CHAPTER 9

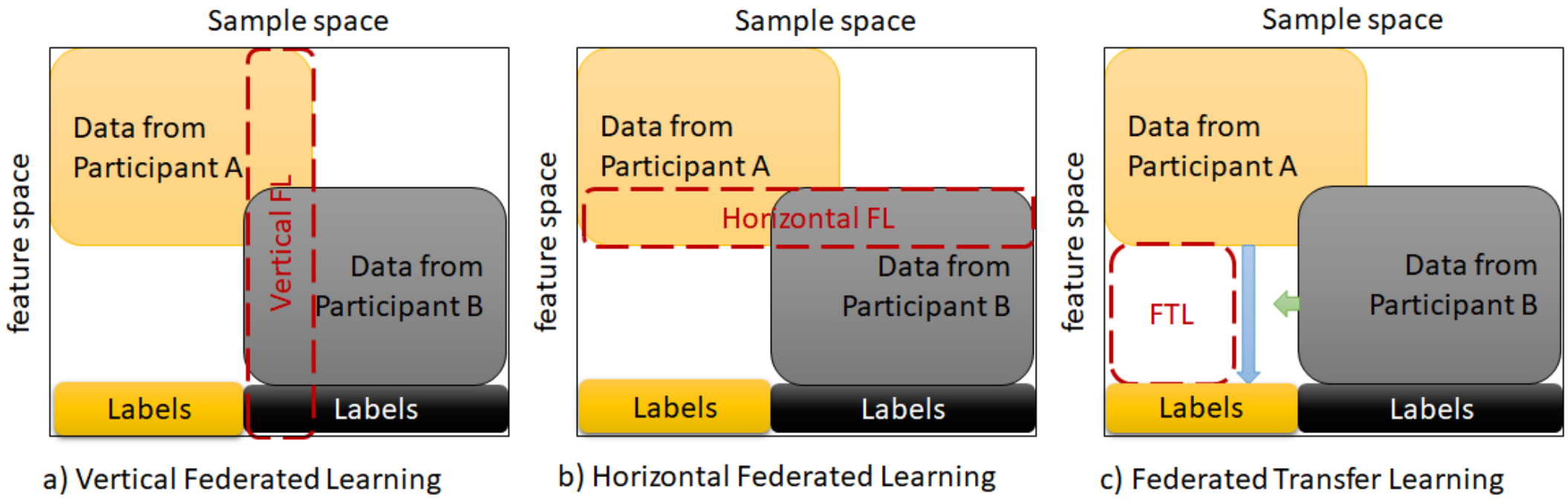
Federated Learning for Privacy-Preserving Internet of Things

Aggregation Technique	Challenge	Primary notion	Discussion
FedSGD	Statistical	Based on the configurations large-batch synchronous stochastic gradient descent.	- local gradients are shared instead of parameters - single step of gradient descent is performed per communication round
FedAvg		Participants carry out multiple batch upgrades using the local data to upload the updated parameters to the FL servers instead of local gradients.	- Statistically, the FedAvg is demonstrated to diverge under situations where the data is irregularly dispersed among participants. - Systematically, FedAvg did not permit participants to execute varying quantities of local learning depending on relevant restraints.
FedProx		The local training for each participant incorporates a proximate factor aiming to restrict the contribution of local upgrades to the global model	- finetune the convergence of models in case of high heterogeneity data. - Like FedAvg, the FedProx did not consider the computing power of participants, and thereby treat them evenly during the aggregation.
FedMA		Consider the mutation invariance of the neurons prior to completing the aggregation to facilitate adjustment of the size of the final model.	- Employ Bayesian non-parametric technique to adapt the size of the global network to the heterogeneousness dissemination of data. - The FedMA is susceptible to contaminating attack, in which an opponent could effortlessly trap the federate scheme to enlarge the final network to set up contaminated local network.
FedPAQ	Communication	The participants are allowed to conduct several local parameter updates before sharing the updated parameters with the server.	- FedPAQ compute the global parameters by averaging the local parameters, which necessitates high complication in either greatly convex or non-convex situations.
HierFAVG		A tiered participant-edge-cloud aggregation construction in which edge tier aggregate the local updates from the participants, then upload them to the FL server at the cloud.	- This multi-level configuration facilitates effective model interchange throughout the present edge-cloud network. - it is prone to the troubles of laggards and machine failures.
Turbo-Aggregate	Communication and security	A multi-grouping scheme that divides the participants into multiple groups where the parameter upgrades are common between parties in a rotary fashion. A collective trusted communicating method is employed to protect the confidentiality of local data.	- It is relatively appropriate for wireless network topology, where network circumstances and user accessibility can change rapidly. - The employed secure aggregation method is effective in handling user failures, yet unable to acclimate to new participants joining the network. Thus, it necessitates developing a self-configurable protocol to assist new participants by in such a way that preserve the privacy.

