

PhD Research Proposal (3-Year Duration)

Kalasalingam Academy of Research and Education (KARE)

Title: Enhancing Generalization and Robustness in Machine Learning Models through Adaptive Representation Learning

1. Introduction

Machine Learning (ML) plays a vital role in modern applications but struggles in real-world environments where data is noisy, imbalanced, or experiences distribution shift. This research aims to create adaptive representation learning methods to improve reliability and robustness of ML models.

2. Problem Statement

Traditional deep learning systems lack the ability to dynamically adjust to new or evolving data distributions. This results in poor performance, overfitting, and unstable predictions. The proposed research focuses on developing adaptive feature-learning mechanisms to address these challenges.

3. Research Objectives

- Develop adaptive representation learning techniques.
- Improve generalization across unseen and shifting domains.
- Enhance robustness to noise and adversarial attacks.
- Provide interpretable feature adaptation insights.

4. Research Questions

- How can ML models adapt representations dynamically?
- Can meta-learning and self-supervised learning increase robustness?
- What metrics can measure representation stability?

5. Proposed Methodology

The methodology integrates self-supervised learning, meta-learning, and contrastive learning with a dynamically adaptive gating mechanism. The model will be evaluated on image, NLP, and time-series datasets to measure generalization, robustness, and stability.

6. Expected Results

The proposed method is expected to:

- Improve accuracy by 10–15% over baseline models.
- Reduce robustness drops under noise by 30–40%.
- Show better latent space organization and interpretability.
- Improve low-data and cross-domain learning performance.

7. Three-Year Timeline

Year 1:

- Comprehensive literature review.
- Initial framework design.
- Preliminary experiments with baseline models.

Year 2:

- Full adaptive representation learning model development.
- Testing on multiple datasets (vision, NLP, time-series).

- Refinement of robustness and generalization modules.

Year 3:

- Large-scale evaluation and benchmarking.
- Final optimization and integration of interpretability tools.
- Documentation, thesis writing, publication submissions, and defense preparation.

8. Conclusion

This 3-year research aims to deliver theoretically strong, practically robust adaptive ML models for real-world applications. The outcomes align with KARE's focus on innovation, academic excellence, and impactful AI research.