Title: Robust Private AI Framework Using Federated Learning and Homomorphic Encryption for Electric Utility Infrastructure Defect Detection

Abstract:

In modern times, electric utility companies are utilizing on-ground and aerial drone imagery to identify physical defects on transmission and distribution infrastructure to plan for more effective maintenance. To deploy faster and more cost-efficient maintenance decisions, many utility companies are using in-house and outsourcing third-party analysts to develop artificial intelligence (A.I.) models that can analyze the imagery and make predictions on infrastructure conditions. However, for the AI technology to be effectively trained for real-world implementation, there is a need for cross-collaboration among a vast number of utility companies to share their imagery and analysis to improve the global AI model. The primary challenge of this collaboration comes at the expense of requiring data cleaning, a manual process to ensure sensitive data is removed from shared imagery. In this paper, we present a Private AI framework that leverages Federated Learning and Homomorphic Encryption techniques to permit this secured collaboration among utility companies and third-party analysts. First, we determine a homomorphic-encryption friendly activation function that is compatible with image classification data. Next, we determine which homomorphic-encryption schemes will be used and implemented into the layers of the AI model. Then, we devise a robust cloud server to facilitate federated learning strategies among multiple clients. Lastly, we test the robustness, accuracy, and effectiveness of our framework using multiple clients training well-known image datasets.