DT4CHIPS-Secure: Digital Twin Framework for Chip Manufacturing Processes Security

Yu-Zheng Lin† , Sicong Shao‡ , Md Habibor Rahman∗ , Mohammed Shafae∗ , and Pratik Satam∗
†Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ 85721 USA
∗Department of Systems and Industrial Engineering, University of Arizona, Tucson, AZ 85721 USA
‡School of Electrical Engineering and Computer Science, University of North Dakota, Grand Forks, ND 58202 USA
Email: { ∗yuzhenglin, †habiborrahman, † shafae1, †pratiksatam}@arizona.edu; ‡ sicong.shao@und.edu

THE UNIVERSITY OF ARIZONA

FUSENANO 2024

Abstract and Introduction

- The semiconductor manufacturing process, with its interconnected devices, poses information security risks alongside increased production efficiency.
- DT4CHIPS-Secure utilizes Digital Twin to model physical characteristics, effectively managing and deploying digital twin models. Anomaly detection safeguards devices against security threats, improving semiconductor yield.
- The framework's associated reports optimize device behavior, further enhancing semiconductor yield.

Main Features

- This framework uses the MLOps concept to build Digital-Twin with cloud computing for continuous integration (CI), continuous delivery (CD), and continuous training (CT).
- In the signal reconstruction stage, aimed at detecting anomalies in power consumption signals for various attack scenarios, this study utilizes a 1D CNN-based autoencoder to create a DT model based on normal consumption signal.
- In the anomaly detection stage, this work highlights using dynamic (instead of static) thresholds to improve attack detection performance compared to the DT predictions.

