

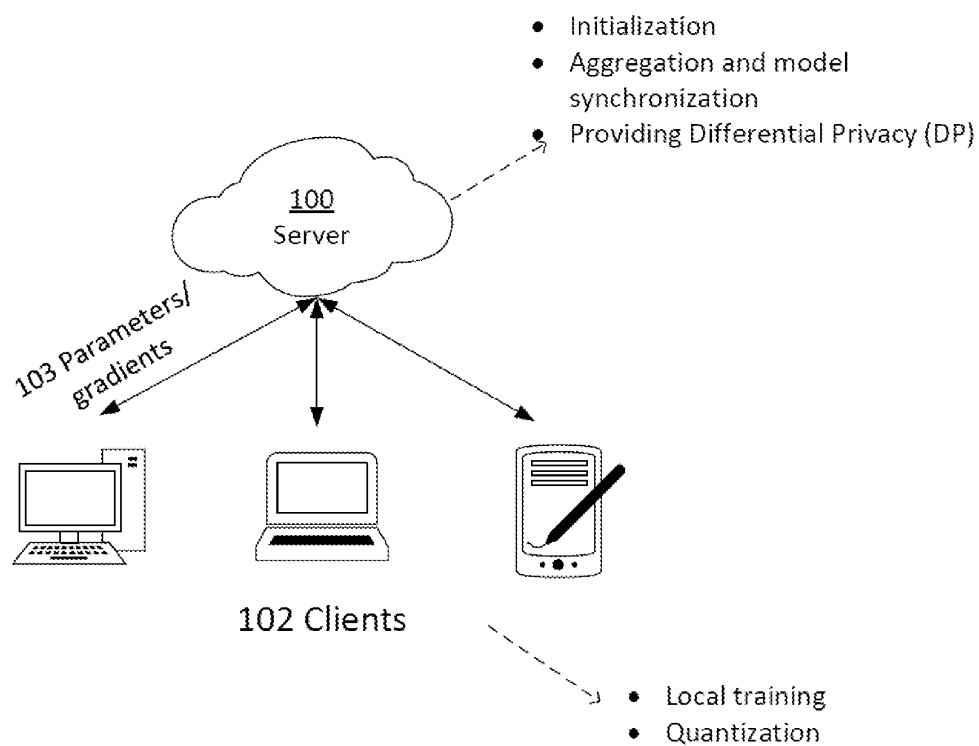


FIG. 1

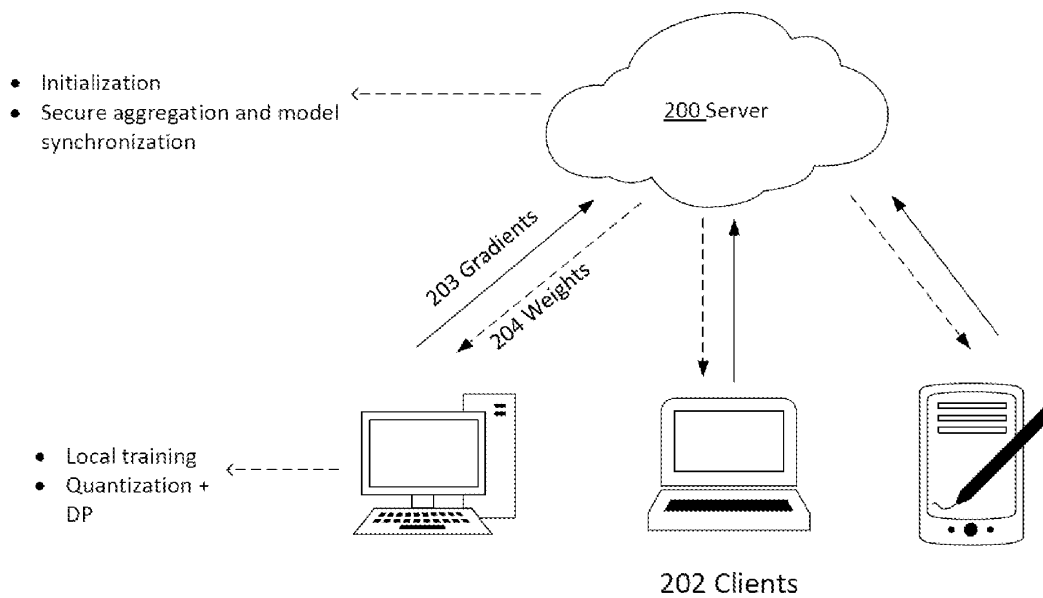


FIG. 2

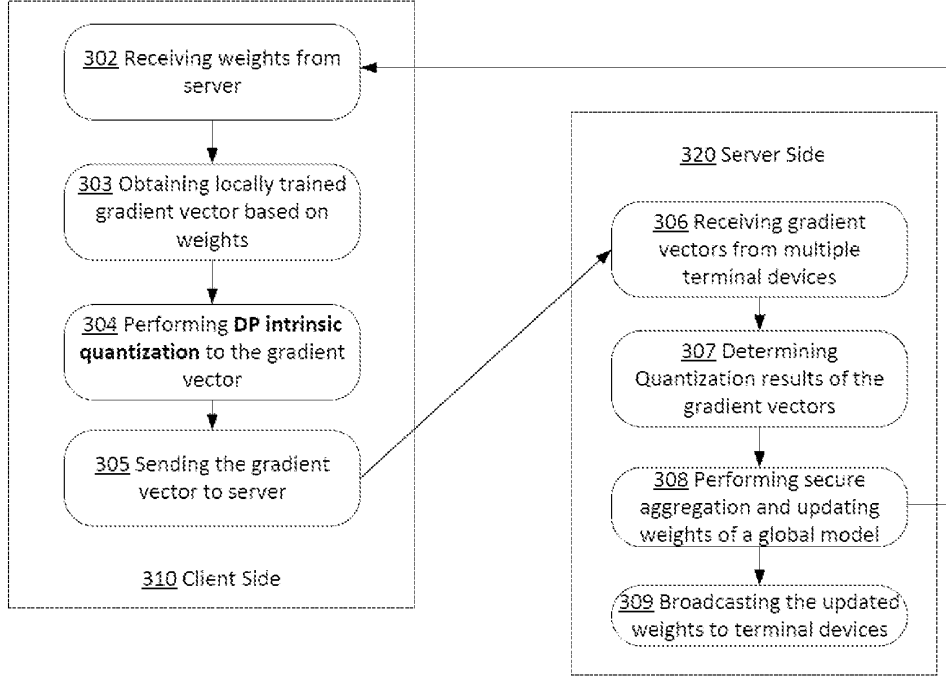


FIG. 3

400

Require: Initialize $\mathbf{w}_0$.

- 1: **for** each round $t = 1, \dots, T$ **do**
- 2: **Select** a random subset $\mathcal{K}$ of clients:
- 3: $N_{k,t} = |\text{PS}_t(\mathbf{X}_k)|$
- 4: $\mathbf{g}_{k,t} = \frac{1}{N_{k,t}} \sum_{\mathbf{x}_j \in \text{PS}_t(\mathbf{X}_k)} \text{CL}[\nabla \ell_k(\mathbf{w}_t; \mathbf{x}_j); C]$
- 5: Send $Q[\mathbf{g}_{k,t} + \mathbf{n}_{k,t} + \mathbf{v}_{k,t}]$ to the server
- 6: **Server receives** $Q[\mathbf{g}_{k,t} + \mathbf{n}_{k,t} + \mathbf{v}_{k,t}]$ **from** k -th client **and executes:**
- 7: $\tilde{\mathbf{g}}_{k,t} = Q[\mathbf{g}_{k,t} + \mathbf{n}_{k,t} + \mathbf{v}_{k,t}] - \mathbf{v}_{k,t}, \forall k \in [K]$
- 8: $\mathbf{g}_t = \text{SecureAgg}\left(\frac{1}{\sum_{k=1}^K N_{k,t}} \sum_{k=1}^K N_{k,t} \tilde{\mathbf{g}}_{k,t}\right)$
- 9: $\mathbf{w}_{t+1} = \mathbf{w}_t - \eta \mathbf{g}_t$
- 10: Send $\mathbf{w}_{t+1}$ to each client
- 11: **end for**

