PerfSPEC Learning Phase

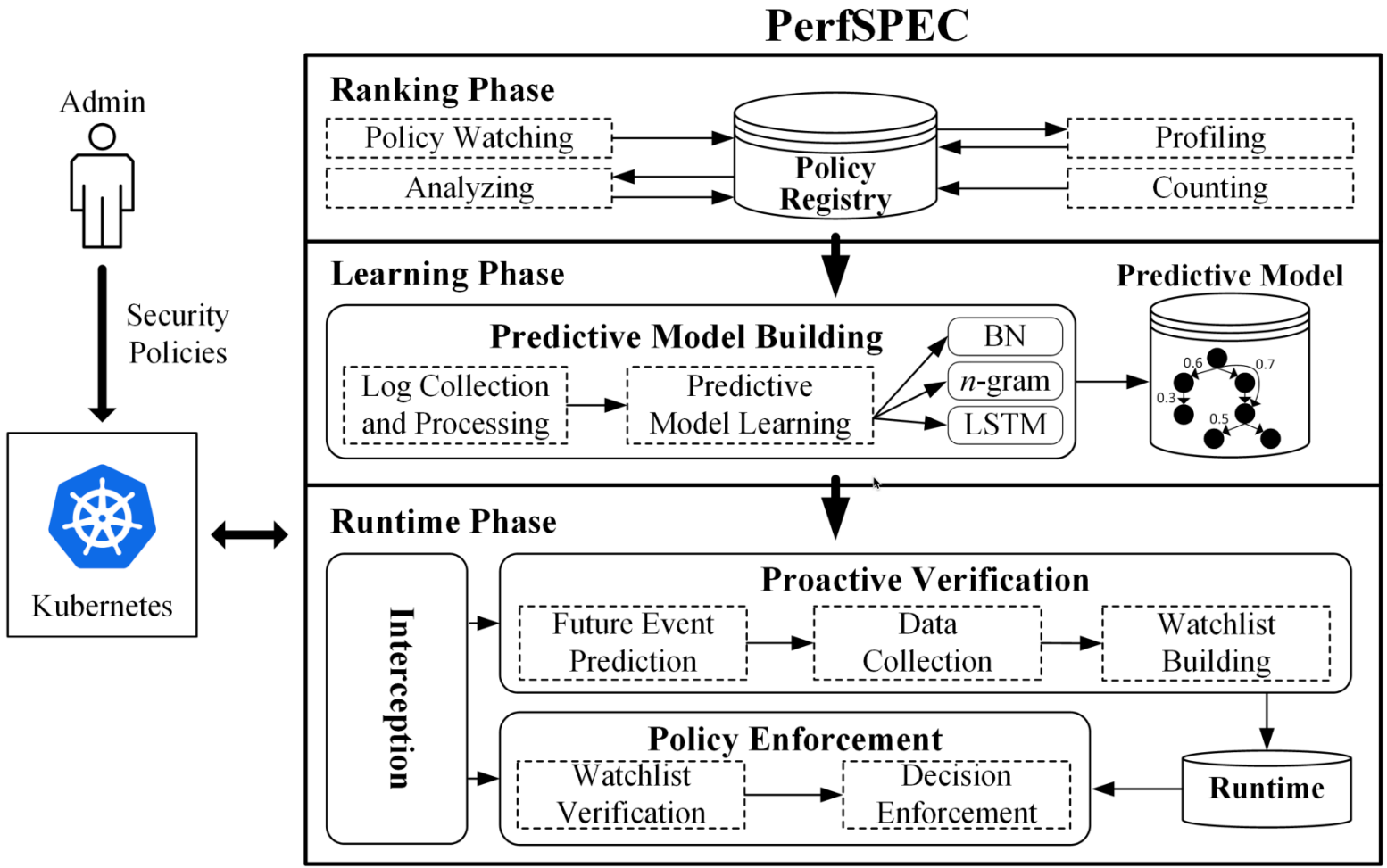
Aplicación proactiva de políticas de seguridad
basadas en perfiles de rendimiento
para contenedores

H. Kermabon-Bobinnec et al.,
"PerfSPEC: Performance Profiling-based Proactive Security Policy Enforcement for Containers,"
in IEEE Transactions on Dependable and Secure Computing,
doi: 10.1109/TDSC.2024.3420712

Aplicación proactiva de políticas de seguridad basadas en perfiles de rendimiento para contenedores

Performance Profiling-based Proactive Security Policy Enforcement for Containers -- IEEE publication

