# رویکردی نوین برای شناسایی ترافیک رمزنگاری‌شده با استفاده از شبکهٔ کلموگورف-آرنولد

**علی رهنما[1*]، زهرا آخوداد[2]**

دانشجوی دکترای فناوری اطلاعات، دانشگاه قم، قم، ایران[1*]

هیأت علمی پژوهشگاه توسعهٔ فناوری‌های پیشرفته، تهران، ایران[2]

## چکیده

**یکی از مشکلات اصلی در شبکه‌های مدرن، طبقه‌بندی ترافیک رمزنگاری‌شده‌ای است که از جریان داده‌های پردازش‌نشده به‌دلیل مشکل در ساختار و الگوهای پنهان به‌وجود می‌آید. در این مقاله، چهارچوبی جدید به‌نام seqKAN معرفی شده‌است که با ترکیب شبکه‌های LSTM و یا CNN برای استخراج وابستگی‌های زمانی و معماری KAN برای مدل‌سازی روابط غیرخطی، عملکرد دقیقی در تحلیل جریان‌های شبکه ارائه می‌دهد. برای افزایش دقت و قابلیت اطمینان، این مدل با روش‌های RKHS و ODE ترکیب و تأثیر مستقل و ترکیبی هر کدام، از طریق یک مطالعهٔ حذفی[1] بررسی شده‌است. نتایج روی مجموعه‌داده‌های واقعیِ رمزنگاری‌شده نشان می‌دهد افزودن لایهٔ RKHS نقش مؤثری در افزایش دقت و مقاومت مدل دارد؛ همچنین، با استفاده از تحلیل‌های کمی SHAP و LIME و قابلیت بصری‌سازی ذاتی KAN، نحوه شناسایی ویژگی‌های موثر و یادگیری خودکار روابط معنادار در مدل بررسی شده‌است. معماری پیشنهادی تعادلی مناسب میان دقت، کارایی و تفسیرپذیری برقرار کرده و راه‌کاری مؤثر برای تحلیل هوشمند ترافیک شبکه ارائه می‌دهد.**

**واژگان کلیدی: شناسایی ترافیک، شبکه کلموگورف-آرنولد، یادگیری عمیق.**

# SeqKAN: A Novel Approach to Encrypted Traffic Identification Using Kolmogorov-Arnold Network

**Ali Rahnema[1]*, Zahra Akhoodad[2]**

Ph.D. student of IT, University of Qom, Qom, Iran[1]*

Faculty Member, Research Center for Development of Advanced Technology, Tehran, Iran[2]

## Abstract

**With the growing usage of encryption protocols like VPN, and Tor in digital communication, identification and classification of encrypted traffic has been one of the core issues in network security and traffic management. It is a major contributor to quality of service (QoS) assurance, resource allocation, user identification, and anomaly detection. But the sophistication of encrypted traffic structure and the vagueness of behavioral patterns have drastically decreased the effectiveness of conventional approaches like deep packet inspection (DPI). In spite of the progress, typical deep learning models also encounter great difficulties in dealing with encrypted data; they typically need a huge amount of labeled data and lack the capacity to analyze unbalanced data.**

**To tackle these difficulties, this study proposes a novel hybrid architecture named seqKAN with enhanced interpretability and high accuracy. seqKAN integrates the temporal modeling capability of sequential networks like LSTM with the distinctive characteristics of Kolmogorov-Arnold networks (KAN), such as examining nonlinear relationships and intrinsic mathematical transparency. The framework also enjoys high flexibility and generalizability with the use of modules like Reproducible Hilbert Space Mapping (RKHS) and Neural Ordinary Differential Equations (ODE). Experiments are performed on benchmark datasets comprising Tor and VPN traffic (ISCXTor2016 and ISCXVPN2016). In this context, by meticulously filtering out the streams and addressing unbalanced data via class weighting, the model's stable performance is guaranteed. Ablation Study demonstrate that the inclusion of the RKHS layer significantly contributes to the improvement of the model's accuracy and robustness, particularly in encrypted settings. Among the models compared, the seqKAN approach delivered the**

[1] Ablation Study

* نویسندهٔ عهده‌دار مکاتبات

* Corresponding author

• تاریخ ارسال مقاله: ۱۴۰۳/۱۲/۲۵ • تاریخ پذیرش: ۱۴۰۴/۱۱/۱۹ • تاریخ انتشار: ۱۴۰۴/۱۲/۲۹ • نوع مطالعه: پژوهشی

**best performance in F1 score and demonstrated clear superiority in the classification of encrypted traffic. In addition, the interpretability of the model was quantitatively and qualitatively demonstrated with standard feature importance analysis techniques (SHAP and LIME) and KAN's inherent visual analysis. seqKAN successfully automatically extracted key features and patterns in the flow packets and clearly explained each decision; this transparency evidently illustrates the model's superiority over typical methods.**

**Finally, this research shows that the seqKAN architecture provides a comprehensive, efficient, and reliable solution for intelligent traffic analysis in complex network environments by creating a smart balance between accuracy, computational efficiency, and interpretability. The findings of this research highlight the high potential of KAN-based hybrid models as the basis for the next generation of transparent and reliable network security tools.**

**Keywords: Encrypted Traffic Classification, Kolmogorov-Arnold Network (KAN), Deep Learning, Model Interpretability, Ablation Study0.**

## ۱-مقدمه

به فرایند انتساب جریان‌های ورودی شبکه به دسته‌های ازپیش تعیین‌شده، *طبقه‌بندی ترافیک شبکه* گویند؛ این کار در شبکه از اهمیت ویژه‌ای برخوردار است[۱-۳]. از طبقه‌بندی ترافیک شبکه می‌توان در کاربردهای مشابه و مختلفی مانند افزایش کیفیت خدمات (QoS)، مدیریت بهتر منابع، شناسایی کاربران [۴]، تشخیص فعالیت‌های مخرب و جداکردن جریان‌های رمزنگاری‌شده از غیر آن استفاده کرد[۳، ۵، ۶]؛ برای مثال طبقه‌بندی دقیق ترافیک می‌تواند برنامهٔ درحال استفاده، نوع ترافیک رمزنگاری‌شده، یا رفتارهای خاص کاربران مانند نوع ویدیوی مشاهده‌شده در یوتیوب را مشخص کند.[۷-۹]

با وجود اهمیت بالای طبقه‌بندی ترافیک در مدیریت و امنیت شبکه، این فرایند با مشکلات زیادی روبه‌روست؛ یکی از مهم‌ترین مشکلات، استفاده از پروتکل‌های رمزنگاری است. روش‌های رمزنگاری مانند TLS، VPN و Torباعث می‌شوند که روش‌های سنتی تحلیل محتوای بسته‌های ترافیکی کارایی خود را از دست بدهند؛ زیرا این روش‌ها داده‌ها را رمزگذاری کرده و امکان بررسی مستقیم آن‌ها را از بین می‌برند؛ علاوه‌براین، مدل‌های تشخیص ترافیک باید بدون نیاز به به‌روزرسانی مداوم قادر به شناسایی الگوهای جدید ترافیکی باشند؛ با توجه به سرعت بالای تغییرات در برنامه‌های کاربردی و سرویس‌های اینترنتی، روش‌های رایج در این زمینه که نیاز به بازآموزی و به‌روزرسانی‌های مداوم دارند، ناکارآمد خواهند بود. این موضوع زمانی مشکل می‌شود که مجموعه‌داده‌ها نامتعادل باشند؛ در بسیاری از موارد، برخی انواع ترافیک بسیار نادر هستند و سامانه باید توانایی شناسایی دقیق آن‌ها را داشته باشد، بدون این‌که دقت کلی آن کاهش یابد. محدودیت منابع محاسباتی نیز یکی دیگر از مشکلات است. در بسیاری از محیط‌های شبکه‌ای، پردازش آنی و دقیق ترافیک بدون استفاده از سخت‌افزارهای قدرتمند امکان‌پذیر نیست؛ بنابراین، الگوریتم‌های طبقه‌بندی باید علاوه‌بر دقت بالا، بهینه و سبک باشند تا در شرایط محدودیت منابع نیز کارایی خود را حفظ کنند.

یک رویکرد جدید در طبقه‌بندی ترافیک باید سه ویژگی کلیدی داشته باشد:

۱.دقت بالا حتی با دادهٔ کم –کاهش نیاز به حجم زیادی از داده‌های آموزشی و استفاده از اطلاعات موجود.

۲.حذف وابستگی به مهندسی دستی ویژگی‌ها –بهره‌گیری از یادگیری عمیق و روش‌های خودکار برای استخراج ویژگی‌های مهم ترافیک.

۳.تضمین عملکرد پایدار در محیط‌های گوناگون –سازگاری با انواع شبکه‌ها و شرایط مختلف بدون نیاز به تغییرات اساسی در مدل.

رسیدن به این اهداف، مستلزم استفاده از روش‌های هوشمند و جدیدی است که بتوانند با چالش‌های طبقه‌بندی ترافیک در دنیای امروز سازگار شوند.

در گذشته، روش‌های سنتی همواره در برآورده‌کردن نیازهای دسته‌بندی ترافیک شبکه با مشکلات جدی روبه‌رو بوده‌اند؛ روش‌های مبتنی‌بر درگاه و بررسی عمیق بسته‌ها (DPI) به‌طور معمول به ویژگی‌های دستی وابسته بودند که تعریف و نگهداری آن‌ها مستلزم تلاش انسانی قابل‌توجه و منابع محاسباتی سنگین بود. این روش‌ها برای حفظ دقت، نیازمند به‌روزرسانی مداوم قوانین و امضاهای شناسایی بودند، اما با آمدن رمزنگاری پیشرفته و تغییرات سریع در پروتکل‌های شبکه، کارایی خود را از دست دادند[۱۰، ۱۱].

با آمدن روش‌های یادگیری ماشین، مدل‌های اولیه مانند درخت‌های تصمیم و ماشین‌های بردار پشتیبان (SVMs) تلاش شد تا این مشکلات برطرف شود؛ هرچند این روش‌ها نسبت به روش‌های سنتی دقت بیشتری داشتند و امکان طبقه‌بندی خودکار ترافیک را فراهم می‌کردند؛ بااین‌حال، همچنان به مهندسی دستی ویژگی‌ها وابسته بودند؛ به این معنا که برای عملکرد بهینه، نیاز به استخراج و انتخاب ویژگی‌های مناسب از داده‌های شبکه داشتند؛ همچنین، این مدل‌ها انعطاف‌پذیری محدودی در برابر الگوهای جدید ترافیکی داشتند و برای حفظ عملکرد مطلوب، نیازمند بازآموزی مکرر بودند [۲]. درمجموع، اگر چه یادگیری ماشین گامی روبه‌جلو در بهبود چالش‌های طبقه‌بندی ترافیک شبکه به‌حساب می‌آید، اما در مدل‌های اولیه همچنان چالش‌های مربوط به مهندسی ویژگی، به‌روزرسانی مداوم و انعطاف‌پذیری محدود وجود دارد، که این امر زمینه را برای توسعهٔ روش‌های پیشرفته‌تر مانند یادگیری عمیق فراهم کرد. این رویکردهای

نوین قادرند به‌طور خودکار الگوهای معنادار را از داده‌های خام ترافیکی استخراج کنند، بدون آن‌که نیاز به مهندسی دستی ویژگی‌ها داشته باشند. این ویژگی، آن‌ها را به روشی قدرتمند برای تحلیل ترافیک پیچیده و رمزنگاری‌شده تبدیل کرده‌است[۶، ۱۲].

مدل‌های یادگیری عمیق روش‌های پایهٔ مختلفی را برای تحلیل داده‌های ترافیکی ارائه کرده‌اند؛ برای مثال:

- شبکه‌های حافظهٔ طولانی-کوتاه‌مدت (LSTM) با پردازش داده‌های ترتیبی ترافیک، قادر به یادگیری وابستگی‌های زمانی بین بسته‌ها هستند؛ این ویژگی به‌ویژه برای شناسایی الگوهای رفتاری در جریان‌های ترافیکی مختلف مفید است.
- شبکه‌های عصبی پیچشی (CNN) توالی بسته‌های شبکه را به نمایش‌های تصویری تبدیل کرده و با استخراج ویژگی‌های مکانی-زمانی، امکان تحلیل دقیق‌تر جریان ترافیک را فراهم می‌کنند [۱۲].
- برخی دیگر از مقالات از روش‌های جدید مانند ترنسفورمرها [۱۳– ۱۵] و روش‌های یادگیری خودنظارتی [۱۶، ۱۷] استفاده کرده‌اند.

علاوه‌براین رویکردها، در مقالات روش‌های پیشرفته‌تری نیز برای مدل‌سازی بهتر جریان‌های ترافیکی معرفی شده‌اند:

- معادلات دیفرانسیل عادی عصبی (Neural ODEs): در این روش از فواصل زمانی بین ورود بسته‌ها برای مدل‌سازی بهتر رفتار زمانی یک دنبالهٔ ترافیکی استفاده می‌شود تا بدین صورت امکان تحلیل بهتر الگوهای ارتباطی آن فراهم آید [۱۱]. شبکه‌های مبتنی‌بر معادلات دیفرانسیل معمولی، روشی جدید برای مدل‌سازی داده‌های پیوسته در طول زمان است؛ برخلاف شبکه‌های عصبی رایج که در آن داده‌ها در لایه‌های مختلف شبکه به‌صورت گسسته و مرحله‌به‌مرحله پردازش می‌شوند، در اینجا تغییرات داده‌ها، به‌عنوان یک فرایند پیوسته درنظر گرفته می‌شود؛ برای این منظور در این شبکه داده‌ها با استفاده از یک تابع دیفرانسیلی مدل می‌شود که این تابع به‌صورت یک‌پارچه در طول زمان یاد گرفته می‌شود. این ویژگی باعث می‌شود که این شبکه در تحلیل سری‌های زمانی، مانند ترافیک شبکه، بسیار کارآمد باشند؛ زیرا می‌توانند تغییرات ظریف در رفتار بسته‌های ترافیکی را در طول زمان به‌درستی نشان کنند. این روش به‌ویژه در شناسایی الگوهای پنهان در ترافیک رمزنگاری‌شده مفید است و قادر است با بهره‌گیری از اطلاعات زمانی بین بسته‌ها، ویژگی‌های پنهان را استخراج کند و وابستگی‌های پیچیده را به‌طور خودکار بیاموزد.
- فضای هیلبرت بازتولیدکننده (RKHS): این روش با تغییر ابعاد داده‌ها، نمایش بهتری از داده‌ها ایجاد می‌کند؛ به بیان دیگر با این کار می‌توان هم ویژگی‌های ثابت ترافیک و هم تغییرات رفتاری آن در طول زمان را بهتر مشخص کرد [۱۲].

