Journal of Applied And Basic Machine Intelligence Research (ABMIR)

پژوهش‌های نظری و کاربردی هوش ماشینی

سال دوم، شماره دوم، پاییز و زمستان ۱۴۰۳، صفحات۲۹ – ۱۷

ارائه راهکاری نوین برای طبقه‌بندی ترافیک رمزنگاری‌شده با بهره‌گیری از یادگیری عمیق

پویا ربیعی دولت‌آبادی[۱]، مصطفی بستام[۲*]، خدیجه آقاجانی[۲]

[۱]کارشناسی ارشد گروه مهندسی کامپیوتر، دانشکده فناوری و مهندسی، دانشگاه مازندران، بابلسر، ایران

[۲]استادیار گروه مهندسی کامپیوتر، دانشکده فناوری و مهندسی، دانشگاه مازندران، بابلسر، ایران

مقاله پژوهشی

تاریخ دریافت:
۱۴۰۳/۹/۲۵
تاریخ پذیرش:
۱۴۰۳/۱۱/۲۷

کلیدواژه‌ها:
یادگیری عمیق، تحلیل ترافیک شبکه، ترافیک رمزشده، مدل VGG16، مدیریت ترافیک شبکه

نویسنده‌مسئول:
Bastam@umz.ac.ir

چکیده

تحلیل ترافیک شبکه یکی از ارکان اساسی در بهبود امنیت و مدیریت کارآمد شبکه‌های کامپیوتری است. با توجه به گسترش روزافزون شبکه‌های کامپیوتری و پیچیدگی‌های ترافیک موجود در آن‌ها، شناسایی دقیق و سریع انواع ترافیک ازجمله ترافیک رمزنگاری‌شده، از اهمیت ویژه‌ای برخوردار است. در این راستا، استفاده از تکنیک‌های یادگیری ماشین می‌تواند ابزار قدرتمندی برای تحلیل و شناسایی دقیق الگوهای ترافیکی باشد. این مقاله به بررسی روش‌های پیشرفته شناسایی ترافیک در شبکه‌های کامپیوتری با بهره‌گیری از تکنیک‌های یادگیری ماشین پرداخته است. هدف اصلی این تحقیق، توسعه مدلی کارآمد و دقیق برای شناسایی و طبقه‌بندی انواع مختلف ترافیک شبکه، به‌ویژه ترافیک رمزنگاری‌شده، است. در این راستا، از مدل یادگیری عمیق VGG16 استفاده‌شده است. این مدل به دلیل ساختار لایه‌ای عمیق و توانایی تحلیل داده‌های حجیم، عملکرد برجسته‌ای در شناسایی الگوهای پیچیده ترافیک شبکه ارائه داده است. VGG16 قادر است با دقت بالا، انواع مختلف ترافیک شبکه را شناسایی و طبقه‌بندی کند، که این امر منجر به بهبود مدیریت ترافیک در شبکه می‌شود. در سناریوهای بررسی‌شده در این تحقیق، این مدل توانست دقت ۹۹ درصدی را در شناسایی ترافیک رمزنگاری‌شده به‌دست آورد.

: 10.22034/ ABMIR.2025.22525.1084

E-ISSN: 2821-2037

۱- مقدمه

در دنیای امروز، شبکه‌های کامپیوتری به بخش جدایی‌ناپذیر از زندگی دیجیتال تبدیل‌شده‌اند و با رشد روزافزون استفاده از اینترنت و ارتباطات آنلاین، حجم داده‌های ترافیکی که در این شبکه‌ها تولید می‌شود، به طرز چشمگیری افزایش‌یافته است. این داده‌ها نه‌تنها ازنظر حجمی زیاد هستند، بلکه به‌طور عمده ناهمگن و از منابع مختلفی چون دستگاه‌ها، برنامه‌های مختلف و سرویس‌های ابری ایجاد می‌شوند. این تنوع در داده‌ها باعث می‌شود که مدیریت و تحلیل ترافیک شبکه به‌ویژه به‌صورت بلادرنگ با چالش‌های پیچیده‌ای مواجه شود. ازجمله چالش‌ها می‌توان به شناسایی ترافیک رمزنگاری‌شده، تشخیص حملات سایبری و مدیریت منابع شبکه اشاره کرد که نیاز به راهکارهای دقیق و سریع دارد [۱].

تحلیل ترافیک شبکه به فرآیند شناسایی و بررسی الگوهای موجود در داده‌های عبوری از شبکه‌ها اشاره دارد. این تحلیل می‌تواند به روش‌های مختلفی انجام شود: ۱- روش‌های سنتی تحلیل ترافیک شبکه و ۲-تحلیل ترافیک رمزنگاری‌شده.

روش‌های سنتی تحلیل ترافیک معمولاً شامل استفاده از ابزارهای مانیتورینگ و تحلیل‌گرهای ترافیکی (مانند Wireshark، Tcpdump) برای تجزیه‌وتحلیل بسته‌ها[1] هستند. این ابزارها می‌توانند اطلاعاتی نظیر آدرس‌های IP مبدأ و مقصد، پروتکل‌های مورداستفاده، تعداد بسته‌ها و حجم داده‌ها را جمع‌آوری و تحلیل کنند. این روش‌ها برای ترافیک‌های غیر رمزنگاری‌شده یا ترافیک‌هایی که شفافیت بیشتری دارند مناسب هستند[۲, ۳]. با رشد روزافزون رمزنگاری ترافیک شبکه، تحلیل سنتی ترافیک شبکه با چالش‌های جدیدی مواجه شده است. تحلیل ترافیک رمزنگاری‌شده (مثل HTTPS ، VPN) به دلیل انتقال داده‌ها به‌صورت غیرقابل‌خواندن، با استفاده از روش‌های سنتی دشوار است. این چالش موجب می‌شود که استفاده از روش‌های مبتنی بر یادگیری ماشین به‌عنوان یک راهکار ضروری برای تحلیل این نوع ترافیک مطرح شود. تحلیل ترافیک رمزنگاری‌شده با استفاده از روش‌های یادگیری ماشین مزایای متعددی دارد، ازجمله شناسایی الگوهای پیچیده بدون نیاز به رمزگشایی، افزایش دقت در پردازش داده‌های حجیم و پیچیده، و کاهش نیاز به داده‌های برچسب‌دار که در تحلیل ترافیک رمزنگاری‌شده محدود هستند. این روش‌ها همچنین سریع‌تر و مقیاس‌پذیرتر از روش‌های سنتی هستند و امکان پردازش خودکار ترافیک شبکه را در زمان واقعی فراهم می‌کنند [۴-۹]. .یادگیری عمیق، به‌ویژه با استفاده از مدل‌هایی مانند شبکه‌های عصبی کانولوشنی(CNN)، توانایی شناسایی دقیق ویژگی‌های پنهان در داده‌های ترافیکی را دارد و به تحلیل و پیش‌بینی وضعیت شبکه کمک می‌کند. این روش‌ها نه‌تنها شناسایی ترافیک‌های مخرب را تسهیل می‌کنند، بلکه به بهبود مدیریت منابع شبکه نیز کمک می‌کنند[۱۰-۱۲].