Abstract—Container environments provide cloud native applications with scalability, flexibility, and portable support. As a popular container orchestrator, Kubernetes facilitates automatic deployment and maintenance of a large number of containerized applications. However, potential misconfigurations, vulnerabilities, or implementation flaws may empower attackers to exploit the Kubernetes cluster. Although existing solutions such as runtime security policy enforcement may prevent an attack, they can be inefficient in large scale container environ- ments. In this paper, we propose a performance profiling-based proactive security policy enforcement solution, namely, PerfSPEC. First, we accelerate the proactivization of policies (which typically requires significant manual effort) by proposing to profile and rank existing policies according to their induced overhead. This allows us to better focus our efforts and greatly improve the overall response time (e.g., by 98% in contrast to less than 49%). Then, we address the performance limitations of existing solutions by leveraging learning-based approaches to predict future events and compute their verification results in advance. As a result, PerfSPEC achieves a viable response time (e.g., less than 10 ms in contrast to 600 ms with one of the most popular existing approaches) even for large container environments (up to 800 Pods).



PrefSPEC Learning Phase

Proceso

- ## Recolección logs

  Recopilación de logs de eventos del entorno. Para ello, PerfSPEC primero requiere habilitar la función de **auditoría en logs** de Kubernetes

- ## Procesado

  - Se extraen los eventos de los datos históricos y se genera un log de autitoría realista y representativo.
  - Se extraen los campos *objectRef[resource]* y métodos de los logs de eventos y se almacenan en un archivo
  - Usando herramientas de análisis de datos, se procesa cada entrada tipificando los eventos, a los que se asigna al par (método, recurso) una cadena *metodo_recurso* (tipo de evento).

- ## Modelo Aprendizaje Predictivo

  Implementar una de las tres diferentes aproximaciones propuestas: *Bayesian network*, *n-gram* y *LSTM*.

Recolección logs

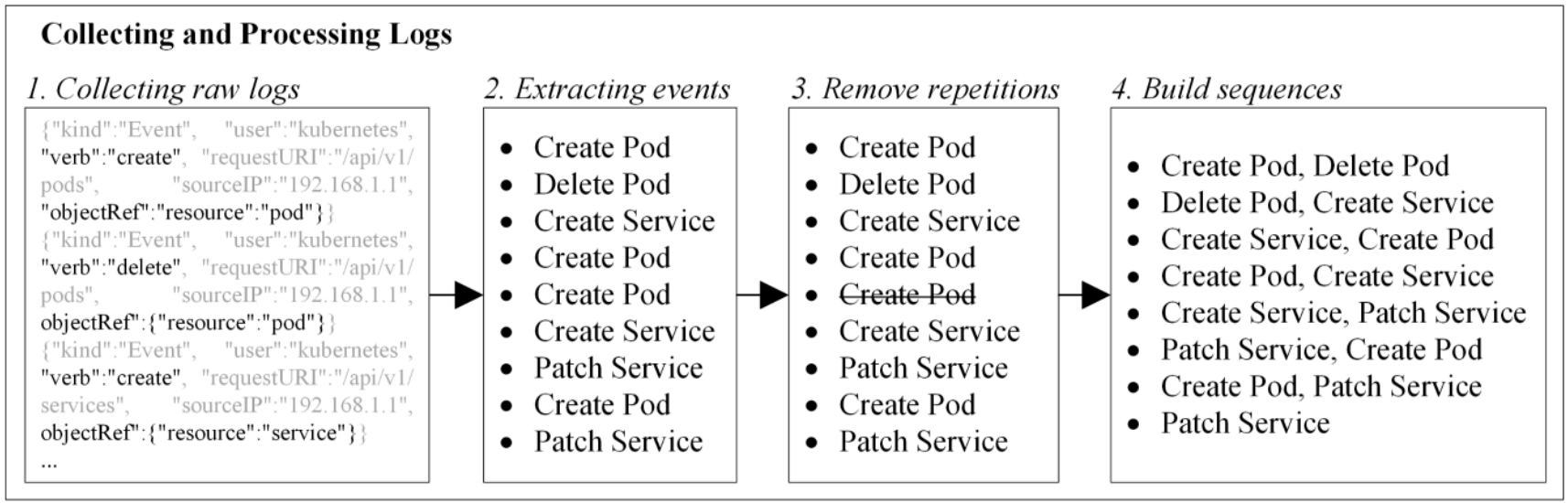
Metodología

- Para generar eventos, se adoptan los 60 **Helm** más populares disponibles en ArtifactHub que se implementan y eliminan a intervalos regulares para simular operaciones administrativas.
- Como estos paquetes de software son utilizados comúnmente por los usuarios para implementar aplicaciones y servicios en Kubernetes, se considera que las secuencias de operaciones realizadas para cada implementación y eliminación son **realistas y representativas**.
- Guardamos los eventos utilizando los logs de auditoría de Kubernetes