ترکیب این روش‌ها با روش‌های پایهٔ تحلیل زمانی باعث شده‌است که روش‌های مدرن طبقه‌بندی ترافیک توانایی تحلیل جریان‌های پیچیده و رمزنگاری‌شده را به‌طور قابل‌توجهی بهبود بخشند؛ برخلاف روش‌های سنتی که در برابر رمزنگاری و تغییرات سریع در پروتکل‌های شبکه ناکارآمد بودند، مدل‌های یادگیری عمیق عملکرد بهتری در شناسایی و طبقه‌بندی ترافیک ارائه می‌دهند.

این پیشرفت‌ها، مسیر را برای توسعهٔ سامانه‌های طبقه‌بندی ترافیک هوشمندتر و مقاوم‌تر هموار کرده‌اند، این مدل‌ها می‌توانند به‌طور مداوم با تغییرات دنیای واقعی سازگار شوند و تحلیل دقیقی از ترافیک شبکه ارائه دهند، حتی در شرایطی که روش‌های سنتی ناکارآمد هستند؛ باوجود این، بسیاری از آن‌ها هنوز با محدودیت‌هایی مانند دقت پایین در داده‌های رمزنگاری‌شده و نبود شفافیت در انتخاب ویژگی مواجه‌اند.

این پژوهش در راستای پاسخ به این نیاز، به ارزیابی جامع یک دستهٔ نوین از شبکه‌های عصبی؛ یعنی شبکه‌های کولموگروف-آرنولد (KAN)، در حوزهٔ طبقه‌بندی ترافیک رمزنگاری‌شده می‌پردازد. نوآوری اصلی این پژوهش، ارائه یک چهارچوب ارزیابی ماژولار و معرفی یک معماری ترکیبی با عنوان seqKAN است. در این معماری، توانایی شبکه‌های پردازش دنباله مانند LSTM و غیره در استخراج وابستگی‌های زمانی از ویژگی‌های پایه (اندازه و زمان بسته) با قابلیت‌های شبکه KAN در مدل‌سازی روابط غیرخطی و تفسیرپذیری ذاتی، تلفیق شده‌است؛ همچنین در این چهارچوب، تأثیر هر یک از مؤلفه‌های کلیدی مانند RKHS و ODE بر عملکرد نهایی، از طریق یک مطالعهٔ حذفی جامع (AblationStudy)، مورد سنجش قرار می‌گیرد. نتایج تجربی ما نشان می‌دهد که ترکیب هوشمندانهٔ این ماژول‌ها، منجر به دست‌یابی به عملکردی برتر در طبقه‌بندی ترافیک رمزنگاری‌شده می‌شود؛ علاوه‌براین، با بهره‌گیری از روش‌های استاندارد (SHAP/LIME) و تحلیل ذاتی KAN، قابلیت انتخاب ویژگی خودکار و شفافیت مدل به صورت کمی و کیفی به اثبات رسیده‌است.

مشارکت‌های اصلی این مقاله را می‌توان به‌شرح زیر خلاصه کرد:

- معرفی و اعتبارسنجی یک معماری ترکیبی نوین (seqKAN): برای نخستین‌بار، یک معماری که از قدرت شبکه‌های دنباله‌ای برای درک توالی و از KAN برای مدل‌سازی توابع پیچیده و قابل تفسیر بهره می‌برد، برای طبقه‌بندی ترافیک شبکه ارائه شده‌است.
- انجام یک مطالعهٔ حذفی جامع: تأثیر مستقل و ترکیبی ماژول‌های KAN, ODE و RKHS بر روی شبکه‌های پایهٔ متنوع به‌صورت دقیق ارزیابی و تحلیل شده‌است تا مؤثرترین ترکیب معماری شناسایی شود.

•اثبات تجربی تفسیرپذیری کمی و کیفی: با بهره‌گیری از روش‌های استاندارد (SHAP/LIME) و بصری‌سازی ذاتی توابع KAN، قابلیت انتخاب ویژگی خودکار و شفافیت مدل پیشنهادی به اثبات رسیده‌است.

همچنین روش ارائه‌شده دارای ویژگی‌های زیر نیز است؛ این ویژگی‌ها در روش‌های مشابه [۱۱، ۱۸] نیز وجود داشت:

•برخلاف روش‌های سنتی که در آن نیاز به بررسی دقیق محتوای بسته‌ها (DPI) یا استخراج مجموعه‌ای گسترده از ویژگی‌های ترافیکی است، روش پیشنهادی تنها از دو ویژگی کلیدی اندازهٔ بسته[1] و زمان بین رسیدن بسته‌ها[2] استفاده می‌کند. این ویژگی‌ها اطلاعات مهمی در مورد رفتار ترافیکی ارائه می‌دهند و برای شناسایی الگوهای مختلف ترافیک کافی هستند [۱۱، ۱۸].

•از دیگر مزایای روش پیشنهادی، کمترین نیاز آن به داده‌است. این مدل می‌تواند تنها با داشتن بیست تا سی بستهٔ ترافیکی جریان داده (البته بعد از فرایند پیش‌پردازش به‌منظور حذف داده‌های مربوط به TLS Handshake) الگوهای رفتاری جریان‌های داده را شناسایی کند. این ویژگی، SeqKAN را به گزینه‌ای مناسب برای محیط‌های با محدودیت منابع، مانند جایی که جمع‌آوری داده‌های زیاد امکان‌پذیر نیست یا در کاربردهایی که تأخیر در پردازش داده‌ها باید در کمترین حد باشد، مناسب می‌سازد.

به‌دلیل شباهت مسئله، از روش پیشنهادی می‌توان در طیف گسترده‌ای از وظایف طبقه‌بندی ترافیک نیز استفاده کرد؛ برای مثال از این روش می‌توان در تشخیص تفاوت بین جریان‌های رمزگذاری‌شده و غیررمزگذاری‌شده، طبقه‌بندی ترافیک، شناسایی کاربران و سایر موارد نیز بهره برد.

در ادامه، این مقاله به‌شرح زیر سازماندهی شده‌است: در بخش دو، به مرور ادبیات موضوع پرداخته و محدودیت‌های روش‌های موجود در دسته‌بندی ترافیک رمزگذاری‌شده بررسی می‌شود. در بخش سه، مجموعه‌داده‌ها و روش‌های پیش‌پردازش به‌کاررفته شرح داده می‌شود. در بخش چهارم، روش‌شناسی نوآورانه پژوهش معرفی می‌شود که شامل نحوهٔ ادغام شبکه‌های کولموگراف-آرنولد (KAN)، شبکه‌های معادلات دیفرانسیل معمولی (ODE) و بازنمایی فضای هیلبرت بازسازی‌شده (RKHS) است. در بخش بعد، معماری کلی مدل پیشنهادی شرح داده و تصمیمات طراحی و مزایای کلیدی رویکرد ترکیبی پژوهش بیان می‌شود. در ادامه، تنظیمات آزمایشی و نتایج ارائه شده و عملکرد مدل در مقایسه با روش‌های پیشرفتهٔ موجود سنجیده می‌شود و محدودیت‌ها و چالش‌های آن مورد بررس قرار می‌گیرد؛ درنهایت، در بخش «نتیجه‌گیری و کارهای آینده» یافته‌ها خلاصه شده و راه‌های پیشنهادی برای پژوهش‌های آینده مورد بحث قرار می‌گیرد.

[1] Packet Size
[2] Inter-Arrival Time

## ۲-ادبیات موضوع

طبقه‌بندی ترافیک شبکه در طی سال‌ها تکامل قابل توجهی یافته است و طیف گسترده‌ای از روش‌ها را از روش‌های سنتی مبتنی‌بر ویژگی‌های دستی گرفته تا روش‌های پیشرفتهٔ یادگیری عمیق و ترکیبی شامل می‌شود. این رویکردها را می‌توان درکل در چند دسته طبقه‌بندی کرد:

**• رویکردهای اولیه: از بازرسی بسته تا یادگیری ماشین کلاسیک**

در مراحل اولیهٔ پژوهش‌های مربوط به طبقه‌بندی ترافیک شبکه، روش‌های سنتی بیشتر به ویژگی‌های آماری که به‌صورت دستی طراحی شده متکی بودند. این ویژگی‌ها شامل معیارهایی مانند زمان بین ورود بسته‌ها، توزیع اندازهٔ بسته‌ها و مدت زمان جریان‌های شبکه می‌شدند[۱۹]. ایدهٔ اصلی این روش‌ها این بود که با استخراج و تحلیل این ویژگی‌ها، بتوان الگوهای رفتاری ترافیک را و طبقه‌بندی کرد.

این رویکردها در شرایط کنترل‌شده و با داده‌های مشخص عملکرد قابل قبولی داشتند؛ با این‌حال، با افزایش پیچیدگی ترافیک شبکه و ظهور فناوری‌های جدید مانند رمزگذاری ترافیک، پروتکل‌های پویای ارتباطی و شبکه‌های توزیع‌شده، این روش‌ها دچار چالش‌های متعددی شدند؛ یکی از مهم‌ترین محدودیت‌های آن‌ها وابستگی شدید به دانش تخصصی و تلاش فراوان برای مهندسی ویژگی‌ها بود، درواقع، طراحی یک سامانهٔ طبقه‌بندی دقیق نیازمند شناخت عمیق از پروتکل‌های شبکه، رفتار کاربران و الگوهای ارتباطی بود؛ علاوه‌براین، با افزایش مقیاس داده‌های شبکه، کارایی این روش‌ها کاهش یافت و نیاز به رویکردهای یک‌پارچه؛ خودکار و تطبیقی‌تر احساس شد.

**• رویکردهای مبتنی‌بر یادگیری عمیق**

با ورود مدل‌های یادگیری عمیق مانند شبکه‌های عصبی پیچشی[3]، شبکه‌های عصبی بازگشتی[4] و خودرمزگذارها[5]، چشم‌انداز طبقه‌بندی ترافیک شبکه دست‌خوش تغییرات اساسی شده‌است[۶]. این روش‌ها قادرند بدون اینکه نیازی به انتخاب ویژگی‌های دستی باشد، الگوهای معنادار را مستقیم از داده‌های خام ترافیک استخراج کنند. این ویژگی، این دسته از روش‌ها را از روش‌های سنتی متمایز می‌کند و امکان کشف روابط پیچیده را در داده‌های شبکه فراهم می‌آورد؛ با این‌حال، مدل‌های یادگیری عمیق به‌طور معمول به منابع محاسباتی بالایی نیاز دارند که ممکن است اجرای آن‌ها را در محیط‌های عملی با محدودیت‌های سخت‌افزاری دشوار کند؛ علاوه‌براین، این روش‌ها بیشتر تفسیرپذیری کمتری نسبت به روش‌های سنتی دارند؛ به این معنا که درک نحوهٔ تصمیم‌گیری مدل و تحلیل خطاها در آن‌ها پیچیده‌تر است؛ این مسئله چالش‌هایی

[3] CNNs
[4] RNNs
[5] Autoencoders

را برای استقرار عملی و اشکال‌زدایی[1] ایجاد می‌کند، به‌ویژه در سناریوهایی که شفافیت مدل و امکان توضیح تصمیمات آن از اهمیت بالایی برخوردار است.

**• رویکردهای ترکیبی و مبتنی‌بر تصویر**

پژوهش‌های اخیر به بررسی تبدیل داده‌های ترافیک شبکه به نمایش‌های مشابه تصویر پرداخته‌اند؛ یکی از این روش‌ها، FlowPic است که فرادادههای جریان شبکه را به فرمت‌های بصری تبدیل می‌کند تا بتوان آن‌ها را با استفاده از معماری‌های استاندارد شبکه‌های عصبی پیچشی پردازش کرد[۹]. این رویکردها به‌دلیل قابلیت پردازش داده‌های با ابعاد بالا و توانایی استخراج الگوهای پیچیده، به‌ویژه در طبقه‌بندی ترافیک رمزگذاری‌شده عملکرد قابل‌توجهی دارند.

این روش‌ها نیازمند پیش‌پردازش دقیق و حجم بالایی از توان محاسباتی هستند. این امر باعث می‌شود که در برخی از سناریوها، مانند تحلیل ترافیک در مراکز داده و سامانه‌های دارای منابع محاسباتی قوی، بسیار مؤثر باشند، اما در محیط‌هایی که منابع سخت‌افزاری محدودند، استفاده از این روش‌ها ممکن است چالش‌برانگیز و از نظر عملیاتی کمتر کارآمد باشد.

**• رویکردهای نوآورانهٔ برجسته**

به‌منظور رفع چالش‌های طبقه‌بندی ترافیک، مانند استخراج خودکار ویژگی‌ها، کارایی محاسباتی و مدیریت ترافیک رمزنگاری‌شده در مطالعات متعدد، روش‌های جدیدی معرفی شده‌اند که به چالش‌های دیرینه در طبقه‌بندی ترافیک پرداخته‌اند؛ ازجملهٔ این مطالعات عبارت‌اند از:

طبقه‌بندی ترافیک رمزگذاری‌شده از انتها به انتها: *وانگ و همکاران*[۱] از داده‌های جریان TCP نرمال‌شده به‌عنوان ورودی برای شبکه‌های عصبی مصنوعی[2] استفاده کردند. این روش امکان استخراج خودکار ویژگی‌ها را فراهم می‌کند و دیگر نیازی به برچسب‌گذاری دستی ویژگی‌ها نیست؛ به این ترتیب، کارآیی سامانه بهبود چشم‌گیری می‌یابد و بخش‌های مهم داده‌ها از طریق تحلیل وزن‌ها شناسایی و مشخص می‌شوند؛ این رویکرد همچنین نیاز به دخالت دستی در استخراج ویژگی‌ها را کاهش می‌دهد و خودکار ویژگی‌های کلیدی را شناسایی می‌کند.