در این مقاله، به‌طور ویژه به تحلیل کاربردهای یادگیری عمیق در شناسایی ترافیک شبکه و چالش‌های موجود در این حوزه خواهیم پرداخت. یکی از مدل‌های برجسته یادگیری عمیق که در این تحقیق مورداستفاده قرارگرفته است، معماری VGG[2] است. این معماری به‌عنوان یک شبکه عصبی پیچیده و عمیق (CNN) با ساختار لایه‌ای خود، در شناسایی الگوهای پیچیده ترافیکی عملکردی برجسته از خود نشان داده است. نوآوری و دستاورد اصلی این تحقیق، ترکیب مدل VGG16 با داده‌های ترافیکی تصویری (FlowPic) و داده‌های کمکی (Aux) برای شناسایی و طبقه‌بندی دقیق‌تر ترافیک رمزنگاری‌شده است. در این تحقیق، داده‌های ترافیکی ابتدا به‌طور عمدی به تصاویر FlowPic تبدیل‌شده‌اند تا از تکنیک‌های پردازش تصویر و قدرت مدل‌های شبکه عصبی کانولوشنی (CNN) برای شناسایی الگوهای پیچیده ترافیک شبکه بهره‌برداری شود. مدل VGG16، که به‌طورمعمول در شناسایی الگوهای پیچیده تصاویر به کار می‌رود، در این تحقیق به‌منظور شناسایی و طبقه‌بندی ترافیک رمزنگاری‌شده استفاده‌شده است. تبدیل ترافیک به تصاویر به‌ویژه به شناسایی الگوهای پیچیده کمک می‌کند، اما این تبدیل ممکن است برخی از ویژگی‌های زمانی ترافیک را نادیده بگیرد. برای جبران این نقص، از داده‌های کمکی (Aux)استفاده‌شده است که ویژگی‌های زمانی ترافیک را پوشش

[1] Packet-level Analysis

[2] Visual Geometry Group

می‌دهند و به‌طور جامع‌تری مدل را در شناسایی ترافیک رمزنگاری‌شده تقویت می‌کنند. این تحقیق، با دستیابی به‌دقت ۹۹,۳۷ درصد در طبقه‌بندی، گامی مهم در ارتقای تحلیل ترافیک رمزنگاری‌شده به شمار می‌آید. این مدل نه‌تنها توانسته است دقت شناسایی ترافیک را به‌طور قابل‌توجهی افزایش دهد، بلکه امکان پیش‌بینی و مدیریت بهتر ترافیک در شبکه‌های کامپیوتری را نیز فراهم کرده است.

این مقاله، به شرح ذیل سازمان‌دهی شده است: در بخش ۲، مطالعات پیشین مورد بررسی قرار می‌گیرند تا زمینه‌ای برای درک بهتر پژوهش فراهم گردد. بخش ۳ به رویکرد پیشنهادی تحقیق اختصاص دارد و رویکردهای مختلف طبقه‌بندی ترافیک شبکه با استفاده از یادگیری عمیق تشریح می‌شود. در بخش ٤، نتایج آزمایش‌ها به‌طور کامل ارائه و تحلیل می‌شوند و درنهایت، بخش ۵ به نتیجه‌گیری و پیشنهادهایی برای پژوهش‌های آتی اختصاص دارد.

۲- کارهای مرتبط

ون تانگو و همکاران [۱۳]، روش جدیدی برای طبقه‌بندی ترافیک QUIC[1] با استفاده از شبکه‌های عصبی کانولوشنی پیشنهاد کرده‌اند. این روش با ترکیب ویژگی‌های مبتنی بر جریان و بسته، شناسایی دقیق سرویس‌های مبتنی بر QUIC مانند Google Hangout، Chat، Voice Calls، YouTube، File Transfer و Google Play Music را ممکن می‌سازد. این رویکرد شامل دو مرحله طبقه‌بندی است: ابتدا از ویژگی‌های مبتنی بر جریان برای طبقه‌بندی گروه‌ها استفاده می‌شود، سپس ویژگی‌های مبتنی بر بسته و شبکه‌های CNN برای طبقه‌بندی دقیق‌تر به کار گرفته می‌شوند. این روش ترافیک رمزگذاری‌شده را با پیش‌پردازش بسته‌های QUIC، استخراج ویژگی‌های جریان و بسته، و استفاده از CNN برای کاهش ابعاد و طبقه‌بندی به‌طور مؤثر پردازش می‌کند، آن‌ها مقدار F1-Score ۹۹,۲٤ درصد را به‌عنوان نتیجه ارائه داده‌اند.

شهباز رضایی و شین لئو [۱٤]، یک روش یادگیری نیمه‌نظارت‌شده برای طبقه‌بندی ترافیک شبکه پیشنهاد می‌کنند که با استفاده از مجموعه داده‌های بدون برچسب برای پیش‌آموزش، به‌دقت بالا با حداقل داده‌های برچسب‌دار دست می‌یابد. این روش شامل دو مرحله است: ابتدا، یک شبکه عصبی کانولوشنی (CNN) بر روی یک مجموعه داده بزرگ بدون برچسب پیش‌آموزش داده می‌شود تا ویژگی‌های آماری مانند میانگین طول بسته‌ها و زمان بین رسیدن بسته‌ها را از ویژگی‌های سری زمانی نمونه‌برداری شده پیش‌بینی کند. این مدل پیش‌آموزش‌دیده الگوهای عمومی ترافیک را بدون نیاز به داده‌های برچسب‌دار استخراج می‌کند. در مرحله بعد، پارامترهای یاد گرفته‌شده مدل به یک مجموعه داده کوچک برچسب‌دار منتقل‌شده و با آن تنظیم دقیق می‌شود که نیاز به برچسب‌گذاری را به‌طور چشمگیری کاهش داده و عملکرد بالایی را حفظ می‌کند. برای بهینه‌سازی تحلیل بسته‌ها، نویسندگان سه تکنیک نمونه‌برداری شامل گام ثابت، تصادفی، و افزایشی را بررسی می‌کنند که بسته‌ها را از بخش‌های مختلف جریان انتخاب می‌کنند، به‌جای اینکه تنها به بسته‌های اولیه تکیه شود. این رویکرد باعث می‌شود مدل الگوهای متنوع ترافیک، ازجمله رفتارهای کاربر که در میانه جریان رخ می‌دهد را شناسایی کند. روش پیشنهادی با دقت نزدیک به روش‌های پیشرفته، ازجمله دقت ۹۸,۵۳ درصد برای طبقه‌بندی ترافیک QUIC کارایی خود را در سناریوهایی با داده‌های برچسب‌دار محدود نشان داده است.

ایال هورورویتز و همکاران [۱۵] روش جدیدی برای طبقه‌بندی ترافیک با استفاده از تقویت‌های mini-FlowPic ارائه دادند که به‌طور مؤثر به چالش کمبود داده‌های برچسب‌دار پاسخ می‌دهد. این روش از FlowPic، یک نمایش تصویری مبتنی بر هیستوگرام دوبعدی از ترافیک شبکه، استفاده کرده و آن را با mini-FlowPics با اندازه کوچک‌تر برای کاهش هزینه‌های محاسباتی گسترش می‌دهد. با بهره‌گیری از یادگیری نمایشی متضاد بدون نظارت از طریق چارچوب SimCLR، این روش مدلی ایجاد می‌کند که در آن نمونه‌های مشابه به هم نزدیک می‌شوند، و امکان طبقه‌بندی تنها با چند نمونه برچسب‌دار در هر کلاس را فراهم می‌سازد. برای بهبود کارایی آموزش، نویسندگان تکنیک‌های تقویتی خاصی را معرفی می‌کنند که رفتارهای شبکه را شبیه‌سازی می‌کند، ازجمله تغییرات در زمان رفت‌وبرگشت (RTT[2])، تغییرات

[1] Quick UDP Internet Connections

[2] Round Trip Time

زمانی، و از دست دادن بسته‌ها، که عملکردی بهتر از تقویت‌های تصویری سنتی ارائه می‌دهد. این مطالعه اثربخشی این روش را درمجموعه داده‌هایی مانند QUIC و ISCX نشان می‌دهد که به‌دقتی تا ۹۴,۵ درصد دست می‌یابد. این نوآوری راه‌حلی عملی و مقیاس‌پذیر برای طبقه‌بندی ترافیک رمزگذاری‌شده، به‌ویژه در سناریوهایی با کمبود داده‌های برچسب‌دار، ارائه می‌کند.

