Comparative Analysis of BERT, sciBERT and secBERT Fine-Tuning for Cybersecurity Technique Classification

By Michael Garrett

Berkeley
UNIVERSITY OF CALIFORNIA

Project

- How does the baseline performance of BERT, sciBERT, and secBERT comparison a cybersecurity technique classification task?
- What improvements in classification performance can be achieved through fine-tuning a model that is pretrained on cybersecurity corpora?

I HAVE ALTERED THE PROJECT SCOPE
PRAY I DO NOT ALTER IT FURTHER

Data

- Found on HuggingFace with no data card
- Highly skewed
- 14k rows → 15k rows
  - TextAttack Data Augmentation for upscaling

W266 Final Project

Data

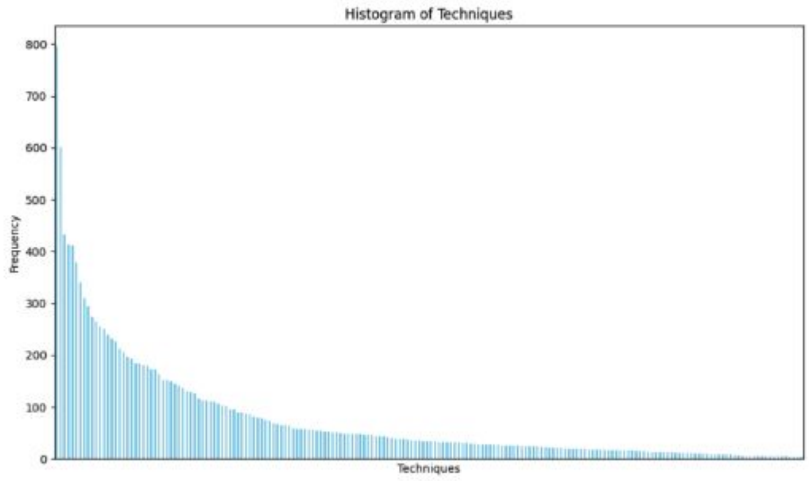


Figure 1: Original Distribution of the data before any preprocessing.

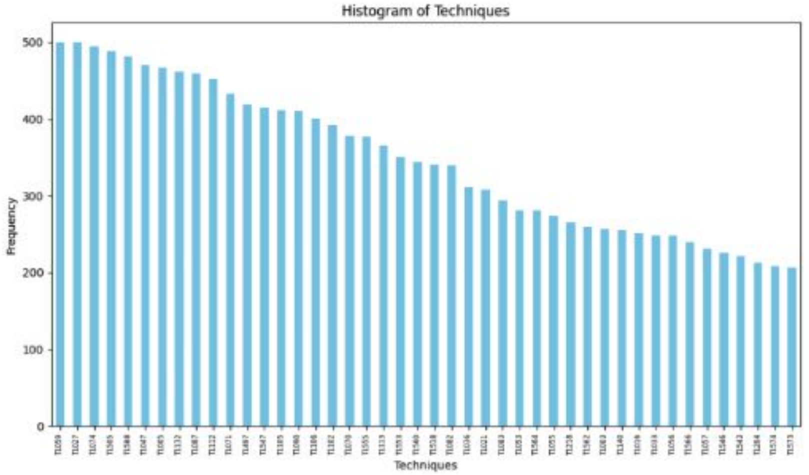
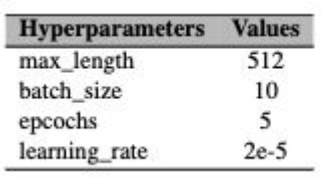


Figure 4: Final distribution of data.

Berkeley
UNIVERSITY OF CALIFORNIA

Models

- BERT – Baseline
- sciBERT – TRAM
- secBERT – Experiment
- TensorFlow vs PyTorch
- 

Hyperparameters	Values
max_length	512
batch_size	10
epcochs	5
learning_rate	2e-5

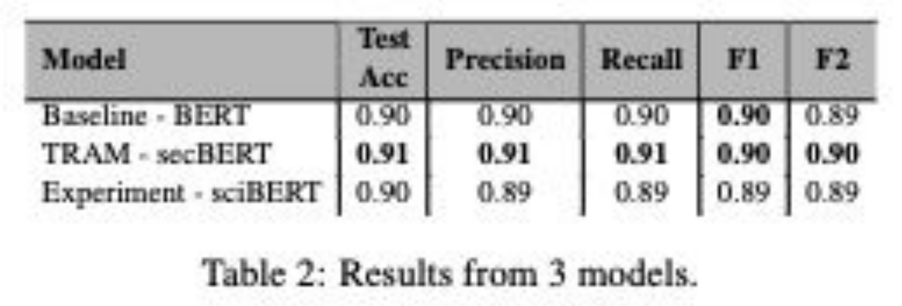
Results

- Hypothesis
  - secBERT > others
- Conclusion
  - Failed to reject!