*لطف‌اللهی و همکاران*[۶] چهارچوب Deep Packet را معرفی کردند که فرایند استخراج ویژگی‌ها و طبقه‌بندی را به‌طور یک‌پارچه ادغام می‌کند. این روش به‌طور خاص از شبکه‌های عصبی کانولوشنی (CNNs) و اتوانکودرها برای تحلیل ترافیک شبکه‌های VPN و غیر VPN- استفاده می‌کند. یکی از مزایای این چهارچوب این است که بدون نیاز به بازرسی سنتی بسته‌ها، توانست نرخ بازیابی بالایی به‌دست آورد. این ویژگی باعث می‌شود که حریم خصوصی کاربران حفظ شود و درعین‌حال دقت تشخیص ترافیک VPN از غیر VPN- افزایش چشم‌گیری یابد. این رویکرد نه‌تنها کارآمد است بلکه امنیت و حریم خصوصی را نیز در فرایند طبقه‌بندی ترافیک شبکه تضمین می‌کند.

در مقالهٔ [۳] اثربخشی شبکه‌های عصبی کانولوشنی یک‌بعدی برای طبقه‌بندی ترافیک رمزگذاری‌شده[3] برای طبقه‌بندی ترافیک رمزگذاری‌شده از انتها به انتها نشان داده شده‌است. این روش با پردازش مستقیم جریان‌های بایت متوالی، از مهندسی ویژگی دستی اجتناب می‌کند و عملکرد بهتری نسبت به روش‌های سنتی مبتنی‌بر CNN از خود نشان می‌دهد؛ بدین ترتیب، این رویکرد هم در دقت طبقه‌بندی و هم در سرعت پردازش نسبت به روش‌های پیشین پیشرفت قابل توجهی داشته‌است.

*شاپیرا و شویت*[۹] روش FlowPic را معرفی کردند که با تبدیل جریان‌های ترافیکی به نمایش‌های تصویری، فرایند طبقه‌بندی را تسهیل می‌کند. این رویکرد به‌جای استفاده از ویژگی‌های عددی سنتی، از تصاویر برای تحلیل داده‌های ترافیکی استفاده می‌کند. برای انجام این کار، داده‌های مربوط به جریان‌های ترافیکی به تصویری تبدیل می‌شوند که می‌تواند به‌وسیلهٔ شبکه‌های عصبی کانولوشنی (CNN) پردازش شود. در اینجا، از معماری شبکهٔ عصبی کانولوشنی LeNet-5 الهام گرفته شده‌است که برای تشخیص ویژگی‌های پیچیده در تصاویر مناسب است. یکی از مزایای قابل توجه FlowPic این است که حتی در مواجهه با داده‌های نامتعادل، که به‌طور معمول در بسیاری از مسائل طبقه‌بندی ترافیک وجود دارد، عملکرد خوبی از خود نشان داد. این ویژگی به‌ویژه در سناریوهای ترافیک رمزگذاری‌شده اهمیت دارد؛ زیرا این نوع ترافیک بیشتر با داده‌های کم یا نامتعادل همراه است. با استفاده از این روش، FlowPic قادر است با حفظ دقت و استحکام بالا، ویژگی‌های پیچیده و الگوهای پنهان در ترافیک رمزگذاری‌شده را شناسایی و طبقه‌بندی کند.

*روی و همکاران*[۱۱] در پژوهش خود شبکهٔ معادلات دیفرانسیل معمولی (ODEs) را با شبکه‌های عصبی طولانی‌مدت[4] ترکیب کردند تا یک مدل طبقه‌بندی ترافیک دقیق و کارآمد ایجاد کنند. این مدل ترکیبی به‌طور خاص برای کاهش نیاز به داده‌های ورودی طراحی شده‌است و می‌تواند تنها با ده تا سی بستهٔ ترافیکی، طبقه‌بندی دقیقی انجام دهد. این ویژگی به‌ویژه در شرایطی که حجم داده‌های موجود محدود باشد، مزیت قابل توجهی است. معادلات دیفرانسیل معمولی در این مدل به‌عنوان ابزاری برای مدل‌سازی رفتار دینامیک ترافیک شبکه مورد استفاده قرار می‌گیرند. این امر به مدل کمک می‌کند تا الگوهای پیچیده و تغییرات مداوم در جریان‌های ترافیکی را بهتر درک کرده و از آن‌ها بهره‌برداری کند. شبکهٔ LSTM، ازسوی دیگر، برای یادگیری و حفظ

[1] Debugging
[2] ANNs
[3] 1D-CNNs
[4] LSTM

اطلاعات در طول زمان و به‌ویژه در توالی‌های طولانی مناسب است که باعث می‌شود این مدل ترکیبی قادر به شبیه‌سازی دقیق‌تری از رفتار ترافیک باشد. این ترکیب باعث می‌شود که مدل ODE-LSTM دقت بالایی در شناسایی و طبقه‌بندی ترافیک، حتی در شرایط کمبود داده ارائه دهد؛ علاوه‌براین، به‌دلیل نیاز کم به داده‌ها، این مدل برای کاربردهای زمان واقعی که در آن پردازش سریع و دقیق اهمیت ویژه‌ای دارد، مهم است.

*چن و همکاران* [۱۲] رویکرد Seq2Img را معرفی کردند که دنباله‌های بسته‌ها را به تصاویر چندکاناله تبدیل می‌کند تا رفتارهای ایستا و پویا را هم‌زمان ثبت کند؛ این تصاویر سپس با استفاده از شبکه‌های عصبی کانولوشنی طبقه‌بندی می‌شوند، که باعث می‌شود نیازی به استخراج ویژگی‌های دستی نباشد و عملکرد بالایی در سناریوهای دنیای واقعی به‌دست آید؛ با استفاده از این روش، دنباله‌های بسته‌های ترافیکی که به‌طور معمول داده‌های پیچیده و چندبعدی هستند، به تصویری قابل پردازش برای شبکه‌های عصبی تبدیل می‌شوند. این تصویرسازی از داده‌ها به مدل این امکان را می‌دهد که به‌طور مؤثری ویژگی‌های مختلف ازجمله الگوهای رفتاری ایستا و پویا را شناسایی کند. این رویکرد نه‌تنها پردازش داده‌های ترافیکی را ساده‌تر می‌کند، بلکه نیاز به دخالت دستی برای استخراج ویژگی‌ها را از بین می‌برد، که به‌ویژه در سناریوهای واقعی که داده‌ها پیچیده و متنوع‌اند، بسیار کارآمد است.

*ورد و همکاران* [۴] از مدل‌های مارکوف پنهان[1] برای شناسایی کاربران پشت دستگاه‌های NAT استفاده کردند. در این روش، از رکوردهای NetFlow برای استخراج الگوهای رفتاری کاربران استفاده شد و مدل‌های مارکوف پنهان (HMM) برای طبقه‌بندی مؤثر ترافیک آموزش داده شدند. این رویکرد به‌طور خاص قادر است، ترافیک کاربران مختلف را بر اساس الگوهای رفتاری‌شان شناسایی و تفکیک کند. با بهره‌گیری از رکوردهای NetFlow که شامل اطلاعات دقیقی از جریان‌های ترافیکی هستند، مدل‌های HMM توانستند الگوهای پنهان در ترافیک را شناسایی و به این ترتیب، شناسایی کاربران پشت دستگاه‌های NAT را در شبکه‌های پیچیده تسهیل کنند؛ این روش علاوه‌بر دقت بالا، در شرایطی که تفکیک ترافیک برحسب معمول دشوار است، عملکرد مؤثری دارد.

*دابین و همکاران* [۷] از شبکه‌های عصبی کانولوشنی برای شناسایی جریان‌های ویدئویی رمزگذاری‌شده استفاده کردند. این رویکرد با استفاده از تحلیل دقیق الگوهای ترافیکی، توانست ویژگی‌های خاص جریان‌های ویدئویی رمزگذاری‌شده را شناسایی کند، که از آن برای تفکیک ترافیک ویدئویی از دیگر انواع ترافیک در شبکه‌های پیچیده بهره بردند. تحلیل الگوهای زمانی در این روش به شناسایی دقیق و سریع انواع مختلف ترافیک ویدئویی، به‌ویژه زمانی که داده‌ها رمزگذاری شده‌اند، کمک می‌کند.

*زاندر و همکاران* [۲] به چالش‌های شناسایی ترافیک روز صفر با استفاده از خوشه‌بندی و مدل‌های یادگیری عمیق پرداختند. روش‌های آن‌ها امکان شناسایی الگوهای ترافیکی را که پیش‌تر دیده نشده بودند، فراهم کرد، که این امر نیاز به آموزش مجدد مکرر را کاهش داده و قابلیت انطباق سامانه‌های طبقه‌بندی ترافیک را به‌طور چشمگیری افزایش داد. این رویکرد با استفاده از خوشه‌بندی، توانست الگوهای جدید ترافیکی را شناسایی کند که پیش از این در داده‌های آموزشی وجود نداشتند؛ از طرف دیگر، مدل‌های یادگیری عمیق قادر به یادگیری ویژگی‌های پیچیده و پنهان ترافیک شبکه بودند که به شناسایی بهتر ترافیک روز صفر کمک می‌کرد. این ویژگی‌ها باعث شد سامانه‌ها توانایی انطباق سریع با تغییرات جدید ترافیکی را بدون نیاز به آموزش مکرر و منظم داشته باشند.

**•رویکردهای معماری‌های پیشرفتهٔ ترنسفورمرها:**

در سال‌های اخیر، با الهام از موفقیت‌های چشم‌گیر معماری ترنسفورمر در پردازش زبان طبیعی، پژوهش‌گران این مدل‌ها را برای طبقه‌بندی ترافیک شبکه نیز به‌کار گرفته‌اند. مدل‌هایی مانند [۱۳–۱۵] با بهره‌گیری از سازوکار توجه[2]، قادرند الگوهای مهم در توالی بسته‌ها را شناسایی کرده و وابستگی‌های بلندمدت را بهتر از شبکه‌های بازگشتی مدل‌سازی کنند. این رویکردها دقت بالایی را نشان داده‌اند، اما هزینهٔ محاسباتی بالا و نیاز به داده‌های آموزشی حجیم، از چالش‌های اصلی آن‌ها محسوب می‌شود.

*لین و همکاران* [۱۳] برای کاهش وابستگی مدل‌های سنتی به داده‌های برچسب‌دار و افزایش دقت طبقه‌بندی ترافیک رمزگذاری‌شده، چهارچوب ET-BERT را ارائه کردند. در این روش، جریان‌های ترافیک به بخش‌های کوچکی به‌نام «BURST» تقسیم می‌شوند که هرکدام شامل دنباله‌ای از بسته‌های دادهٔ یک‌طرفه هستند؛ سپس مدل با استفاده از حجم زیادی داده بدون برچسب، از طریق دو وظیفهٔ پیش‌آموزشی ویژه؛ یعنی پیش‌بینی بخش‌های پنهان برای یادگیری روابط بین داده‌ها و پیش‌بینی منبع مشترک برای درک ساختار انتقال، آموزش می‌بینند؛ پس از این مرحله، مدل با مقدار کمی دادهٔ برچسب‌دار برای وظایف خاص تنظیم می‌شود و به نتایج دقیق و قابل اتکایی در طبقه‌بندی ترافیک شبکه می‌رسد.

*لیو و همکاران* [۱۴] برای بهبود طبقه‌بندی ترافیک رمزگذاری‌شده، مدل TransECA-Net را معرفی کردند که با ترکیب ماژول‌های ECA-Net و رمزگذار ترنسفورمر، هم‌زمان به استخراج ویژگی‌های محلی و مدل‌سازی وابستگی‌های زمانی می‌پردازد. این مدل با استفاده از سازوکار توجه چندسر، قادر به

[1] HMMs

[2] Attention

شناسایی الگوهای پیچیدهٔ ترافیکی بوده و در مقایسه با روش‌های پایه، عملکرد دقیق‌تر و پایدارتری از خود نشان داده‌است.

کوکولیس و همکاران [۱۵] چهارچوبی خودنظارتی مبتنی‌بر یادگیری مقابله‌ای و ترنسفورمر معرفی کردند که مستقیم روی بسته‌های خام شبکه کار می‌کند. این روش با جایگزینی هوشمندانهٔ بسته‌ها در جریان‌های ترافیکی، بازنمایی‌های عمیق و معناداری از داده‌ها می‌آموزد. نتیجهٔ کار، تشخیص دقیق‌تر ناهنجاری‌ها به‌ویژه در شرایط بین‌مجموعه‌داده‌ای است و عملکرد بهتری نسبت به روش‌های مبتنی‌بر NetFlow دارد.

چهارچوب FlowTransformer، ارائه‌شده در [۲۰]، رویکردی نوین برای بهبود سامانه‌های تشخیص نفوذ شبکهٔ مبتنی‌بر مدل‌های ترنسفورمر است. این چهارچوب با جایگزینی و بهینه‌سازی اجزای مختلف مدل، ازجمله رمزگذاری ورودی و بخش طبقه‌بندی، انعطاف‌پذیری بالایی فراهم می‌آورد.

**•یادگیری خودنظارتی:**

رویکردهای یادگیری خودنظارتی[1]، برای غلبه بر مشکل نیاز به داده‌های برچسب‌دار توسعه یافته‌اند. این روش‌ها با یادگیری بازنمایی‌های مناسب از داده‌های بدون برچسب، نیاز به برچسب‌گذاری دستی را کاهش می‌دهند؛ برای مثال *گو و همکاران* [۱۶] چهارچوب نیمه‌نظارتی CoMask را برای طبقه‌بندی ترافیک رمزگذاری‌شده معرفی کردند که با استفادهٔ هم‌زمان از داده‌های برچسب‌دار و بدون برچسب، فضای ویژگی را بهینه کرده و توان تعمیم‌پذیری مدل را افزایش می‌دهد. این روش با ترکیب آموزش متقابل روی داده‌های بدون برچسب برای یادگیری بازنمایی‌های مقاوم و یادگیری مقابله‌ای نظارت‌شده روی داده‌های برچسب‌دار برای نزدیک‌کردن نمونه‌های هم‌طبقه و دورکردن نمونه‌های متفاوت، مرزهای بین طبقه‌ها را با دقت بیشتری تعیین می‌کند. CoMask با این رویکرد دوگانه و تمرکز بر توالی‌های چندمقیاسی، در آزمایش‌ها نسبت به روش‌های پیشرفتهٔ دیگر عملکردی بهتر و پایدارتر داشته است.