در مقاله [۱۶]، FlowPic به‌عنوان یک روش نوآورانه برای طبقه‌بندی ترافیک رمزگذاری‌شده و شناسایی اپلیکیشن‌ها معرفی‌شده است. در این روش، داده‌های جریان شبکه به هیستوگرام‌های دوبعدی تبدیل می‌شوند که FlowPic نامیده شده و به یک شبکه عصبی کانولوشنی برای طبقه‌بندی وارد می‌شوند. این هیستوگرام‌ها با ترسیم اندازه بسته‌ها در مقابل زمان رسیدن آن‌ها ساخته‌شده و ویژگی‌های زمانی و اندازه‌ای ترافیک را ثبت می‌کنند. این نمایه جدید نیاز به ویژگی‌های دستی‌سازی‌شده را حذف کرده و از توانایی‌های تکنیک‌های طبقه‌بندی تصویر بهره می‌برد. این مطالعه نشان می‌دهد که FlowPic می‌تواند با چالش‌های مختلفی ازجمله دسته‌بندی ترافیک، شناسایی اپلیکیشن و تکنیک‌های رمزگذاری مانند VPN و Tor به‌خوبی مقابله کند. نتایج چشمگیری ازجمله دقت ۹۹,۷ درصد برای طبقه‌بندی اپلیکیشن‌های VoIP و ویدیو بر روی ترافیک VPN و بیش از ۹۶ درصد برای دسته‌بندی ترافیک غیر-VPN به‌دست‌آمده است. مهم‌تر از همه، این روش حتی برای اپلیکیشن‌ها و انواع ترافیکی که در مرحله آموزش‌دیده نشده‌اند، عملکرد قابل‌اعتمادی دارد و توانایی تعمیم‌دهی بالا بدون نیاز به آموزش اضافی را نشان می‌دهد. این رویکرد گامی مهم در طبقه‌بندی ترافیک رمزگذاری‌شده است که هم مسائل مربوط به حریم خصوصی و هم کارایی محاسباتی را مدنظر قرار داده است.

درمجموع باوجود پیشرفت‌های چشمگیر در طبقه‌بندی ترافیک رمزنگاری‌شده، برخی چالش‌ها همچنان پابرجا هستند. یکی از مسائل اصلی، از دست رفتن بخشی از اطلاعات در فرآیندهایی مانند تبدیل داده‌ها به تصاویر در روش‌هایی مانندFlowPic است که می‌تواند بر دقت نهایی مدل تأثیر بگذارد. علاوه بر این، مدل‌های موجود اغلب در تعمیم‌پذیری به الگوهای ترافیکی ناشناخته یا رفتارهای جدید برنامه‌ها ضعف دارند، به‌ویژه زمانی که این الگوها در داده‌های آموزشی نمایان نیستند. همچنین، ادغام وابستگی‌های متنی و زمانی در یک چارچوب یکپارچه کمتر موردتوجه قرارگرفته است. این شکاف‌ها نیاز به توسعه چارچوبی را برجسته می‌کند که نه‌تنها دقت و کارایی را ارتقا دهد، بلکه از تکنیک‌های پیشرفته برای پوشش‌دهی بهتر به تنوع ترافیک رمزنگاری‌شده استفاده کند و محدودیت‌های موجود را کاهش دهد.

در پژوهشی که اخیراً انجام‌شده [۱۷]، طبقه‌بندی ترافیک شبکه رمزگذاری‌شده Tor و غیر Tor-بررسی‌شده است. این تحقیق بر ویژگی‌های خاص ترافیک Tor تمرکز دارد که به‌دلیل استفاده از رمزگذاری لایه‌ای چندگانه، از ترافیک‌های دیگر متمایز می‌شود. در ابتدا، فرض بر این بود که تفاوت قابل‌توجهی بین بسته‌های رمزگذاری‌شده Tor و غیر Tor-وجود ندارد. اما تحلیل آماری نشان داد که این دو نوع ترافیک ویژگی‌های متمایز دارند، به‌ویژه در نمایش‌های هگزادسیمال. در این مطالعه، الگوریتم‌های یادگیری برای طبقه‌بندی ترافیک بر اساس ویژگی‌های استخراج‌شده از بسته‌های رمزگذاری‌شده استفاده شدند. نتایج نشان می‌دهند که روش‌های سنتی در تمایز بین داده‌های رمزگذاری‌شده یک‌لایه و سه‌لایه مشکل دارند، درحالی‌که روش پیشنهادی با شناسایی الگوهای هگزادسیمالی، دقت بالایی در طبقه‌بندی ترافیک Tor از سایر ترافیک‌های رمزگذاری‌شده به دست می‌آورد. مقاله [۱۸] دو تکنیک نوین افزایش داده را معرفی می‌کند که هدف آن‌ها بهبود طبقه‌بندی ترافیک اینترنت رمزگذاری‌شده است. نویسندگان به چالش‌هایی اشاره می‌کنند که ناشی از توسعه سریع پروتکل‌ها و رمزگذاری است و منجر به محدودیت دسترسی به مجموعه داده‌های آموزشی می‌شود. تکنیک میانگین‌گیری با ترکیب میانگین نمونه‌ها در یک کلاس، نمونه‌های مصنوعی جدیدی تولید می‌نماید و تنوع مجموعه داده را افزایش می‌دهد. آزمایش‌های انجام‌شده روی مجموعه داده‌های آکادمیک و تجاری نشان‌دهنده بهبود عملکرد مدل‌ها است. یافته‌ها تأکید دارند که این روش‌ها می‌توانند محدودیت‌های داده‌های موجود را رفع نمایند و دقت طبقه‌بندی ترافیک رمزگذاری‌شده را افزایش دهند. جدول ۱ به‌طور خلاصه مطالعات انجام‌شده را بررسی و مدل پیشنهادی را با آن‌ها مقایسه

می‌کند. مقایسه نتایج مدل پیشنهادی با روش‌های اخیر در تحلیل ترافیک رمزنگاری‌شده نشان می‌دهد که استفاده از یادگیری عمیق و ترکیب داده‌های تصویری و کمکی (Aux) توانسته است دقت مدل را به‌طور قابل‌توجهی افزایش دهد. این تحقیق با دستیابی به‌دقت ۹۹,۳۷ درصد در شناسایی ترافیک رمزنگاری‌شده نسبت به کارهای پیشین پیشرفت چشمگیری را نشان می‌دهد.

