSW-NB15 and NSL-KDD datasets with machine learning algorithms," *Bitlis Eren Üniversitesi Fen Bilimleri Dergisi,* vol. 12, no. 2, pp. 465-477, Jun. 2023.

[31] L. A. Maghrabi, "Automated network intrusion detection for Internet of things security enhancements," *IEEE Access,* vol. 12, pp. 30839-30851, 2024.

[32] K. Pramilarani and P. V. Kumari, "Cost based random forest classifier for intrusion detection system in Internet of things," *Applied Soft Computing,* vol. 151, Article ID: 111125, Jan. 2024.

[33] S. More, M. Idrissi, H. Mahmoud, and A. T. Asyhari, "Enhanced intrusion detection systems performance with UNSW-NB15 data analysis," *Algorithms,* vol. 17, no. 2, Article ID: 64, 2024.

آرمان سمیعی تحصیلات خود را در مقاطع کارشناسی و کارشناسی ارشد مهندسی برق گرایش الکترونیک به‌ترتیب در سال‌های ۱۳۹۹ و ۱۴۰۳ از دانشگاه آزاد اسلامی تهران مرکزی و دانشگاه علم و صنعت ایران به پایان رسانده است و هم‌اکنون در زمینه طراحی و توسعه مدل‌های یادگیری عمیق فعالیت می‌کند. نام‌برده در پروژه‌های پژوهشی خود به توسعه و پیاده‌سازی شبکه‌های عصبی برای تشخیص ناهنجاری، طبقه‌بندی داده‌ها و پردازش تصویر و همچنین به‌کارگیری روش‌های یادگیری عمیق در سامانه‌های تشخیص نفوذ پرداخته است. وی همچنین در زمینه بینایی ماشین و توسعه مدل‌های مبتنی بر شبکه‌های عصبی کانولوشنی فعالیت داشته است. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: یادگیری عمیق، یادگیری انتقالی، بینایی ماشین، پردازش تصویر، تشخیص ناهنجاری و سامانه‌های تشخیص نفوذ.

عرفان خدرصلح در سال ۱۳۹۷ مدرک کارشناسی مهندسی برق خود را از دانشگاه صنعتی جندی‌شاپور و در سال ۱۴۰۰ مدرک کارشناسی ارشد مهندسی برق خود را از دانشگاه علم و صنعت ایران دریافت نمود. نام‌برده پس از آن فعالیت‌های علمی و پژوهشی خود را در زمینه هوش مصنوعی لبه و بهینه‌سازی مدل‌های یادگیری ماشین و معماری شبکه‌های عصبی ادامه داده و در پژوهش‌های خود به توسعه و به‌کارگیری روش‌های یادگیری ماشین، یادگیری انتقالی و شتاب‌دهی سخت‌افزاری الگوریتم‌های هوشمند پرداخته است. زمینه‌های علمی و تحقیقاتی مورد علاقه ایشان عبارتند از: هوش مصنوعی لبه، بهینه‌سازی مدل‌های یادگیری ماشین و معماری شبکه‌های عصبی است.

هادی‌شهریار شاه‌حسینی در سال ۱۳۶۷ مدرک کارشناسی مهندسی برق – الکترونیک خود را از دانشکده فنی دانشگاه تهران و در سال ۱۳۷۲ مدرک کارشناسی ارشد مهندسی برق – الکترونیک را از دانشگاه آزاد تهران و مدرک دکترای مهندسی برق در سال ۱۳۷۸ از دانشگاه علم و صنعت ایران دریافت نمود. وی از همان سال ۱۳۷۸ به عنوان عضو هیأت علمی در دانشکده مهندسی برق دانشگاه علم و صنعت ایران مشغول به فعالیت می‌باشد. زمینه‌های علمی مورد علاقه نام‌برده پردازش موازی و معماری کامپیوتر، مدیریت شبکه‌های کامپیوتری، یادگیری ماشین و الگوریتم‌های تکاملی و هوشمند می‌باشد.