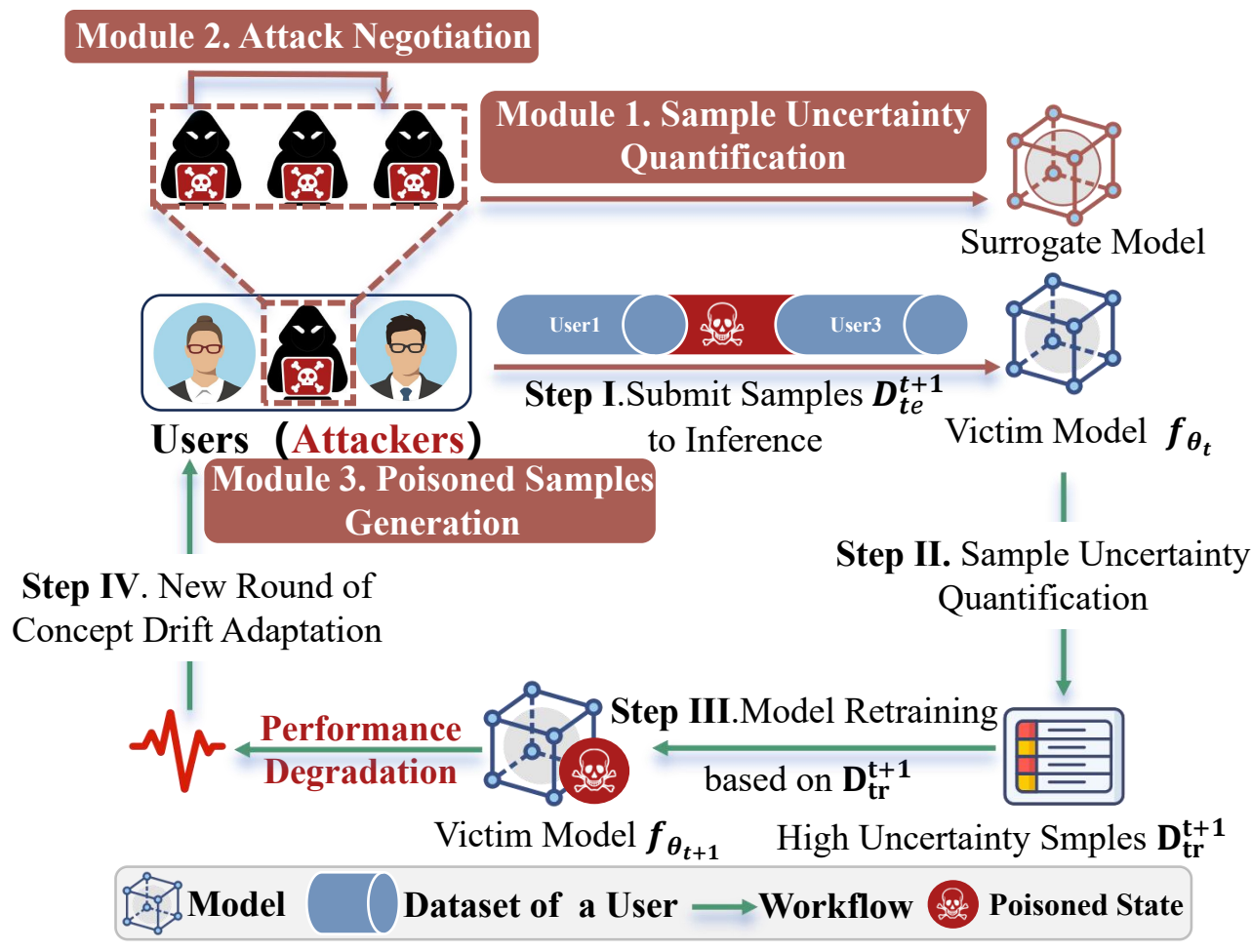
Module 2. Attack Negotiation
Module 1. Sample Uncertainty Quantification
Surrogate Model
User1
User3
Users (Attackers)
Step I.Submit Samples D_{te}^{t+1} to Inference
Victim Model f_{θ_t}
Module 3. Poisoned Samples Generation
Step II. Sample Uncertainty Quantification
Step IV. New Round of Concept Drift Adaptation
Performance Degradation
Step III.Model Retraining based on D_{tr}^{t+1}
Victim Model $f_{\theta_{t+1}}$
High Uncertainty Smples D_{tr}^{t+1}
Model
Dataset of a User
Workflow
Poisoned State