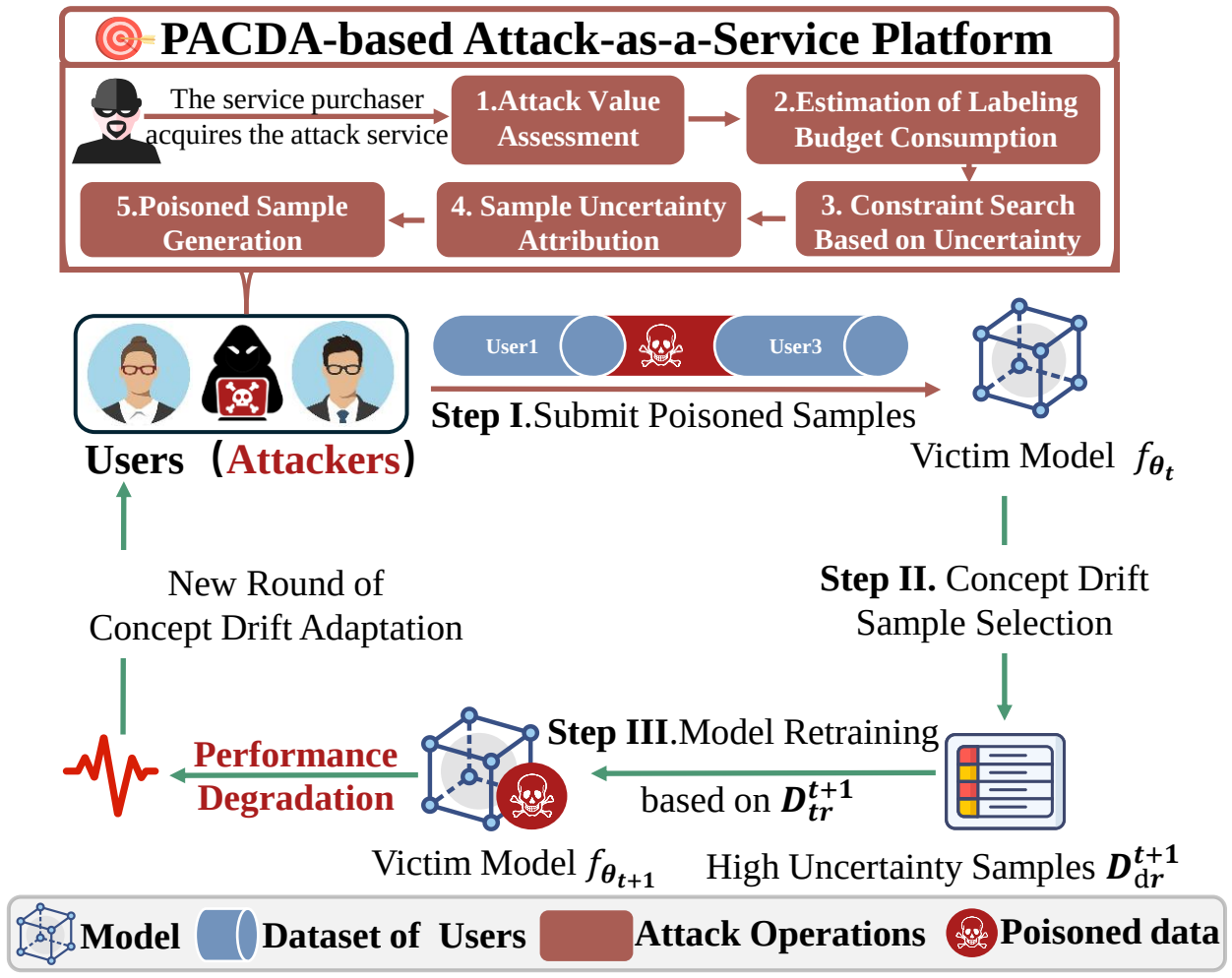
PACDA-based Attack-as-a-Service Platform
The service purchaser acquires the attack service
1.Attack Value Assessment
2.Estimation of Labeling Budget Consumption
3. Constraint Search Based on Uncertainty
4. Sample Uncertainty Attribution
5.Poisoned Sample Generation
User1
User3
Step I.Submit Poisoned Samples
Users (Attackers)
Victim Model f_{θ_t}
Step II. Concept Drift Sample Selection
Step III.Model Retraining based on D_{tr}^{t+1}
High Uncertainty Samples D_{dr}^{t+1}
Victim Model $f_{\theta_{t+1}}$
Performance Degradation
New Round of Concept Drift Adaptation
Model
Dataset of Users
Attack Operations
Poisoned data