UNIVERSITÀ DEGLI STUDI DI MILANO
DIPARTIMENTO DI INFORMATICA

Towards Secure and Interoperable Digital Twins for Healthcare Systems

Chiara Braghin, Stelvio Cimato, Andrea Marchesini,
Fabio Palazzesi, Simone Pesci, Elvinia Riccobene

Università degli studi di Milano

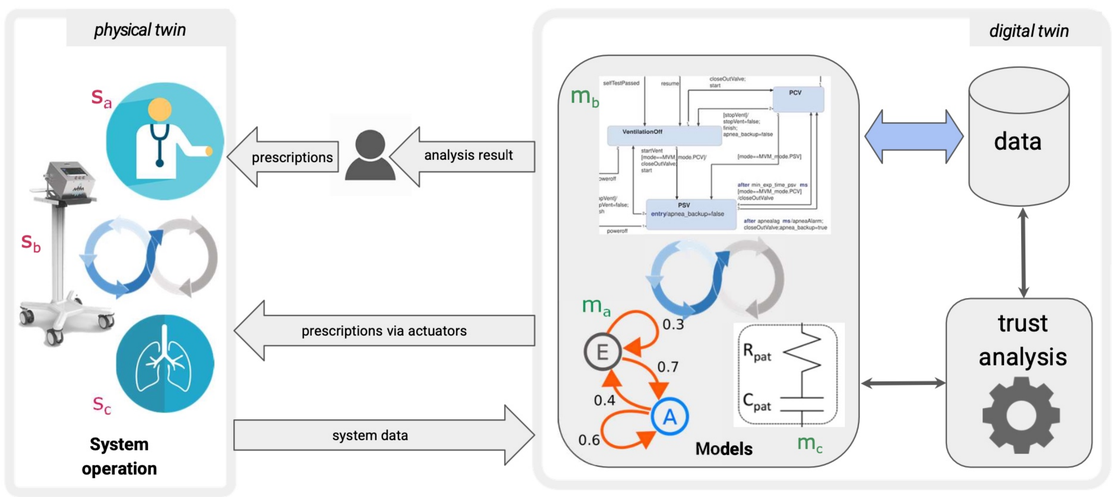
Abstract

Digital Twins are emerging as a key solution in Healthcare 4.0, offering real-time monitoring, decision-making, and risk assessment. Despite their potential, implementing Digital Twins in healthcare presents significant challenges. The required infrastructure is complex, highly distributed, and shared, making healthcare data a prime target for malicious attacks. Therefore, the multi-tenant big data pipeline must implement robust access control mechanisms to protect sensitive data while ensuring a secure and trustworthy environment that facilitates data sharing for enhanced diagnostic and predictive capabilities. Moreover, standardizing data formats is essential to ensure infrastructure reusability and interoperability, extending its utility across various healthcare applications.

SAFEST PRIN Project

SAFEST (*Trust assurance of Digital Twins for medical cyber-physical systems*) aims to develop robust, trustworthy methodologies that enable secure, adaptive digital twin frameworks for critical healthcare systems. It relies on the integrated use of *formal methods*, *runtime monitoring*, and *data-driven adaptation*.

Ensuring *secure data governance* is crucial for the integrated and safe use of heterogenous healthcare data



Reference scenario: Digital Twin of a lung mechanical ventilator

UNIMI Scope in the Project

Our work focuses on three key aspects of the *digital twin pipeline*:

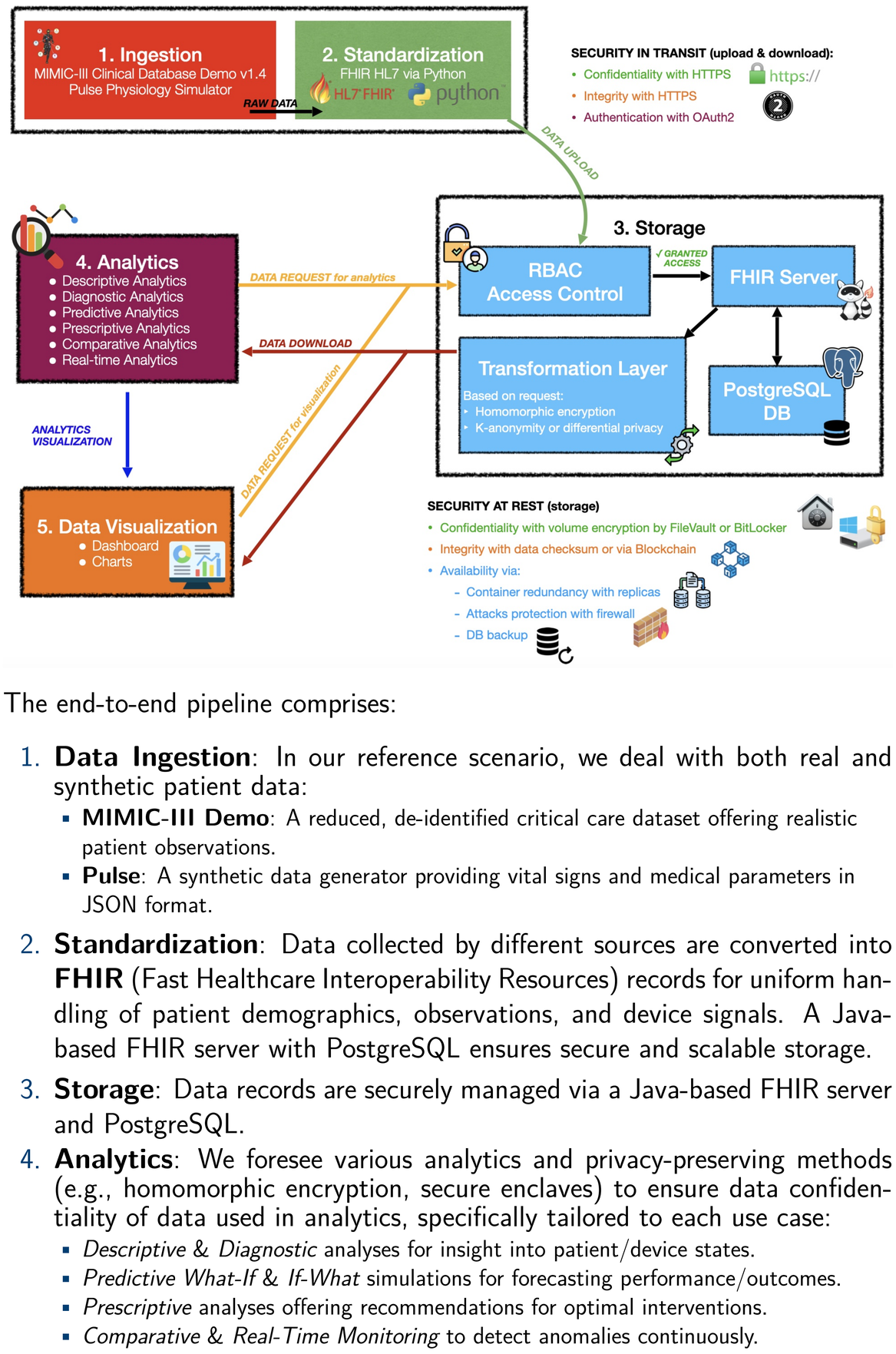
Data: Securely ingest and standardize heterogeneous healthcare data (from sensors and clinical workflows) into FHIR-compliant records.

Trust Analysis: Continuously validate and calibrate the digital twin against the physical twin by assessing data integrity and model accuracy.

System Data: Manage and secure the complete data flow from ingestion and storage to real-time analytics ensuring reliable decision-making.

Securing the Data Pipeline

Sensitive data must be protected at every stage of its life cycle.



The end-to-end pipeline comprises:

1. **Data Ingestion**: In our reference scenario, we deal with both real and synthetic patient data:
   - **MIMIC-III Demo**: A reduced, de-identified critical care dataset offering realistic patient observations.
   - **Pulse**: A synthetic data generator providing vital signs and medical parameters in JSON format.
2. **Standardization**: Data collected by different sources are converted into **FHIR** (Fast Healthcare Interoperability Resources) records for uniform handling of patient demographics, observations, and device signals. A Java-based FHIR server with PostgreSQL ensures secure and scalable storage.
3. **Storage**: Data records are securely managed via a Java-based FHIR server and PostgreSQL.
4. **Analytics**: We foresee various analytics and privacy-preserving methods (e.g., homomorphic encryption, secure enclaves) to ensure data confidentiality of data used in analytics, specifically tailored to each use case:
   - *Descriptive* & *Diagnostic* analyses for insight into patient/device states.
   - *Predictive What-If* & *If-What* simulations for forecasting performance/outcomes.
   - *Prescriptive* analyses offering recommendations for optimal interventions.
   - *Comparative* & *Real-Time Monitoring* to detect anomalies continuously.
5. **Data Visualization**: We envision various types of visualizations tailored to different user categories.

Security Considerations

Our approach safeguards healthcare data by ensuring confidentiality, integrity, availability, anonymity, and authentication:

- **Encryption at Rest & In Transit:** AES-256 (via PostgreSQL pgcrypto) and TLS/SSL (HTTPS) secure data in transit and at rest.
- **Access Control & Auditing:** RBAC for granular permissions, OAuth2 for authentication, with detailed audit trails.
- **Blockchain & Integrity:** Tamper-evident logging via blockchain and SHA-3 hashing for data integrity.
- **Redundancy & Privacy:** Kubernetes cluster redundancy, firewall protection against DDoS, and privacy measures such as k-anonymity and differential privacy.

References

- Bersani M. M., Braghin C., Gargantini A., Mirandola R., Riccobene E., & Scandurra P. (2022). *Engineering of Trust Analysis-Driven Digital Twins for a Medical Device.* In *European Conference on Software Architecture*. Springer
- De Benedictis A., Mazzocca N., Somma A., & Strigaro C. (2023). *Digital Twins in Healthcare - An Architectural Proposal and Its Application in a Social Distancing Case Study.* IEEE Journal of Biomedical and Health Informatics
- Alazab, M., et al. (2023). *Digital Twins for Healthcare 4.0 - Recent Advances, Architecture, and Open Challenges*. IEEE Consumer Electronics Magazine
- Björnsson B., et al. (2020). *Digital Twins to Personalize Medicine*. Genome Medicine, Springer Nature
- Jørgensen C., Shukla A. & Katt B. (2024). *Digital Twins in Healthcare: Security, Privacy, Trust and Safety Challenges*. In ESORICS 2023 International Workshops, Springer
- Gonsard A., Genet M. & Drummond D. (2024). *Digital twins for chronic lung diseases*. European Respiratory Review, PubMed Central

simone.pesci@unimi.it elvinia.riccobene@unimi.it

Digital Twins Workshop 2025, Padova, 19 - 20 February 2025