FedTMOS: Efficient One-Shot Federated Learning with Tsetlin Machine

Shannon How, Jagmohan Chauhan, Geoff V Merrett, Jonathan Hare

University of Southampton

Overview

One-shot Federated Learning (OFL):
A method to collaboratively train a global model across decentralized devices in a single communication round

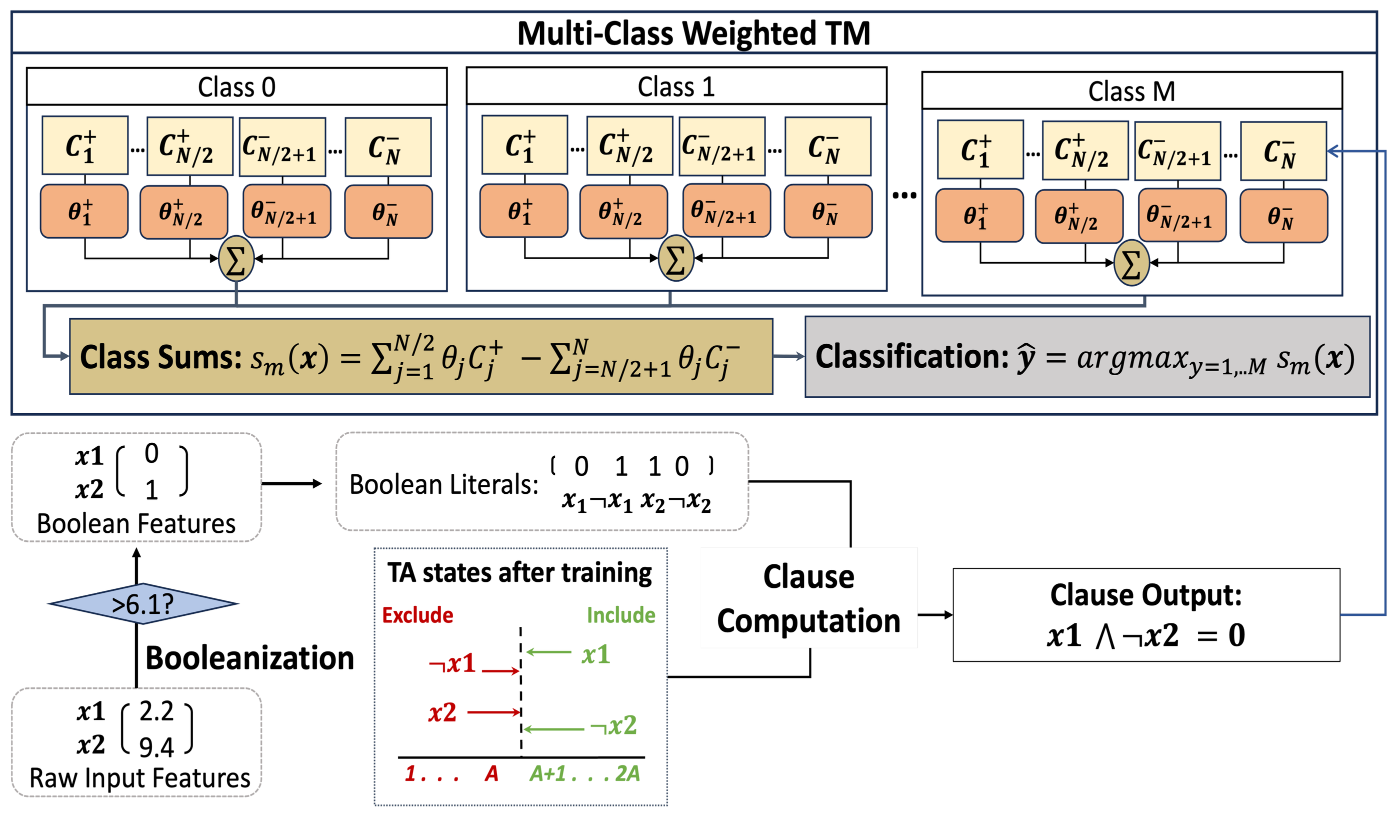
Challenges in Existing OFL approaches:

- **Data Availability:** Relies heavily on public datasets, which might not be accessible
- **Aggregation Latency:** Require server-aide computations, introducing latency
- **Data Heterogeneity:** Misalignment of models trained on heterogeneous dataset, impacting model generalization