DataSet

- 60 paquetes
- 16.548 eventos

Procesado



Aprendizaje Predictivo

Approach	Size of Window	Accuracy	Offline Learning Time	Runtime Inference Time
Bayesian Network	*N.A.*	79.7%	4.29 s	1e-4 s
LSTM	1	92.3%	24.01 s	0.06 s
	2	97.6%	32.75 s	0.07 s
n-grams	1	88.2%	0.01 s	1e-4 s
	2	97.3%	0.07 s	2e-4 s

LSTM

Long Short Term Memory

python™

PrefSPEC Learning Phase

CONDA Conda package manager

pandas Pandas Data Analysis

marimo Python notebooks

jupyter Python notebooks

TensorFlow Machine learning

Rust Developer & Cloud Architect

Python package and project manager in Rust

Polars DataFrames Rust

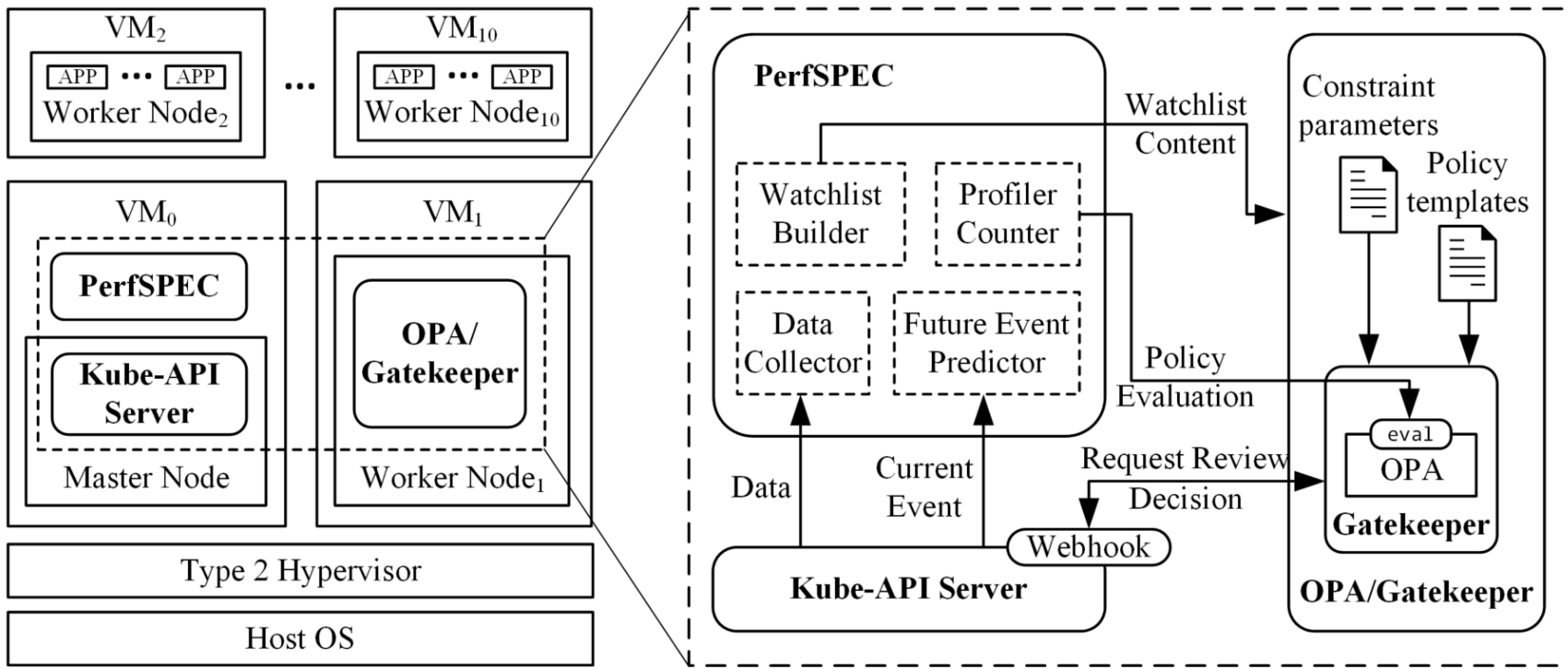
Nushell + Dataframes a Rust shell

Deep Learning Framework Rust

Rust Developer & Cloud Architect

PrefSPEC Runtime Phase

Integración con Kubernetes



Arquitectura inicial