Intrusion Detection in Cyber Attacks Using Deep Learning

Abstract

In the face of increasingly sophisticated cyber attacks, this proposal presents a Deep Learning–based approach combining CNN and LSTM architectures to detect intrusions. Using the CICIDS2017 dataset, the model aims for ≥ 95% accuracy and ≤ 5% false-alarm rate. Expected results will demonstrate superior adaptability compared to traditional methods.

Introduction

Computer networks are the lifeblood of modern organizations—and prime targets for hackers. Rule-based IDS solutions struggle to keep pace with novel attack patterns. Deep Learning offers automated feature extraction and anomaly detection, acting as a vigilant guard that never tires.

Literature Review

- Rule-based IDS (Snort, Suricata): easy to deploy but inflexible.
- ML-based IDS: Random Forest, SVM improve accuracy but require manual feature engineering.
- Deep Learning IDS:
  - Kim et al. (2019) used LSTM for sequence anomalies → recall ~90%.
  - Khan et al. (2020) proposed a CNN-LSTM hybrid → precision ~92%.

DL demands large data and training time, but delivers robust performance once trained.

Methodology

1. Dataset: CICIDS2017 – contains 14 common attack types (Brute Force, DDoS, XSS, etc.).
2. Preprocessing: Remove nulls and outliers; Min–Max normalization for 80 numeric features; One-hot encoding for protocol and service fields.
3. Model Architecture: Input (80-dim) → CNN (Conv1D+MaxPool) → LSTM → Dense → Softmax; Optimizer: Adam (lr=0.001); Regularization: Dropout(0.5), Early stopping (patience=5).
4. Training: batch size=64, epochs≤50, split 70/15/15.
5. Baseline: Random Forest & SVM on same preprocessed data.

Evaluation Plan

Metrics: Accuracy, Precision, Recall, F1-score, ROC-AUC.
Procedure: 5-fold cross-validation.
Comparison: DL model vs. RF & SVM.
Deliverables: Confusion matrices, ROC curves.

Timeline

Phase	Weeks	Tasks
Data Preparation & Collection	1–2	Download CICIDS2017, cleaning, EDA
Preprocessing & Feature Eng.	3–4	Normalization, encoding, dimensionality reduction
Model Building & Training	5–7	Implement CNN-LSTM, hyperparameter tuning
Evaluation & Benchmarking	8–9	Cross-validation, compare with RF/SVM
Report Writing & Slides Design	10	Finalize proposal report and presentation

References

• Denning, D. E., “An Intrusion-Detection Model,” IEEE, 1987.

• Sharafaldin, I., Lashkari, A. H., Ghorbani, A. A., “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” CICIDS2017, 2018.

• Kim, D. et al., “LSTM-based Network Intrusion Detection,” Journal of Cybersecurity, 2019.

• Khan, S. U. et al., “Hybrid Deep Learning for IDS,” IEEE Access, 2020.

• Scikit-learn developers, “Random Forest Classifier,” 2021.