هورورویچ و همکاران [۱۷] برای کاهش وابستگی به داده‌های برچسب‌دار در طبقه‌بندی ترافیک، یک چارچوب یادگیری خودنظارتی مبتنی‌بر یادگیری مقابله‌ای پیشنهاد دادند. این روش با تبدیل جریان‌های ترافیک به تصاویر کوچک موسوم به mini-FlowPics و به‌کارگیری روش‌های افزایش داده خاصِ ترافیک (مانند شبیه‌سازی تغییر زمان رفت‌وبرگشت (RTT) ) بازنمایی‌های مؤثری از داده‌های خام به‌دست می‌آورد. مدل ابتدا با داده‌های بدون برچسب آموزش می‌بیند و سپس با تعداد بسیار کمی نمونه برچسب‌دار، به دقت بالایی در طبقه‌بندی می‌رسد، به‌گونه‌ای که عملکرد آن از روش‌های نظارت‌شده سنتی فراتر می‌رود.

[1] Self-Supervised Learning

**•مدل‌های سبک:**

*سان و همکاران* [۲۱] مدلی سبک‌وزن مبتنی‌بر MobileNetV3 برای طبقه‌بندی ترافیک در دستگاه‌های لبه پیشنهاد دادند. آن‌ها با تبدیل جریان‌های ترافیک به تصاویر خاکستری ۲۸×۲۸ و استفاده از سازوکار توجه و ماژول ترکیب ویژگی چندمقیاسی، مدلی کم‌حجم با توانایی طبقه‌بندی بلادرنگ روی Raspberry Pi طراحی کردند.

## ۲-۱-شکاف پژوهشی و جایگاه این پژوهش

مرور ادبیات نشان می‌دهد که در طبقه‌بندی ترافیک، افزایش دقت مدل‌ها به‌طور معمول به پیچیدگی و هزینهٔ محاسباتی بیشتر منجر می‌شود؛ با این‌حال، نیاز به معماری‌هایی که توازنی میان دقت، کارایی و تفسیرپذیری برقرار کنند، همچنان باقی است. قابلیت تفسیرپذیری به پژوهش‌گر کمک می‌کند بفهمد مدل چگونه و بر اساس کدام ویژگی‌ها تصمیم می‌گیرد. در این پژوهش، شبکه‌های کولموگروف–آرنولد (KAN) را که در اصل تفسیرپذیرند، بررسی کرده و معماری ترکیبی seqKAN معرفی می‌شود. این مدل با تلفیق ویژگی‌های زمانی LSTM و ساختار KAN، راه‌کاری دقیق، کارآمد و شفاف ارائه می‌دهد که می‌تواند با مدل‌های پیچیده‌ای مانند ترنسفورمر رقابت کند.

## ۳-مجموعه‌داده

برای ارزیابی روش پیشنهادی خود، از ترکیب مجموعه‌داده‌هایی استفاده شد که مشابه مجموعه‌های دادهٔ رایج در ادبیات پژوهشی بودند[2]. این مجموعه‌ها شامل داده‌های ترافیک [۲۲ و ۲۳] از دانشگاه نیوبرانزویک بودند. این مجموعه‌ها با تنوع بالای طبقه‌بندی ترافیک، روش‌های رمزگذاری و چالش‌های عملی که ارائه می‌دهند، امکان ارزیابی دقیق و جامع روش ما را فراهم می‌سازند. در ادامه ویژگی‌های این مجموعه‌داده‌ها بیان می‌شود.

۱.مجموعه‌دادهٔ ISCX-VPN [۲۲]: این مجموعه شامل جلسات ترافیکی است که در هشت دستهٔ مختلف (مانند VoIP، چت) ضبط شده‌اند. این داده‌ها در دو حالت غیررمزگذاری VPN و رمزگذاری VPN قرار دارند.

۲. مجموعه‌دادهٔ ISCX-Tor [۲۳]: مشابه مجموعه ISCX-VPN، این مجموعه نیز همان دسته‌ها را شامل می‌شود، اما در شرایط غیررمزگذاری Tor و رمزگذاری Tor ضبط شده‌است.

برای حفظ انسجام و قابلیت اعتماد در تحلیل، تمرکز پژوهش بر چند دستهٔ ترافیکی؛ یعنی ترافیک VoIP، ویدئو، گفت‌گوی اینترنتی، مرورگر و انتقال فایل و ... قراگرفت: این دسته‌ها تحت سه شرایط رمزگذاری مورد بررسی قرار گرفتند

[2] مجموعه‌دادهٔ مورد استفاده در این پژوهش با مجموعه‌دادهٔ مقالات [۱۱] , [۱۸] کمی متفاوت بوده و شامل مجموعه‌دادهٔ اختصاصی آن‌ها نیست.

که عبارت‌اند از: ترافیک رمزنگاری‌نشده، ترافیک تحت عبور از VPN و درنهایت ترافیک تحت شرایط رمزگذاری با استفاده از شبکهٔ Tor.

هر فایل pcap در مجموعه‌داده، به‌طور مشخص به یک برنامه، دستهٔ ترافیکی و نوع رمزگذاری تعلق دارد؛ بااین‌حال، به‌دلیل اجرای هم‌زمان چند سرویس یا برنامهٔ کاربردی در هنگام ضبط، ممکن است، یک فایل شامل جریان‌هایی از چند دستهٔ ترافیکی متفاوت باشد. برای تضمین یک‌پارچگی و برچسب‌گذاری صحیح، ابتدا یک مرحلهٔ پالایش اولیه انجام شد که طی آن، تمامی جریان‌هایی که با دستهٔ ترافیکی اصلی فایل هم‌راستا نبودند (با استفاده از پالایهٔ پروتکل‌ها یا مقاصد نامرتبط) حذف شدند. این کار تضمین می‌کند که هر فایل تنها حاوی جریان‌های سازگار با برچسب اعلام‌شده باشد.

پس از این مرحله، هر فایل pcap به جریان‌های یک‌طرفه[1] تقسیم می‌شود که با یک پنج‌تایی منحصربه‌فرد شامل IP و درگاه مبدأ، IP و درگاه مقصد و نوع پروتکل (TCP یا UDP) شناسایی می‌شوند.

مراحل دقیق پیش‌پردازش به‌صورت زیر است:

**۱.حذف TLS Handshake:**

یکی از چالش‌های کلیدی در تحلیل ترافیک رمزنگاری‌شده، خطر بیش‌برازش مدل روی الگوهای تکراری و عمومی مرحلهٔ برقراری ارتباط (مانند TLS Handshake) است. یادگیری این الگوها، باعث کاهش قدرت تعمیم‌پذیری مدل در محیط‌های واقعی می‌شود. برای رفع این مشکل، در فرایند پیش‌پردازش جریان‌های مبتنی‌بر TCP، بسته‌های ابتدایی مرتبط با فرایند TLS Handshake شناسایی و حذف می‌شوند.

**۲.استخراج نمونه و افزایش داده:**

پس از حذف ناحیهٔ Handshake، از بخش باقی‌ماندهٔ جریان‌ها، توالی‌هایی با طول ثابت بیست بسته به‌صورت غیرهم‌پوشان[2] استخراج می‌شوند. این روش ضمن استانداردسازی ورودی، به‌عنوان یک روش افزایش داده نیز عمل می‌کند و امکان تولید چندین نمونه از جریان‌های بلندتر را فراهم می‌سازد؛ درنتیجه، هم تنوع نمونه‌ها افزایش می‌یابد و هم مدل از الگوهای رفتاری متنوع‌تری یاد می‌گیرد.

**۳.استخراج ویژگی:**

برای هر یک از بیست بسته در هر نمونه، دو ویژگی کلیدی استخراج می‌شود: طول بسته و زمان بین ورود بسته‌ها؛ درنهایت، هر نمونه به‌صورت یک ماتریس با ابعاد ۲۰×۲ نمایش داده می‌شود.

**۴.نرمال‌سازی:**

برای یکسان‌سازی مقیاس داده‌ها، طول بسته‌ها با فرض بیشینهٔ اندازهٔ MTU (۱۵۰۰ بایت) نرمال‌سازی شده و مقادیر IAT با استفاده از روش min-max مقیاس‌بندی می‌شوند.

**۵.تفکیک مجموعه‌داده بر حسب روش رمزنگاری:**

با توجه به نبود توازن در توزیع داده‌ها میان طبقه‌های مختلف مرتبط با رمزنگاری، سه مجموعه‌دادهٔ مجزا شامل داده‌های رمزنگاری‌شده، داده‌های رمزنگاری‌نشده و همچنین ترکیب کامل داده‌ها شکل گرفت. ارزیابی‌های جامع و متعددی به‌منظور بررسی عملکرد و تحلیل نتایج مدل‌ها بر روی هر یک از این مجموعه‌داده‌ها انجام شد.

فرایند پیش‌پردازش به‌گونه‌ای طراحی شده‌است که از یادگیری مدل بر اساس بخش‌های مشترک و غیرتفکیک‌پذیر جلوگیری کرده و تنها الگوهای رفتاری خاص را در معرض یادگیری قرار دهد؛ همچنین تأکید می‌شود که تمام نتایج گزارش‌شده در مقاله، مبتنی‌بر داده‌هایی هستند که طبق این فرایند پالایش‌شده و استاندارد، تولید شده‌اند.

## ۴-مبانی نظری و ابزارهای مورد استفاده

در این بخش، ابتدا مبانی نظری و ویژگی‌های کلیدی هر یک از مؤلفه‌های اصلی روش پیشنهادی بررسی می‌شوند:

**•شبکه‌های پردازش دنباله**

شبکه‌های LSTM نوعی از شبکه‌های عصبی بازگشتی (RNN) هستند که برای پردازش داده‌های دنباله‌ای طراحی شده‌اند و توانایی یادگیری وابستگی‌های بلندمدت در داده‌ها را دارند؛ به‌عبارت دیگر، این شبکه‌ها می‌توانند اطلاعات مهم گذشته را در حافظه نگه‌دارند و از آن برای پیش‌بینی یا تحلیل داده‌های بعدی استفاده کنند؛ از طرف دیگر، شبکه‌های Conv1D نوعی شبکهٔ عصبی کانولوشنی هستند که به‌جای تصاویر، روی داده‌های یک‌بُعدی مانند دنباله‌های زمانی یا سیگنال‌ها کار می‌کنند و با استفاده از پالایه‌های کانولوشنی می‌توانند الگوهای محلی و ویژگی‌های مهم در طول دنباله را استخراج کنند؛ هر دو این شبکه‌ها برای استخراج ویژگی‌های مهم از داده‌های ترتیبی کاربرد فراوانی دارند و در بسیاری از مسائل پردازش سیگنال و تحلیل توالی استفاده می‌شوند.

**•شبکهٔ کولموگوروف-آرنولد (KAN)**

این شبکه یک معماری جدید در یادگیری ماشین است که بر پایهٔ یک اصل ریاضی بنیادین شکل گرفته است؛ این اصل بیان می‌کند که هر تابع پیچیده‌ای را می‌توان با ترکیب تعدادی تابع سادهٔ یک‌متغیره بازسازی کرد؛ برخلاف شبکه‌های عصبی سنتی که ارتباط بین گره‌ها از طریق وزن‌های عددی ثابت برقرار می‌شود، در KAN هر گره به‌جای یک مقدار عددی، یک تابع فعال‌ساز قابل یادگیری را در خود جای می‌دهد. این ساختار به مدل اجازه می‌دهد تا روابط غیرخطی و پیچیدهٔ موجود در داده‌ها با دقت بیشتری شناسایی و بازنمایی شود.

ویژگی برجستهٔ دیگر KAN، تفسیرپذیری بالای آن است؛ زیرا هر تابع نقش مشخصی در تصمیم‌گیری نهایی ایفا می‌کند که می‌توان با نمایش آن، تأثیر هر قسمت از شبکه را بر خروجی مشاهده کرد. ترکیب دقت، انعطاف‌پذیری و شفافیت،

[1] Unidirectional Flows
[2] non-overlapping

KAN را به معماری توانمند و متمایز در مقایسه با شبکه‌های عصبی متداول تبدیل کرده‌است.

ایدهٔ اصلی KAN طبق قضیهٔ کولموگوروف-آرنولد این است که هر تابع پیوستهٔ چندمتغیره مانند $\boldsymbol{f(x_1, \dots, x_n)}$ را می‌توان به‌عنوان مجموع محدود توابع یک‌متغیره نمایش داد:

$$f(x_1, \dots, x_n) = \sum_{q=1}^{2n+1} \Phi_q \left( \sum_{p=1}^{n} \varphi_{q,p}(x_p) \right) \quad (1)$$

که در آن $\varphi_{q,p}: [0,1] \to R$ توابع یک‌متغیره و $\Phi_q: R \to$ تابعی برای ترکیب توابع یک‌متغیره به‌منظور بازسازی $\mathbf{x}$ است. در شبکهٔ KAN، $\Phi_q$ ها به‌عنوان وزن‌های قابل آموزش پیاده‌سازی می‌شود که توابع پایهٔ یک‌متغیره را جمع‌آوری می‌کنند و مدلی می‌سازند که به‌طور مؤثر روابط نهفتهٔ درون داده‌ها را درک می‌کند.

مدل KAN با ساختار ساده‌تری که دارد، نیاز به منابع محاسباتی کمتری دارد و می‌تواند سریع‌تر آموزش ببیند. این ویژگی برای کاربردهایی که نیاز به پردازش سریع دارند، بسیار ارزشمند است.

یکی از بزرگترین مزایای KAN این است که می‌توان به‌راحتی رفتار مدل را مورد بررسی و تحلیل قرار داد؛ برای مثال، می‌توان به‌راحتی دید که چگونه تغییرات در هر متغیر ورودی بر خروجی مدل تأثیر می‌گذارد.

**•شبکه‌های معادلات دیفرانسیل معمولی (ODE)**

شبکه‌های معادلات دیفرانسیل معمولی ODE، نوعی از شبکه‌های عصبی هستند که در آن به‌جای استفاده از لایه‌های معمولی و گسسته، فرایند یادگیری به‌صورت یک تبدیل پیوسته تعریف که به‌وسیلهٔ معادلات دیفرانسیل توصیف می‌شود؛ درواقع، در این شبکه‌ها، تغییرات داده‌ها و ویژگی‌ها مداوم در طول زمان یا فضای ویژگی‌ها مدل‌سازی می‌شوند.

در شبکه‌های عصبی رایج، داده‌ها از لایه‌ای به لایهٔ دیگر به‌طور گسسته حرکت می‌کنند و در هر لایه یک پردازش مشخص انجام می‌شود؛ اما در ODE، به‌جای استفاده از پردازش‌های گسسته، شبکهٔ تغییرات داده‌ها را به‌طور پیوسته و از طریق یک معادلات دیفرانسیل مدل می‌کند. این امر باعث می‌شود که شبکه قادر به پردازش داده‌های پیوسته مانند سری‌های زمانی یا فرایندهایی که به‌طور مداوم تغییر می‌کنند (مانند داده‌های رمزنگاری‌شده)، باشد.