Contributions: A novel, efficient, **data-free** OFL approach using the Tsetlin Machine that **eliminates the need for server-side training** and is **robust to data heterogeneity**

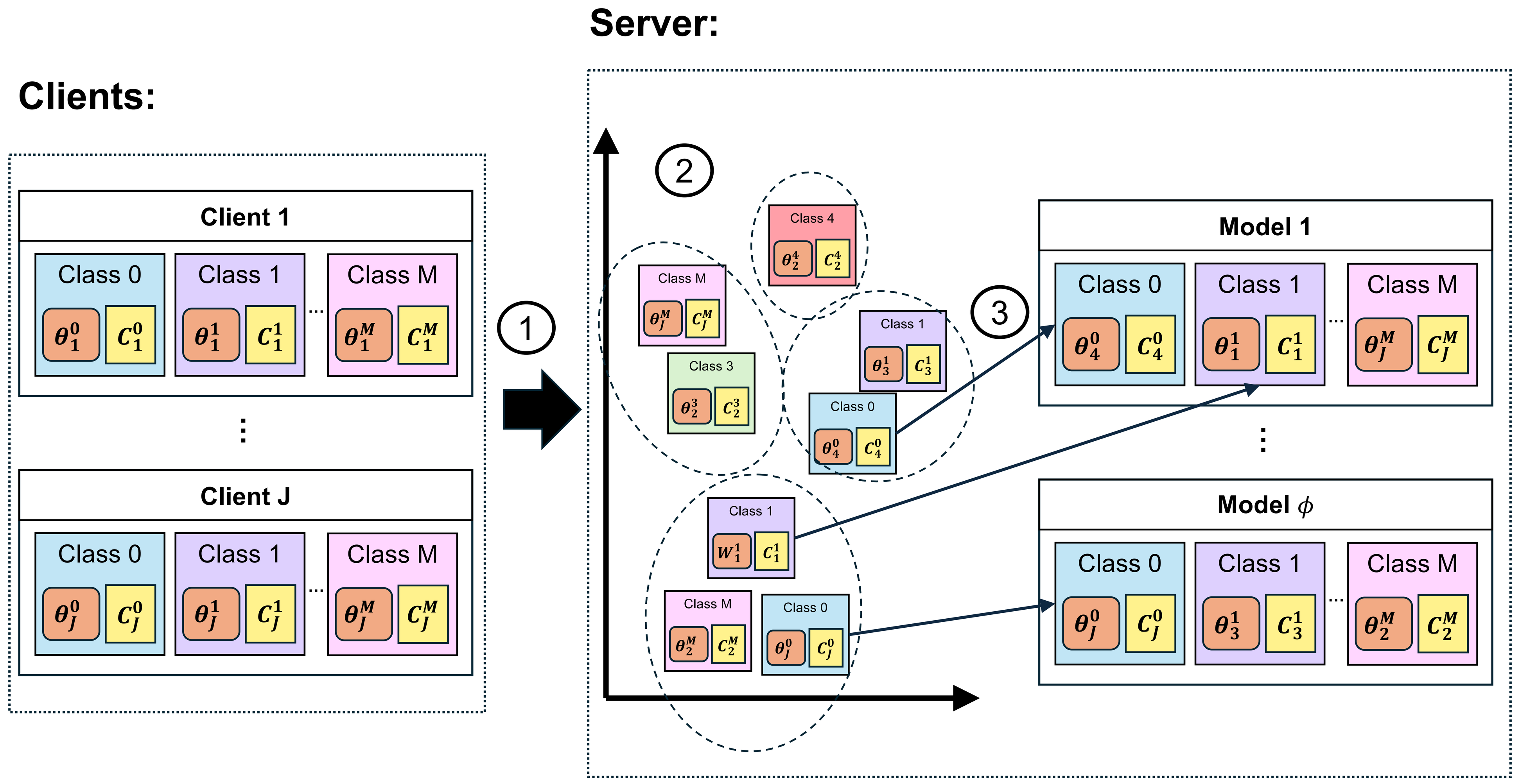
The Tsetlin Machine

The TM is a machine learning method grounded in propositional logic and bit-based representation, leveraging Tsetlin Automata (TA) and game theory principles to derive logical propositions for classification



