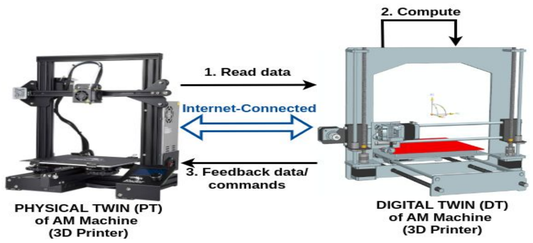
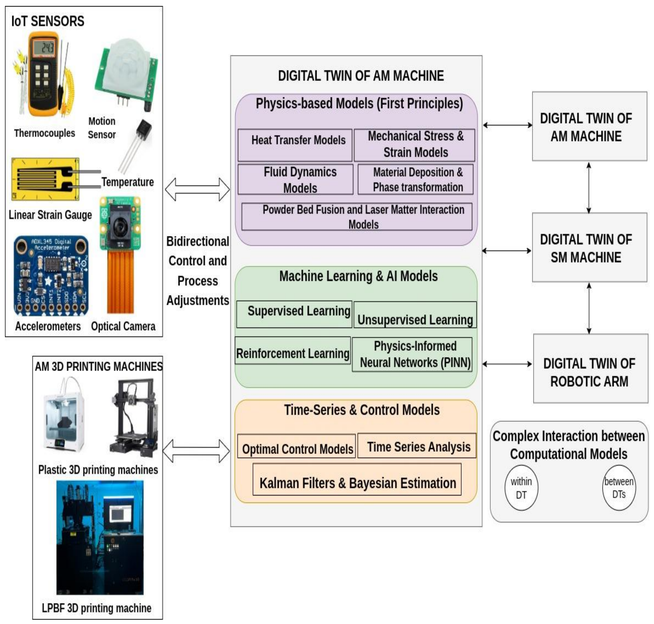
Secure Collaborative Digital Twins of Smart Factories

Anusha Vangala, Jack Wyeth, Prof. Sajal K. Das

U.S. Workshop on Multidisciplinary Digital Twins in the Built Environment

Digital Twin = interacting computational models + Real-time data from physical assets





Networked Digital Twins in AM Factory Security Vulnerabilities

- Device Diversity
- Weak Communication Protocols

Data outflow from machines and sensors and influx into digital twins - vice-versa

Goal: accessibility, integrity, accuracy, trust

Data Sharing
MiTM
Forgery/ spoofing
Injection
DoS
Insider attacks

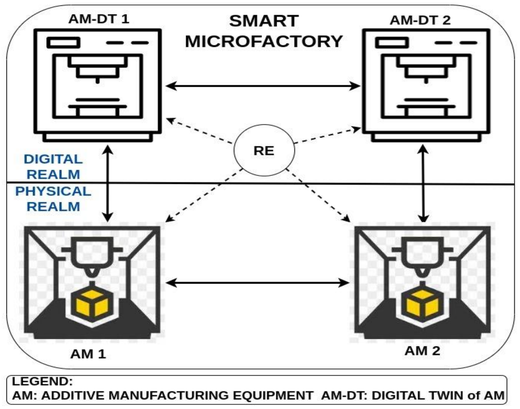
Solution: Authentication Access Control Confidentiality

Research Objectives

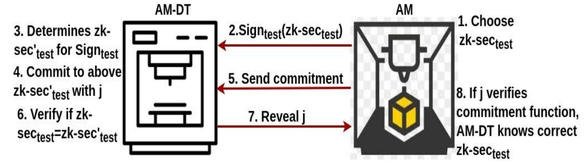
- Authenticated twins
- Secure data sharing

Undeniable Authentication of Digital Twins of Smart Microfactory

- Restrict commands/design specs to synchronized twins
- Accountability for actions undertaken by twins
- Inculpability for actions not undertaken by twins
- Prevent Unsynchronized twins from identifying the twins which exchanged the commands/ design specs



