REPUBLIQUE TUNISIENNE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Carthage

Institut National des Sciences Appliquées et de Technologie

End Of Year Project

Subject:

AI-Enhanced Kubernetes Security & Anomaly Detection

Prepared By:

Nour Elhouda Belhadj Fradj

Ghofran Aloui

Nada Jarboui

Supervised By:

Mr Noureddine Hamdi, INSAT

Examined By:

Mr. Abderrazek Jemai

4th Year Computer Networks and Telecommunications

(RT4)

2024-2025

Abstract

This report presents a project aimed at enhancing the security of Kubernetes clusters through an innovative AI-based anomaly detection approach.

Due to the complexity and dynamic nature of cloud-native environments, traditional monitoring approaches, which rely on static rules, struggle to identify evolving threats such as network intrusions or resource abuse.

Our project implements a Kubernetes cluster integrated with a robust monitoring stack (Prometheus) to collect and centralize system and application metrics. Using machine learning techniques, we train a model capable of detecting abnormal behaviors in real-time, based on simulated scenarios (normal behaviors and attacks).

The results highlight the effectiveness of AI in overcoming the limitations of existing solutions, offering proactive and adaptive detection. This work provides perspectives for improving the resilience and security of Kubernetes infrastructures. .

Keywords: Kubernetes, anomaly detection, artificial intelligence, machine learning, Prometheus, cloud-native security, system metrics, monitoring, Random Forest

Acknowledgments

We express our deep gratitude to all those who contributed to the realization of this project.

Our thanks go first and foremost to our supervisor, **Mr. Noureddine Hamdi**, for his valuable advice and constant support throughout this study.

We also thank our university for providing the necessary resources to carry out this work.

Finally, we extend our appreciation to the jury for their thorough evaluation and constructive feedback, which enriched this project.

Contents

List of Tables

List of Figures

General Introduction

Meeting the growing demands for scalability, resilience, and portability in cloud-native architectures, **Kubernetes** has become one of the most widely used container orchestrators in production environments for deploying distributed applications. Its popularity stems from its ability to automate the deployment, scaling, and management of containerized applications. Today, Kubernetes is at the heart of digital transformation, supporting both startups and critical infrastructures.

However, this increased complexity also introduces new security challenges. The dynamic and distributed nature of Kubernetes clusters makes detecting abnormal behaviors difficult, potentially exposing systems to attacks such as privilege escalations, network intrusions, or resource abuse. According to a 2024 Red Hat study, 67% [4] of companies using Kubernetes reported at least one security breach related to misconfigurations or inadequate anomaly detection, highlighting the urgent need to strengthen security in these environments.

In a Kubernetes cluster, attacks or abnormal behaviors may go unnoticed if they are not associated with precise detection rules. However, traditional approaches [5], [6], [5], based on static rules, quickly become ineffective against evolving and complex threats.

In this context, the main objective of our project is to establish a Kubernetes environment capable of collecting, centralizing, and structuring metrics representative of cluster activity, with the aim of enabling future anomaly detection through artificial intelligence techniques.

This project thus seeks to bridge the gap between current monitoring capabilities and the security needs of Kubernetes environments by proposing a proactive AI-based approach to anticipate threats before they cause harm.

This report is structured around four chapters: the first chapter provides a review of the state of the art on Kubernetes, monitoring, and the role of AI in anomaly detection; Chapter 2 describes the system architecture; Chapter 3 details data collection via *Prometheus* and scenario simulation; Chapter 4 addresses the preprocessing and training of the AI model; finally, a conclusion highlights perspectives for improvement.