

Generalization

Stability

Privacy

Assumption: Training with noise enhances model generalization and stability by introducing controlled perturbations during learning, which can also contribute to improved privacy protection through techniques like differential privacy.

Question 1: How does the incorporation of noise in different locations within the model structure or the data affect training outcomes?

Solution: Comparison of different noise-infused mechanisms in deep learning under varying noise levels in centralized and federated settings.

Solution: Comparison of three CNN architectures with noisy hidden layers under varying noise layers in centralized and federated settings.

Question 2: How can we estimate the level of additive noise prior to detecting a significant model performance decrease?

Solution: Introducing Signal-to-Noise Ratio as a measure of the trade-off between generalization and accuracy.

Solution: Introducing Price of Stability and Price of Anarchy as measures of the trade-off between model performance and privacy as a result of increasing noise levels.