جدول ۱: مقایسه مدل پیشنهادی با مطالعات پیشین در زمینه تحلیل ترافیک رمزنگاری‌شده

مدل پیشنهادی	شهباز رضایی و شین لئو[۱۴]	هورووینتز و همکاران[۱۵]	شاپیرا و همکاران[۱۶]	زیون و همکاران [۱۸]	کورود[۱۷]	ون تانگو و همکاران[۱۳]	ویژگی‌ها / روش‌ها
✓	✗	✗	✗	✗	✗	✗	پشتیبانی و استفاده از داده‌های کمکی
✓	✓	✓	✗	✗	✗	✓	کارایی در داده‌های برچسب‌دار محدود
✓	✗	✗	✗	✗	✗	✗	پشتیبانی از انتقال یادگیری
✓	✓	✓	✓	✓	✗	✓	مقیاس‌پذیری
✓	✓	✓	✗	✗	✗	✗	تعمیم‌پذیری به ترافیک ناشناخته
✓	✓	✓	✓	✓	✗	✗	مدیریت تغییرات شبکه
✓	✗	✗	✗	✗	✗	✗	از دست نرفتن اطلاعات در پیش‌پردازش

۳- رویکرد پیشنهادی

در این بخش، رویکردهای مختلفی که در این تحقیق برای شناسایی و طبقه‌بندی ترافیک شبکه با استفاده از یادگیری عمیق به کار گرفته‌شده‌اند، به‌تفصیل شرح داده می‌شود. ابتدا فرآیند پیش‌پردازش داده‌ها و آماده‌سازی مجموعه داده توضیح داده می‌شود. سپس، دو نوع داده اصلی شامل داده‌های تصویری (FlowPic) و داده‌های کمکی (Aux) معرفی می‌شوند که به‌طور هم‌زمان برای تقویت قابلیت مدل در شناسایی دقیق‌تر ترافیک شبکه، به‌ویژه ترافیک رمزنگاری‌شده، استفاده‌شده‌اند. در ادامه، جزئیات معماری شبکه عصبی VGG16 و نحوه ترکیب این داده‌ها برای بهبود عملکرد مدل، بیان خواهد شد. هدف از این بخش، تشریح مراحل آماده‌سازی داده‌ها، پیاده‌سازی مدل و ترکیب اطلاعات به‌منظور دستیابی به نتایج دقیق‌تر در تحلیل ترافیک شبکه است. در مرحله اول، عملیات پیش‌پردازش داده بر روی یک فایل متنی ۱,۵ گیگابایتی دربرگیرنده مجموعه داده[1] UCDAVIS19 [۲۲] انجام خواهد شد. در این راستا، داده‌های متنی به فرمت CSV تبدیل می‌شوند که برای تحلیل‌های بعدی بسیار مناسب‌تر است. همچنین در این مرحله، داده‌ها برای کاهش حجم و تمرکز بر جزئیات مهم‌تر فیلتر می‌شوند؛ به‌عنوان مثال، بازه‌های زمانی مشخص (۱۵ ثانیه[2] [۱۸–۲۰]) از داده‌ها استخراج می‌گردند که این تکنیک در

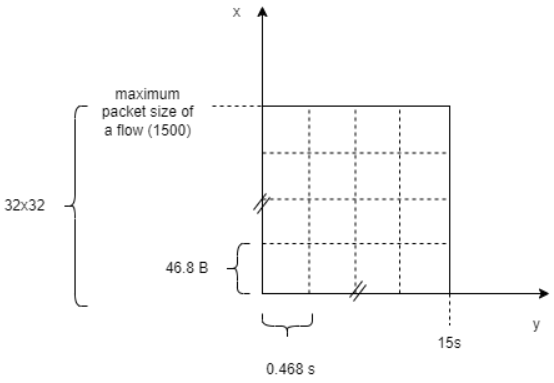
[1] Dataset

[2] زمان ۱۵ ثانیه مطابق با پژوهش‌های مشابه انتخاب گردیده است.

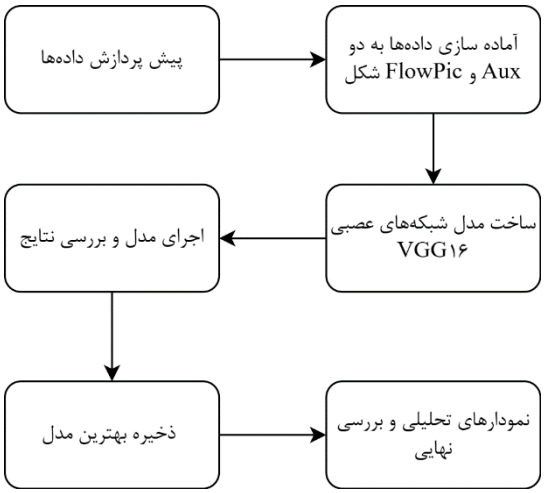
کاربردهایی مانند پردازش صوت و ویدیو رایج است. برای درک و پیش‌بینی رفتار ترافیک شبکه و بهبود الگوریتم‌های مدیریت ترافیک، تحلیل دقیق زمان شروع جریان اهمیت بسزایی دارد درواقع رفتار منحصربه‌فرد ترافیک هر جریان عمدتاً به بازه زمانی شروع جریان وابسته است [۲۱]. این وابستگی ناشی از ماهیت پویا و متغیر ترافیک شبکه است، که در آن عوامل مختلفی مانند شرایط لحظه‌ای شبکه، تعداد اتصالات هم‌زمان، میزان ازدحام، و اولویت‌بندی بسته‌ها بر رفتار جریان تأثیر می‌گذارند [۲۳]. پس از پردازش و فیلترسازی که به‌منظور کاهش پیچیدگی داده‌ها و بهبود عملکرد مدل‌های یادگیری ماشین انجام می‌شود. داده‌ها را به شکل ساختاریافته و تمیز آماده می‌کند، داده‌های مختلف باهم ترکیب یا هماهنگ می‌شوند تا یک مجموعه داده یکپارچه و ساختاریافته ایجاد شود.

در مرحله بعد، داده‌ها به دودسته Aux و FlowPic تقسیم می‌شوند. FlowPic یک نمایش تصویری از جریان داده‌ها است. بدین شکل که جریان داده تنها با سه ویژگی در شبکه، به روی دو محور زمان و اندازه بسته، نقش می‌گیرد. ویژگی اول زمان رسیدن بسته، ویژگی دوم اندازه بسته و ویژگی سوم، تعداد بسته در واحد زمان مشخص‌شده، است. محور زمان درنهایت ۱۵ ثانیه را نشان می‌دهد اما محور اندازه بسته، با توجه به هر جریان متغیر بوده و توزیع متفاوتی را برای هر جریان ارائه می‌دهد. به‌طور مثال اگر در یک جریان اندازه ماکسیمم یک بسته ۱۰۰۰ بایت باشد، مقیاس محور با این اندازه تنظیم می‌شود و چنانچه ماکسیمم یک بسته در یک جریان ۱۵۰۰ بایت باشد نیز مقیاس با این اندازه منطبق می‌شود. درنهایت این تصاویر در اندازه ۳۲*۳۲ تولید می‌شوند. برای رسیدن به این اندازه می‌بایست اندازه نهایی هر محور به ۳۲ تقسیم شود تا اندازه هر قسمت از پیکسل‌ها مشخص گردد. در اینجا با توجه به اینکه زمان همواره در آستانه ۱۵ ثانیه است. هر قسمت زمانی در تصاویر جریان ما حدود ٤٥٨ هزارم ثانیه را نشان می‌دهد. شکل ۱ ساختار FlowPic را نشان می‌دهد.

داده‌های Aux به‌عنوان یک مجموعه داده کمکی از دو ویژگی اصلی زمان (Time) و اندازه بسته‌ها (Packet Size) استخراج شده است. برای هر جریان داده که به بازه‌های ۱۵ ثانیه‌ای تقسیم‌شده است، این دو ویژگی پردازش می‌شوند تا اطلاعات آماری مفیدی به دست آید. به‌طور خاص، برای هر بازه، چهار شاخص حداکثر (Max)، حداقل (Min) ، انحراف معیار (Std) ، و میانگین (Avg) محاسبه می‌شوند. این محاسبات برای هر دو ویژگی زمان و اندازه بسته انجام می‌شود، که درمجموع ۸ ویژگی عددی جدید تولید می‌کند. این ویژگی‌ها به‌صورت یکپارچه ذخیره‌شده و به مجموعه داده‌ای موسوم به Aux تبدیل می‌شوند که نمایی خلاصه و مفید از جریان‌های داده ارائه می‌دهد.



