ProFact

A Provenance-based Analytics Framework for Access Control Policies

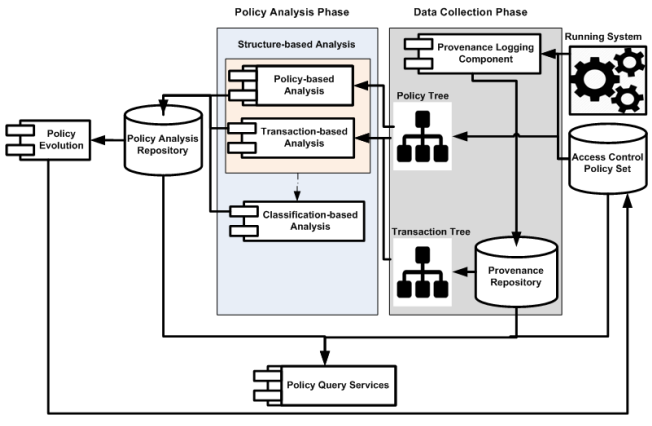
Amani Abu Jabal (Purdue University), **Maryam Davari** (Purdue University), **Elisa Bertino** (Purdue University), **Christian Makaya** (IBM), **Seraphin Calo** (IBM), **Dinesh Verma** (IBM), **Christopher William** (DSTL).

Policy Quality Requirements

"Good Quality" Policies should be:

- **Consistent:** to reduce conflicts
- **Complete:** to enhance the predictability of device behaviors
- **Minimal:** to reduce the size of the policy set and enhance security
- **Relevant:** to minimize exploitations
- **With minimal exceptions:** to reduce the number of user administrative actions at run-time

Framework Architecture



Policy Analysis Services

1. Policy-based Analysis:

Static analysis using the policy tree.

2. Transaction-based Analysis:

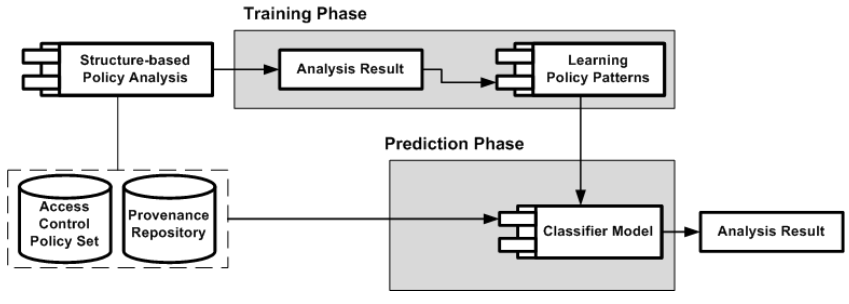
Dynamic analysis on the executed transactions along with their associated policies.

	Policy-based Analysis	Transaction-based Analysis
Inconsistency	✓	✓
Exception	✘	✓
Incompleteness	✘	✓
Redundancy	✓	✓
Irrelevancy	✓	✘

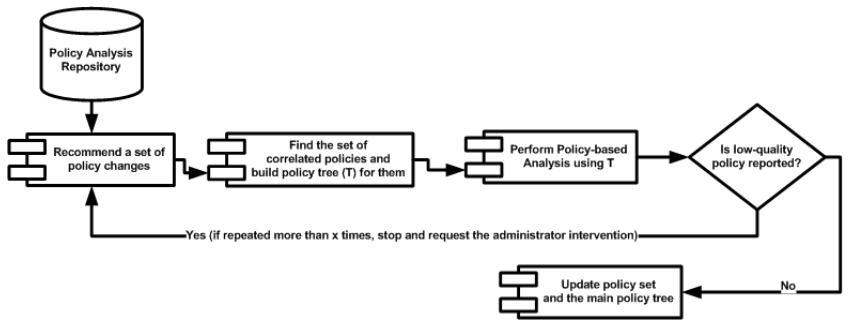
3. Classification-based Analysis:

Generate patterns of policies that are of "low quality" and create categories (i.e., classes) of policies.

- **One Classifier:** uses one of the state-of-the-art classifiers (e.g., SVM).
- **Combined Classifiers:** a set of classifiers.



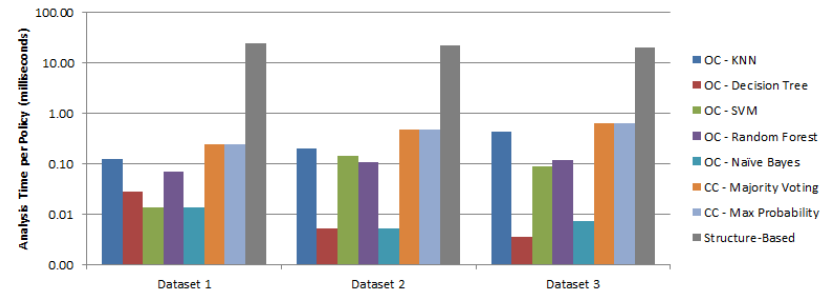
Policy Evolution



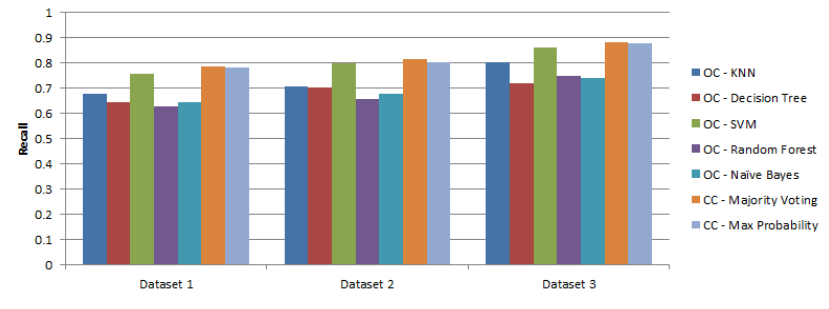
Experiment Results

- **Performance (Policy-based vs. Transaction-based Analysis)**

- **Performance (Classification-based Analysis)**



- **Efficiency (Classification-based)**



Distributed Analytics and Information Science International Technology Alliance
Annual Fall Meeting, September 2018