Berkeley
UNIVERSITY OF CALIFORNIA

W266 Final Project

Results



Model	Test Acc	Precision	Recall	F1	F2
Baseline - BERT	0.90	0.90	0.90	**0.90**	0.89
TRAM - secBERT	**0.91**	**0.91**	**0.91**	**0.90**	**0.90**
Experiment - sciBERT	0.90	0.89	0.89	0.89	0.89

Table 2: Results from 3 models.

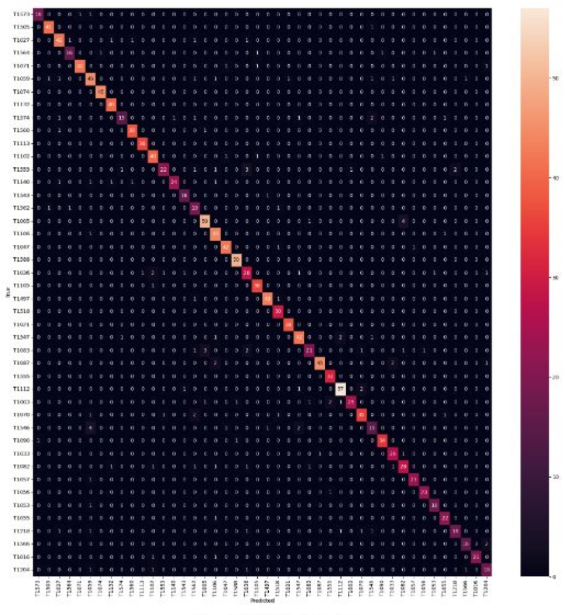


Figure 6: BERT Confusion Matrix

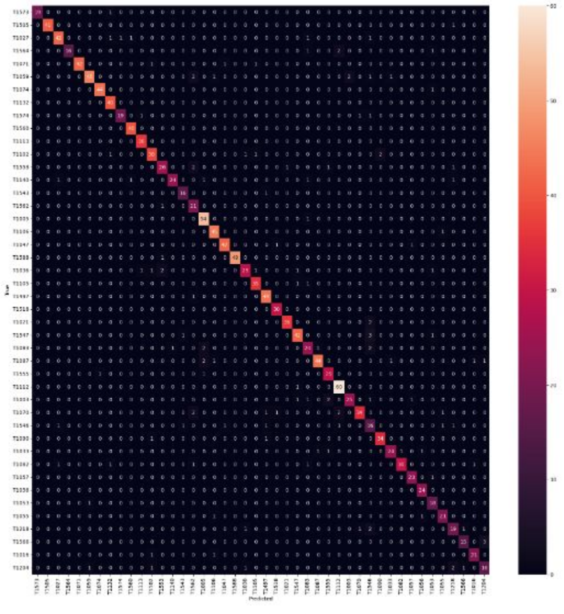


Figure 7: sciBERT Confusion Matrix

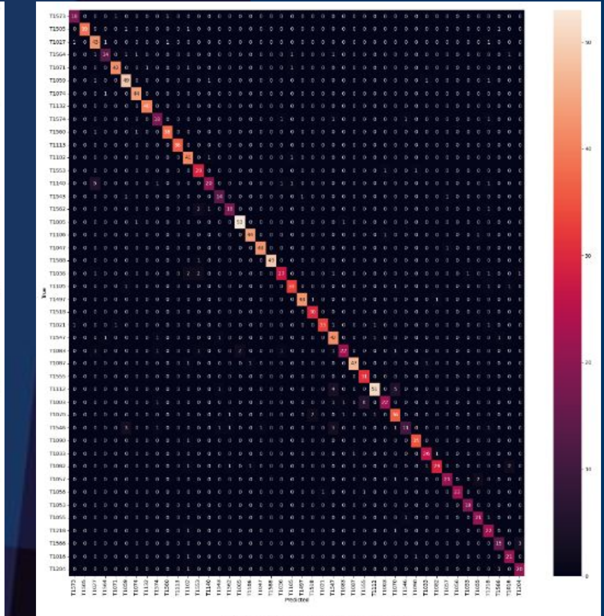


Figure 8: secBERT Confusion Matrix