Seminar 10 (Week 10)

Q1. This is a group activity based on the seminar lecture on Federated Machine Learning. Please attend the seminar lecture and answer the following questions:

I. Please explain what is Federated Machine Learning.
II. Please explain the differences among Centralized, Decentralized and Distributed systems.
III. Please define the types of Federated Machine Learning.
IV. Please explain the differences between Horizontal Federated Learning and Cross-Device Federated Learning.
V. Please explain one security attack with example for the Federated Machine Learning infrastructure.
VI. Please explain one privacy attack and its mitigation technique for the Federated Machine Learning infrastructure.