DT4CHIPS-Secure Framework

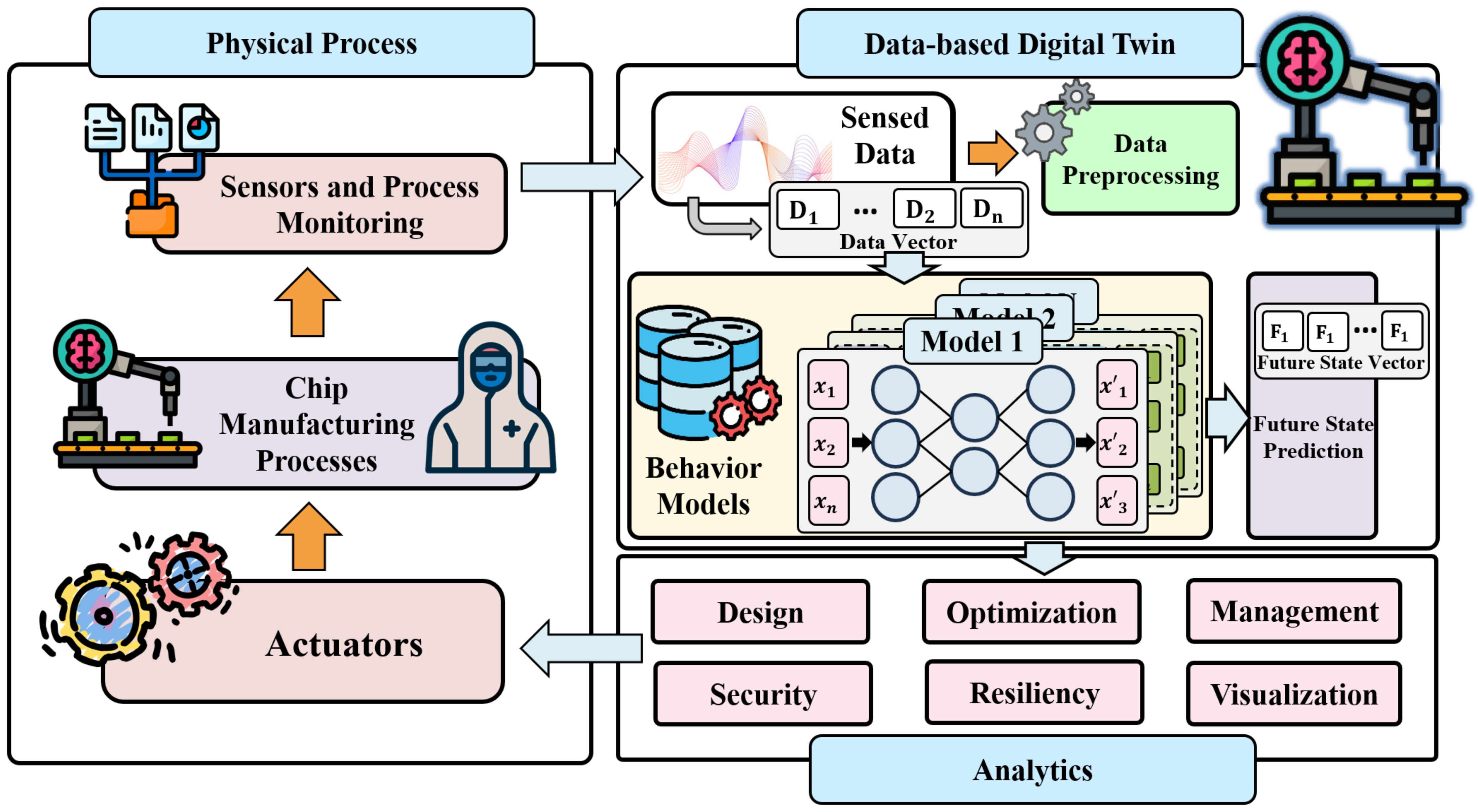


Fig1. Digital Twin Framework for Chip Manufacturing Processes Security (DT4CHIPS-Secure Architecture).

