InfoSec Project Report

Chapter 1 : Introduction

The project focuses on a distributed machine learning setup where multiple servers train models independently and send their model weights to a central server. The central server aggregates these weights to form a single, enhanced model. This approach leverages the advantages of distributed computing while maintaining data privacy and reducing bandwidth usage.

Chapter 2 : Related Work

The concept is akin to federated learning, a technique where multiple edge devices or servers collaboratively learn a shared prediction model while keeping all the training data local. Similar methodologies are discussed in research for enhancing privacy and efficiency in machine learning.

Chapter 3 : Security Algorithm

The security aspect of the project involves ensuring the integrity and confidentiality of data as it is transmitted across networks. While the current implementation focuses on basic transmission using sockets, future enhancements could include encryption protocols like SSL/TLS to secure the communication channels.

Chapter 4 : ML/DL Algorithm

Each server in the network, including the client, trains a model referred to as `CTScanModel` on its local dataset. This model, tailored for processing and analyzing CT scan images, exemplifies the use of machine learning in medical imaging. The specifics of the learning algorithm and the model architecture are critical. After training, each server sends the model weights to a central server, which aggregates them by computing their mean. This aggregation enhances the overall model's performance by integrating diverse data insights.

Chapter 5 : Model Performance

Performance evaluation could involve comparing the accuracy, precision, and recall of the models before and after weight aggregation. This section would ideally include a table comparing these metrics to demonstrate the effectiveness of the aggregation method.