

Creditability-based Weighted Voting to Reduce False Positives and Negatives in Intrusion Detection

Student: Wei-Hsuan Tai
學生：戴維炫

Advisor: Ying-Dar Lin
指導教授：林盈達

Problems:

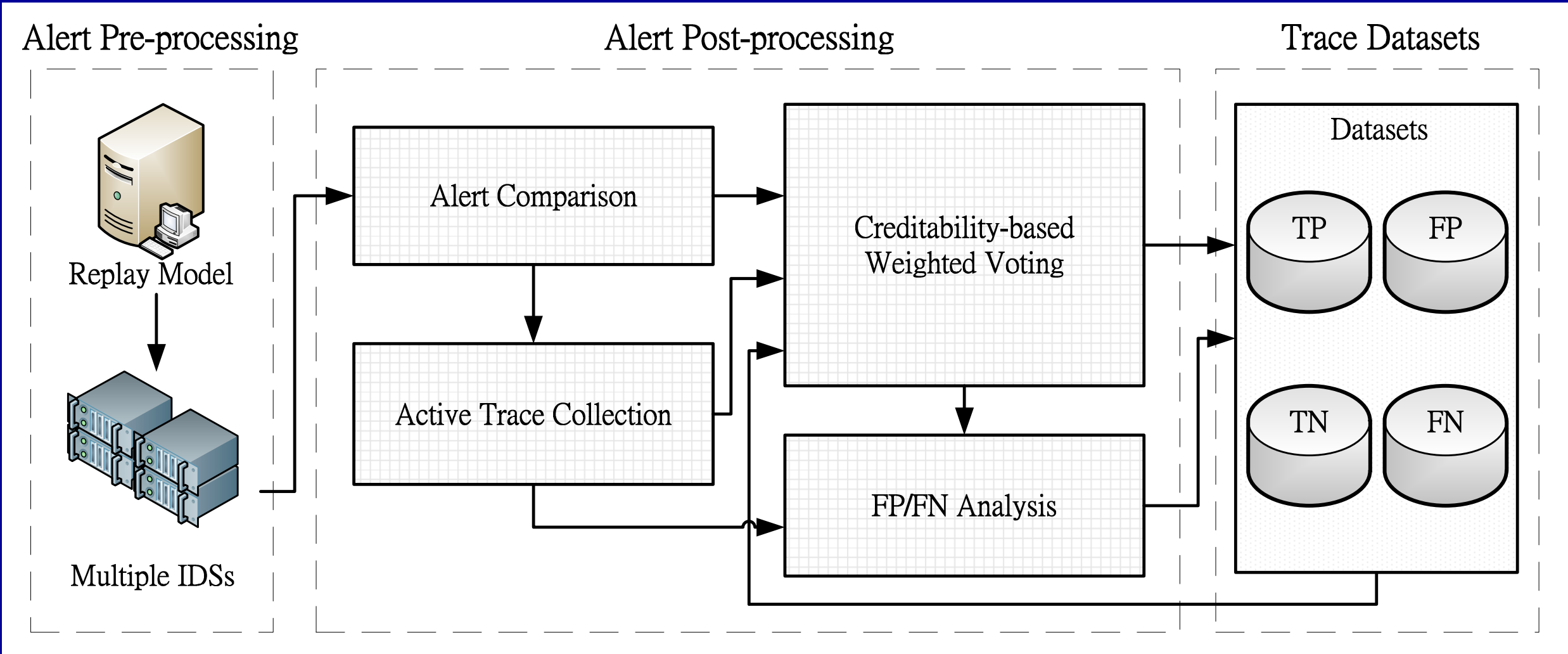
- A large number of alerts from IDS anomaly analysis
- Leverage multiple IDSs' domain knowledge to reduce both FPs and FNs

Approach:

