2025, Volume 12, Number 2 (pp. 77--77)
http://www.jcomsec.org

Journal of Computing and Security

تشخیص نفوذ در شبکه‌های کامپیوتری با استفاده از یک شبکه ترکیبی CNN-BiLSTM

مینا زمین کار[آ]، مینا کلینی[آ،*]

[آ] گروه مهندسی کامپیوتر، دانشکده مهندسی، دانشگاه شهید اشرفی اصفهانی، اصفهان، ایران.

اطلاعات مقاله

تاریخچه مقاله:
دریافت: 24 May 2025
اصلاح: 17 November 2025
پذیرش: 01 December 2025
انتشار آنلاین: 05 January 2025

کلمات کلیدی:
داده کاوی، شبکه‌های کامپیوتری، سیستم تشخیص نفوذ، شبکه‌های عصبی کانولوشن، شبکه BiLSTM.

چکیده

سیستم‌های تشخیص نفوذ (IDS) برای ایمن‌سازی شبکه‌های کامپیوتری با شناسایی و تجزیه و تحلیل فعالیت‌های غیرمجاز یا غیرطبیعی و در نتیجه جلوگیری از حملات سایبری بسیار مهم هستند. با توجه به پیچیدگی و حجم فزاینده داده‌های شبکه، تقاضای فزاینده‌ای برای روش‌های پیشرفته و کارآمد تجزیه و تحلیل داده‌ها وجود دارد. این مطالعه یک مدل یادگیری عمیق ترکیبی را پیشنهاد می‌کند که شبکه‌های عصبی کانولوشن (CNN) و شبکه‌های حافظه کوتاه‌مدت بلندمدت دو جهته (BiLSTM) را برای افزایش دقت و استحکام تشخیص نفوذ ترکیب می‌کند. در ابتدا، CNNها برای استخراج ویژگی‌های مکانی از داده‌های خام ترافیک شبکه به کار گرفته می‌شوند. سپس این ویژگی‌ها توسط یک شبکه BiLSTM پردازش می‌شوند تا وابستگی‌های زمانی و روابط زمینه‌ای را ثبت کنند. برای بهبود بیشتر عملکرد طبقه‌بندی، سه طبقه‌بندی‌کننده یادگیری ماشین ــ نزدیک‌ترین k-همسایه (k-NN)، درخت تصمیم‌گیری و ماشین بردار پشتیبان (SVM) ــ بر روی ویژگی‌های استخراج‌شده آموزش داده می‌شوند و خروجی‌های آنها با استفاده از یک روش گروهی رأی‌گیری وزنی ادغام می‌شوند. مدل پیشنهادی با استفاده از مجموعه داده‌های NSL-KDD ارزیابی شده و به دقت ۹۹٪ در طبقه‌بندی دودویی و ۹۹.۱۲٪ در طبقه‌بندی چندکلاسه دست یافته است. نتایج، اثربخشی رویکرد ترکیبی CNN-BiLSTM را در تشخیص دقیق الگوهای حمله شناخته شده و پیچیده در ترافیک شبکه نشان می‌دهد.

* نویسنده مسئول.
آدرس‌های رایانامه: zaminkar@ashrafi.ac.ir (م. زمین کار)،
m.koleini@ashrafi.ac.ir (م. کلینی)
 ISSN: 2322-4460