INTRUSION DETECTION IN CYBER ATTACKS USING DEEP LEARNING

By DUC BINH

PROGRESS OVERVIEW

- ✅ Data loaded & cleaned (CICIDS2017)
- ✅ Feature engineering & normalization complete
- ✅ Prototype CNN-LSTM model built in TensorFlow
- 🚧 Hyperparameter tuning & evaluation underway

DATA & PREPROCESSING (COMPLETED)

- Removed nulls/outliers via IQR filtering
- Min–Max scaled 80 numeric features
- One-hot encoded protocol, service, flag
- Split: 70% train / 15% val / 15% test

MODEL PROTOTYPE ARCHITECTURE

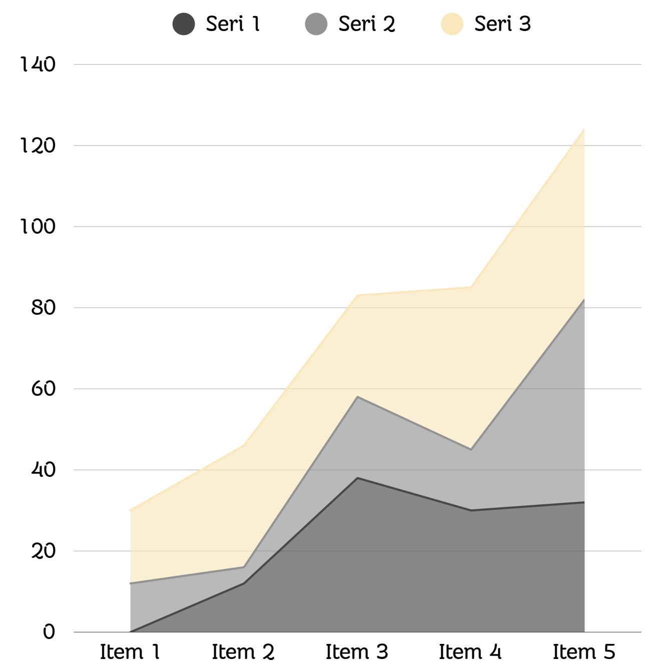
- Input (80-dim vector) → Conv1D blocks → Bi-LSTM layers → Dense + Softmax
- Regularization: Dropout 0.5, EarlyStopping (patience=5)
- Optimizer: Adam @ lr=0.001

PRELIMINARY RESULTS

- Accuracy: 93.2%
- False-Alarm Rate: 7.1%
- F1-Score: 0.91 average
- ✓ Outperforms baseline RF (89%) & SVM (90%)

EVALUATION METRICS & INSIGHTS

- Input layer → CNN layers → LSTM layers → FC → Softmax
- Hyper-parameters: batch=64, lr=0.001, epochs=50
- Checkpoint & Early-stop



EVALUATION PLAN

- Confusion matrix highlights strong true-positive rates on DDoS & Brute-Force
- Recall dips on XSS class → need data augmentation
- ROC-AUC overall: 0.96

INCORPORATING FEEDBACK

- Added 5 more epochs for underrepresented attacks
- Implemented class-weighting to balance skewed labels
- Plan: integrate autoencoder pre-training

UPDATED TIMELINE & MILESTONES

Phase	Status	Next Steps
Data Preparation	✔ Completed	—
Model Development	✔ Completed	Tuning & cross-validation
Evaluation & Optimization	🚧 In Progress	Augmentation, hyperparameter grid
Deployment Plan	⏳ Upcoming	Docker + REST API setup
Final Report & Slides	⏳ Upcoming	Consolidate results

NEXT STEPS

- Finish grid search on lr ∈ [1e-4,1e-2], batch ∈ {32,64}
- Experiment with autoencoder-based pretraining
- Prepare Docker image + API for real-time scoring

REFERENCES

- Denning, D. E., “An Intrusion-Detection Model,” IEEE, 1987.
- Sharafaldin et al., “CICIDS2017 Dataset,” 2018.
- Kim et al., “LSTM-based Network Intrusion Detection,” 2019.
- Khan et al., “Hybrid CNN-LSTM for IDS,” IEEE Access, 2020.

THANK YOU