

Server



$\mathcal{V}_{full}$

$$\mathcal{M}^{e+1} = \sum_j \alpha_j^f \cdot \mu_j$$

$\mu_1^{e-1}, \mu_2^{e-1} \dots \mu_k^{e-1}$

$\mu_1^{e-1}, \mu_2^{e-1} \dots \mu_k^{e-1}$

$w_1^e$

$\mathcal{M}^e$

$\mu_1^e$

$w_2^e$

$\mathcal{M}^e$

$\mu_2^e$

$\mu_1^{e-1}, \mu_2^{e-1} \dots \mu_k^{e-1}$

$\mu_k^e$

$w_k^e$

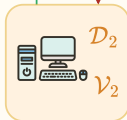
$\mathcal{M}^e$



$\mathcal{D}_1$

$\mathcal{V}_1$

Client 1



$\mathcal{D}_2$

$\mathcal{V}_2$

Client 2



$\mathcal{D}_k$

$\mathcal{V}_k$

Client k