Methodology

Given J clients, each having local datasets $D_1, D_2, \dots, D_J$. The objective is to aggregate the local TM models, $\boldsymbol{T} = \{T_1, T_2, \dots, T_J\}$, into ϕ server models ($\phi < J$) that generalizes well over $\boldsymbol{D} \equiv \cup_{i \in J} D_i$ in one communication round



1. Clients **upload** their **scaled** clause weights: $\theta_j^i = \frac{|D_j^i|}{|D_j|}\theta_j^i$ and states parameters to balance representation across classes, preventing minority classes from being overshadowed by dominant ones

2. Scaled weights undergo **k-means clustering** to facilitate smoother weight reassignment and maintain balance, thereby averting significant class weight disparities and enhancing efficiency

3. **Weights reassigned** to ϕ models by maximizing the inter-class distance based on the cluster centroids the class belongs:

$$maximize\ \frac{1}{\phi}\sum_{m=1}^{\phi}\sum_{i\neq j}\left\|\mu_m^i - \mu_m^j\right\|^2,$$

ensuring that each model maintains distinct class boundaries

Final Classification: The classification output is obtained by the class with the highest value from the aggregated sum of all ϕ TMs:

$$\hat{y} = argmax_m \sum_{i=1}^{\phi} \frac{1}{a^i} s_m^i(x)$$

Experimental Results

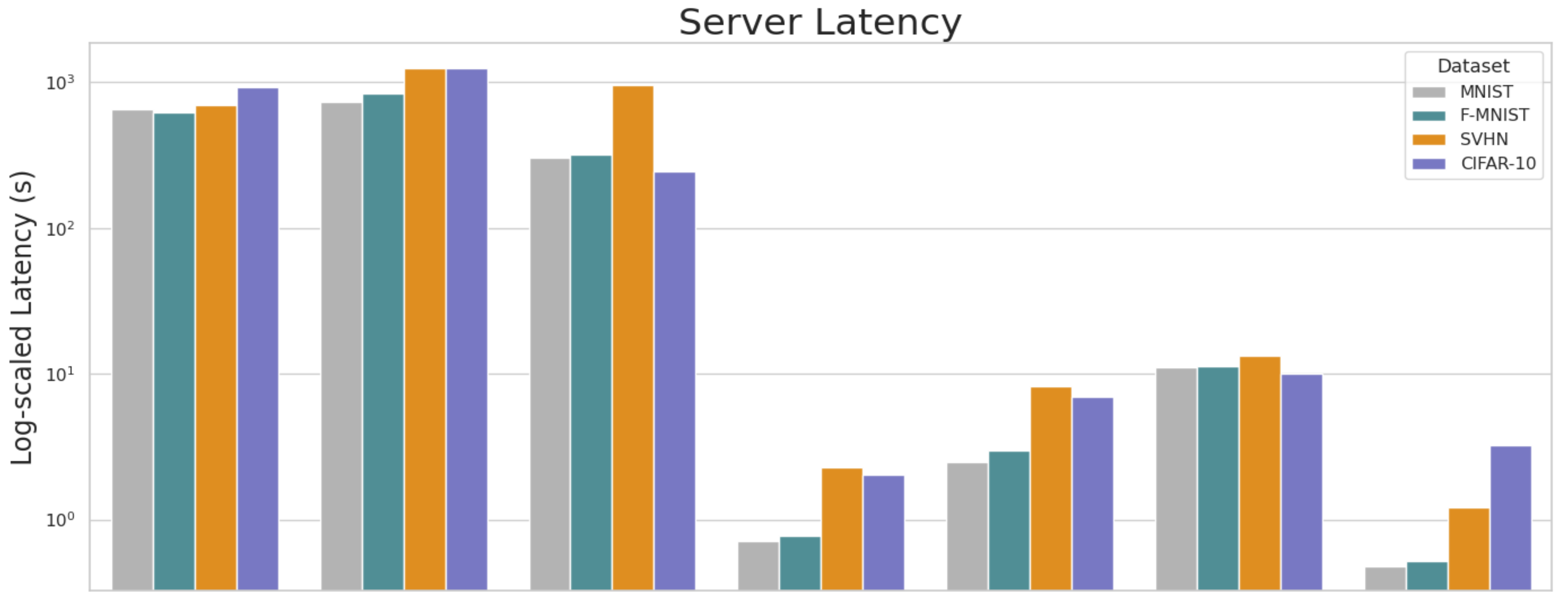
Server model performance under data heterogeneity

