Deep Learning-Based Detection of Phishing Websites

David Toluwani Ehigie

Week 2 Progress

Week 2 Objective

- Build Deep Learning models using raw URLs
- Compare LSTM and CNN architectures
- Evaluate against Week 1 baseline

Dataset Representation

- Used URL text only
- Character-level tokenization
- Sequences padded to length 150

Experiment 1: LSTM v1

Results:

- Accuracy: 65.9%
- High precision but low recall
- Model underfitting observed

Experiment 2: Improved LSTM

Improvements:

- Bidirectional LSTM
- Larger embeddings
- More epochs

Results:

- Accuracy: 87.3%

Experiment 3: CNN Model

CNN captures local phishing patterns:

- login-
- verify-account
- secure-paypal

Results:

- Accuracy: 91.9%

Model Comparison

- Random Forest: 96.9%
- LSTM v1: 65.9%
- Improved LSTM: 87.3%
- CNN: 91.9%

Key Insights

- CNN outperforms LSTM for URL detection
- Engineered features remain strongest
- Deep Learning works well on raw URLs

Next Week

- Hybrid model (DL + engineered features)
- Feature selection
- Performance improvement