# CIS 6930: Trustworthy Machine Learning Project Proposal: Title of the Project

Tanvi Jain (Point of Contact) tjain@ufl.edu Nimish Bajaj nimishbajaj@ufl.edu

September 21, 2021

### 1 Introduction

Determine whether explainable / interpretable ML techniques like LIME and others can provide useful insights into the cause of the unfairness.

A model's accuracy is not always enough to state weather it will perform well in the wild because the accuracy highly depends the data that was used to train and test the model. Explaining the results of a model, and identifying what lead to a particular classification can help provide insights into the model. Once you add interpretability to the model, its result can be easily understood by a domain expert can be verified for correctness. This greatly enhances the trustworthyness of the model.

We are proposing to build a text classification model and explaining the results using LIME, and validate if LIME is able to provide stable and meaningful features.

## 2 Background and Related Work

Since the data contains technical words which are sometimes outside of the english vocabulary, we are going to tune word embeddings for the problem domain.

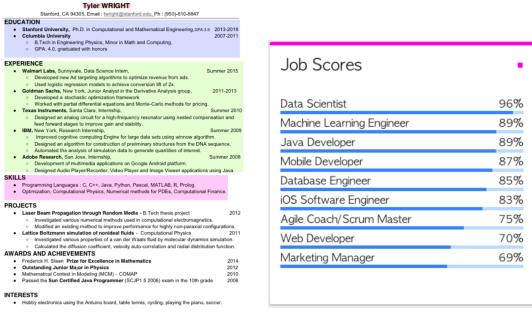
Write here.

You can cite related publications like so [1] and non-publications (e.g., websites) like so 1.

### 3 Proposed Approach & Plan

Following is the approach we are going to take:

- 1. Fetch data and take samples as per the distribution of data for train, test and validation
- 2. Clean and vectorize the data for Neural Network (NN) approach
- 3. Build a NN architecture to learn classification labels
- 4. Train, test and validate the neural network
- 5. Use LIME for model inferencing
- 6. Manually validate LIME output



(a) Example Input

(b) Model prediction

Figure 1: Model output description

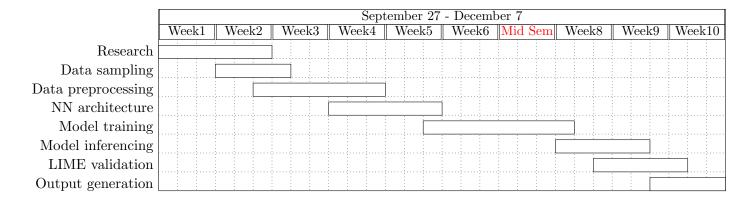


Figure 2: Gantt Chart

### 4 Timeline

#### References

[1] Vladimir Vapnik, Esther Levin, and Yann Le Cun. Measuring the vc-dimension of a learning machine. Neural computation, 6(5):851–876, 1994.

<sup>&</sup>lt;sup>1</sup>Google scholar: https://scholar.google.com