INTRUSION DETECTION IN CYBER ATTACKS USING DEEP LEARNING

By DUC BINH

THE PAIN POINT

Hackers are getting more and more sophisticated, traditional firewalls + IDS are “in the dust” 😤

Leaks, DDoS attacks, APTs… the risk is escalating

Need a “soldier” who is self-learning, self-adaptive, and tireless

GOALS AND CONTRIBUTIONS

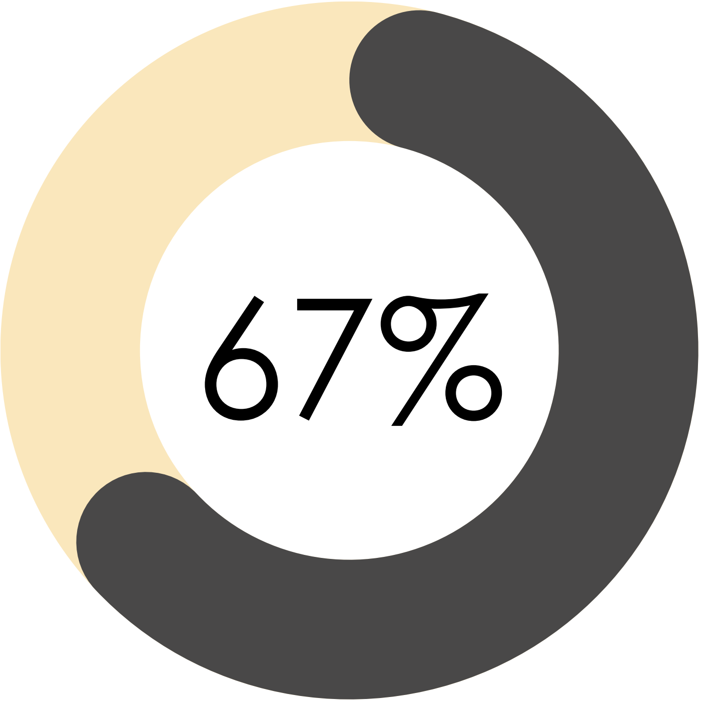
- Building Deep Learning model (CNN/LSTM/hybrid) to detect intrusions
- Improve accuracy ≥ 95%, reduce false-alarm to ≤ 5%
- End-to-end pipeline framework: collection → preprocessing → training → deployment

OVERVIEW OF DEEP LEARNING FOR IDS

- CNN: good at “catching patterns” from network data
- LSTM: sensitive to time series, detecting abnormal sequences
- Hybrid: “daring” combination to fight hackers

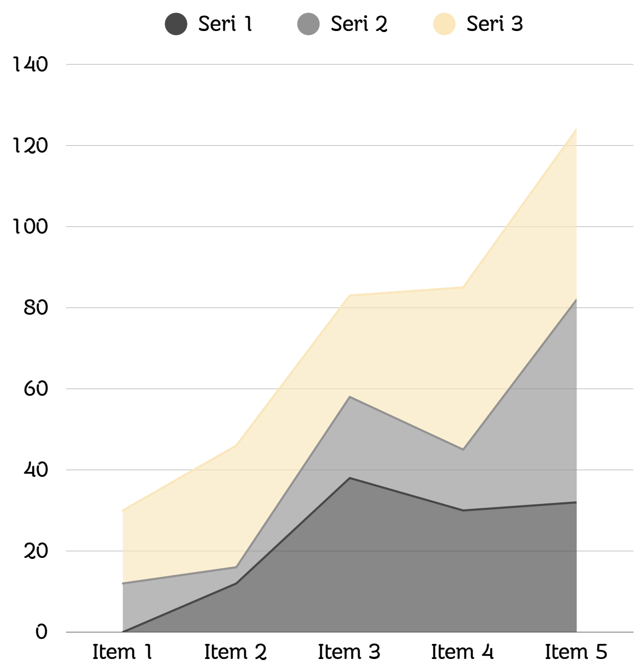
DATA AND PREPROCESSING

- Dataset: CICIDS2017 (diversity attack)
- Preprocessing:
  - Remove outliers, normalize features
  - One-hot encoding for categorical attributes



MODEL ARCHITECTURE

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



EVALUATION PLAN

Metrics: Accuracy, Precision, Recall, F1-score, ROC-AUC

Cross-validation 5 folds

Compare with baseline: Random Forest, SVM

TIMELINE & MILESTONES

Phase	Duration	Key Deliverable
Data Collection & Cleanup	2 weeks	Cleaned dataset
Model Development & Training	3 weeks	DL prototype
Evaluation & Optimization	2 weeks	Results report & tuning
Report & Slides Preparation	1 week	Submission-ready materials

CONCLUSION & NEXT STEPS

- Expectations: a self-learning, self-evolving “shield”
- Extension: real-time deployment, SIEM integration

REFERENCES

- [1] D. E. Denning, “An Intrusion-Detection Model,” IEEE, 1987.

- [2] I. Sharafaldin et al., “CICIDS2017 Dataset,” 2018.

THANK YOU