Defense Implemented: Randomization

Randomization Approach: Random Resizing

Metric	Clean	No Defense Attack	w/ Defense Attack
Loss	0.033	0.27	0.0166
Accuracy	98%	91%	98%

Example Misclassifications:

Number of misclassified images for Clean: 1
Attack: pgd_bim_attack
Dataset: MNIST
Training Epochs: 10
Trained Clean Images: 54210
Test Images: 140
Accuracy: 0.98
Precision: 0.99
Recall: 0.99
F1-score: 0.99
ROC AUC Score: 1.00

Misclassifications:
0 -> 3: 1

Number of misclassified images for No Defense Attack: 6
Attack: pgd_bim_attack
Dataset: MNIST
Training Epochs: 10
Adversarial Training Images: 12686
Test Images: 140
Accuracy: 0.91
Precision: 0.95
Recall: 0.94
F1-score: 0.95
ROC AUC Score: 1.00

Misclassifications:
0 -> 2: 2
0 -> 3: 2
0 -> 8: 1
0 -> 9: 1

Number of misclassified images for w/ Defense Attack: 1

Attack: pgd_bim_attack
Dataset: MNIST
Training Epochs: 10
Retrained Clean and Adversarial Images: 66896
Test Images: 140
Accuracy: 0.98
Precision: 0.99
Recall: 0.99
F1-score: 0.99
ROC AUC Score: 1.00

Misclassifications:
0 -> 8: 1