Privacy-Preserving NLP: Protecting User Data

Attribute Inference

Training Data Extraction

Membership Inference

Model Inversion

Language Model

Data Minimization

Differential Privacy

Federated Learning

Secure Aggregation
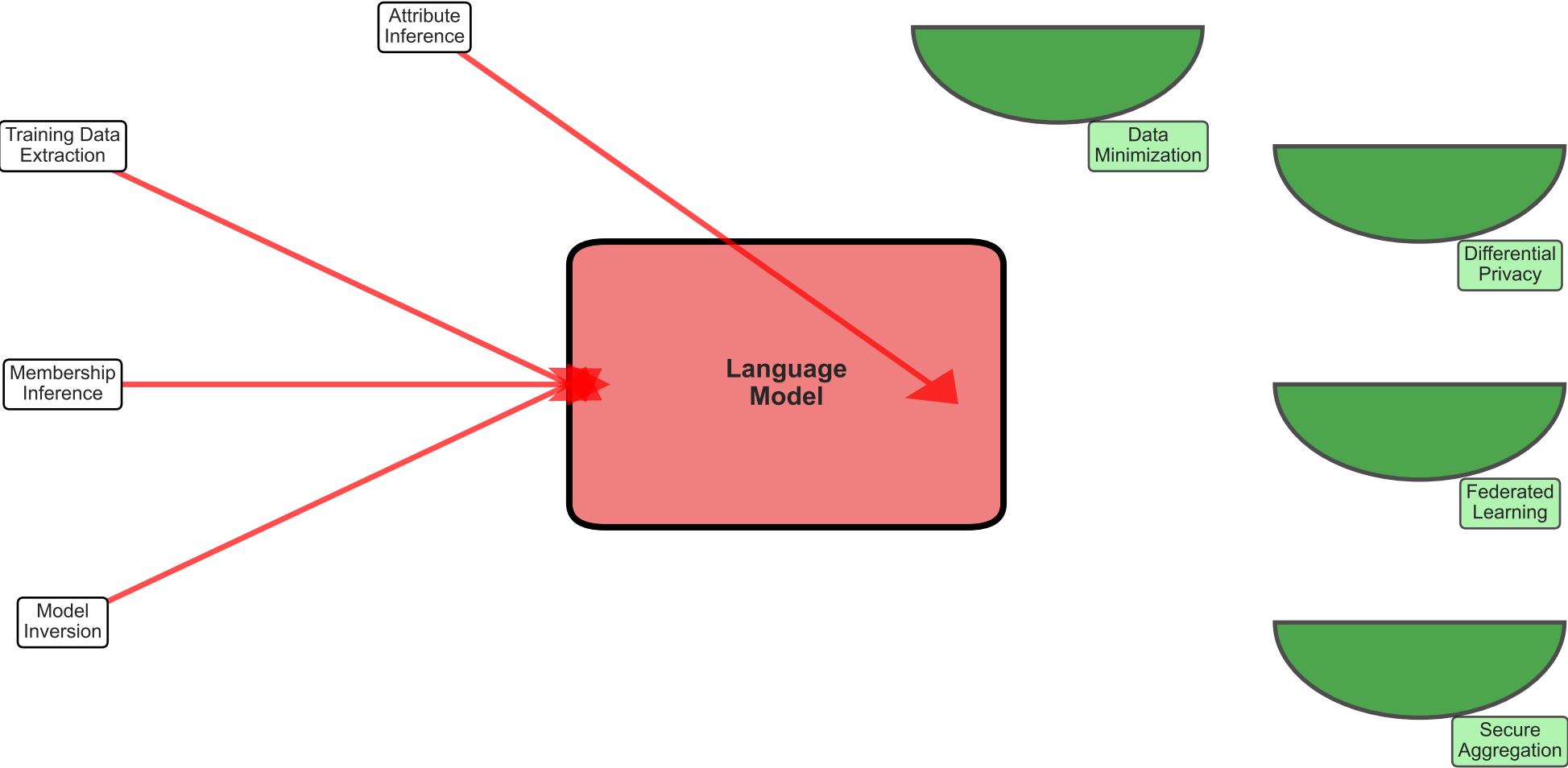
☐ Collect only what's needed

☐ Protect data in transit & rest

☐ Limit access & retention

☐ Enable user control