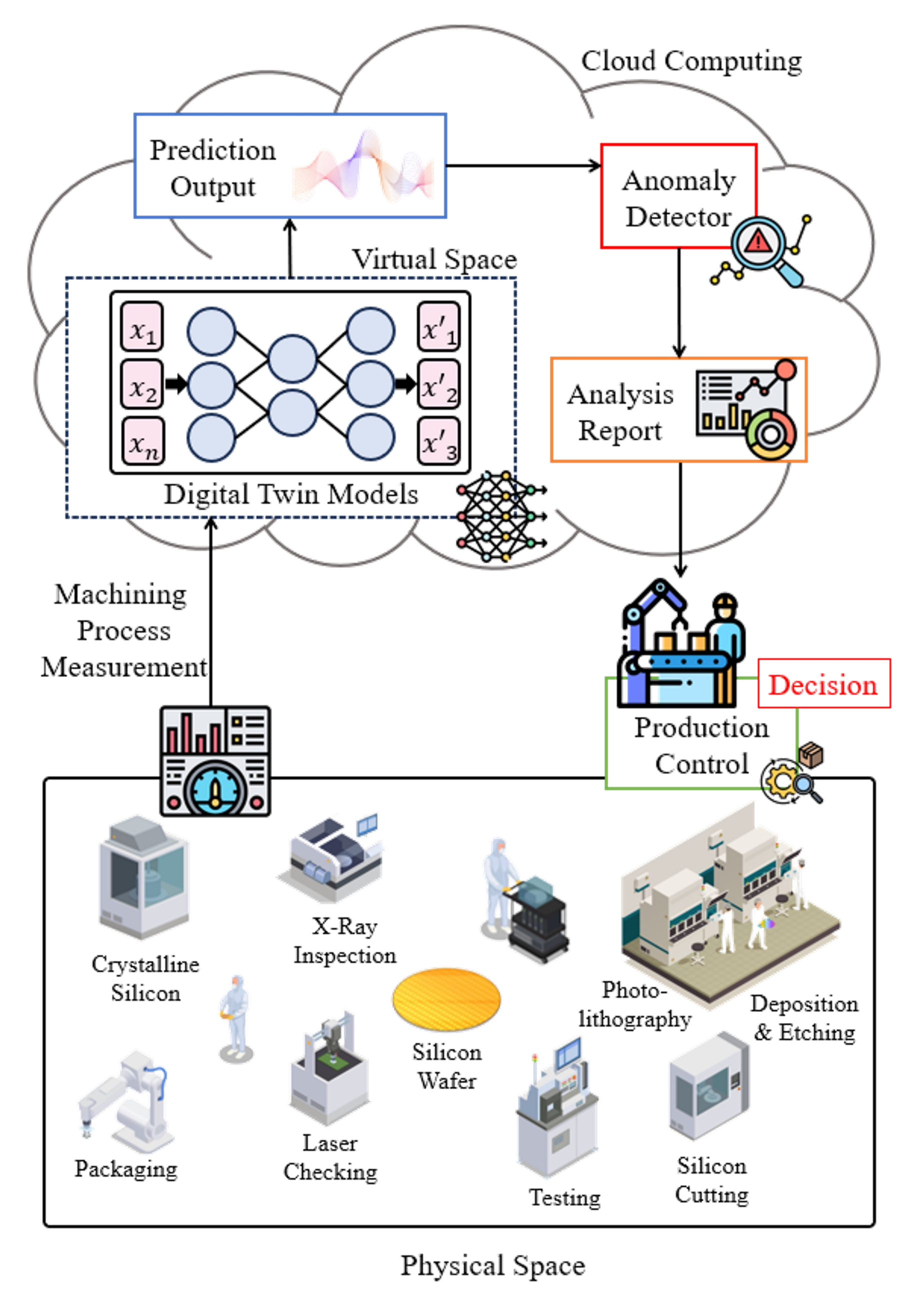


Fig 2. The Architecture of DT4CHIPS-Secure for security service.

