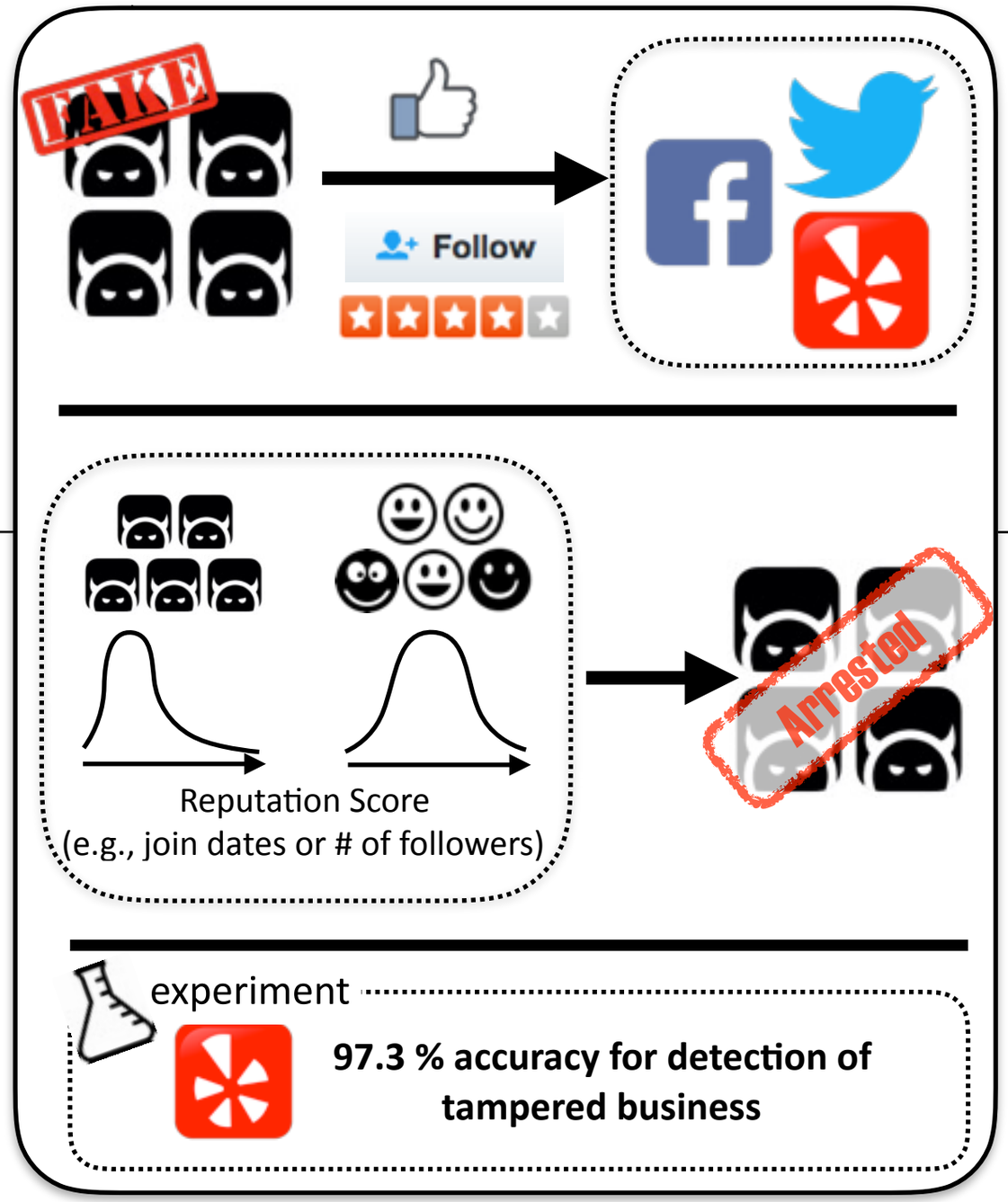
Towards Robust Crowd Computations

Motivation:

- **Sybil attacks** on crow computation systems (e.g., manipulating crowd opinion with faked identities)
- It is very hard to detect each Sybil identities

Approach:

- Focus on large groups not each identities using statistical analysis technique (e.g., KL-divergence score)
- Use unforgeable timestamps to foil adaptive attackers (e.g., join dates)



Scientific Impact:

- Distribution of tampered computations are highly skewed
- Using Yelp datasets, we show that our approach can detect most of highly tampered computations with 97.3% accuracy

Broader Impact:

- Our approach raises the bar for defense against adaptive attackers
- Social and e-commerce sites which rely on crow computing can directly use our approach to detect tampered crowd computation (e.g., Yelp, Twitter, or etc.)

Project Number	CNS-1421444
Institution	Northeastern University
Contact	amislove@ccs.neu.edu