ODE ها می‌توانند به‌طور دقیق‌تری با داده‌های واقعی تعامل کنند و تغییرات پیوسته را بهتر شبیه‌سازی کنند؛ به‌همین دلیل، این شبکه‌ها برای مسائل پیچیده‌ای که شامل داده‌های زمانی یا پیوسته‌اند (مانند پیش‌بینی روندها در داده‌های زمانی یا مدل‌سازی سامانه‌های فیزیکی و طبیعی) بسیار مناسب و کارآمدند.

در شبکه‌های مبتنی‌بر معادلات دیفرانسیل به‌طور معمول به‌جای استفاده از لایه‌های جدا و ثابت، حالت داخلی شبکه به‌صورت پیوسته و با استفاده از یک معادلهٔ دیفرانسیل به‌روزرسانی می‌شود. در شبکه‌های معمولی پردازش توالی، حالت پنهان یا حافظهٔ سامانه به‌صورت گسسته به‌روزرسانی می‌شود که این فرایند را می‌توان به شکل زیر نشان داد:

$$h_{t+1} = h_t + f(h_t, \theta_t) \quad (2)$$

که در آن $\boldsymbol{h_t}$ حالت پنهان در زمان $\boldsymbol{t}$ و $\boldsymbol{f(h_t, \theta)}$ تابعی است که تغییرات حالت را تعیین می‌کند، اما در شبکه‌های مبتنی‌بر معادلات دیفرانسیل (ODE)، به‌جای تغییرات گسسته، حالت مخفی سامانه به‌صورت پیوسته و نرم بر اساس یک معادلهٔ دیفرانسیل به‌روزرسانی می‌شود:

$$f(h_t, t, \theta) = \frac{dh_t}{dt} \quad (3)$$

در این روش، تغییرات حالت شبکه به شکل یک فرایند مداوم و پیوسته مدل می‌شوند که این موضوع باعث انعطاف‌پذیری بیشتر و توانایی بهتر در مدل‌سازی رفتارهای پویا پیچیده می‌شود.

مزایای کلیدی ODE عبارت‌اند از:

- **کارایی حافظه:** برخلاف شبکه‌های عصبی سنتی، ODE تمام حالت‌های مخفی میانی را ذخیره نمی‌کنند، که باعث کاهش قابل توجه بار حافظه می‌شود.
- **دقت تطبیقی:** این شبکه‌ها می‌توانند با استفاده از حل‌کننده‌های پیشرفته ODE دقت بالاتری نسبت به روش‌های سنتی مانند روش اویلر (با دقت مرتبهٔ نخست) ارائه دهند.
- **انعطاف‌پذیری برای داده‌های نامنظم:** ODE در پردازش داده‌های سری زمانی که به‌طور نامنظم نمونه‌برداری شده‌اند، برتری دارند و برای سناریوهایی که نقاط داده در فواصل ثابت نیستند، مناسب‌اند.
- **مقیاس‌پذیری:** این شبکه‌ها بدون توجه به اندازهٔ مجموعه‌داده، دقت و پایداری بالایی را حفظ می‌کنند و در مجموعه‌داده‌های کوچک و بزرگ به‌خوبی عمل می‌کنند.

به‌طور کلی، ODE با ترکیب ریاضیات پیوسته و روش‌های مدرن یادگیری ماشین، انعطاف‌پذیری، دقت و کارایی محاسباتی را افزایش می‌دهند و جایگزینی ارزشمند برای معماری‌های سنتی در تحلیل سری‌های زمانی و وظایف پیوسته هستند.

**•فضای هیلبرت هسته‌ای بازتولیدکننده (RKHS)**

این روش امکان نمایش داده‌ها در فضایی با ابعاد بالاتر را فراهم می‌سازد. در این فضا، به‌جای کارکردن با ویژگی‌های اولیه، داده‌ها با استفاده از نگاشتی غیرخطی و از طریق تابع هسته به فضایی منتقل می‌شوند که در آن، روابط پیچیده‌تر میان داده‌ها به‌صورت خطی قابل تفکیک‌اند. این ویژگی، به مدل‌های یادگیری اجازه می‌دهد تا الگوهای پنهان در داده‌ها را بهتر شناسایی کنند. استفاده از RKHS در این مقاله به‌منظور بهبود تفکیک‌پذیری طبقه‌ها و افزایش توان مدل در یادگیری

ساختارهای غیرخطی انجام شده‌است. استفاده از RKHS در این مقاله با هدف بهبود تفکیک‌پذیری طبقه‌ها و افزایش توان مدل در یادگیری ساختارهای غیرخطی انجام شده‌است.

فضای RKHS چهارچوبی ریاضی است که امکان نمایش توابع اعمال‌شده روی داده‌ها را به شکل بردارهایی در یک فضای جدید فراهم می‌کند. در این فضا، می‌توان شباهت و رابطهٔ بین توابع را با استفاده از معیارهایی مانند ضرب داخلی سنجید.

ترفند هسته‌ای نگاشت ضمنی به فضای RKHS ایجاد می‌کند؛ اما استفادهٔ مستقیم از آن در شبکه‌های عصبی نیازمند نگاشت صریح است. در این پژوهش، با استفاده از ویژگی‌های فوریه تصادفی (RFF)، داده‌ها ابتدا با یک ماتریس وزن تصادفی ثابت نگاشت شده‌است [۲۴]؛ سپس توابع سینوس و کسینوس روی آن‌ها اعمال می‌شود. نتیجه، نماینده‌ای صریح از فضای RKHS است که به‌عنوان ورودی به لایه‌های بعدی شبکه استفاده می‌شود.

استفاده از این روش مزایا مهم زیر را به همراه خواهد داشت:

**نمایش ساده‌تر توزیع‌ها:** در RKHS، توزیع‌های احتمالاتی به شکل بردارهایی در یک فضای خاص نشان داده می‌شوند که این کار انجام محاسبات و مقایسهٔ بین آن‌ها را آسان‌تر می‌کند، بدون اینکه نیاز به مدل‌سازی پیچیده باشد.

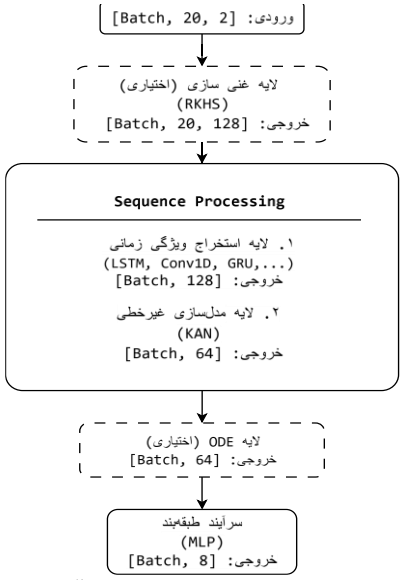
**تقریب بهتر توابع پیچیده:** توابع پیچیده می‌توانند به ترکیبی از توابع ساده‌تر تبدیل شوند که باعث می‌شود مدل‌ها ساده‌تر و قابل فهم‌تر باشند و درعین‌حال عملکرد بهتری روی داده‌های جدید داشته باشند. این ویژگی در روش‌هایی مانند ماشین بردار پشتیبان کاربرد زیادی دارد.

**توانایی تحلیل روابط غیرخطی:** با استفاده از ترفند هسته‌ای، داده‌ها به فضایی با ابعاد بالاتر منتقل می‌شوند تا روابط غیرخطی به‌صورت خطی قابل تحلیل باشند، بدون این‌که لازم باشد ویژگی‌های جدید را به‌صورت دستی تعریف کنیم. این قابلیت باعث شده‌است RKHS در زمینه‌هایی مانند پردازش تصویر و تحلیل داده‌های سری زمانی بسیار مؤثر باشد.

باتوجه به مبانی مطرح‌شده، در بخش بعدی ساختار کلی و نحوهٔ ترکیب این مؤلفه‌ها در چهارچوب پیشنهادی این مقاله تشریح خواهد شد.

## ۵-معماری پیشنهادی

طبقه‌بندی دقیق ترافیک رمزگذاری‌شده نیازمند معماری‌هایی است که بتوانند هم‌زمان وابستگی‌های زمانی، روابط غیرخطی پیچیده و ویژگی‌های خاص داده‌های رمزنگاری‌شده مانند فواصل زمانی نامنظم و نوفه‌دار را مدل‌سازی کنند. در این مقاله، با بهره‌گیری از مبانی مطرح‌شده در بخش پیشین، معماری جدیدی به نام SeqKAN معرفی شده‌است. در این معماری، توانایی شبکه‌های پردازش دنباله و استخراج وابستگی‌های زمانی، با قابلیت‌های شبکهٔ KAN در مدل‌سازی روابط غیرخطی و تفسیرپذیری ذاتی ترکیب می‌شود؛ همچنین به‌صورت دل‌خواه از نگاشت داده‌ها به فضای RKHS برای افزایش توانایی مدل در نمایش پیچیدگی‌های داده و از ODE برای تحلیل دقیق‌تر رفتار دینامیکی داده‌ها، مانند داده‌های ترافیکی رمزنگاری‌شده با فواصل زمانی نامنظم، استفاده شده‌است. این ترکیب تفسیرپذیری بالا و دقت مناسبی در طبقه‌بندی ترافیک رمزگذاری‌شده فراهم می‌آورد؛ علاوه‌براین، در این چهارچوب، تأثیر هر یک از مؤلفه‌های کلیدی مانند RKHSو ODE بر عملکرد نهایی از طریق یک مطالعهٔ حذفی جامع[1] مورد ارزیابی قرار گرفته‌است.




**(شکل-۱): معماری پیشنهادی[2]**

**(figure-1): Proposed Architecture**

همان‌طور که در (شکل-۱) مشاهده می‌شود، معماری پیشنهادی شامل لایه‌های زیر است:

۱.لایهٔ ورودی: مدل پیشنهادی، دو ویژگی پایهٔ هر بسته؛ یعنی اندازه و زمان بین بسته‌ها را دریافت می‌کند. هر دنباله شامل بیست بستهٔ غیرهم‌پوشان از بخش‌های مختلف جریان ترافیکی است که پس از حذف ناحیهٔ Handshake، از بخش باقی‌ماندهٔ جریان‌ها انتخاب می‌شوند.

۲.لایه RKHS (بهبود ویژگی): این لایه به‌عنوان یک مرحلهٔ پیش‌پردازش قدرتمند عمل می‌کند. وظیفهٔ آن، نگاشت ویژگی‌های پایه و کم‌بعد (اندازه و زمان بسته) به یک فضای ویژگی غنی‌تر و با ابعاد بالاتر است. این کار باعث می‌شود الگوهای غیرخطی پنهان در داده‌ها، آشکارتر و برای لایه‌های بعدی قابل یادگیری‌تر شوند؛ در اینجا، از لایهٔ ویژگی‌های فوریه تصادفی (RFF) استفاده شده‌است که ورودی‌ها را به فضایی با ابعاد بالاتر (۱۲۸) نگاشت می‌کند تا الگوهای غیرخطی کشف شوند.

[1] Ablation Study

[۲] لایه‌هایی که به‌صورت خط‌چین نمایش داده شده، اختیاری است و درصورت فعال‌سازی برای بهبود دقت مدل استفاده می‌شود.

۳.لایهٔ پردازش ترتیبی[1] (مدل‌سازی روابط): این لایه به‌عنوان هستهٔ اصلی مدل، مسئول استخراج ویژگی‌های زمانی تفسیرپذیر از دنبالهٔ بسته‌ها است. این لایه‌ها وظیفه دارند تا الگوهای زمانی (با LSTM) و روابط عملکردی پیچیده (با KAN) را استخراج کنند و درواقع شامل دو بخش اصلی زیر است:

- **بخش استخراج وابستگی‌های زمانی:**

برای این کار می‌توان از شبکه‌های بازگشتی مانند LSTM به‌منظور استخراج وابستگی‌های زمانی کوتاه‌مدت و بلندمدت از داده‌های ترتیبی استفاده کرد؛ همچنین، شبکه‌هایی مانند Conv1D نیز به‌منظور استخراج ویژگی‌های محلی و ناحیه‌ای در دنباله‌ها قابل استفاده هستند.

- **شبکهٔ KAN:**

ویژگی‌های استخراج‌شده از مرحلهٔ پیشین به شبکهٔ KAN وارد می‌شوند. این شبکه با استفاده از نمایش‌های ریاضی قابل تفسیر، تعاملات پیچیدهٔ میان ویژگی‌ها را به‌صورت نمادین مدل می‌کند؛ برخلاف روش شبکه‌های عصبی عمیق رایج، KAN وابستگی‌ها را از طریق ترکیبی از توابع ساده (مانند چندجمله‌ای‌ها، سینوس، تانژانت و غیره) نمایش می‌دهد که این کار قدرت تفسیرپذیری بالایی به مدل داده و امکان بازنمایی بهتری برای آن فراهم می‌آورد.

از این به بعد در این نوشتار به مجموعهٔ LSTM و KAN به‌اختصار seqKAN گفته می‌شود.

۴.لایهٔ ODE: پس از استخراج ویژگی‌های زمانی، به‌منظور مدل‌سازی پیوسته تغییرات ویژگی‌ها در طول زمان، از لایهٔ مبتنی‌بر ODE استفاده می‌شود. این لایه، برخلاف LSTM یا GRU که مدل‌سازی را بر پایهٔ نقاط گسسته انجام می‌دهند، رفتار سامانه را به‌صورت یک فرایند پیوسته مدل می‌کند.

استفاده از ODE در شرایطی که داده‌ها دارای فواصل زمانی نامنظم یا نوسان‌دار هستند (که در ترافیک‌های رمزگذاری‌شده رایج است)، باعث بهبود دقت مدل، با مدل‌سازی پیوستهٔ روند تغییرات زمانی و کاهش حساسیت به گام‌های زمانی نابرابر می‌شود.

گفتنی است که در این معماری لایهٔ ODE جایگزین استخراج ویژگی‌های زمانی نیست؛ بلکه مکمل آن بوده و با مدل‌سازی پیوسته ساختار داده‌ها پس از استخراج ویژگی‌ها، درک عمیق‌تری از دینامیک داده فراهم می‌کند.

۵. لایهٔ خروجی: یک لایهٔ MLP خروجی نهایی را به طبقه‌های ترافیکی مورد نظر نگاشت می‌کند.