شکل (۱) :شمای تشکیل FlowPic



شکل (۲): فلوچارت کلی

هدف از تولید داده‌های Aux، ارائه اطلاعات عددی تکمیلی به مدل است که رفتار کلی جریان‌ها، ازجمله تغییرات زمانی و حجمی، را به‌خوبی نشان می‌دهد. این داده‌ها در کنار داده‌های تصویری (FlowPic) به مدل یادگیری عمیق کمک می‌کنند تا علاوه بر تحلیل الگوهای تصویری، از اطلاعات عددی و تحلیلی برای بهبود

پیش‌بینی‌ها بهره‌مند شود. به‌این‌ترتیب، Aux و FlowPic یک نمای مکمل و جامع از داده‌ها فراهم می‌کنند که به یادگیری و تصمیم‌گیری دقیق‌تر مدل کمک می‌کند. درواقع در این مقاله سعی شده است تا ترافیک شبکه متعلق به هر جریان تبدیل به تصویر شود و با استفاده از روش‌های مؤثر و کارا در پردازش تصویر، ترافیک شبکه رمز شده متعلق به هر جریان شناسایی شود. شکل ۲، یک نمای شماتیک از رویکرد پیشنهادی در این مقاله است.

۳-۱ شبکه عصبی VGG16

در این تحقیق، به‌منظور تحلیل ترافیک شبکه از شبکه عصبی کانولوشنی (CNN) استفاده‌شده است. به‌طورمعمول، شبکه‌های CNN برای پردازش داده‌هایی با ویژگی‌های مکانی طراحی می‌شوند. در این مقاله، ترافیک شبکه ابتدا به تصاویر FlowPic تبدیل‌شده‌اند که ویژگی‌های زمانی و اندازه‌ای بسته‌ها را در هر بازه زمانی خاص نمایش می‌دهند. این تصاویر به‌عنوان ورودی به شبکه CNNداده می‌شوند تا مدل بتواند الگوهای پیچیده ترافیک رمزنگاری‌شده را شناسایی کند. این رویکرد به‌ویژه برای شناسایی رفتارهای پیچیده ترافیک شبکه در طول زمان مؤثر است، زیرا تصاویر FlowPic اطلاعات زمانی ترافیک را به‌طور تصویری نمایان می‌کنند، درحالی‌که ویژگی‌های مربوط به‌اندازه بسته‌ها نیز در آن‌ها قابل مشاهده است.

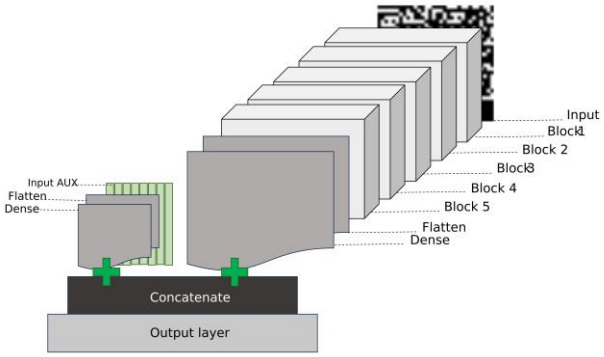
VGG16 یک شبکه عصبی پیچشی (CNN) است که در سال ۲۰۱٤ توسط کارن سیمونیان و اندرو زیسرمن از دانشگاه آکسفورد معرفی شد. این مدل با استفاده از ۱۳ لایه کانولوشنی و ۳ لایه کاملاً متصل، درمجموع ۱٦ لایه، به‌دقت ۹۲,۷٪ در تشخیص تصاویر مجموعه داده ImageNet دست‌یافت. ویژگی بارز VGG16 استفاده از فیلترهای کوچک ۳×۳ در تمام لایه‌های کانولوشنی است که امکان استخراج ویژگی‌های پیچیده را فراهم می‌کند. باوجود تعداد بالای پارامترها (حدود ۱۳۸ میلیون)، این مدل به‌طور گسترده در وظایف مختلف بینایی کامپیوتر مانند طبقه‌بندی تصاویر و استخراج ویژگی‌ها مورداستفاده قرارگرفته است [۲۳، ۲٤]. باوجوداینکه مدل VGG16 به‌طورمعمول در زمینه بینایی کامپیوتر برای شناسایی تصاویر حیوانات درImageNet استفاده می‌شود، در این تحقیق از این مدل برای شناسایی الگوهای پیچیده در ترافیک رمزنگاری‌شده استفاده‌شده است. داده‌های ترافیکی با استفاده از روش FlowPic به تصاویر تبدیل‌شده‌اند که ویژگی‌های مهم ترافیک را به‌طور تصویری نمایش می‌دهند. این ویژگی‌ها امکان شناسایی دقیق‌تر الگوهای ترافیک را فراهم می‌کنند که VGG16قادر به تحلیل آن‌ها به‌طور مؤثر است. استفاده از شبکه VGG16در این مدل به دلیل توانایی بالای آن در استخراج ویژگی‌های پیچیده از داده‌های تصویری مانند تصاویر تولیدشده توسط FlowPic است. معماری ساده و مؤثر VGG16 با لایه‌های کانولوشنی کوچک (۳×۳) به‌صورت متوالی، امکان شناسایی تدریجی ویژگی‌ها را فراهم می‌کند و برای تحلیل الگوهای پیچیده ترافیک رمزنگاری‌شده مناسب است. این شبکه به دلیل عملکرد اثبات‌شده در وظایف طبقه‌بندی و توانایی تطبیق با داده‌های تصویری، انتخابی ایده‌آل برای شناسایی الگوهای موجود در ترافیک رمزنگاری‌شده است. تبدیل داده‌های ترافیکی به تصاویر FlowPicممکن است برخی ویژگی‌های زمانی ترافیک را نادیده بگیرد. به‌منظور جبران این نقص، در این تحقیق از داده‌های کمکی (Aux)استفاده کرده‌ایم که ویژگی‌های زمانی ترافیک را پوشش می‌دهند. این داده‌های کمکی به مدل این امکان را می‌دهند که رفتارهای پویای شبکه را نیز تحلیل کرده و درنتیجه شناسایی دقیق‌تری از ترافیک رمزنگاری‌شده انجام دهد.

۳-۲ مدل پیشنهادی

در مدل پیشنهادی، داده‌های کمکی (AUX) نقش مهمی در غنی‌سازی ویژگی‌های ورودی برای بهبود دقت مدل ایفا می‌کنند. همان‌طور که در ابتدای این بخش توضیح داده شد، ابتدا داده‌های AUX وارد یک لایه Flatten می‌شوند تا به یک بردار یک‌بعدی تبدیل شوند. این مرحله تضمین می‌کند که داده‌ها برای پردازش در لایه‌های بعدی مناسب باشند. سپس این بردار از یک لایه Dense عبور می‌کند، که با اعمال یک ترکیب خطی و غیرخطی، ویژگی‌های کلیدی را از این داده‌ها استخراج و بهینه می‌کند.

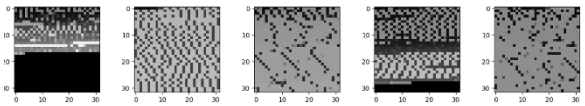
در ادامه، خروجی حاصل از داده‌های AUX با خروجی داده‌های تصویری، که از بخش دیگری از مدل (شبکه CNN مانند VGG16) به‌دست‌آمده است، ترکیب می‌شود. این ترکیب با استفاده از عملیات Concatenateانجام می‌شود که باعث ادغام

اطلاعات متنوع از دو منبع مختلف می‌گردد. این رویکرد به مدل امکان می‌دهد که نه‌تنها از ویژگی‌های غنی موجود در داده‌های تصویری بهره‌برداری کند، بلکه اطلاعات تکمیلی و زمینه‌ای موجود در داده‌های AUX را نیز در تصمیم‌گیری نهایی لحاظ کند. این ادغام داده‌ها یک مرحله کلیدی در طراحی مدل است که با هدف تقویت یادگیری و افزایش دقت در شناسایی و طبقه‌بندی ترافیک رمزنگاری‌شده انجام می‌شود. شکل ۲ مدل پیشنهادی را نشان می‌دهد.