FIG. 4

500

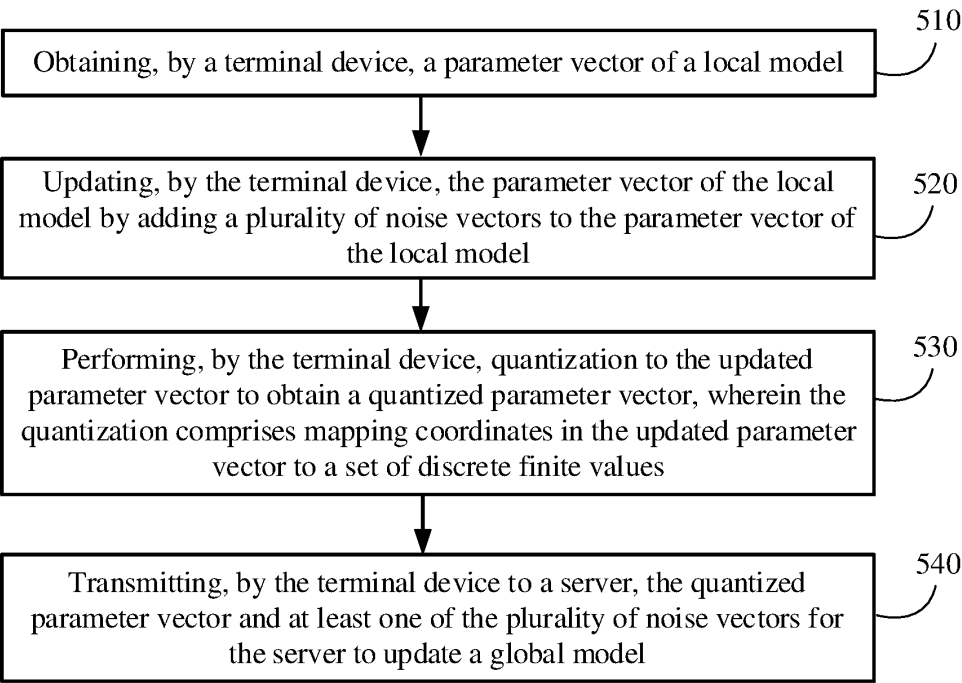


FIG. 5

600

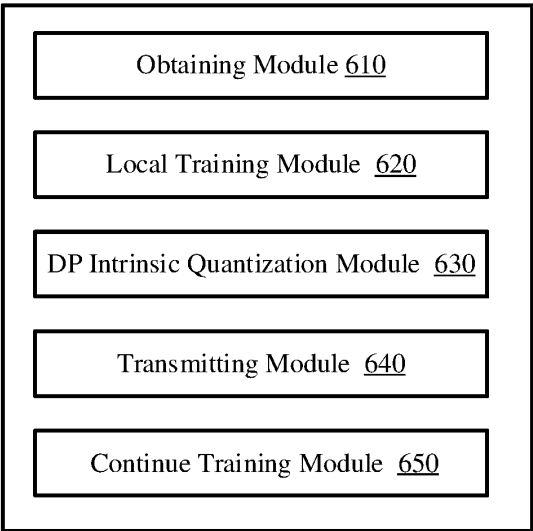


FIG. 6

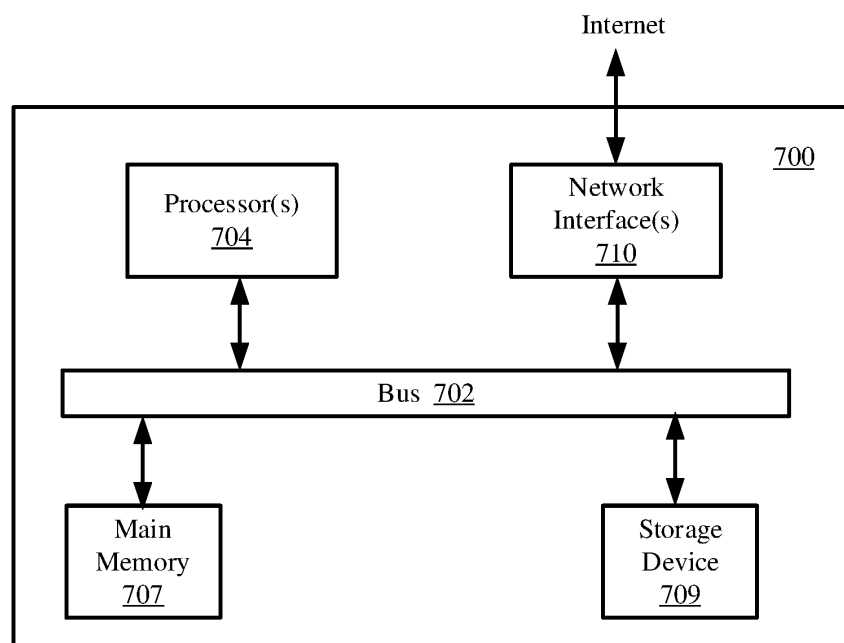


FIG. 7