A Real-Time, Flexible Logging Infrastructure for MonPoly

Bachelor's Thesis

Jonas Degelo

ETH Zürich

February 24, 2023

MonPoly

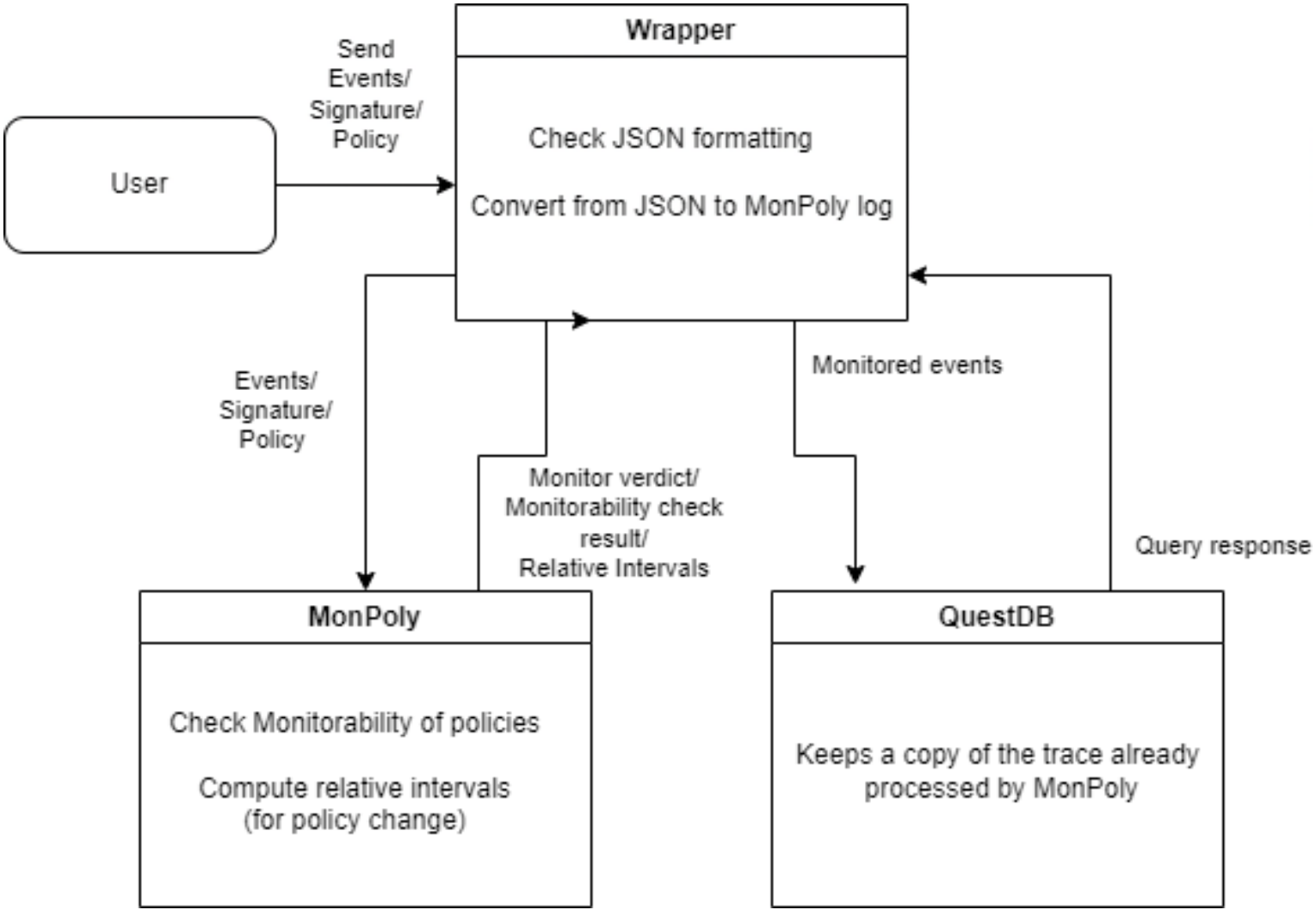
- Runtime Monitor
- Metric First Order Temporal Logic (MFOTL)

Time-Series Databases

Motivation

Combining logging and monitoring. Missing policy change in MonPoly

The Wrapper


Wrapper
Send
Events/
Signature/
Policy
User
Check JSON formatting
Convert from JSON to MonPoly log
Events/
Signature/
Policy
Monitor verdict/
Monitorability check
result/
Relative Intervals
Monitored events
Query response
MonPoly
Check Monitorability of policies
Compute relative intervals
(for policy change)
QuestDB
Keeps a copy of the trace already
processed by MonPoly