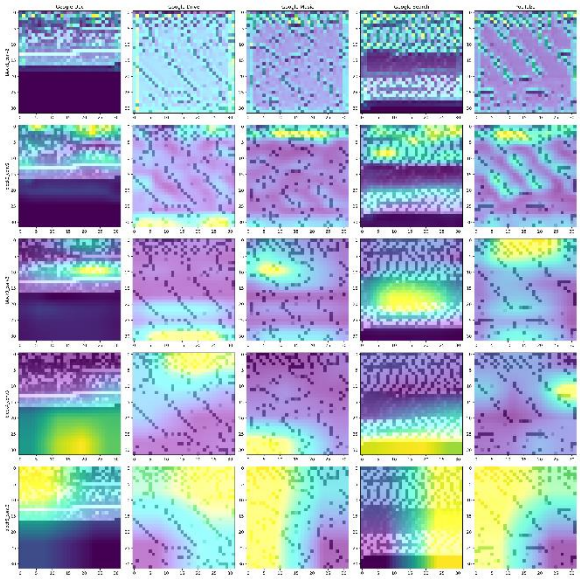
شکل (۳): مدل پیشنهادی

ورودی مدل به‌صورت تصاویر (FlowPic) بوده و با توجه به ساختار شبکه عصبی VGG در پنج بلوک، عملیات استخراج ویژگی انجام می‌گیرد و سپس بعد از ورود داده‌های AUX و ادغام جواب نهایی در پنج کلاس موجود درمجموعه داده UCDAVIS19 طبقه‌بندی می‌گردد. همان‌طور که قبلاً اشاره شد، تصاویر دارای ابعاد ۳۲*۳۲ بوده نمایی از تبدیل جریان‌ها به FlowPic در شکل ٤ آمده است.



شکل (٤): نمایی از FlowPic ایجادشده

انتخاب این شبکه به‌طور اتفاقی نبوده است و بر اساس آزمایش‌های قبلی و نیازهای خاص، داده‌ها به این شبکه اختصاص یافته است. روش‌هایی مانندNaïve Bayes ، به دلیل عدم در نظر گرفتن وابستگی‌های میان داده‌ها، نتوانستند نتایج مطلوبی در این آزمایش ارائه دهند؛ زیرا ماهیت داده‌های استفاده‌شده ذاتاً وابسته است. روش‌های دیگری مانند درخت تصمیم و جنگل‌های تصادفی به‌طور طبیعی نتایج بهتری ارائه کردند، اما در مقایسه با روش‌های پیشین و پژوهش‌های دیگر محققین، نتایج آن‌ها نیز چشمگیر نبودند. با توجه به‌دقت‌های بالایی که دیگر محققین بر روی این دیتاست به دست آورده بودند و الهام از روش‌های موفق بر روی دیتاست‌های دیگر، درنهایت آزمایش این شبکه و ادغام آن با داده‌هایی که قبلاً در پژوهش‌های دیگر نادیده گرفته می‌شد، توانست نتیجه قابل قبولی ارائه دهد.

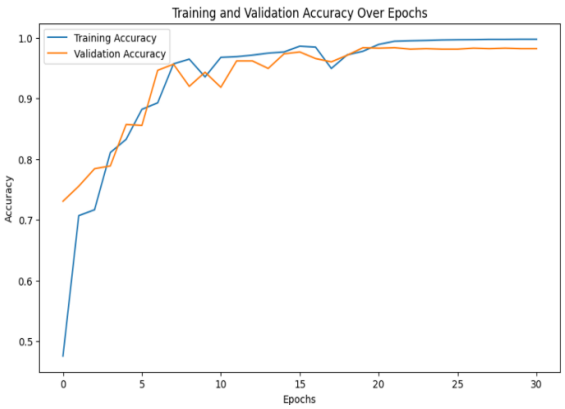


شکل (٥): نقشه گرمایی تشخیص ویژگی‌ها در هر بلوک

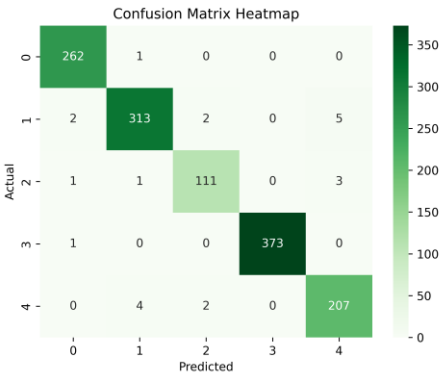
٤- ارزیابی مدل

مجموعه داده استفاده‌شده در این پژوهش UCDAVIS19 است [١٤]. این مجموعه داده که در آزمایشگاه دانشگاه کالیفرنیا، دیویس جمع‌آوری‌شده است، اطلاعاتی از پنج سرویس محبوب گوگل (Google Drive، YouTube، Google Docs، Google Search و Google Music) را شامل می‌شود. داده‌ها با استفاده از سیستم‌های مختلف شامل ویندوز ۷، ۸، ۱۰ و اوبونتو ١٦,٤ و ۱۷ گردآوری شده‌اند. برای شبیه‌سازی رفتار انسانی، اسکریپت‌هایی با ابزارهای Selenium WebDriver و AutoIt نوشته شده است که امکان جمع‌آوری حجم زیادی از داده را بدون نیاز به تلاش دستی فراهم می‌کند. در مرحله پیش‌پردازش، تمامی ترافیک‌های خارج از دسته‌بندی مشخص‌شده حذف و جریان‌های داده برچسب‌گذاری شده‌اند، این مجموعه داده با مقایسه روش‌های نظارت کامل و

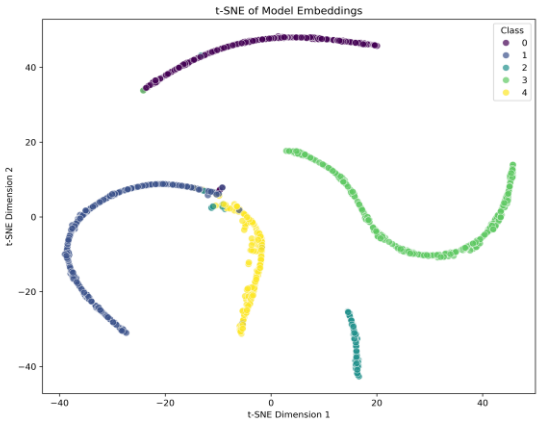
نیمه‌نظارت، فرصت ارزشمندی برای تحقیق در زمینه تحلیل ترافیک شبکه و یادگیری ماشین فراهم می‌کند. مطابق با شکل ۵ در لایه‌های اولیه (ردیف اول یعنی Block1)، شبکه ویژگی‌های ساده و ابتدایی مثل لبه‌ها، بافت‌ها و الگوهای ساده را شناسایی می‌کند. نقشه‌های گرمایی این لایه‌ها معمولاً نواحی گسترده‌ای از تصویر را پوشش می‌دهند و تمرکز خاصی روی بخش‌های کوچک‌تر ندارند. در لایه‌های میانی (مثل Block2،Block3) شبکه ویژگی‌های پیچیده‌تری مثل اشکال و ساختارهای جزئی‌تر را شناسایی می‌کند. نقشه‌های گرمایی در این لایه‌ها به‌مرور متمرکزتر شده و بخش‌های خاص‌تری از تصویر را برجسته می‌کنند. اما در لایه‌های عمیق‌تر (مثل Block4، Block5)، شبکه بر ویژگی‌های سطح بالاتری تمرکز می‌کند که به‌طور مستقیم با دسته مرتبط هستند. این اظهارات با توجه به نتایج به‌دست‌آمده از شکل، قابل استنباط است. دقت مدل در این روش به ۹۸,۳۷ درصد رسیده است که نسبت به مدل‌های قبلی افزایش داشته است. نمودار دقت داده تست و اعتبار سنجی در شکل ٦ آمده است.