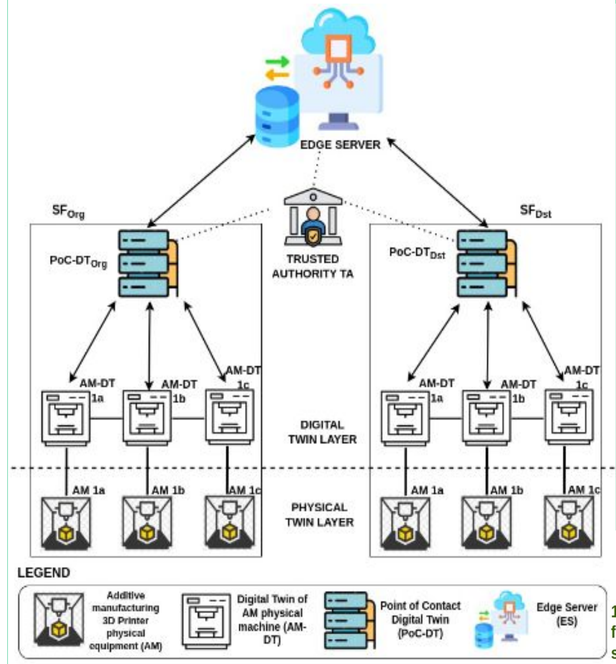
Confirmation Protocol



Disavowal Protocol

Data Relay in Federated Digital Twins of Smart factories

- Fidelity Levels: Network Digital twin, AM Digital twin
- Data relay: AM-DTOrg -> PoC-DT->ES->PoC-DT-> AMDT
- Commands/Design specs hidden from PoC-DTs and ES



Elliptic Curve based Proxy Re-encryption scheme

Originator PoC-DT: **PRESIF Protocol**

embeds file content into elliptic curve point M and computes its hash h=H(M)

Chooses random secret r

Computes ciphertext as $C_{Org} = (C_T, C_M, h_M)$

Where $C_T = r \cdot Pk_{Org} \quad C_M = r \cdot P + M.$

Edge Server (proxy):

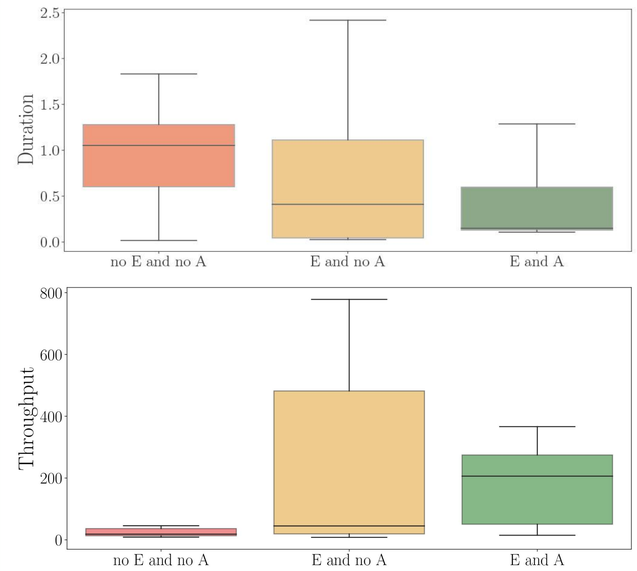
Re-encrypts: $C_{Proxy} = (C'_T, C_M, h_M)$

Where $C'_T = C_T \cdot rk_{Org \to Dst} \quad rk_{Org \to Dst} = sk^{-1}_{Org} \cdot sk_{Dst}$

Destination PoC-DT:

Decrypts $M^{Dst} = C_M - sk^{-1}_{Dst} \cdot C'_T$ Checks $h_M \stackrel{?}{=} H(M^{Dst})?$

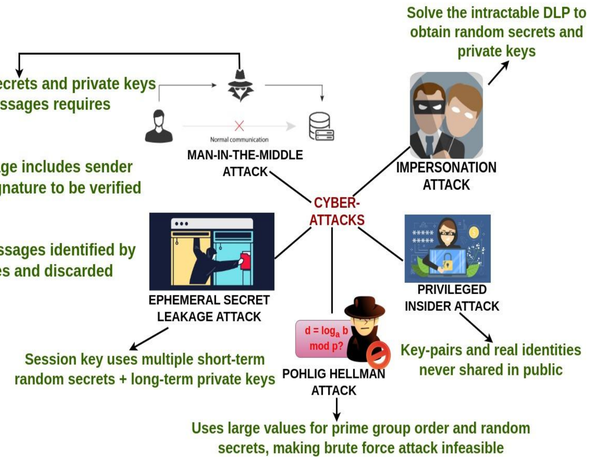
RESULTS



No significant delay introduced

$$Prob_{Forge} = \frac{2*q_s}{p-1} + \frac{2*q_d}{k+1}.$$

High unforgeability for large p, k



MISSOURI S&T