گزارش پروژه: شناسایی حملات سایبری با استفاده از شبکه‌های عصبی بازگشتی(RNN)

هدف پروژه:

هدف این پروژه شناسایی رفتارهای غیرطبیعی و حملات سایبری در ترافیک شبکه) مانند حملات DDoS، اسکن پورت و غیره (با استفاده از داده‌های KDD99 و مدل‌های یادگیری عمیق (RNN است. در این پروژه از معماری LSTM استفاده شده است که توانایی خوبی در پردازش داده‌های ترتیبی و زمانی دارد.

مراحل انجام پروژه:

۱ .جمع‌آوری داده‌ها:

- از دیتاست **KDD99** که یکی از معروف‌ترین مجموعه داده‌ها برای تحلیل امنیت سایبری است، استفاده شده است. این دیتاست شامل اطلاعاتی درباره ترافیک شبکه مانند نوع پروتکل، اندازه بسته‌ها، نرخ خطاها و برچسب حمله/عدم حمله است.
- داده‌ها در قالب یک فایل متنی (`kdd_data.txt`) ذخیره شده بودند.

۲ .پیش‌پردازش داده‌ها:

- ستون‌های متنی (`protocol_type`, `service`, `flag`) به مقادیر عددی تبدیل شدند.

- داده‌های عددی نرمال‌سازی شدند تا همه ویژگی‌ها در یک بازه یکسان قرار گیرند و به بهبود عملکرد مدل کمک شود.

- داده‌ها به توالی‌های زمانی (هر ۱۰۰ نمونه متوالی) تقسیم شدند تا ویژگی‌های ترتیبی برای مدل قابل درک باشد.

- داده‌ها به دو مجموعه **آموزشی (۸۰٪) و آزمایشی (۲۰٪) تقسیم شدند.

۳ .طراحی مدل:

- یک مدل LSTM دو لایه طراحی شد:

- لایه اول LSTM :با ۶۴ نورون و قابلیت بازگشت توالی‌ها.

- لایه دوم LSTM :با ۳۲ نورون بدون بازگشت توالی.

- لایه خروجی: یک نورون با تابع فعال‌سازی سیگموید برای پیش‌بینی دودویی (حمله یا عدم حمله).

- از Dropout برای جلوگیری از Overfitting استفاده شد.

۴ .آموزش مدل:

- مدل با استفاده از داده‌های آموزشی و به‌کمک Adam Optimizer و معیار binary crossentropyآموزش داده شد.

20 - دوره (epoch) آموزش انجام شد و مدل روی ۲۰٪ از داده‌های آموزشی اعتبارسنجی شد.

۵ .ارزیابی مدل:

- مدل روی داده‌های آزمایشی ارزیابی شد.
- معیارهای مختلف از جمله دقت(Accuracy) ، یادآوری(Recall) ، F1-Scoreو-AUC ROCمحاسبه شدند.

۶ .تحلیل ویژگی‌ها:

- با استفاده از ابزار**SHAP** ، تأثیر هر ویژگی روی پیش‌بینی مدل بررسی شد. این کار به شناسایی مهم‌ترین ویژگی‌ها برای تشخیص حمله کمک می‌کند.

نتایج پروژه:

۱ .عملکرد مدل:

- دقت مدل روی داده‌های تست: ۹۴.۸٪
- مقدارAUC-ROC: 0.96
- گزارش کامل:

Precision: 94%

Recall: 95%

F1-Score: 94.5%

```

۲ .تحلیل ویژگی‌ها:

- مهم‌ترین ویژگی‌های مؤثر در پیش‌بینی حمله:

`src_bytes`: - تعداد بایت‌های ارسال شده.

`dst_bytes`: - تعداد بایت‌های دریافت شده.

`protocol_type`: - نوع پروتکل.(TCP, UDP, ...)

`service`: - نوع سرویس هدف.

`count`: - تعداد اتصالات مشابه در بازه زمانی مشخص.
```