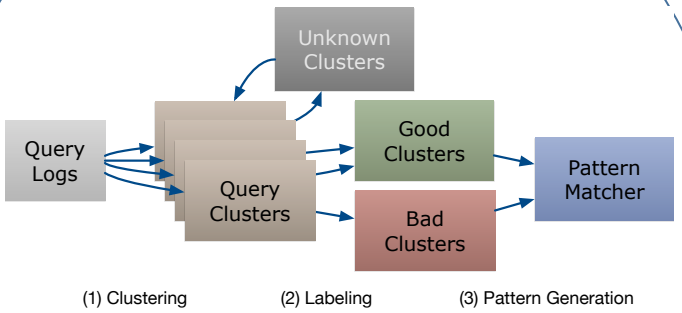
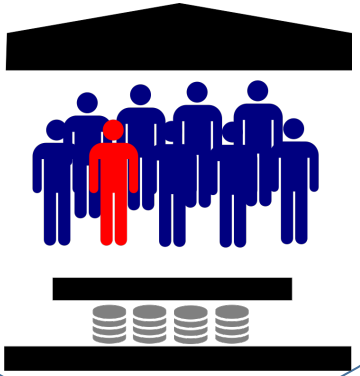
Data is Social: Exploiting Data Relationships to Detect Insider Attacks

Challenge:

Identifying threats posed by malicious insiders and helping security analysts detect them





Solution:

- One of our biggest challenges so far has has been modeling "expected behavior"
- Develop machine learning based models and detection algorithms to identify deviations from expected behavior

Awards: 1409551, 1409303

PIs: *Kennedy*, Chandola, Upadhyaya, Ngo (UB); *Nguyen* (Michigan)

Scientific Impact:

- Developing a new threat model and assessment methodology for insider attack mitigation
- New methods to understand behavior using database queries
- Hierarchical modeling and statistical inference for discrete and complex structures such as database queries and hyper-graphs

Broader Impact:

- Solutions will provide a practical tool for insider threat detection in finance and defense sectors
- Tangential impact on modeling query workloads
- Currently supporting 3 PhD students and 2 undergraduates at UB, 1 PhD student at UM
- Outreach via UB's NSA-certified center of excellence in Information Assurance.