Network Intrusion Detection

DATA 586

Avishek Saha, Vimaljeet Singh, Noman Mohammad

BACKGROUND INFORMATION - INTRUSIONS

Detecting whether a network connection is genuine or an anomaly is crucial for network security.

Causes: Malicious attacks, software bugs, or hardware failures.

Consequences: Data breaches, system downtime, or loss of sensitive information.

Requirement: Strong understanding of network protocols, traffic patterns, and behavior.

Aids: Machine Learning Algorithms, Anomaly Detection Models, and Intrusion Detection Systems.

BACKGROUND INFORMATION - DATA SET

- NSL-KDD dataset used.

- Helps researchers compare different intrusion detection methods.

- Redundant records removed.

- Evaluation results are consistent and can be compared across different research studies.

RESEARCH OBJECTIVES

Importance: Accurate detection of network anomalies for robust network security

Approach: Utilize features from the dataset to classify connections as normal or attacks

Key Features: Duration, Protocol_type, Service, Flag, Src_bytes, Etc…

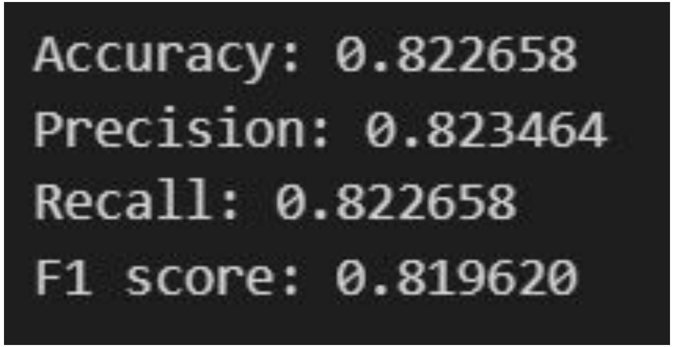
Goal: Using the most significant features for classifying network connections as normal or attacks using advanced ML tools

EXPERIMENTAL PROCEDURES

- Data pre-processing
  - Configuring training and testing sets
- EDA
  - Categorical / Numerical, Continuous / Discrete
  - Categorize the attack types into DOS, Probe, U2R, R2L
  - Check occurrence of each attack and decide what constitutes a normal vs suspicious connection
- Feature Engineering
  - Variable selection
- Model Training
  - Logistic Regression, NN (all features), **NN (selected features)**

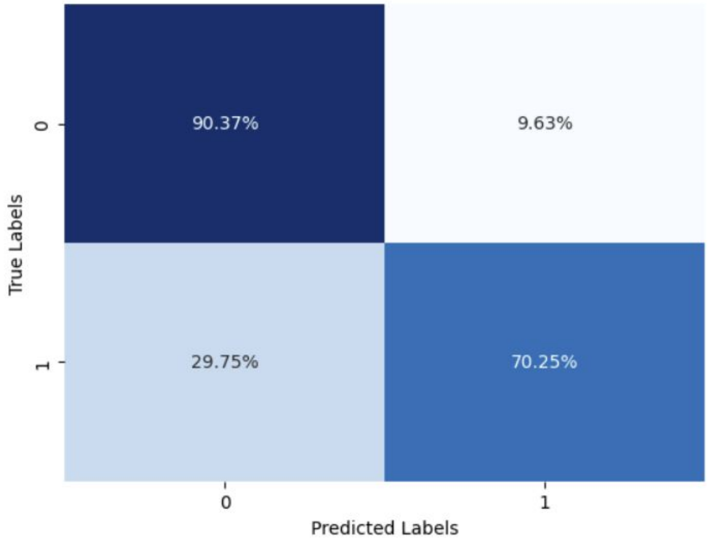
RESULT & ANALYSIS

- Accuracy Assessment
    - Highlighting the best model

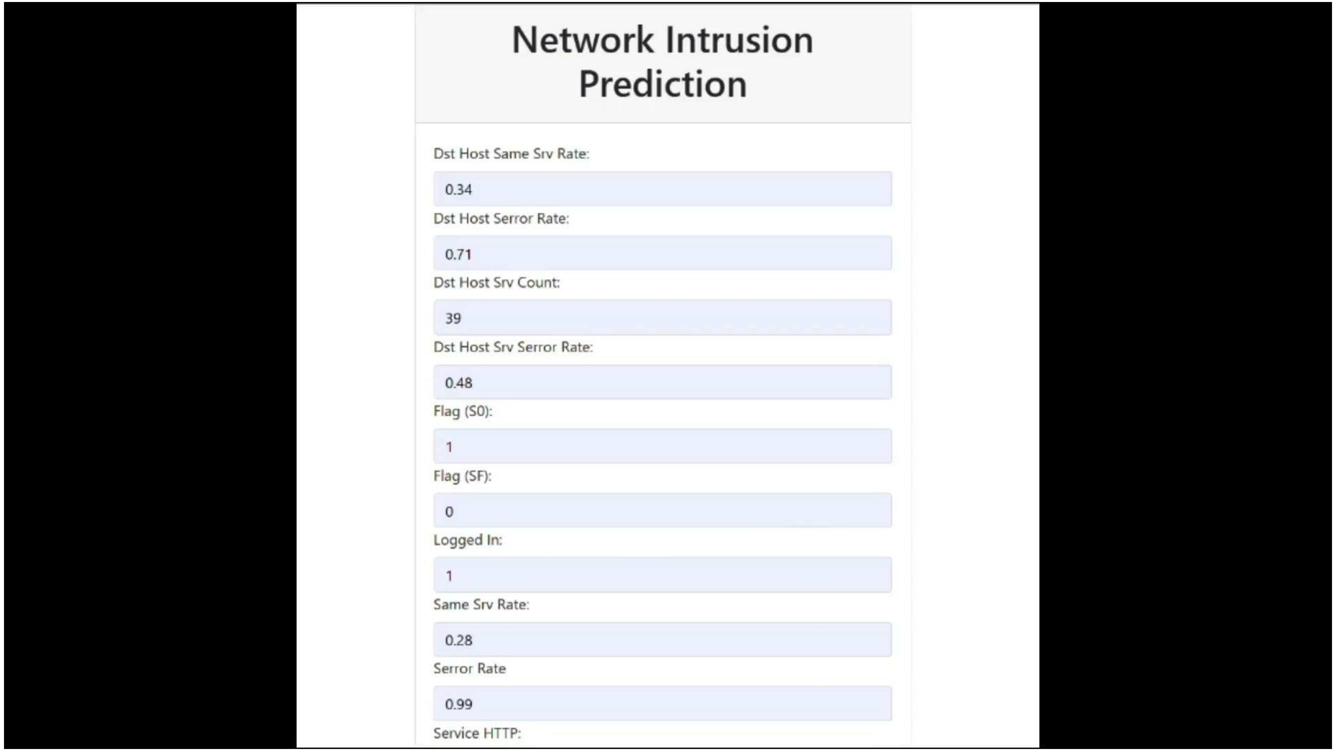


```
Accuracy: 0.822658
Precision: 0.823464
Recall: 0.822658
F1 score: 0.819620
```

0 = Normal
1 = Attack



- Demo
    - user-friendly interface for testing new data



Network Intrusion Prediction

Dst Host Same Srv Rate:

0.34

Dst Host Serror Rate:

0.71

Dst Host Srv Count:

39

Dst Host Srv Serror Rate:

0.48

Flag (S0):

1

Flag (SF):

0

Logged In:

1

Same Srv Rate:

0.28

Serror Rate

0.99

Service HTTP: