

Experimental Digital Twin Framework for Cybersecurity Risk Analysis

Nathanaël STEMME¹, Manuel MUNIER¹, and Ali LARBI²

¹ LIUPPA, Université de Pau et des Pays de l'Adour, E2S UPPA, Mont-de-Marsan, France

² ETIS, CY Cergy Paris Université, Cergy, France

Abstract. Digital Twins (DTs) are increasingly adopted across domains such as smart cities, Industry 4.0, connected agriculture, and education, where they enable real-time monitoring and decision-making. However, securing end-to-end DT architectures (panning IoT data acquisition, data governance, and AI-driven analytics) remains a significant challenge. In particular, the lack of experimental and reproducible environments hinders systematic cybersecurity evaluation and research.

This paper proposes a baseline experimental digital twin environment dedicated to cybersecurity analysis, with a focus on machine learning-based anomaly detection. We design and implement a minimal yet realistic DT pipeline that ingests sensor data, enforces data governance constraints, and integrates lightweight AI components for monitoring and threat detection. Representative cyber threats are simulated to expose security issues that are specific to DT architectures.

The main contribution of this work lies in providing a reproducible, pedagogical experimental setup that serves as a foundation for further research. The proposed baseline enables readers to understand core DT cybersecurity challenges, replicate the experiments, and extend the environment toward sector-specific digital twins and more advanced machine learning-based security mechanisms.

Keywords: Digital twin · cybersecurity · risk management · anomaly detection.

1 Introduction

Digital twins (DTs) are moving rapidly from proofs of concept to mission-critical deployments. DTs make monitoring, predictive analytics and control of a system possible by joining all real-world data in one place. This capability is transforming domains as varied as urban mobility, industrial automation and connected agriculture. Yet the strengths that make DTs attractive also allow for threats to appear, whether on networks, data pipelines, information security, and AI. This article places cybersecurity as an important design concern for DTs and proposes practical, testable defenses.

DTs are getting increasingly popular, as seen with the number of papers written on the subject accelerating [5]. Their ability to turn gathered data into