**Navya Annapareddy and Jade Preston**

**MLSys for Fairness**

**Problem Description:** Currently, there are many contexts where data sharing is difficult or constrained by security and distribution limitations. One common domain where this is a consideration is in Healthcare where data is often governed by data-use-ordinances like HIPAA. On the other hand, larger sample sizes allow models to better generalize on account of the potential for more variability and balancing underrepresented classes.

Federated learning is a type of distributed learning model that allows data to be trained in a decentralized manner. This, in turn, addresses data security, privacy, and vulnerability considerations as data itself is not shared across a given learning network’s nodes. Some challenges to federated learning include: node data may not be independent and identically distributed (iid), relatively high levels of communication between network machines is needed, and heterogeneity in the individual nodes with respect to bias and size of data samples.

**Proposed Contribution:** We propose a decentralized federated learning framework and evaluate it in the context of fairness. We define fairness here as the ability to create balanced datasets due to greater data access enabled by federated learning, thereby mitigating bias in the systems as a whole. Specifically, we will evaluate the ensemble model of the decentralized framework with different nodes against a given non-distributed node with the goal of proving to what degree the federated model sharing results in less bias. We will also explore how to distribute data to nodes to simulate a real world context with heterogeneous nodes to best compare against.

**Considerations:** Federated learning has much potential to curb security vulnerabilities normally present in data sharing processes. Data protection would still need to be enforced at the host level but would not require a dedicated TEE to ensemble or share models unless desired. Distributed training methods typically focus on parallelization to obtain less computationally expensive training while federated methods have focused on addressing node heterogeneity. While local systems are considered suitable, HPC systems might be necessary for high dimensional data. Encryption can be enforced at the model sharing level through secure communication protocols or with data keys (envelope encryption). Finally, secure addition of peers to a network must also be considered.

**Proposed Benchmark Datasets:**

Depression Classification Source: [Depression Anxiety Stress Scales (DASS)](http://www2.psy.unsw.edu.au/dass/) - The dataset from this source was obtained via a survey following a health assessment and consisted of 42 questions assessing the mental state and risk of a patient. Patients were able to respond using an ordinal scale of 1 - 4. Another unique feature was that durations times were recorded for the amount of time a patient spent reading pages/questions and responding to questions. The survey also incorporated a personality questionnaire that allowed patients to respond on an ordinal scale ranging from 1 - 7 of Strongly Disagree to Strongly Agree. The patients were then requested to fill-out a checklist determining their familiarity with a word in a binary response. Finally, the following demographic details were recorded creating many segmentable groups: education level, childhood environment, gender, native language, age, hand-dominance, religion, sexual orientation, race, voting recency, family- size, and survey source of discovery.