Signature to Database Schema 1

```
loc_accessed(user_id: int, purpose: string)
perm_granted(user_id: int)
perm_revoked(user_id: int)
```

Figure: Sample MonPoly Signature

Signature to Database Schema 2

```
CREATE TABLE perm_revoked(x1 INT,
                          time_stamp TIMESTAMP,
                          time_point INT)
                          timestamp(time_stamp);
CREATE TABLE perm_granted(x1 INT,
                          time_stamp TIMESTAMP,
                          time_point INT)
                          timestamp(time_stamp);
CREATE TABLE loc_accessed(x1 INT, x2 STRING,
                          time_stamp TIMESTAMP,
                          time_point INT)
                          timestamp(time_stamp);
CREATE TABLE ts( time_stamp TIMESTAMP,
                 time_point INT)
                 timestamp(time_stamp);
```

Figure: SQL Schema for Sample Policy

Policy Change

Relative Intervals

Definition

The relative interval of the formula ϕ, $\mathsf{RI}(\phi) \subseteq \mathbb{Z}$ is defined recursively over the formula structure: $\mathsf{RI}(\phi) =$

$$
\begin{cases}
\{0\} & \text{atomic formula,} \\
\mathsf{RI}(\psi) & \neg\psi,\ \exists x.\psi, \\
 & \text{or } \forall x.\psi, \\
\mathsf{RI}(\psi) \uplus \mathsf{RI}(\chi) & \psi \vee \chi, or \psi \wedge \chi, \\
(-b, 0] \uplus ((-b, -a] \oplus \mathsf{RI}(\psi)) & \bullet_{[a,b)}\psi, \\
[0, b) \uplus ([a, b) \oplus \mathsf{RI}(\psi)) & \bigcirc_{[a,b)}, \\
(-b, 0] \uplus ((-b, 0] \oplus \mathsf{RI}(\psi)) \uplus ((-b, -a] \oplus \mathsf{RI}(\chi)) & \psi\, \mathcal{S}_{[a,b)} \chi, \\
[0, b) \uplus ([0, b) \oplus \mathsf{RI}(\psi)) \uplus ([a, b) \oplus \mathsf{RI}(\chi)) & \psi\, \mathcal{U}_{[a,b)}\, \chi, \\
[0, b) \uplus ([0, b) \oplus \mathsf{RI}_{\mathsf{reg}}(\rho)) & \triangleright_{[a,b)}\ \rho, \text{ and} \\
(-b, 0] \uplus ((-b, 0] \oplus \mathsf{RI}_{\mathsf{reg}}(\rho)) & \blacktriangleleft_{[a,b)}\ \rho.
\end{cases}
$$

Extended Relative Intervals

Definition

Let M and N be two masked predicate maps and T a positive interval, then

$$
\begin{aligned}
M \ddot{\Cup} N =& \{p(I) \to (I \Cup J) \mid p(I) \to I \in m \text{ and } p(I) \to J \in n\} \\
&\cup \{p(I) \to I \mid (p(I) \to I \in m \text{ and } p(I) \in \mathrm{k}(M) \setminus \mathrm{k}(N))\} \\
&\cup \{p(I) \to I \mid (p(I) \to I \in n \text{ and } p(I) \in \mathrm{k}(N) \setminus \mathrm{k}(M))\} \\
T \dot{\Cup} M =& \{p(I) \to (T \Cup I) \mid p(I) \to I \in M\} \\
T \dot{\oplus} M =& \{p(I) \to (T \oplus I) \mid p(I) \to I \in M\}
\end{aligned}
$$

Extended Relative Intervals

Definition

The extended relative interval of the formula φ, $\mathrm{ERI}(\varphi)$ is defined recursively over the formula structure: $\mathrm{ERI}(\varphi) =$

$$\begin{cases} \{\} & \text{if } \varphi \text{ is an atomic formula} \\ & \text{and not a predicate,} \\ \{p(m) \to [0,0]\} & \text{if } \varphi \text{ is a predicate with name} \\ & p \text{ and mask } m, \\ \mathrm{ERI}(\psi) & \text{if } \varphi \text{ is of the form } \neg\psi, \exists x.\psi, \\ & \text{or } \forall x.\psi, \\ \ldots & \end{cases}$$

Partial Policy Change in MonPoly

- Named formulas
- `NAME[f1, name1] OR NAME[f2 and f3, name2]`
- Commands to add or remove conjuncts or disjuncts

Performance Overhead