بنابراین، RKHS داده‌ها را آماده و غنی می‌سازد، seqKAN

[1] Sequence Processing

**(جدول-۱): نتایج مطالعهٔ حذفی جامع**

**(table-1): Ablation Study Table**

| | | | | | | |
|---|---|---|---|---|---|---|
| LSTM+KAN+ODE+RKHS | NonVPN | ۹۸ | ۹۸ | ۹۸ | ۹۸ | ۰ |
| | NonEncrypted Traffic | ۹۳ | ۹۴ | ۹۵ | ۹۳ | ۰ |
| | Overall (All Traffic) | ۹۱ | ۹۲ | ۹۳ | ۹۱ | ۰ |
| | Encrypted Traffic | ۸۷ | ۸۸ | ۹۰ | ۸۷ | ۰ |
| | Non-Tor | ۸۷ | ۸۸ | ۸۸ | ۸۷ | ۱ |
| | Tor | ۸۵ | ۸۷ | ۸۹ | ۸۵ | ۰ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| LSTM+KAN+RKHS | NonVPN | ۹۸ | ۹۸ | ۹۸ | ۹۸ | ۰ |
| | NonEncrypted Traffic | ۹۴ | ۹۴ | ۹۵ | ۹۴ | ۰ |
| | Overall (All Traffic) | ۹۰ | ۹۱ | ۹۳ | ۹۰ | ۰ |
| | Non-Tor | ۸۷ | ۸۸ | ۸۹ | ۸۷ | ۰ |
| | Encrypted Traffic | ۸۶ | ۸۸ | ۹۰ | ۸۶ | ۰ |
| | Tor | ۸۶ | ۸۷ | ۸۹ | ۸۶ | ۰ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| LSTM+KAN+ODE | NonVPN | ۹۷ | ۹۷ | ۹۸ | ۹۷ | ۰ |
| | NonEncrypted Traffic | ۹۰ | ۹۱ | ۹۴ | ۹۰ | ۰ |
| | Overall (All Traffic) | ۸۸ | ۹۰ | ۹۲ | ۸۸ | ۰ |
| | Tor | ۸۴ | ۸۶ | ۸۸ | ۸۴ | ۱ |
| | Encrypted Traffic | ۸۴ | ۸۶ | ۸۹ | ۸۴ | ۰ |
| | Non-Tor | ۸۱ | ۸۲ | ۸۴ | ۸۱ | ۱ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| LSTM+KAN | NonVPN | ۹۷ | ۹۷ | ۹۸ | ۹۷ | ۰ |
| | NonEncrypted Traffic | ۹۰ | ۹۲ | ۹۴ | ۹۰ | ۰ |
| | Overall (All Traffic) | ۸۹ | ۹۰ | ۹۳ | ۸۹ | ۰ |
| | Encrypted Traffic | ۸۴ | ۸۵ | ۸۵ | ۸۴ | ۰ |
| | Tor | ۸۲ | ۸۴ | ۸۷ | ۸۲ | ۰ |
| | Non-Tor | ۷۸ | ۷۹ | ۸۲ | ۷۸ | ۰ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| Conv1D+RKHS | NonEncrypted Traffic | ۸۸ | ۹۰ | ۹۳ | ۸۸ | ۰ |
| | Overall (All Traffic) | ۸۵ | ۸۷ | ۹۱ | ۸۵ | ۰ |
| | Encrypted Traffic | ۸۵ | ۸۶ | ۸۹ | ۸۵ | ۰ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| Conv2D+RKHS | NonEncrypted Traffic | ۸۶ | ۸۸ | ۹۳ | ۸۶ | ۰ |
| | Overall (All Traffic) | ۸۵ | ۸۷ | ۹۰ | ۸۵ | ۰ |
| | Encrypted Traffic | ۸۴ | ۸۵ | ۸۷ | ۸۴ | ۰ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| LSTM-Only | NonEncrypted Traffic | ۸۶ | ۸۸ | ۹۳ | ۸۶ | ۰ |
| | Overall (All Traffic) | ۸۵ | ۸۷ | ۹۱ | ۸۵ | ۰ |
| | Encrypted Traffic | ۸۱ | ۸۲ | ۸۵ | ۸۱ | ۰ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| LSTM+RKHS | NonEncrypted Traffic | ۸۵ | ۸۷ | ۹۱ | ۸۵ | ۰ |
| | Encrypted Traffic | ۸۳ | ۸۵ | ۸۷ | ۸۳ | ۰ |
| | Overall (All Traffic) | ۸۰ | ۸۴ | ۹۰ | ۸۰ | ۰ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| LSTM+ODE+RKHS | NonEncrypted Traffic | ۸۲ | ۸۶ | ۹۲ | ۸۲ | ۱ |
| | Encrypted Traffic | ۸۴ | ۸۵ | ۸۷ | ۸۴ | ۰ |
| | Overall (All Traffic) | ۸۰ | ۸۴ | ۸۹ | ۸۰ | ۱ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| MLP+RKHS | NonEncrypted Traffic | ۸۵ | ۸۸ | ۹۲ | ۸۵ | ۰ |
| | Encrypted Traffic | ۸۵ | ۸۵ | ۸۷ | ۸۵ | ۰ |
| | Overall (All Traffic) | ۷۷ | ۸۱ | ۸۸ | ۷۷ | ۰ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| KAN+ODE+RKHS | NonEncrypted Traffic | ۸۴ | ۸۷ | ۹۲ | ۸۴ | ۰ |
| | Overall (All Traffic) | ۸۲ | ۸۴ | ۸۸ | ۸۲ | ۰ |
| | Encrypted Traffic | ۸۱ | ۸۳ | ۸۶ | ۸۱ | ۱ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| KAN+RKHS | NonEncrypted Traffic | ۸۴ | ۸۶ | ۹۱ | ۸۴ | ۰ |
| | Overall (All Traffic) | ۸۲ | ۸۴ | ۸۸ | ۸۲ | ۰ |
| | Encrypted Traffic | ۸۲ | ۸۳ | ۸۴ | ۸۲ | ۰ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| Conv1D+ODE+RKHS | NonEncrypted Traffic | ۸۴ | ۸۶ | ۹۱ | ۸۴ | ۱ |
| | Encrypted Traffic | ۸۴ | ۸۵ | ۸۷ | ۸۴ | ۰ |
| | Overall (All Traffic) | ۷۶ | ۸۱ | ۸۸ | ۷۶ | ۱ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| Conv2D-Only | NonEncrypted Traffic | ۸۵ | ۸۷ | ۹۱ | ۸۵ | ۰ |
| | Encrypted Traffic | ۸۲ | ۸۳ | ۸۴ | ۸۲ | ۰ |
| | Overall (All Traffic) | ۷۹ | ۸۲ | ۸۷ | ۷۹ | ۰ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| KAN-Only | NonEncrypted Traffic | ۸۳ | ۸۶ | ۹۱ | ۸۳ | ۰ |
| | Overall (All Traffic) | ۷۸ | ۸۲ | ۸۸ | ۷۸ | ۰ |
| | Encrypted Traffic | ۷۸ | ۸۰ | ۸۴ | ۷۸ | ۰ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| KAN+ODE | NonEncrypted Traffic | ۸۲ | ۸۶ | ۹۲ | ۸۲ | ۰ |
| | Overall (All Traffic) | ۷۸ | ۸۲ | ۸۸ | ۷۸ | ۰ |
| | Encrypted Traffic | ۷۸ | ۸۰ | ۸۴ | ۷۸ | ۱ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| MLP-Only | NonEncrypted Traffic | ۸۲ | ۸۵ | ۹۰ | ۸۲ | ۰ |
| | Overall (All Traffic) | ۷۸ | ۸۱ | ۸۷ | ۷۸ | ۰ |
| | Encrypted Traffic | ۸۰ | ۸۱ | ۸۳ | ۸۰ | ۰ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| Conv2D+ODE+RKHS | Encrypted Traffic | ۸۵ | ۸۵ | ۸۶ | ۸۵ | ۰ |
| | NonEncrypted Traffic | ۸۰ | ۸۲ | ۸۸ | ۸۰ | ۱ |
| | Overall (All Traffic) | ۷۱ | ۷۶ | ۸۵ | ۷۱ | ۱ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| LSTM+ODE | NonEncrypted Traffic | ۸۱ | ۸۵ | ۹۱ | ۸۱ | ۱ |
| | Overall (All Traffic) | ۸۱ | ۸۴ | ۸۸ | ۸۱ | ۱ |
| | Encrypted Traffic | ۷۵ | ۷۶ | ۷۹ | ۷۵ | ۰ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| Conv2D+ODE | NonEncrypted Traffic | ۸۳ | ۸۵ | ۸۹ | ۸۳ | ۱ |
| | Encrypted Traffic | ۸۰ | ۸۱ | ۸۳ | ۸۰ | ۰ |
| | Overall (All Traffic) | ۷۲ | ۷۶ | ۸۲ | ۷۲ | ۱ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| Conv1D-Only | Encrypted Traffic | ۸۲ | ۸۳ | ۸۴ | ۸۲ | ۰ |
| | NonEncrypted Traffic | ۷۰ | ۷۲ | ۷۷ | ۷۰ | ۰ |
| | Overall (All Traffic) | ۴۵ | ۴۶ | ۶۸ | ۴۵ | ۰ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| Conv1D+ODE | Encrypted Traffic | ۸۲ | ۸۳ | ۸۵ | ۸۲ | ۰ |
| | NonEncrypted Traffic | ۶۰ | ۶۰ | ۶۹ | ۶۰ | ۱ |
| | Overall (All Traffic) | ۴۵ | ۴۳ | ۶۴ | ۴۵ | ۱ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| MLP+ODE+RKHS | Overall (All Traffic) | ۶۲ | ۵۸ | ۶۷ | ۶۲ | ۱ |
| | NonEncrypted Traffic | ۵۵ | ۵۸ | ۶۴ | ۵۵ | ۱ |
| | Encrypted Traffic | ۵۲ | ۵۰ | ۶۶ | ۵۲ | ۰ |
| ---------- | ---------- | ---- | ---- | ---- | ---- | ---- |
| MLP+ODE | NonEncrypted Traffic | ۶۵ | ۵۹ | ۵۶ | ۶۵ | ۱ |
| | Overall (All Traffic) | ۵۹ | ۵۵ | ۶۳ | ۵۹ | ۱ |
| | Encrypted Traffic | ۴۱ | ۳۵ | ۵۸ | ۴۱ | ۰ |

الگوهای اصلی را استخراج می‌کنند و ODE این الگوها را در یک بستر زمانی پیوسته پالایش می‌کند. مطالعهٔ حذفی ما در ادامه، تأثیر هر یک از این مؤلفه‌ها را به‌صورت تجربی نشان خواهد داد.

## ۶- نتایج پیاده‌سازی

در این بخش، نتایج حاصل از ارزیابی جامع معماری‌های مختلف ارائه می‌شود.

تمام آزمایش‌ها بر روی یک سیستم مجهز به کارت گرافیک NVIDIA GeForce RTX 3060 انجام شد. برای پردازش‌های عمومی از پردازندهٔ Intel Core i7-12700K و ۳۲ گیگابایت حافظهٔ RAM استفاده شد. مدل‌ها با استفاده از فریمورک PyTorch پیاده‌سازی شدند. برای تمام مدل‌ها، از تابع هزینهٔ Cross-Entropy وزن‌دار برای مقابله با نامتوازن‌بودن کلاس‌ها استفاده شد. مدل‌ها به‌مدت چهل دوره[1] آموزش داده شدند.

### ۶-۱-نتایج اصلی و تحلیل حساسیت

برای ارزیابی دقیق نقش هر مؤلفه، یک مطالعهٔ حذفی[2] جامع بر روی مجموعه‌داده‌های مختلف، شامل مجموعه‌داده‌های رمزنگاری‌شده، انجام شد. نتایج کامل در **Error! Reference source not found.** ارائه شده‌است. این جدول بر اساس امتیاز F1مرتب شد تا بهترین مدل‌ها به‌راحتی شناسایی شوند. گفتنی است که جزئیات پیاده‌سازی هر یک از مدل‌ها و دقت آن‌ها بر روی هر یک از طبقه‌ها و دیگر موارد در مخزن گیت پروژه[3] موجود است.

در این تحلیل، خانوادهٔ معماری پیشنهادی seqKAN، درکل عملکرد بهتری از خود نشان دادند و چهار رتبهٔ برتر جدول را به‌خود اختصاص دادند. این موضوع نشان می‌دهد ترکیب استخراج ویژگی‌های زمانی به‌وسیلهٔ LSTM و سپس مدل‌سازی روابط پیچیده و غیرخطی به‌وسیلهٔ KAN، یک استراتژی بسیار مؤثر برای تحلیل ترافیک رمزنگاری‌شده‌است.

افزودن لایهٔ RKHS به‌طور میانگین منجر به بهبود قابل توجهی در F1-Score شد؛ برای مثال، seqKAN+RKHS در مقایسه با seqKAN، امتیاز F1 را حدود سه درصد افزایش داده‌است (از ۸۴.۵۳درصد به ۸۷.۵۵درصد). این نشان می‌دهد که نگاشت ویژگی‌ها به یک فضای ابعادی بالاتر[4] به مدل کمک می‌کند تا الگوهای پنهان در داده‌های نوفه‌ای و رمزنگاری‌شده را بهتر تفکیک کند.

مدل seqKAN+RKHS با امتیاز F1 برابر با ۸۷.۵۵درصد، بهترین عملکرد کلی را در مجموعه‌داده‌های رمزنگاری‌شده (ترکیب VPN و Tor) به‌دست آورد و به‌عنوان مدل بهینه از نظر توازن دقت و سرعت معرفی می‌شود؛ بااین‌حال، مدل seqKAN+ODE+RKHS به‌طور خاص بر روی مجموعه‌دادهٔ Tor که دارای فواصل زمانی نامنظم‌تری است، عملکردی پایدارتر و دقیق‌تر (۸۶.۹۱درصد) را نسبت به سایر روش‌های پایه از خود نشان می‌دهد. این امر نشان می‌دهد که قابلیت مدل‌سازی پیوسته در ODE می‌تواند در شرایط خاص و برای داده‌های دارای نوسانات زمانی شدید، مفید واقع شود

برای سنجش کارایی عملی مدل‌ها، زمان آموزش و استنتاج آن‌ها اندازه‌گیری شد؛ Error! Reference source not found.)؛ این نتایج را مقایسه می‌کند. این جدول نشان می‌دهد که ماژول ODE، اگرچه گاهی به بهبود جزئی دقت کمک می‌کند (مانند مقایسهٔ رتبهٔ نخست و دوم)، اما هزینهٔ محاسباتی بسیار بالایی دارد؛ برای مثال، افزودن ODE به مدل seqKAN+RKHS، زمان استنتاج را ۶ برابر (از ۰.۰۸ به ۰.۴۹ میلی‌ثانیه) افزایش می‌دهد. این هزینهٔ سنگین، استفاده از آن را در بسیاری از کاربردهای عملی غیربهینه می‌سازد؛ درمقابل، مدل seqKAN+RKHS با زمان آموزش و استنتاج معقول، یک گزینهٔ بسیار کارآمد محسوب می‌شود که بهترین توازن را میان دقت و سرعت ارائه می‌دهد.

