

(دنیا پور ابراهیم ادهم)

DDoS برای شناسایی حملات LSTM این کد یک شبکه عصبی در داده‌های ترافیک شبکه پیاده‌سازی می‌کند. مراحل اجرای کد به شرح زیر است:

1. بارگذاری و پیش‌پردازش داده‌ها

- بارگذاری می‌شوند CSV ابتدا داده‌ها از فایل.
- به صورت باینری به دو ("Label" ستون) برچسب داده‌ها .
نگاشت می‌شود (DDoS حمله) مقدار 0 (عادی) و 1
- ویژگی‌هایی که برای مدل انتخاب شده‌اند شامل برخی .
مقادیر مربوط به ترافیک شبکه می‌باشند
- استاندارد StandardScaler سپس داده‌ها با استفاده از .
می‌شوند

- LSTM داده‌ها به شکلی بازسازی می‌شوند که برای ورودی مناسب باشد (به صورت یک توالی زمانی).

2. تقسیم داده‌ها به مجموعه آموزشی و آزمایشی

- داده‌ها به دو مجموعه آموزشی و آزمایشی تقسیم می‌شوند (80٪ برای آموزش و 20٪ برای تست).

3. LSTM تعریف و کامپایل مدل

- است. اولین لایه با 64 LSTM شامل دو لایه LSTM مدل نورون و خروجی بازگشتی و لایه دوم با 32 نورون تعریف شده‌اند.
- یک لایه خروجی برای طبقه‌بندی باینری به کار می‌رود و از تابع فعال‌سازی سیگموئید برای پیش‌بینی احتمال حمله استفاده می‌شود.
- مدل با استفاده از تابع زیان باینری Adam و بهینه‌ساز binary_crossentropy کامپایل می‌شود.

4. آموزش مدل

- مدل با داده‌های آموزشی آموزش داده می‌شود، به طوری که برابر با batch size 64 برابر با 10 و epochs تعداد است. همچنین، از 20٪ داده‌ها برای اعتبارسنجی استفاده می‌شود.

5. ارزیابی مدل

- پس از آموزش، مدل برای پیش‌بینی داده‌های تست استفاده می‌شود.

، فراخوانی (accuracy) معیارهایی از جمله دقت ، محاسبه و نمایش داده AUC-ROC ، F1 ، نمره (recall) می‌شوند تا عملکرد مدل در تشخیص حملات بررسی شود .
را در داده‌های DDoS این مدل به شما کمک می‌کند تا حملات ترافیک شبکه شناسایی کنید و عملکرد آن را با معیارهای ارزیابی مهم بررسی نمایید .