Proposal for a Bachelor’s Thesis

Monitoring Aggregating Compliance Policies: A Comparative Case Study

Supervisor: Srđan Krstić
Professor: Prof. D. Basin

Prerequisites

- Familiarity with linear temporal logic
- Some familiarity with data modeling, databases and triggers

Introduction and Motivation

The main focus of the thesis proposal is the Monitoring problem: Given a stream of time-varying data (coming from a log of execution) and a policy (formulated in a specification language), check whether the policy is satisfied for every prefix of the stream.

Monitoring problem is a very general concept and many popular industrial applications can be reduced to an instance of it, for example monitoring stock market prices, monitoring inventories, security analysis, as well as supporting self-adaptive software systems.

For example, consider the following monitoring instance from the domain of financial services: “Any user must not withdraw from his credit card account more than $10,000 in total within a 31 day period, except if he has previously received a special credit limit.” This seemingly simple policy requires an expressive specification language with aggregations (“in total”), quantification (“any user”), Boolean connectives (“except if”), and qualitative (“has previously received”) and quantitative (“within a 31 day period”) temporal operators.

The above policy should provide a flavor of the types of policies that are used in practice. There are a variety of technological approaches that try to solve the monitoring problem from many different aspects, for instance:

- Monitoring the metric first-order temporal logic with aggregations [2]
- Data stream processing [1]
- Complex event processing [3]
- Incremental database view maintenance [4]

Even though they are all solving the monitoring problem, there is a large gap in the expressiveness, complexity and clarity of semantics between these approaches. This is due to the fact that these tools were historically developed to meet the needs of different application scenarios, and thus no clear distinction exists on what facets of the general monitoring problem they actually address.

Objective

The goal of this thesis is to make the first steps towards a comprehensive and systematic comparison between these different approaches. As an extended case study, we will use monitoring requirements and data coming from the tracking of warehouse commodities. For this, we will use natural language policies provided by the StockScan company (http://www.stockscan.ch/).

With the help of the thesis supervisor the student is to survey the monitoring tools that are suitable to monitor the policies. Then formalize the policies using the specification languages of the selected tools. The tools should then be benchmarked on a data provided by StockScan.

As a baseline for the comparison the student is also asked to implement a custom monitor directly via database triggers.

Tasks

1. Study the monitoring problem [2] and survey the existing monitoring tools.
2. Formalize natural language policies from the case study.
3. Implement a custom monitor directly via database triggers.
4. Evaluate the implementation on the case study and compare it to the existing tools.
5. Discuss advantages and drawbacks of different tools in terms of expressiveness and efficiency.
6. Write the final report and prepare the presentation.

Deliverables

The following deliverables are due at the end of the project:

**Final report** The final report should consist of an introduction; a theoretical background section; one or more sections describing the policy specification, custom monitor implementation; tool comparison and discussion; and a conclusion. The report may be written in English or German. Three copies of the report and any software developed must be delivered to the supervisor.

**Source code** Complete development including easily reproducible case studies.

**Presentation** At the end of the project, a presentation of 20 minutes must be given during an InfSec group seminar. It should give an overview and discuss the most important highlights of the work.

References