**(جدول-۲): مقایسهٔ نتایج در دادهٔ رمزنگاری‌شده**
**(table-2): Comparison Table in Encrypted Data**

| | FlowPic (CNN) | Fast & Lean (LSTM+ODE) | SeqKAN |
|---|---|---|---|
| TOR | ۸۵.۷درصد | ۸۲.۵۸ درصد | ۸۶.۹۱ درصد |
| VPN | ۸۸.۴ درصد | ۸۸.۷۶ درصد | ۹۱.۳ درصد |

### ۶-۲-تحلیل تفسیرپذیری

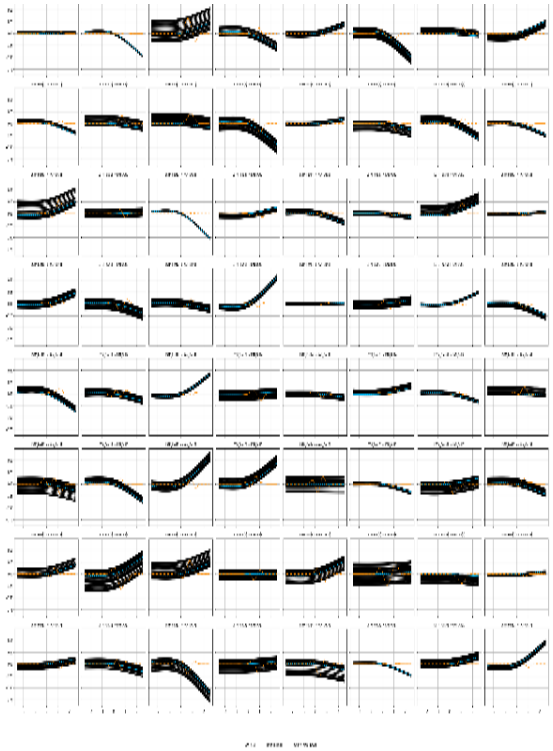
برای اثبات قابلیت تفسیرپذیری و ارزیابی شفافیت مدل پیشنهادی، رویکرد تحلیلی چندجانبه‌ای به‌کار گرفته شد که شامل سه روش مکمل است: تفسیرپذیری ذاتی با KAN، تحلیل اهمیت کلی ویژگی‌ها با SHAP و توضیح محلی پیش‌بینی‌ها با LIME. هماهنگی نتایج این سه روش، دیدی جامع و قابل اطمینان از عملکرد درونی مدل فراهم می‌آورد.

در گام نخست، به تحلیل تفسیرپذیری ذاتی مدل از طریق معماری KAN پرداخته شد. پس از آموزش مدل، توابع فعال‌سازی شبکه KAN استخراج و ترسیم شدند.

**Error! Reference source not found.**) نمونه‌ای از این توابع یادگرفته‌شده را نمایش می‌دهد؛ برخلاف شبکه‌های عصبی معمول که از توابع فعال‌سازی ثابت استفاده می‌کنند، در معماری KAN هر یال تابع فعال‌سازی مستقلی دارد که قابل یادگیری است. این ویژگی امکان مشاهده و تحلیل دقیق روابط ریاضی را فراهم می‌کند که مدل به‌صورت صریح فراگرفته است؛ همان‌طور که در Error! Reference source not found.دیده می‌شود، مدل برای برخی ورودی‌ها توابعی

[1] epoch
[2] Ablation Study
[3] https://github.com/drAliRahnema/seqKAN
[4] feature mapping

ساده و به‌طور تقریبی خطی یاد گرفته است که بیان‌کنندهٔ اهمیت کم و هرس خودکار این مسیرهاست؛ درمقابل، برای ورودی‌های کلیدی، توابع فعال‌سازی غیرخطی و پیچیده‌تری آموزش داده شده‌اند که نقش برجسته‌تر آن‌ها را در پیش‌بینی مدل نشان می‌دهد[1]. این تنوع ساختاری به‌خوبی قدرت معماری KAN را در درک ساختار داده‌ها و افزایش شفافیت مدل نشان می‌دهد.

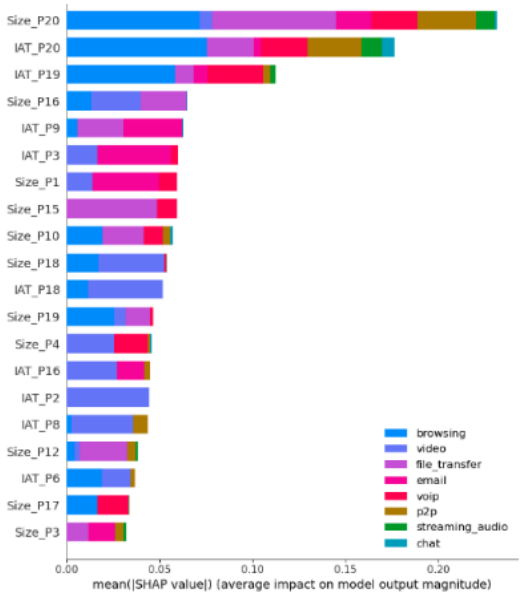


**(شکل-۲): چند نمونه از توابع فعال‌سازی یادگرفته‌شده شبکهٔ KAN**
**(figure-2): kan sample activationFunctions**

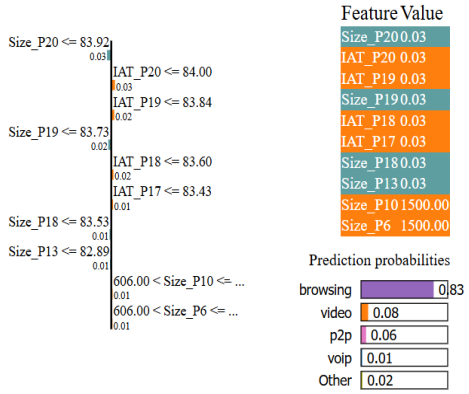
به‌منظور تکمیل تحلیل تفسیرپذیری ذاتی، از ابزارهای SHAP و LIME بهره گرفته شد. تحلیل کلی SHAP نشان می‌دهد که ویژگی‌هایی مانند اندازهٔ بسته‌ها (Size) و فاصلهٔ زمانی بین آن‌ها (IAT) نقش کلیدی در تصمیم‌گیری‌های مدل دارند؛ برای نمونه در تحلیل SHAP موجود در (شکل-۳) ویژگی «اندازهٔ بسته بیستم» به‌عنوان تأثیرگذارترین عامل شناسایی می‌شود. این اهمیت در سطح محلی نیز به‌وسیلهٔ LIMEتأیید می‌شود؛ (شکل-۴). به‌طور مشخص، در نمونه‌ای که مدل با اطمینان بالا آن را به یک طبقهٔ خاص نسبت داده بود، LIME نشان داد که از همین ویژگی به‌عنوان دلیل اصلی و شاهد قطعی برای رد سایر طبقه‌ها استفاده کرده‌است.

نکتهٔ قابل توجه در این تحلیل، سازگاری بالا بین این روش‌هاست؛ به‌طوری که ویژگی که SHAP به‌عنوان عاملی مهم در سطح کلی معرفی می‌کند، در معماری KAN با یک تابع فعال‌سازی پیچیده و غیرخطی مدل شده‌است و در LIME نیز، در یک نمونهٔ واقعی، نشان داده می‌شود که چگونه مقدار مشخص همین ویژگی به تصمیمی منطقی و قابل توضیح منجر شده‌است.

تأیید متقابل نتایج نشان می‌دهد که مدل پیشنهادی فراتر از یک جعبهٔ سیاه عمل می‌کند و به سیستمی شفاف، قابل اعتماد و قابل تفسیر تبدیل شده‌است که توانایی استخراج و یادگیری ویژگی‌های کاربردی و الگوهای معنادار از داده‌ها را دارد. گفتنی است که این تحلیل برای سایر مدل‌هایی که از معماری KAN بهره می‌برند نیز انجام شده و نتایج کامل آن در مخزن گیت پروژه در دسترس است.




**(شکل-۳): تحلیل SAHP**
**(figure-3): SHAP Analyze**




**(شکل-۴): نمونهٔ تحلیل LIME**
**(figure-4): LIME Sample Analyze**

در اینجا tjkd‘ است که روش‌هایی مانند SHAP و LIME تنها میزان تأثیر ویژگی‌ها را نشان می‌دهند، اما KAN با بصری‌سازی ساختار درونی مدل، نحوهٔ واکنش آن به هر

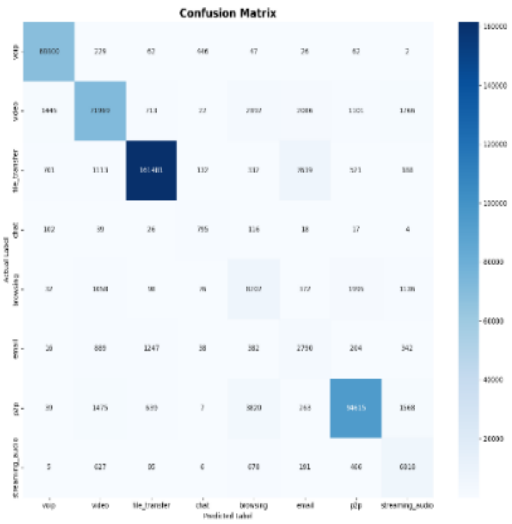
[1] علاوه‌بر شکل توابع، ضخامت خطوط در نمودار نیز اطلاعات ارزشمندی در مورد توزیع داده‌ها ارائه می‌دهد. نواحی با خطوط ضخیم‌تر، نشان‌دهندهٔ تراکم بالای داده‌های آموزشی هستند؛ این یعنی مدل، تابع خود را در این نواحی بر اساس شواهد آماری قوی یاد گرفته است؛ درمقابل، نواحی با خطوط نازک، بیان‌کنندهٔ داده‌های پراکنده و نادر هستند که نشان می‌دهد تابع یادگرفته‌شده در این بخش‌ها ممکن است قابلیت تعمیم‌پذیری کمتری داشته باشد. این دیدگاه دوگانه، به پژوهش‌گر اجازه می‌دهد تا نه‌تنها آنچه مدل یاد گرفته، بلکه میزان اطمینان آن بر اساس داده‌های موجود نیز ارزیابی می‌کند.

ویژگی را آشکار می‌کند. این رویکرد نه‌تنها اهمیت، بلکه شکل دقیق رابطهٔ مدل با ویژگی‌ها (برای مثال خطی، پله‌ای یا سینوسی) را نشان می‌دهد و درکی عمیق‌تر از منطق تصمیم‌گیری مدل فراهم می‌سازد.

## ۶-۳-تحلیل عملکرد طبقه‌بندی

به‌منظور مقایسهٔ عملکرد طبقه‌بندی، ماتریس‌های درهم‌ریختگی در طبقه‌بندی‌های مختلف ترافیک مورد بررسی قرار گرفته است که نتایج کامل آن در مخزن گیت پروژه قابل مشاهده است. این تحلیل به ما اجازه می‌دهد تا علاوه‌بر ارزیابی دقت کلی، رفتار مدل در برابر طبقه‌های خاص نیز بررسی و منابع خطا شناسایی شوند.

در ادامه به تحلیل عملکرد مدل به تفکیک هر طبقه پرداخته می‌شود. مدل در طبقه‌بندی طبقه‌های پرتکرار و دارای الگوهای متمایز مانند voip، file_transfer، p2p و video عملکرد بسیار موفقی داشته و توانسته برای این کلاس‌ها امتیاز F1 بالای نود درصد به‌دست آورد. بالاترین دقت مربوط به طبقهٔ voip با F1 برابر با ۹۷.۷۲درصد است که نشان‌دهندهٔ توان بالای مدل در یادگیری الگوهای ترافیک بلادرنگ است؛ درمقابل، عملکرد مدل در طبقه‌بندی طبقه‌های کم‌نمونه یا دارای الگوهای رفتاری مشابه، از جمله email، chat و browsing، به‌مراتب ضعیف‌تر بوده‌است. به‌ویژه، طبقهٔ email با امتیاز F1 معادل ۲۸.۹۲درصد بیشترین چالش را برای مدل ایجاد کرده‌است. این نتایج با تحلیل ارائه‌شده در بخش مربوط به ماتریس درهم‌ریختگی نیز هم‌راستا هستند و نشان می‌دهند که به‌منظور بهبود عملکرد در این طبقه‌ها، بهره‌گیری از ویژگی‌های سطح بالاتر و معماری‌های مبتنی‌بر توجه که قادر به تمرکز بر تمایزهای ظریف رفتاری هستند، ضروری خواهد بود.




**(شکل-۵): ماتریس درهم‌ریختگی مدل SeqKAN**
**(figure-5): Confusion Matrix of SeqKAN Modle**

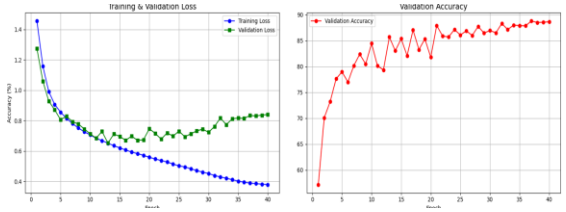
در (Error! Reference source not found.، نتایج حاصل از ماتریس درهم‌ریختگی مدل پیشنهادی برتر بر روی مجموعه‌داده‌ی رمزنگاری‌شده، عملکرد مدل را در سطح هر کلاس نمایش می‌دهد. اعداد قرارگرفته روی قطر اصلی ماتریس نشان‌دهندهٔ توانایی مدل در شناسایی صحیح طبقه‌های مختلف هستند. مدل در طبقه‌بندی طبقه‌هایی مانند file_transfer، video_streaming و p2p عملکرد دقیقی از خود نشان داده و موفق شده‌است الگوهای غالب این ترافیک‌ها (نظیر حجم داده، مدت زمان نشست‌ها و توزیع بین‌زمانی بسته‌ها) را به‌خوبی یاد بگیرد.

درمقابل، تحلیل خانه‌های خارج از قطر اصلی حاکی از وجود برخی الگوهای خطا در مدل است. به‌طور مشخص، نمونه‌هایی از طبقهٔ chat به اشتباه در طبقهٔ browsing طبقه‌بندی شده‌اند؛ خطایی که به احتمال ناشی از شباهت در الگوهای زمانی و اندازهٔ بسته‌ها میان این دو نوع ترافیک و استفادهٔ مشترک آن‌ها از پروتکل‌هایی مانند HTTPS است؛ به‌طور مشابه، بخشی از نمونه‌های طبقهٔ email نیز به‌اشتباه در طبقهٔ file_transfer قرار گرفته‌اند که می‌تواند ناشی از وجود پیوست‌های حجیم در رایانامه‌ها و شباهت جریان دادهٔ آن‌ها با ترافیک انتقال فایل باشد.

این تحلیل نشان می‌دهد که با وجود استفاده از تابع هزینهٔ وزن‌دار برای کاهش اثر متوازن‌نبودن طبقه‌ها، چالش‌هایی ناشی از شباهت ذاتی در رفتار برخی انواع ترافیک همچنان پابرجاست. برای رفع این محدودیت‌ها، پیشنهاد می‌شود در پژوهش‌های آینده از ویژگی‌های سطح بالاتر مبتنی‌بر رفتار دنباله‌ها و همچنین معماری‌های مبتنی‌بر توجه [1] استفاده شود تا مدل بتواند بر جنبه‌های تمایزدهنده و ظریف‌تر تمرکز کرده و دقت طبقه‌بندی را بهبود بخشد.

## ۶-۴-تحلیل نمودار منحنی هم‌گرایی

با دقت در نمودارهای آموزشی (شکل-۶ )مشخص می‌شود که مدل پایه در دوره‌های ابتدایی آموزش، با نرخ هم‌گرایی بالا به‌سرعت به سطح قابل قبولی از عملکرد می‌رسد و روندی پایدار را تا میانه‌های آموزش حفظ می‌کند؛ این پایداری تا حد زیادی حاصل تنظیم مناسب نرخ یادگیری است؛ بااین‌حال، از حدود دورهٔ پانزده به بعد، نشانه‌های بیش‌برازش به‌تدریج ظاهر می‌شود و منحنی دقت نیز پس از رسیدن به حدود ۸۹ درصد، به حالت اشباع می‌رسد. این روند نشان می‌دهد که برای جلوگیری از افت عملکرد تعمیم، به‌کارگیری روش توقف زودهنگام در بازه دوره‌های ۲۵ تا ۳۰ توصیه می‌شود.




**(شکل-۶): نمودارهای آموزشی مدل seqKAN**
**(figure-6): seqKAN training curves**

[1] Attention Mechanisms

## ۷-بحث و محدودیت‌ها

گرچه نتایج این پژوهش امیدوارکننده است، اما باید با دیدی واقع‌بینانه به برخی محدودیت‌ها نیز توجه کرد:

پیچیدگی در تنظیم هایپرپارامترها: معماری‌های ترکیبی مانند SeqKAN+ODE+RKHS دارای تعداد زیادی مؤلفه‌های قابل تنظیم هستند. یافتن ترکیب بهینهٔ این مؤلفه‌ها نیازمند جست‌وجوی گسترده و منابع محاسباتی بالاست.

هزینهٔ محاسباتی ماژول ODE: همان‌طور که نتایج نشان می‌دهد، استفاده از ODE باعث افزایش هزینهٔ محاسباتی مدل می‌شود. این مسئله در کاربردهای زمان‌واقعی (real-time) می‌تواند محدودکننده باشد.

وابستگی به کیفیت داده‌ها: عملکرد مدل به‌شدت به کیفیت و تنوع داده‌های برچسب‌دار وابسته است. نبود داده‌های متعادل یا دقیق می‌تواند باعث کاهش دقت مدل در برخی طبقه‌ها شود.

## ۸-نتیجه‌گیری

این پژوهش، یک ارزیابی جامع از پتانسیل شبکه‌های کولموگروف-آرنولد (KAN) در طبقه‌بندی ترافیک رمزنگاری‌شده ارائه داد. در این پژوهش نشان داده شد که استفاده از KAN در یک معماری ترکیبی مبتنی‌بر توالی مانند seqKAN می‌تواند قدرت مدل‌سازی روابط پیچیدهٔ زمانی را افزایش دهد. این معماری با دست‌یابی به امتیاز F1 بالا، تعادلی بهینه میان دقت، کارایی محاسباتی و تفسیرپذیری فراهم می‌کند.

مطالعهٔ حذفی انجام‌شده نیز نشان داد که هر یک از اجزایKAN ، ODE و RKHS به‌طور مستقل و مکمل در افزایش توان مدل نقش دارند. مقایسه با روش‌های پایه مانند FlowPic و Fast & Lean نیز برتری مدل این پژوهش در مواجهه با داده‌های نامتعادل و ترافیک‌های پیچیده مانند Tor را تأیید می‌کند.

## ۹-پیشنهادات برای کارهای آینده

برای بهبود عملکرد مدل در دسته‌بندی طبقه‌های کم‌نمونه یا مشابه، و نیز افزایش قابلیت تعمیم آن، می‌توان اقدامات زیر را در پژوهش‌های آتی مدنظر قرار داد:

**ترکیب با معماری‌های مبتنی‌بر توجه:** به‌کارگیری سازوکارهای Attention یا Transformerها به‌جای LSTM می‌تواند به مدل در درک بهتر وابستگی‌های بلندمدت و جزئیات رفتاری کمک کند.

در ادامهٔ این پژوهش، یکی از مسیرهای پیشنهادی، به‌کارگیری معماری‌های مبتنی‌بر توجه[1] است. هدف از این کار، کاهش خطاهای ناشی از شباهت آماری میان برخی انواع ترافیک شبکه است. افزودن یک لایهٔ Attention می‌تواند به مدل امکان دهد تا بسته‌های مهم‌تر را در توالی بهتر شناسایی کرده و بر ریزالگوهای متمایزکننده بیشتر تمرکز کند؛ برای مثال، ترافیک چت برحسب معمول شامل بسته‌های کوچک و یک‌نواخت است؛ در حالی‌که ترافیک وب ممکن است الگوهای انفجاری‌تری داشته باشد. سازوکار توجه می‌تواند این تفاوت‌های ظریف را بهتر تشخیص داده و خطاهای مدل را کاهش دهد.

**بهبود معماری برای کاربردهای زمان واقعی:** با ساده‌سازی برخی ماژول‌ها یا جایگزینی آن‌ها با نسخه‌های سبک‌تر، می‌توان سرعت استنتاج مدل را افزایش داد و آن را برای محیط‌های عملیاتی مانند سامانه‌های تشخیص نفوذ آماده‌تر کرد.

**استفاده از داده‌های برخط:** پیاده‌سازی مدل روی داده‌های شبکهٔ واقعی و بررسی عملکرد در شرایط دینامیک و پیوسته، می‌تواند کاربردپذیری مدل را در محیط‌های صنعتی یا شبکه‌های عملیاتی به اثبات برساند

[1] Attention Mechanism

## ۱۰-مراجع 10-References


[1] W. Wang, M. Zhu, J. Wang, X. Zeng, and Z. Yang, "End-To-end encrypted traffic classification with one-dimensional convolution neural networks," in *2017 IEEE International Conference on Intelligence and Security Informatics: Security and Big Data, ISI 2017*, Aug. 2017, pp. 43–48. doi: 10.1109/ISI.2017.8004872.

[2] S. Zander, T. Nguyen, and G. Armitage, "Automated traffic classification and application identification using machine learning," *Proc. - Conf. Local Comput. Networks, LCN*, vol. 2005, pp. 250–257, 2005, doi: 10.1109/LCN.2005.35.

[3] B. Yamansavascilar, M. A. Guvensan, A. G. Yavuz, and M. E. Karsligil, "Application identification via network traffic classification," *2017 Int. Conf. Comput. Netw. Commun. ICNC 2017*, pp. 843–848, 2017, doi: 10.1109/ICCNC.2017.7876241.

[4] N. V. Verde, G. Ateniese, E. Gabrielli, L. V. Mancini, and A. Spognardi, "No NAT'd User left Behind: Fingerprinting Users behind NAT from NetFlow Records alone," Feb. 2014, [Online]. Available: http://arxiv.org/abs/1402.1940

[5] M. Conti, L. V. Mancini, R. Spolaor, and N. V. Verde, "Analyzing Android Encrypted Network Traffic to Identify User Actions," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 1, pp. 114–125, Jan. 2016, doi: 10.1109/TIFS.2015.2478741.

[6] M. Lotfollahi, R. S. H. Zade, M. J. Siavoshani, and M. Saberian, "Deep Packet: A Novel Approach For Encrypted Traffic Classification Using Deep Learning," Sep. 2017, [Online]. Available: http://arxiv.org/abs/1709.02656

[7] R. Dubin, A. Dvir, O. Pele, and O. Hadar, "I Know What You Saw Last Minute - Encrypted HTTP Adaptive Video Streaming

Title Classification," Feb. 2016, doi: 10.1109/TIFS.2017.2730819.
[8] R. Schuster, V. Shmatikov, and E. Tromer, "Beauty and the burst: Remote identification of encrypted video streams," *Proc. 26th USENIX Secur. Symp.*, pp. 1357–1374, 2017.
[9] T. Shapira and Y. Shavitt, "FlowPic: A Generic Representation for Encrypted Traffic Classification and Applications Identification," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 2, pp. 1218–1232, Jun. 2021, doi: 10.1109/TNSM.2021.3071441.
[10] Z. Cao, G. Xiong, Y. Zhao, Z. Li, and L. Guo, "A survey on encrypted traffic classification," *Commun. Comput. Inf. Sci.*, vol. 490, pp. 73–81, 2014, doi: 10.1007/978-3-662-45670-5_8.
[11] S. Roy, T. Shapira, and Y. Shavitt, "Fast and lean encrypted Internet traffic classification," *Comput. Commun.*, vol. 186, pp. 166–173, Mar. 2022, doi: 10.1016/j.comcom.2022.02.003.
[12] Z. Chen, K. He, J. Li, and Y. Geng, "Seq2Img: A sequence-to-image based approach towards IP traffic classification using convolutional neural networks," *Proc. - 2017 IEEE Int. Conf. Big Data, Big Data 2017*, vol. 2018-Janua, pp. 1271–1276, 2017, doi: 10.1109/BigData.2017.8258054.
[13] X. Lin, G. Xiong, G. Gou, Z. Li, J. Shi, and J. Yu, "ET-BERT : A Contextualized Datagram Representation with Pre-training Transformers for Encrypted Traffic Classification," vol. 1, pp. 633–642, doi: 10.1145/3485447.3512217.
[14] Z. Liu, "TransECA-Net : A Transformer-Based Model for Encrypted Traffic Classification," 2025.
[15] Koukoulis, I. Syrigos, and T. Korakis, "Self-Supervised Transformer-based Contrastive Learning for Intrusion Detection Systems".
[16] T. T. T. Nguyen and G. Armitage, "A Semi-Supervised Learning Framework for Encrypted Traffic Classification Based on Supervised Contrastive Learning and Masked Sequence Prediction Tasks," vol. 10, no. 4, pp. 56–76, 2025, doi: 10.1109/ICAACE65325.2025.11020246.
[17] E. Horowicz, T. Shapira, and Y. Shavitt, "Self-Supervised Traffic Classification : Flow Embedding and Few-Shot Solutions," *IEEE Trans. Netw. Serv. Manag.*, vol. PP, no. September, p. 1, 2024, doi: 10.1109/TNSM.2024.3366848.
[18] T. Shapira and Y. Shavitt, "FlowPic: Encrypted Internet Traffic Classification is as Easy as Image Recognition," in *INFOCOM 2019 - IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2019*, Apr. 2019, pp. 680–687. doi: 10.1109/INFCOMW.2019.8845315.
[19] S. Yu and Y. Won, "A survey of methods for encrypted network traffic fingerprinting," *Math. Biosci. Eng.*, vol. 20, no. 2, pp. 2183–2202, 2023, doi: 10.3934/mbe.2023101.
[20] L. D. Manocchio, S. Layeghy, W. W. Lo, G. K. Kulatilleke, M. Sarhan, and M. Portmann, "FlowTransformer : A transformer framework for flow-based network intrusion detection systems," *Expert Syst. Appl.*, vol. 241, no. July 2023, p. 122564, 2024, doi: 10.1016/j.eswa.2023.122564.
[21] C. Sun, B. Chen, Y. Bu, S. Zhang, and D. Zhang, "Lightweight Traffic Classification Model Based on Deep Learning," vol. 2022, no. 2, 2022, doi: 10.1155/2022/3539919.
[22] G. Draper-Gil, A. H. Lashkari, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of encrypted and VPN traffic using time-related features," in *ICISSP 2016 - Proceedings of the 2nd International Conference on Information Systems Security and Privacy*, 2016, pp. 407–414. doi: 10.5220/0005740704070414.
[23] H. Lashkari, G. D. Gil, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of tor traffic using time based features," in *ICISSP 2017 - Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, 2017, vol. 2017-January, pp. 253–262. doi: 10.5220/0006105602530262.
[24] Rahimi and B. Recht, "Random Features for Large-Scale Kernel Machines," no. 1, pp. 1–8.

**علی رهنما،** دانشجوی دکترای مهندسی فناوری اطلاعات دانشگاه قم است، حوزهٔ فعالیت و علاقه‌مندی ایشان هوش مصنوعی و امنیت اطلاعات است.

نشانی رایانامهٔ ایشان عبارت است از:
**a.rahnema@stu.qom.ac.ir**

**زهرا آخوداد،** عضو هیأت علمی پژوهشگاه توسعهٔ فناوری‌های پیشرفته است. ایشان همچنین در سِمَت معاون توسعه و ارزیابی صنعت افتا با مرکز مدیریت راهبردی افتای ریاست جمهوری نیز همکاری دارد. حوزهٔ فعالیت و علاقه‌مندی ایشان، امنیت اطلاعات است.

نشانی رایانامهٔ ایشان عبارت است از:
**akhoodad@rcdat.ir**