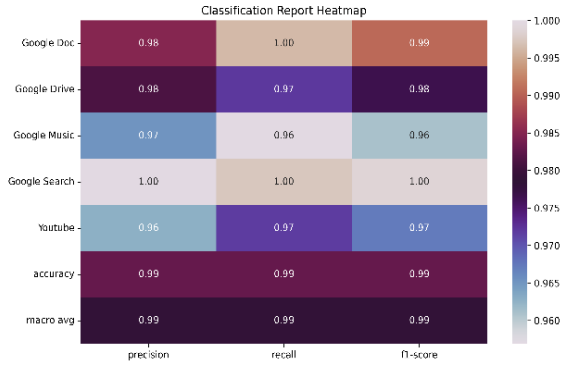
شکل (٦): نمودار دقت مدل



شکل (۷): ماتریس سردرگمی



شکل (۸): نمودار t-SNE لایه انتهایی



شکل (۹): نمودار نقشه-گرمایی ارزیابی مدل

برای ارزیابی مدل، از ماتریس سردرگمی استفاده‌شده است که به‌طور دقیق نحوه پیش‌بینی‌ها را در هر کلاس نمایش می‌دهد و به شناسایی کلاس‌هایی که مدل در آن‌ها عملکرد ضعیف‌تری دارد، کمک می‌کند (شکل ۷). علاوه بر این، نمودار t-SNE برای تجسم داده‌ها در فضای دوبعدی به‌کاررفته است تا نشان دهد مدل چگونه ویژگی‌های مختلف را از هم تفکیک می‌کند (شکل ۸). همچنین، مقادیر Recall ، F1-scoreو Precision در قالب یک نقشه‌گرمایی در شکل ۹ نمایش داده‌شده‌اند. این معیارها نمای کلی از تعادل بین دقت و پوشش مدل ارائه می‌دهند و به مقایسه عملکرد مدل در کلاس‌های مختلف کمک می‌کنند. ترکیب این ابزارها به شناسایی

نقاط قوت و ضعف مدل در طبقه‌بندی و بهبود عملکرد آن کمک کرده است.

۵- نتایج

در جدول شماره ۲ مقایسه دقت‌های به‌دست‌آمده با برخی از روش‌های مرتبط آورده شده است.

جدول (۲): دقت‌های پژوهش‌های مختلف

دیتاست	دقت	روش	مرجع
UCDAVIS19	۹۹/۳۷	VGG16	مدل پیشنهادی
UCDAVIS19	۹۸/۲٤	CNN	ون تانگو – ۲۰۱۸
UCDAVIS19	۹۸/۵۳	CNN	شهباز رضایی – ۲۰۲۰
UCDAVIS19	۹۸/۷	SimCLR	ایال هورورویتز – ۲۰۲۲

تحلیل یافته‌های این پژوهش نشان می‌دهد که استفاده از معماری عمیق شبکه عصبی VGG16 در ترکیب با تکنیک‌های پیش‌پردازش داده مانند تولید داده‌های FlowPic و Aux، منجر به‌دقت بالای ۹۹,۳۷ درصد در طبقه‌بندی ترافیک شبکه شده است. این دقت نه‌تنها از روش‌های پیشین مانند شبکه‌های CNN سنتی و SimCLR بالاتر است، بلکه کاربردپذیری این روش در سناریوهای پیچیده‌تر را نیز تضمین می‌کند. یکی از نقاط قوت برجسته این پژوهش، استفاده از داده‌های کمکی Aux برای غنی‌سازی ورودی مدل و بهبود عملکرد آن است. داده‌های Aux با ارائه اطلاعات آماری مانند حداکثر، حداقل، میانگین، و انحراف معیار در بازه‌های زمانی مشخص، امکان تحلیل دقیق‌تر و پیش‌بینی بهتر الگوهای پیچیده را فراهم کرده است. این روش ترکیبی، نمایشی جامع‌تر از داده‌ها ارائه می‌دهد و نشان می‌دهد که تلفیق ویژگی‌های عددی و تصویری می‌تواند مزایای قابل‌توجهی در تحلیل داده‌ها داشته باشد. همچنین، مقایسه با پژوهش‌های پیشین نشان می‌دهد که این رویکرد در پردازش ترافیک شبکه و طبقه‌بندی دقیق‌تر داده‌های رمزگذاری‌شده بسیار مؤثر بوده است. برای مثال، نتایج این پژوهش در مقایسه با سایر پژوهش‌ها پیشرفت محسوسی را نشان می‌دهد. این دستاورد به دلیل بهره‌گیری بهینه از تکنیک‌های یادگیری عمیق و ترکیب داده محوری به‌دست‌آمده است. بااین‌حال، برخی چالش‌ها مانند محدودیت‌های محاسباتی ناشی از استفاده از مدل‌های پیچیده مانند VGG16 و نیاز به مجموعه داده‌های باکیفیت بالا، همچنان وجود دارند. برای رفع این چالش‌ها، پیشنهاد می‌شود که در آینده از تکنیک‌های فشرده‌سازی مدل و یادگیری انتقالی برای کاهش هزینه‌های محاسباتی و افزایش مقیاس‌پذیری استفاده شود. درمجموع، این پژوهش با معرفی روش جدید و اثربخش در تحلیل ترافیک شبکه، گامی مهم در ارتقای دقت و کارایی سیستم‌های شناسایی شبکه برداشته و می‌تواند زمینه‌ساز پیشرفت‌های بیشتری در این حوزه باشد.

٦- نتیجه‌گیری

در این تحقیق، رویکرد پیشنهادی برای طبقه‌بندی ترافیک رمزنگاری‌شده با استفاده از شبکه عصبی عمیقVGG16 ، ترکیب داده‌های تصویری و کمکی، توانسته است دقت مدل را به ۹۹,۳۷ درصد برساند. این روش به‌طور مؤثر به شناسایی ترافیک رمزنگاری‌شده پرداخته و بهبود قابل‌توجهی در دقت و کارایی سیستم‌های شناسایی ترافیک شبکه ایجاد کرده است. به‌طور خاص، استفاده از داده‌های کمکی Aux به مدل امکان داد تا از الگوهای زمانی و حجمی داده‌ها برای پیش‌بینی دقیق‌تر بهره‌برداری کند. باوجود دقت بالای مدل، محدودیت‌هایی مانند پیچیدگی محاسباتی مدل و نیاز به داده‌های باکیفیت بالا همچنان وجود دارد. این چالش‌ها می‌توانند بر مقیاس‌پذیری مدل در محیط‌های بزرگ تأثیرگذار باشند. پیشنهاد می‌شود که در آینده از تکنیک‌های فشرده‌سازی مدل و یادگیری انتقالی برای کاهش هزینه‌های محاسباتی استفاده شود. به‌طورکلی، این پژوهش می‌تواند به‌عنوان پایه‌ای برای توسعه روش‌های جدید در تحلیل و مدیریت شبکه‌های پیچیده مورداستفاده قرار گیرد. در آینده، می‌توان با بهره‌گیری از تکنیک‌های بهینه‌سازی مدل و روش‌های یادگیری نیمه‌نظارتی یا بدون‌نظارت، این پژوهش را بهبود بخشید و قابلیت‌های آن را برای کاربردهای عملی در مقیاس بزرگ‌تر توسعه داد.