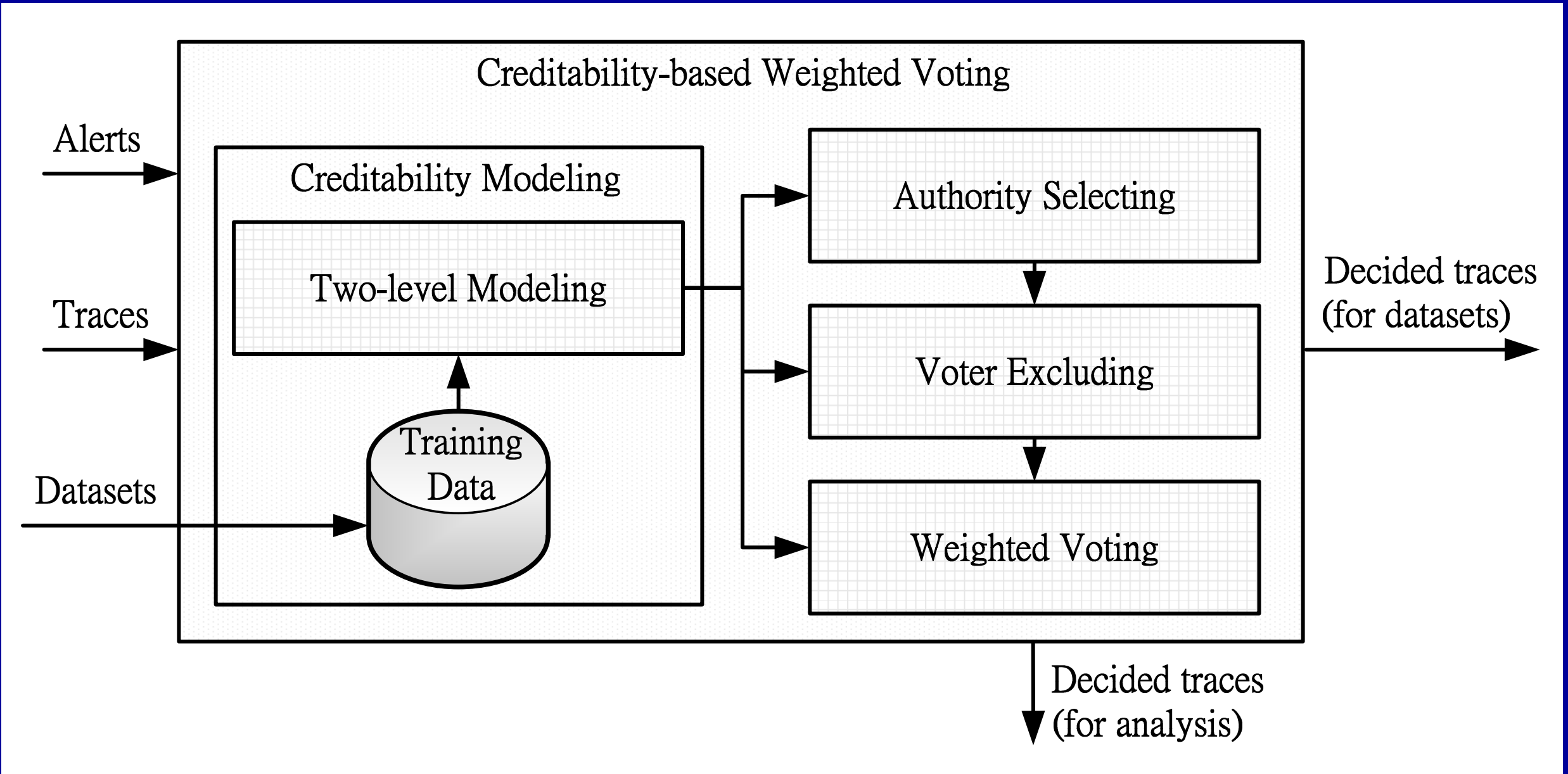
- Creditability Modeling with two levels
 - Alert Message level, Protocol level
- Authority Selecting
 - Directly decide a trace by an authority if it exists
- Weighted Voting
 - Decide a trace with proper voters and weights

Experiment results:

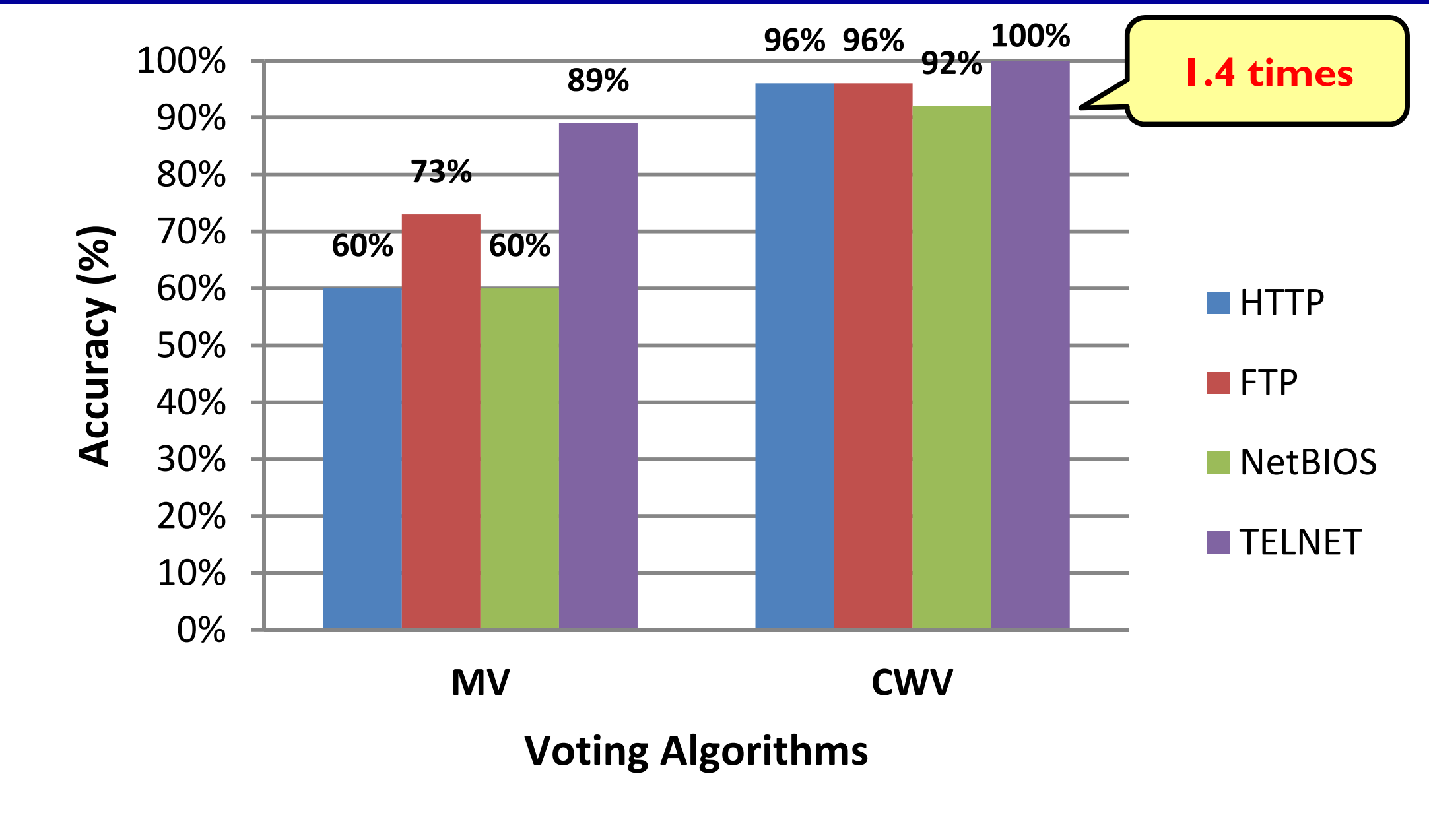
- Accuracy: 96% on the average
- Efficiency: 94%
 - Harmonic mean of TPR and TNR
- Average percentages of FP and FN reduction
 - FP reduction: 21%
 - FN reduction: 58%