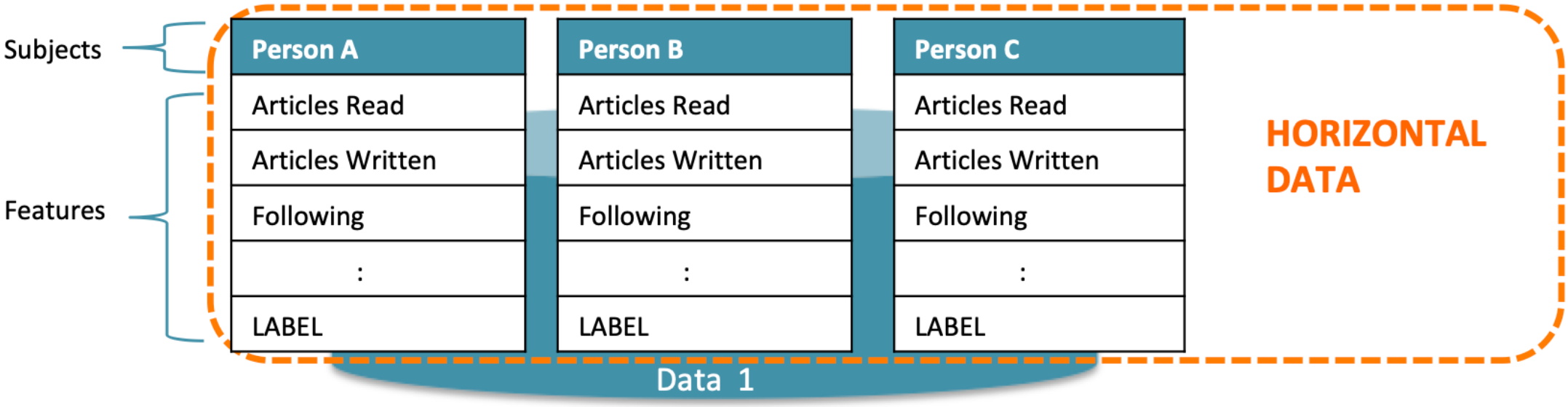
DEFINITION OF FEDERATED LEARNING

Aspect	Categories	Advantage	Applications
splitting methodology	FTL	Upsurge the number of samples and expanding the dimensionality	Knowledge transfer, cross-domain learning
	VFL	Expansion of input dimensionality	Distributed dep learning solutions
	HFL	Rise the number of samples	Learning on resource-constrained devices
privacy-preservation techniques	Secure parameters aggregation	Escape communicating the initial data	Deep federated solutions
	Homomorphic encryption	Clients could compute and handle the encoded data	Distributed learning
	Differential privacy	Could effectively safeguard the confidentiality of users' data by injecting noise	Privacy preserving artificial intelligence solutions
Heterogeneity handling	Asynchronous communication	Enable handling the communication latency issues	Device heterogeneity
	Sampling	Evade immediate learning with various IoT devices	Pulling Reduction with Local Compensation (PRLC)
	Fault-tolerant approaches	Could thwart the entire system from disintegrating	Laying-off techniques, Sensitive applications
	Heterogeneous design	Could handle the issues related to the heterogeneous devices	5G, B5G, 6G systems

TAXONOMY OF FEDERATED LEARNING SOLUTIONS



TAXONOMY OF FEDERATED LEARNING SOLUTIONS



HORIZONTAL FEDERATED LEARNING

VERTICAL FEDERATED LEARNING