References

[1] A. R. Bahlali, A. Bachir, and A. Cheriet, "Malicious encrypted network traffic detection using deep auto-encoder with a custom reconstruction loss," in *2023 International Symposium on Networks, Computers and Communications (ISNCC)*, 2023.

[2] J. Cao et al., "An improved network traffic classification model based on a support vector machine," *Symmetry*, vol. 12, no. 2, p. 301, 2020, doi: 10.3390/sym12020301.

[3] P. Choorod, T. J. Bauer, and A. Aßmuth, "Distinguishing Tor from other encrypted network traffic through character analysis," *arXiv preprint arXiv:2405.09412*, 2024.

[4] Y. Cui and A. Li, "Research on network encrypted traffic detection technology based on CNN + LSTM," in *2024 2nd International Conference on Signal Processing and Intelligent Computing (SPIC)*, 2024.

[5] L. Deri and F. Fusco, "Using deep packet inspection in cybertraffic analysis," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2021, doi: 10.1109/CSR51186.2021.9527976.

[6] C. Hardegen et al., "Predicting network flow characteristics using deep learning and real-world network traffic," *IEEE Trans. Netw. Serv. Manage.*, vol. 17, no. 4, pp. 2662–2676, 2020.

[7] E. Horowicz, T. Shapira, and Y. Shavitt, "Self-supervised traffic classification: Flow embedding and few-shot solutions," *IEEE Trans. Netw. Serv. Manage.*, 2024, doi: 10.1109/TNSM.2024.3366848.

[8] E. Horowicz, T. Shapira, and Y. Shavitt, "A few shots traffic classification with mini-flowpic augmentations," in *Proc. 22nd ACM Internet Measurement Conference*, 2022, doi: 10.1145/3517745.3561436.

[9] S. Li et al., "Network traffic prediction based on the feature of newly-generated network flows," in *2022 IFIP Networking Conference (IFIP Networking)*, 2022.

[10] X. Liu et al., "Mal-lightDet: A light method to detect malicious encrypted traffic based on machine learning," in *Proc. 4th Int. Conf. Control, Robotics and Intelligent System*, 2023, doi: 10.1145/3622896.3622907.

[11] Y. Liu et al., "Encrypted malicious traffic detection based on graph convolutional network and temporal dissection," in *2024 27th Int. Conf. Comput. Supported Cooperative Work in Design (CSCWD)*, 2024.

[12] M. Lotfollahi et al., "Deep packet: A novel approach for encrypted traffic classification using deep learning," *Soft Comput.*, vol. 24, no. 3, pp. 1999–2012, 2020, doi: 10.1007/s00500-019-04030-2.

[13] S. Mascarenhas and M. Agarwal, "A comparison between VGG16, VGG19 and ResNet50 architecture frameworks for image classification," in *2021 Int. Conf. Disruptive Technol. for Multi-Disciplinary Res. and Appl. (CENTCON)*, 2021.

[14] S. Rezaei, B. Kroencke, and X. Liu, "Large-scale mobile app identification using deep learning," *IEEE Access*, vol. 8, pp. 348–362, 2019.

[15] T. Shapira and Y. Shavitt, "FlowPic: A generic representation for encrypted traffic classification and applications identification," *IEEE Trans. Netw. Serv. Manage.*, vol. 18, no. 2, pp. 1218–1232, 2021, doi: 10.1109/TNSM.2021.3071441.

[16] M. Shen et al., "Machine learning-powered encrypted network traffic analysis: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 791–824, 2022, doi: 10.1109/COMST.2022.3208196.

[17] G. Siracusano et al., "Re-architecting traffic analysis with neural network interface cards," in *Proc. 19th USENIX Symp. Netw. Syst. Design and Implementation (NSDI 22)*, 2022.

[18] L. Swarup, "Encrypted traffic analysis for malware detection using deep learning," in *2023 IEEE Int. Conf. ICT in Business Industry & Government (ICTBIG)*, 2023.

[19] V. Tong et al., "A novel QUIC traffic classifier based on convolutional neural networks," in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018.

[20] A. Finamore, C. Wang, J. Krolikowski, J. M. Navarro, F. Chen, and D. Rossi, "Curated UCDAVIS19 dataset for replication: Contrastive learning and data augmentation in traffic classification using a Flowpic input representation," Figshare, Oct. 2023. [Online]. Available: https://doi.org/10.6084/m9.figshare.23538141.

[21] J. Xing and C. Wu, "Detecting anomalies in encrypted traffic via deep dictionary learning," in *IEEE INFOCOM 2020–IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, 2020.

[22] X. Yang, N. Angkawisittpan, and X. Feng, "Analysis of an enhanced random forest algorithm for identifying encrypted network traffic," *EUREKA: Physics and Engineering*,

no. 5, pp. 201–212, 2024, doi: 10.21303/2461-4262.2024.003372.

[23] N. Zhou, "Image recognition in depth: Comparative study of CNN and pre-trained VGG16 architecture for classification tasks," in *Proc. Second Int. Conf. Physics, Photonics, and Optical Engineering (ICPPOE 2023)*, 2024, doi: 10.1117/12.3026829.

[24] Y. Zion, P. Aharon, R. Dubin, A. Dvir, and C. Hajaj, "Enhancing encrypted internet traffic classification through advanced data augmentation techniques," *arXiv preprint arXiv:2407.16539*, 2024.

Journal of Applied And Basic Machine Intelligence Research (ABMIR)

Applied and Basic Machine Intelligence Research

Vol. 2, No. 2, Autumn & Winter 2024, pp. 17 - 29

A Novel Approach for Encrypted Traffic Classification Using Deep Learning

Rabiei Dolatabadi Pooya[1], Bastam Mostafa[2*], Aghajani Khadijeh[2]

[1]M.Sc Computer Engineering, Faculty of Technology and Engineering, University of Mazandaran, Babolsar, Iran

[2]Assistant Professor Department of Computer Engineering, Faculty of Technology and Engineering, University of Mazandaran, Babolsar, Iran

Article Information

Original Research Paper

Received:
2024 December 15

Accepted:
2025 February 15

Keywords:
Deep Learning, Network Traffic Analysis, Encrypted Traffic, VGG16 model, Network Traffic Management

Corresponding Author*:
Bastam@umz.ac.ir

Abstract

Network traffic analysis is a fundamental pillar in enhancing the security and efficient management of computer networks. Given the rapid growth of computer networks and the increasing complexity of their traffic, accurate and fast identification of various types of traffic, including encrypted traffic, has become crucial. In this context, the use of machine learning techniques offers a powerful tool for analyzing and accurately identifying traffic patterns. This paper examines advanced methods for traffic identification in computer networks using machine learning techniques. The primary goal of this research is to develop an efficient and accurate model for identifying and classifying various types of network traffic, particularly encrypted traffic. To achieve this, the deep learning model VGG16 was utilized. Due to its deep layered architecture and capability to analyze large volumes of data, VGG16 demonstrated outstanding performance in identifying complex network traffic patterns. It can accurately detect and classify different types of network traffic, thereby improving traffic management within networks. In the scenarios evaluated in this study, the model achieved a remarkable accuracy of 99% in identifying encrypted traffic.

: 10.22034/ ABMIR.2025.22525.1084

E-ISSN: 2821-2037