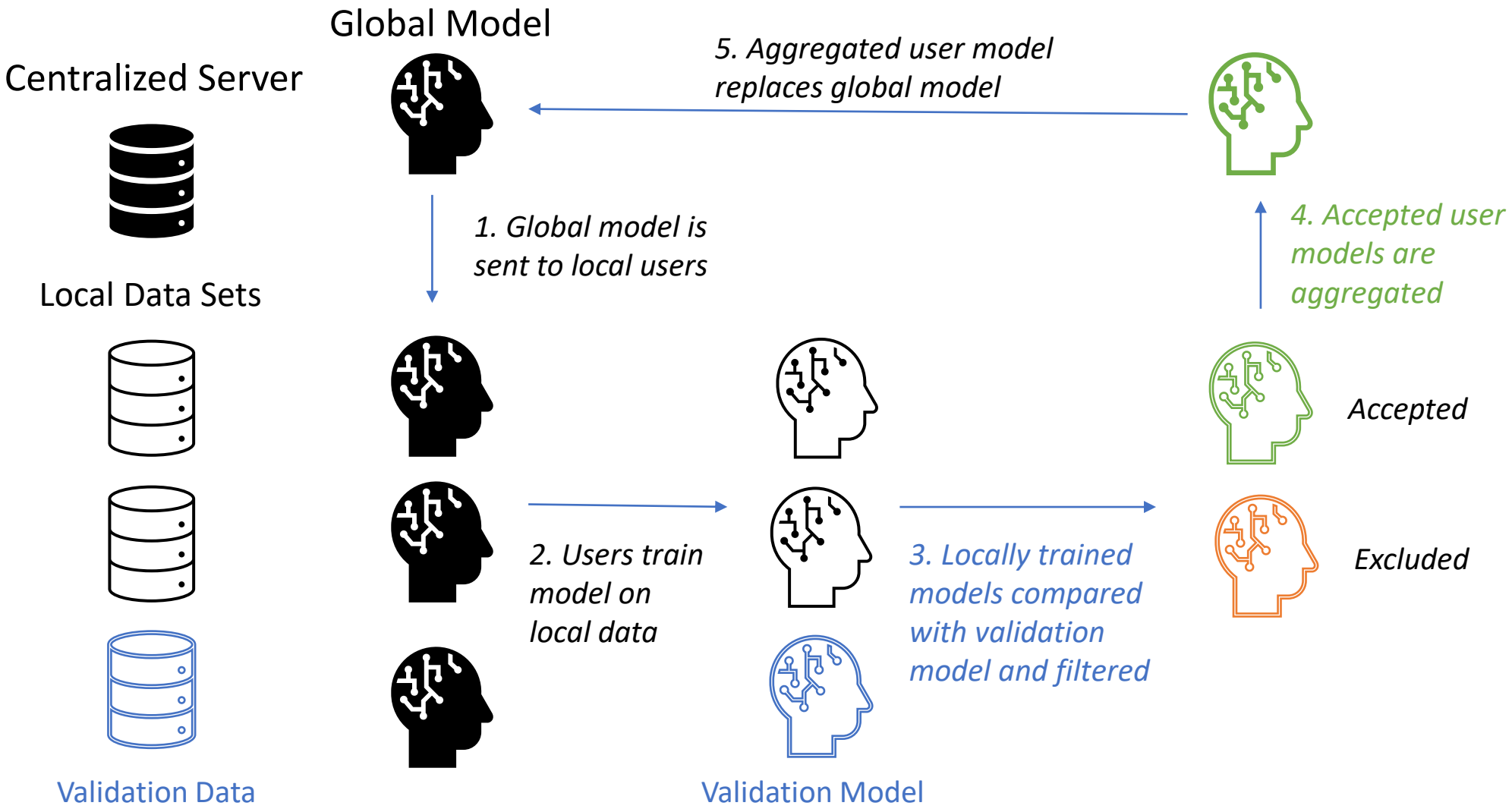
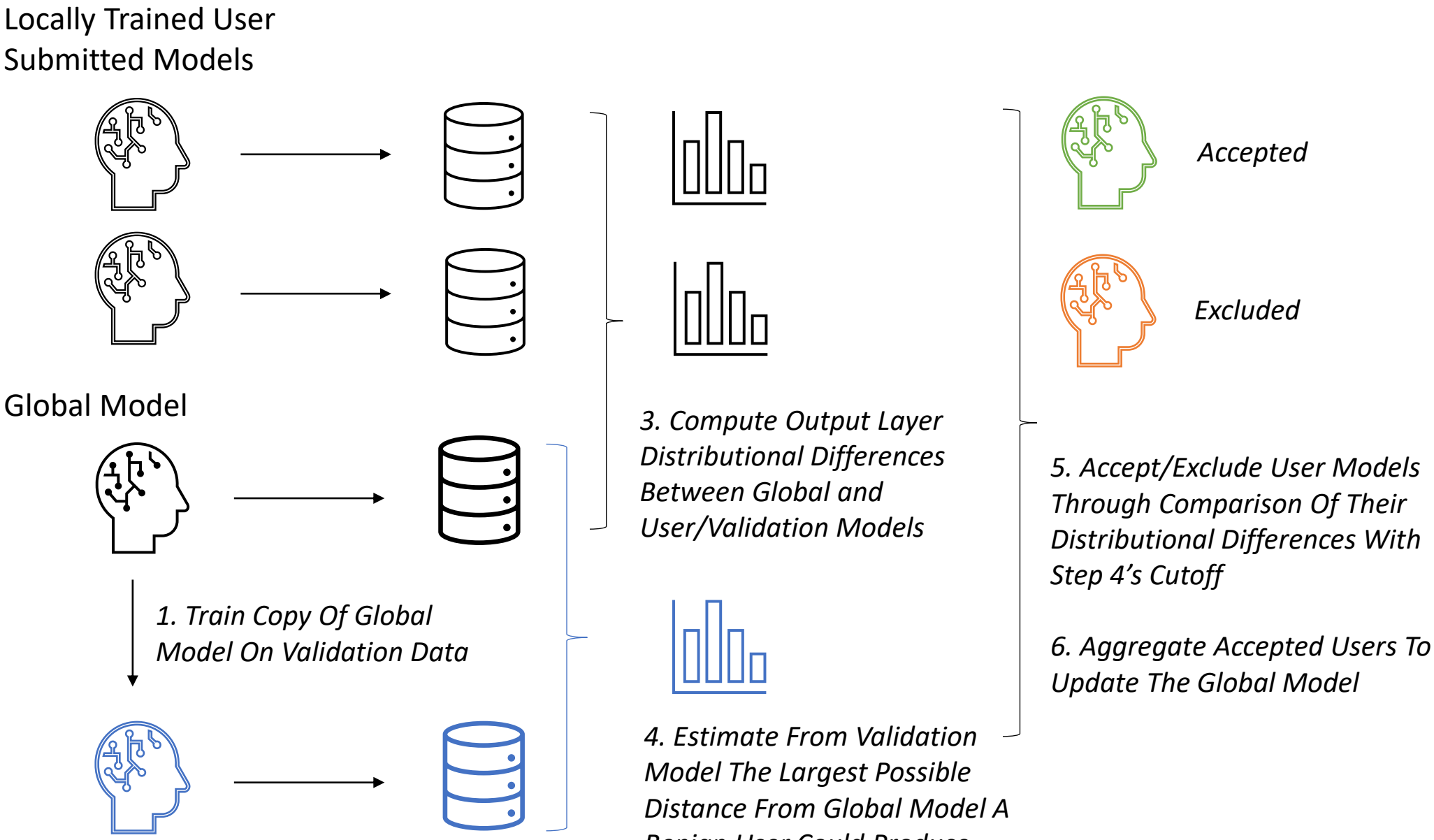

Global Model
Centralized Server
5. Aggregated user model replaces global model
1. Global model is sent to local users
4. Accepted user models are aggregated
Local Data Sets
Accepted
Excluded
2. Users train model on local data
3. Locally trained models compared with validation model and filtered
Validation Data
Validation Model


Locally Trained User Submitted Models
Global Model
1. Train Copy Of Global Model On Validation Data
2. Store Output Layer Predictions Of Each Model On Validation Data
3. Compute Output Layer Distributional Differences Between Global and User/Validation Models
4. Estimate From Validation Model The Largest Possible Distance From Global Model A Benign User Could Produce
5. Accept/Exclude User Models Through Comparison Of Their Distributional Differences With Step 4's Cutoff
6. Aggregate Accepted Users To Update The Global Model
Accepted
Excluded