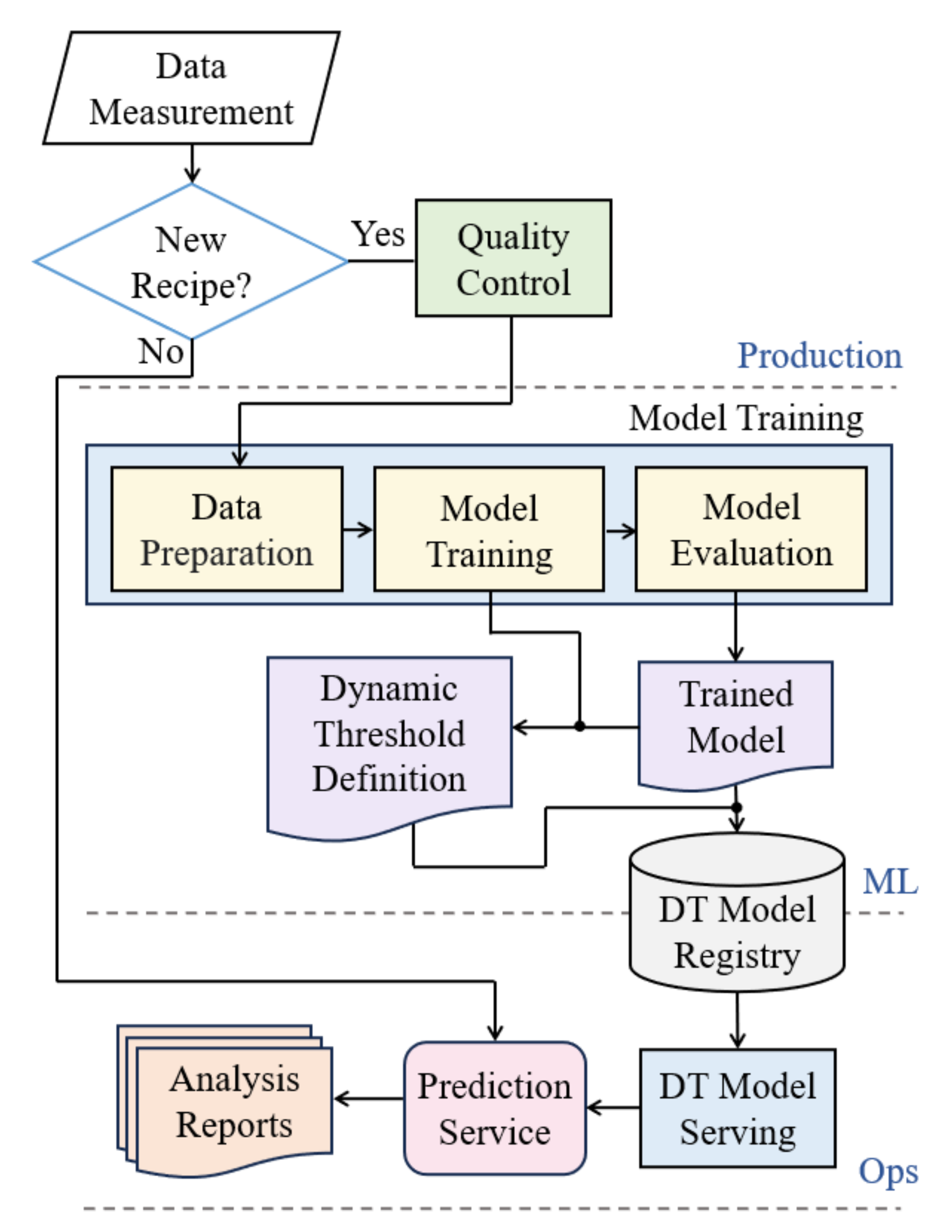


Fig. 3. MLOps Pipeline of DT4I4-Secure.