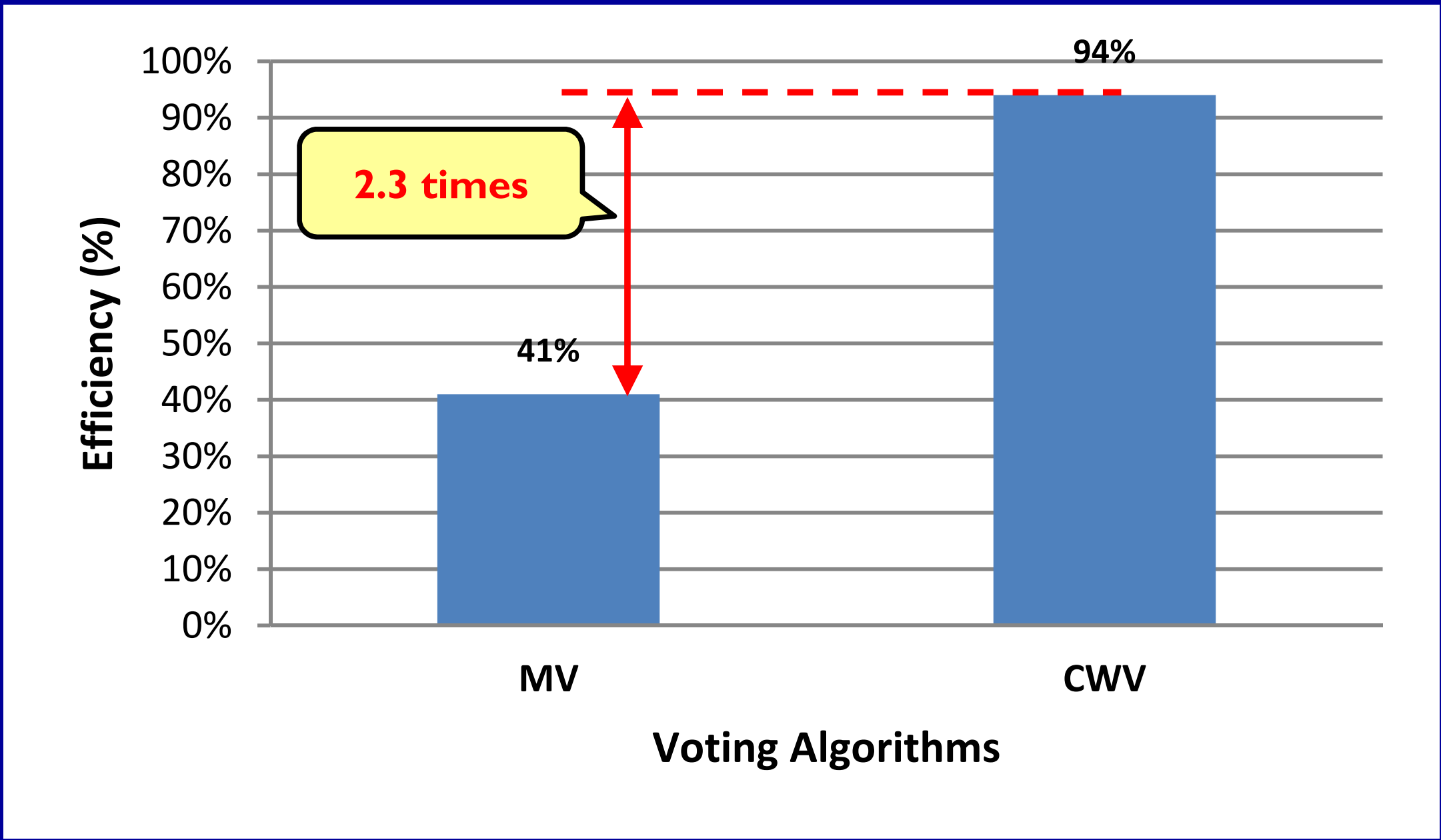
Architecture of our system



Architecture of Creditability-based Weighted Voting



Higher accuracy



Higher efficiency