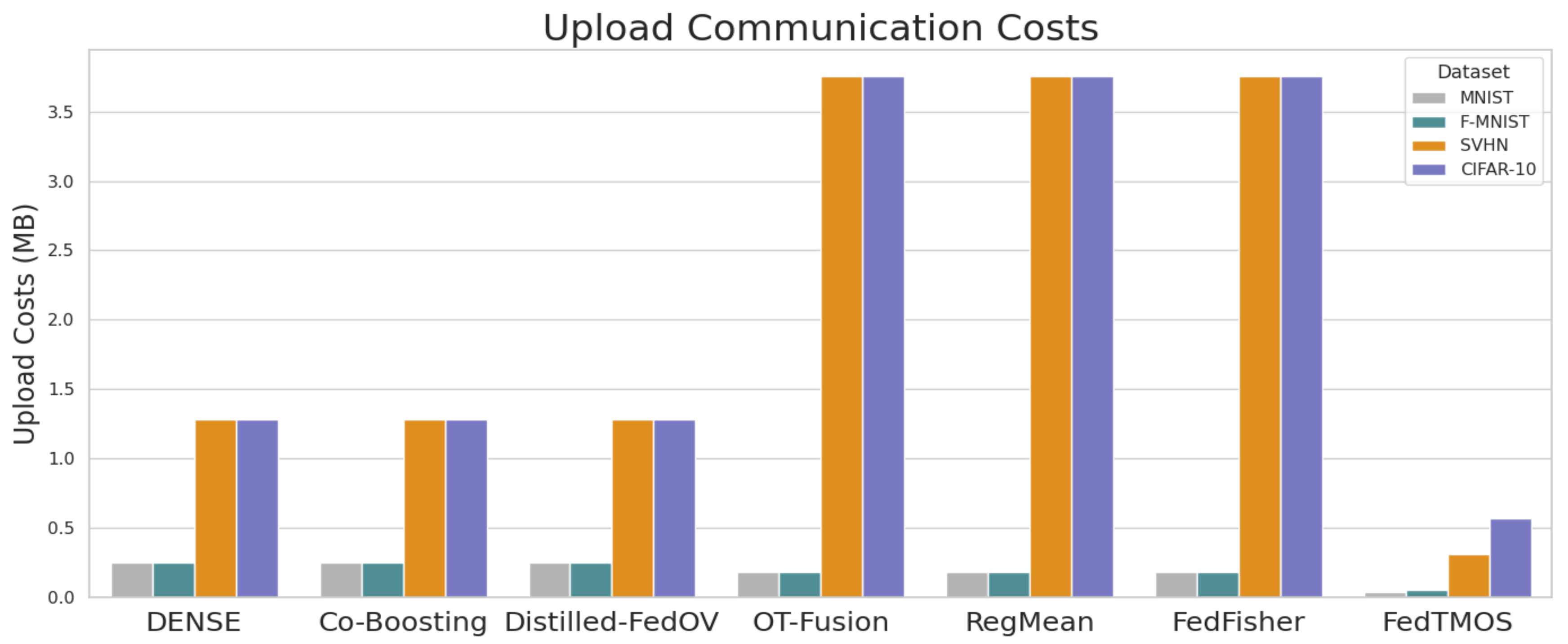
Dataset	Partition	DENSE	Co-Boosting	Distilled-FedOV	OT-Fusion	RegMean	FedFisher	FedTMOS
MNIST	$Dir(0.05)$	68.79±14.19	83.42±7.77	89.34±0.67	52.38±4.74	76.64±4.57	77.14±8.65	**93.80±3.81**
	$Dir(0.1)$	82.05±7.33	91.73±5.80	93.60±0.62	66.20±3.70	85.25±1.80	79.32±3.05	**96.60±1.85**
	$Dir(0.3)$	95.61±1.47	96.41±0.83	97.67±0.15	97.37±0.10	94.37±1.42	92.03±2.52	**98.41±0.10**
	$S(2)$	48.84±12.44	62.57±4.09	56.26±4.88	28.68±7.16	65.92±11.88	36.92±17.01	**92.94±0.51**
	$S(3)$	57.63±8.12	79.85±5.55	86.22±3.20	42.69±3.39	69.92±7.57	62.66±14.46	**95.23±0.47**
	$S(4)$	81.65±7.31	93.91±2.48	70.92±1.07	62.40±11.10	87.58±6.06	85.12±3.04	**96.84±0.50**
F-MNIST	$Dir(0.05)$	51.67±5.31	59.93±10.00	75.39±0.85	42.06±9.06	58.02±2.66	55.02±6.97	**75.45±3.58**
	$Dir(0.1)$	56.97±9.78	60.55±6.47	77.84±1.21	50.66±3.66	63.27±5.35	60.60±4.91	**78.21±3.58**
	$Dir(0.3)$	73.95±2.65	78.94±1.69	83.24±0.58	76.49±4.12	75.14±1.26	75.57±1.69	**84.97±1.39**
	$S(2)$	30.73±8.94	40.94±1.95	56.97±0.71	21.53±3.65	35.29±9.21	32.25±8.06	**59.17±1.56**
	$S(3)$	46.35±7.68	59.94±2.11	74.85±1.06	32.48±5.29	60.34±5.18	46.07±0.91	**74.94±1.78**
	$S(4)$	54.00±4.34	57.24±5.38	61.20±0.42	36.81±2.35	68.87±2.78	65.21±1.88	**78.78±0.77**
SVHN	$Dir(0.05)$	38.09±19.61	35.62±12.99	63.17±0.95	35.97±0.13	55.52±3.07	56.32±2.29	**63.54±2.61**
	$Dir(0.1)$	52.45±11.26	53.42±14.28	64.94±6.22	47.68±1.28	55.28±3.36	54.35±2.84	**69.79±2.33**