Original Concept: DT4I4-Security

Scan for DT4I4-Security Paper

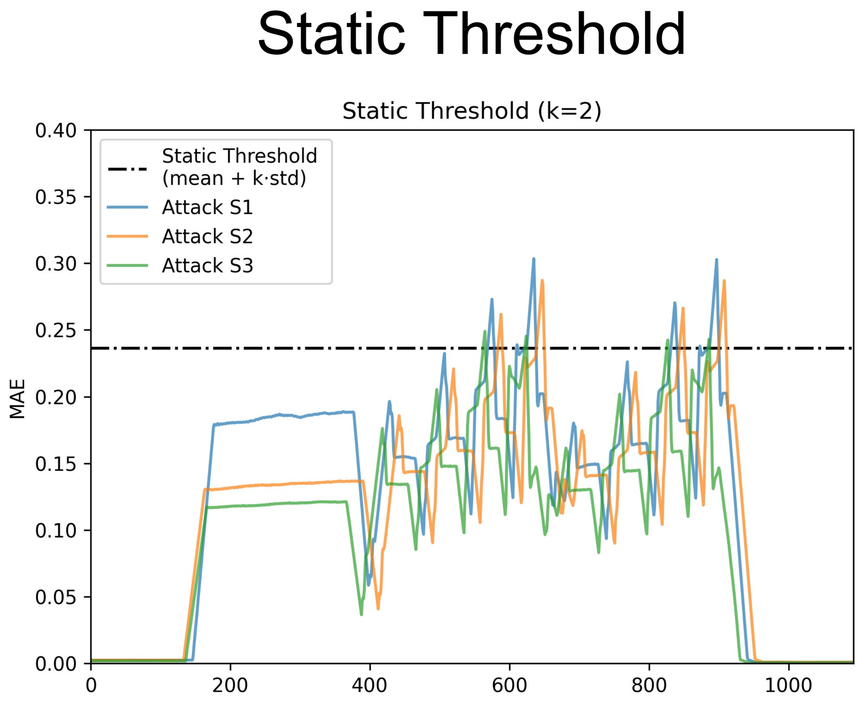
Systems and Security Lab

THE UNIVERSITY OF ARIZONA

UND UNIVERSITY OF NORTH DAKOTA

Proposed Methodology

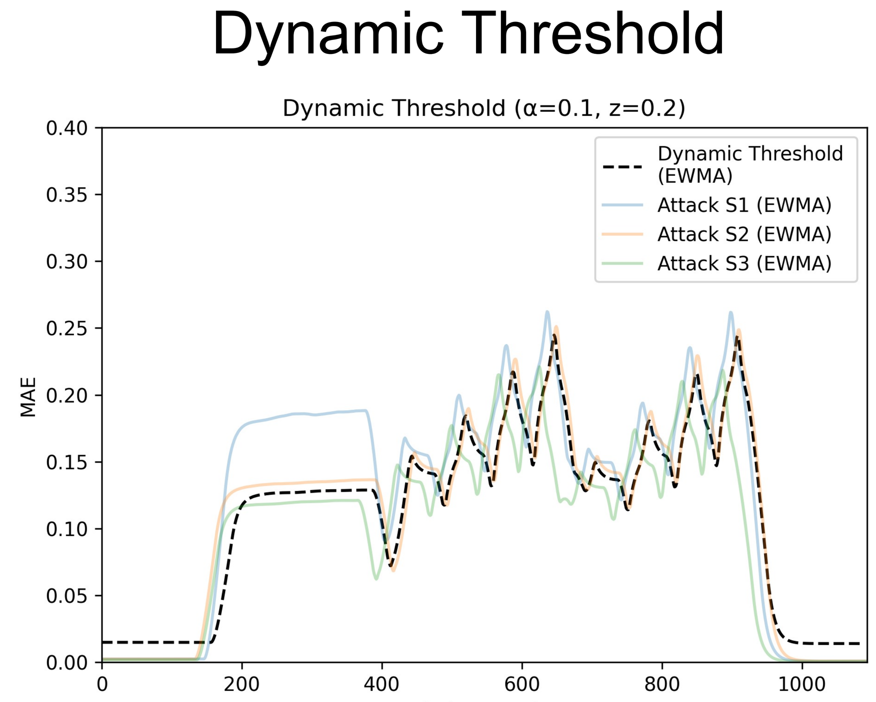
Static Threshold



Input: $\mathbb{T}_{static}$ - static threshold, $\{e^i_{test}\}^n_{i=1}$ - error series of test set, n - number of time steps
Output: θ_i - anomaly status

for i = 1 to n **do**
  if $e^i_{test} > \mathbb{T}_{static}$ **then**
    Set $\theta_i = 1$ // Data is an anomaly.
  else
    Set $\theta_i = 0$ // Data is normal.
  end if
end for
return θ_i

Dynamic Threshold



Input: $\mathbb{T}_{dynamic}$ - dynamic threshold, $\{e^i_{test}\}^n_{i=1}$ - error series of test set, n - number of time steps, α - smoothing constant
Output: θ_i - anomaly status

for i = 1 to n **do**
  Let $e^i_{test\_s} = \alpha \cdot e^i_{test} + (1-\alpha)e^{i-1}_{test\_s}$;
  if $e^i_{test\_s} > T_i$ **then**
    Set $\theta_i = 1$; // Data is an anomaly.
  else
    Set $\theta_i = 0$; // Data is normal.
  end if
end for
return θ_i

Results

Static Threshold

	Attack 1	Attack 2	Attack 3
Accuracy	47.34%	45.78%	87.83%
Precision	86.25%	90.08%	-
Recall	18.81%	17.82%	0%
F1 Score	30.89%	29.75%	-

Dynamic Threshold

	Attack 1	Attack 2	Attack 3
Accuracy	90.56%	88.73%	58.24%
Precision	86.88%	85.21%	14.63%
Recall	100%	99.83%	56.87%
F1 Score	92.98%	91.94%	24.29%

3.45X Improvement