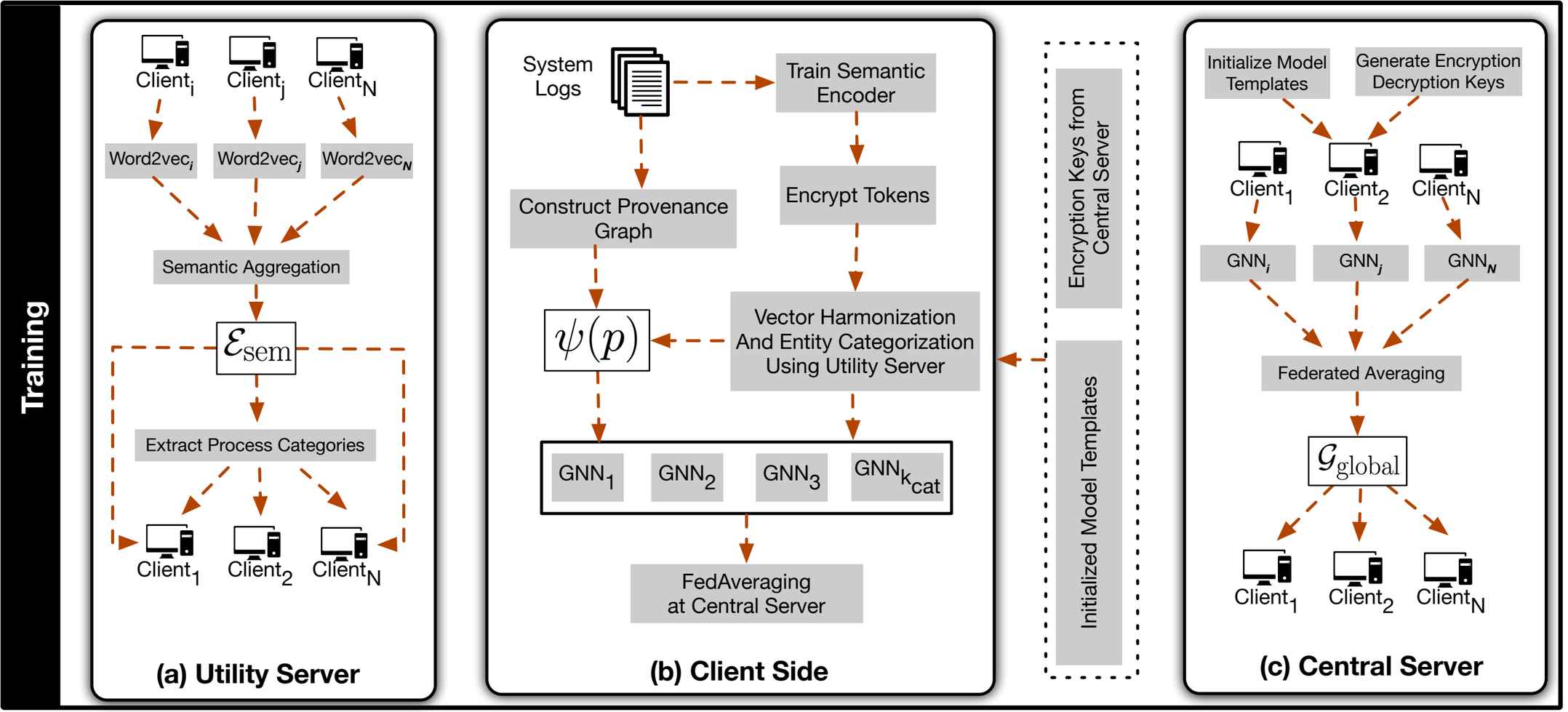
Training
Client$_i$
Client$_j$
Client$_N$
Word2vec$_i$
Word2vec$_j$
Word2vec$_N$
Semantic Aggregation
$\mathcal{E}_{\text{sem}}$
Extract Process Categories
Client$_1$
Client$_2$
Client$_N$
(a) Utility Server
System Logs
Train Semantic Encoder
Construct Provenance Graph
Encrypt Tokens
$\psi(p)$
Vector Harmonization And Entity Categorization Using Utility Server
GNN$_1$
GNN$_2$
GNN$_3$
GNN$_{k_{cat}}$
FedAveraging at Central Server
(b) Client Side
Encryption Keys from Central Server
Initialized Model Templates
Initialize Model Templates
Generate Encryption Decryption Keys
Client$_1$
Client$_2$
Client$_N$
GNN$_i$
GNN$_j$
GNN$_N$
Federated Averaging
$\mathcal{G}_{\text{global}}$
Client$_1$
Client$_2$
Client$_N$
(c) Central Server
Client Side Detection
System Logs
Construct Provenance Graph
Featurization
GNN based Anomaly Detection
Threat Alerts