	$Dir(0.3)$	65.65±8.95	76.09±6.10	77.53±2.30	77.27±0.21	72.43±3.25	76.90±1.04	**78.86±1.27**
	$S(2)$	26.60±5.78	43.29±5.54	54.26±8.80	17.63±3.61	33.25±6.73	34.57±6.66	**61.63±1.13**
	$S(3)$	43.96±5.47	58.89±4.17	74.98±0.75	29.67±7.82	54.66±6.73	57.25±3.96	**78.09±0.25**
	$S(4)$	51.44±4.34	63.88±5.39	73.47±0.56	35.69±4.41	63.89±2.54	64.77±6.53	**75.24±0.68**
CIFAR-10	$Dir(0.05)$	25.97±2.52	26.17±3.85	40.04±5.61	30.70±0.80	33.58±4.59	35.61±1.41	**47.69±2.59**
	$Dir(0.1)$	32.46±3.62	36.71±7.87	46.79±2.66	31.46±1.52	33.49±0.83	39.55±5.36	**52.25±1.71**
	$Dir(0.3)$	43.11±0.95	43.35±2.08	48.24±5.22	49.43±2.94	44.34±1.42	51.18±1.45	**57.03±0.74**
	$S(2)$	15.73±3.77	21.91±6.51	33.90±0.12	18.57±0.59	24.24±2.57	22.23±1.53	**39.95±1.33**
	$S(3)$	29.13±3.26	33.21±4.00	45.64±2.14	24.70±2.77	31.06±1.36	32.36±4.15	**52.18±0.73**
	$S(4)$	31.26±1.61	36.39±1.22	41.17±1.63	33.67±0.62	38.97±1.33	41.46±2.31	**59.59±0.30**

Server model performance with different number of clients

Clients	DENSE	Co-Boosting	Distilled-FedOV	OT-Fusion	RegMean	FedFisher	FedTMOS
20	31.18±6.90	34.55±3.89	37.20±1.55	24.95±3.24	18.55±8.92	32.46±2.34	**50.08±3.62**
50	27.47±3.77	34.33±2.08	30.43±1.56	27.17±1.36	31.74±1.94	37.52±0.37	**50.90±0.94**
80	23.85±11.70	32.47±2.36	25.65±1.04	22.20±1.85	20.86±2.25	33.66±0.95	**49.15±1.08**

Efficiency analysis in terms of server-side latency and upload communication costs





sh2n21@soton.ac.uk