PalStudent Journal
A Palestinian Scientific Journal for the Youth

AL-QUDS UNIVERSITY

ABSTRACTS: VOLUME 8, SPECIAL ISSUE {8th Undergraduate Conference}

# PHISHING AND FRAUD DETECTION IN IMBALANCED DATASETS: A COMPARATIVE STUDY OF ENSEMBLE AND DEEP LEARNING MODELS

**Maria Khalil[1], Nael Abu Halaweh[1]***

**Supervisor: Nael Abu Halaweh[1]**

*[1] Department of Computer Science, Faculty of Science and Technology, Al-Quds University, Palestine*

## Abstract

**Background:** Phishing and fraud attacks remain major challenges in cybersecurity, particularly due to class imbalance, where malicious cases are significantly fewer than legitimate ones. This imbalance complicates detection and often reduces model performance. Although deep learning is widely regarded as a powerful approach, it does not always perform effectively on tabular and highly imbalanced data, highlighting the need to evaluate alternative methods.

**Objectives:** This study aims to compare the performance of an Ensemble Machine Learning model—combining Logistic Regression, Random Forest, and Support Vector Machine—with a Feed forward Neural Network (FNN), to determine which approach performs better across datasets with varying imbalance ratios.

**Methods**: Both models were trained and tested on four phishing and fraud datasets using standardized preprocessing techniques, including normalization and data cleaning. Class imbalance was addressed using cost-sensitive class weighting. Model performance was evaluated using accuracy, precision, recall, F1-score, confusion matrices, as well as training and prediction time.

**Results**: The results showed that both models achieved strong performance on nearly balanced datasets. However, as class imbalance increased, the Ensemble model demonstrated greater stability, higher precision, and more reliable detection of minority classes, particularly in the highly imbalanced credit card fraud dataset. In contrast, the FNN exhibited faster training and prediction times but produced more false positives under extreme imbalance conditions, indicating a trade-off between computational efficiency and detection reliability.

**Conclusion**: The findings partially support the hypothesis, suggesting that Ensemble models are more dependable for real-world imbalanced cybersecurity problems, while deep learning models offer advantages in computational speed. The results indicate that the optimal approach depends on dataset characteristics and the relative importance of accuracy versus efficiency.

**PalStudent Journal**
**Correspondence concerning this article should be addressed to the mentioned authors at the mentioned institutes.**

**E-mail: research@admin.alquds.edu**
**Palestine, Abu Dis, Al-Quds University**

PalStudent Journal
A Palestinian Scientific Journal for the Youth

**Keywords**: Phishing detection, Class imbalance, Ensemble learning, Deep learning, Cost-sensitive learning, Cyber security, Proof of concept.

**PalStudent Journal**
**Correspondence concerning this article should be addressed to the mentioned authors at the mentioned institutes.**

**E-mail: research@admin.alquds.edu**
**Palestine, Abu Dis, Al-Quds University**