CERIAS

the center for education and research in information assurance and security

Database Anomalous Usage Detection*

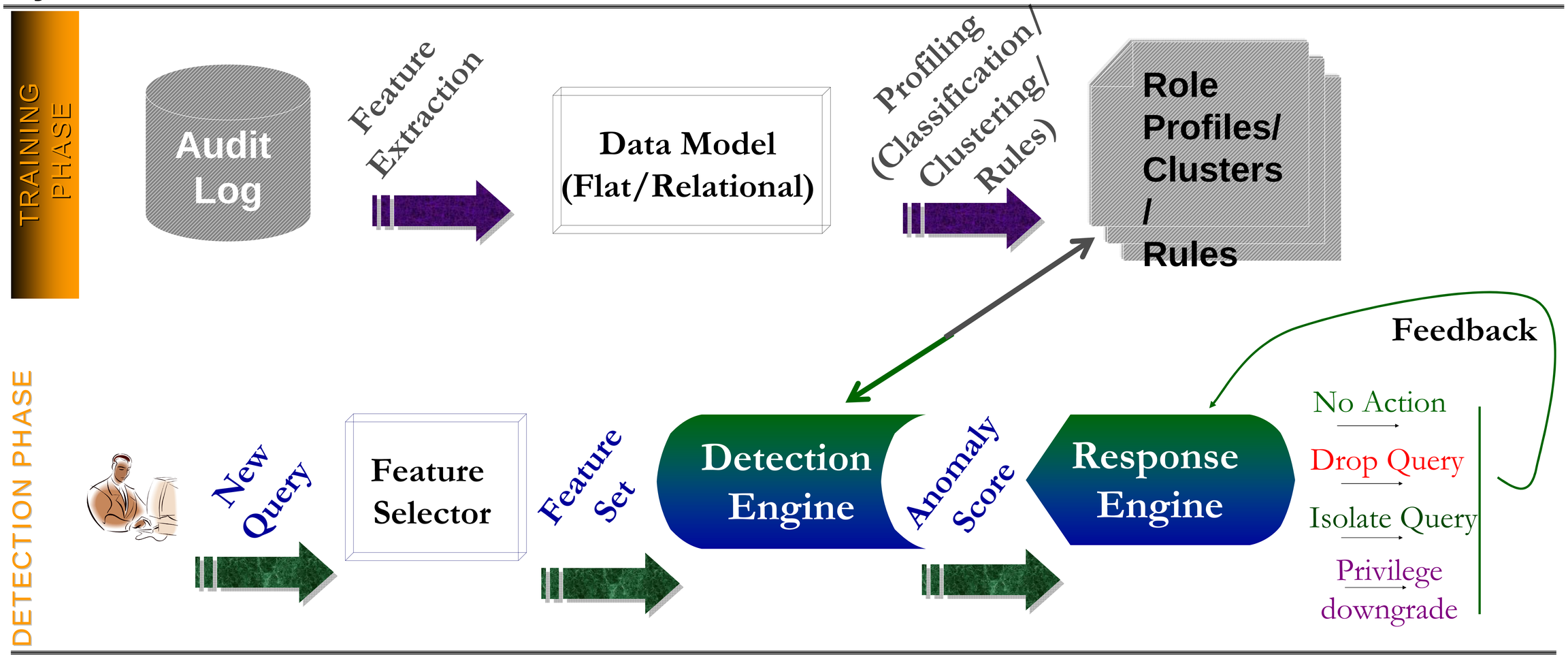
Ashish Kamra and Dr. Elisa Bertino

akamra@purdue.edu ,bertino@cs.purdue.edu

Motivation

- Audit database usage pattern of employees and detect anomalies
- Model SQL Injection attacks as an anomalous database usage problem
- Create an intrusion response mechanism for responding to intrusions

System Architecture



Current Mechanisms

- **Supervised Learning :** When database roles are available, create role profiles and use a naïve bayes classifier to detect anomalous queries
- **Unsupervised Learning :** When no roles are available, group users into clusters using clustering techniques and detect anomalies using outlier detection techniques

Future Work

- Relational data model for feature extraction
- Information theoretic measures for quantifying query semantics
- Intrusion response language and mechanisms

* Supported by NSF under Grant No. 0430274

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center