توصیه های امنیتی

بر اساس تحلیل‌های انجام‌شده و مدل نهایی انتخاب‌شده (KNN روی دیتاست اصلی)، این مدل می‌تواند به‌عنوان یک سیستم تشخیص تهدیدات شبکه با دقت بالا (حدود ۹۹.۸٪) و نرخ شناسایی تهدیدات نزدیک به ۱۰۰٪ به تیم امنیتی کمک کند تا ترافیک مخرب را به‌طور مؤثر شناسایی و مسدود نماید. با این حال، حتی یک مدل با دقت کلی بسیار بالا نیز در صورت داشتن Recall پایین برای کلاس‌های امنیتی (مانند ترافیک غیرمجاز یا حملات) می‌تواند خطرناک باشد، چرا که ممکن است تعداد قابل‌توجهی از تهدیدهای واقعی را نادیده گرفته و باعث نقض امنیتی گردد. برای کاهش این ریسک، توصیه می‌شود:

- نظارت مستمر بر روی معیارهای امنیتی مانند `recall_minority_mean` و `security_score`؛
- به‌روزرسانی دوره‌ی مدل با داده‌های جدید حملات برای حفظ توازن تشخیص؛
- استفاده از رویکرد چندلایه‌ای امنیتی همراه با این مدل برای پوشش نقاط کور احتمالی.

این رویکرد عملیاتی، امکان بهره‌برداری ایمن از مدل را در محیط‌های شبکه‌ای فراهم می‌کند.