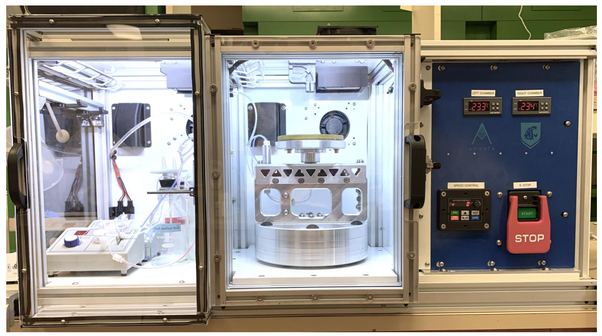
A Model System for Study of Cyberattacks on Biomanufacturing

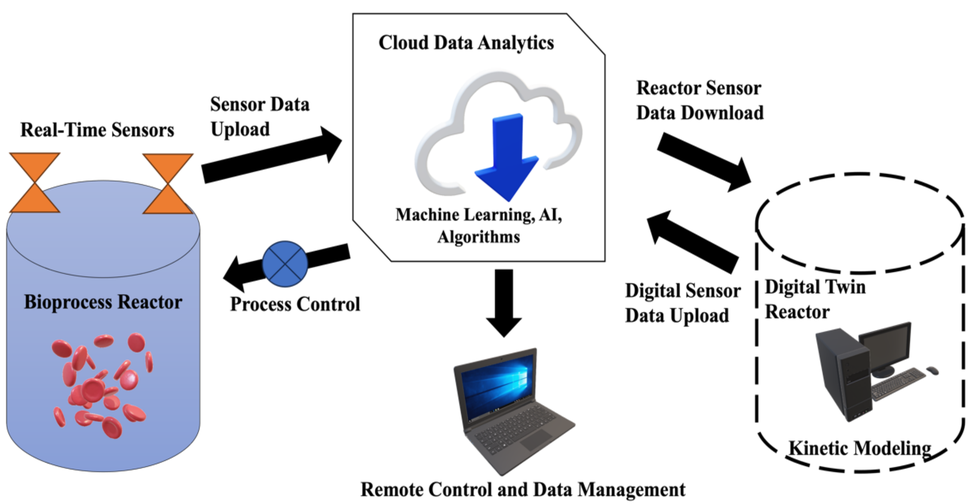
Cayden Calo, Bryan Frederickson, Brenden Fraser-Hevlin, Alec Schuler, Arda Gozen, Bernard Van Wie, Cameron Botelho, Justin Van Der Sluys

BACKGROUND

- Healthcare cyberattacks make up 25% of all hacks, and each one costs avg. $5 million (Nature, 2022)
- Modern manufacturing processes utilize IoT, ML, and digital twins to optimize production and minimize downtime
- Internet-enabled bioreactors are susceptible to attacks that disrupt the biomanufacturing process, can steal trade secrets and developmental data, or reveal protected patient information



IoT-enabled bioreactor for CAR T-Cell expansion

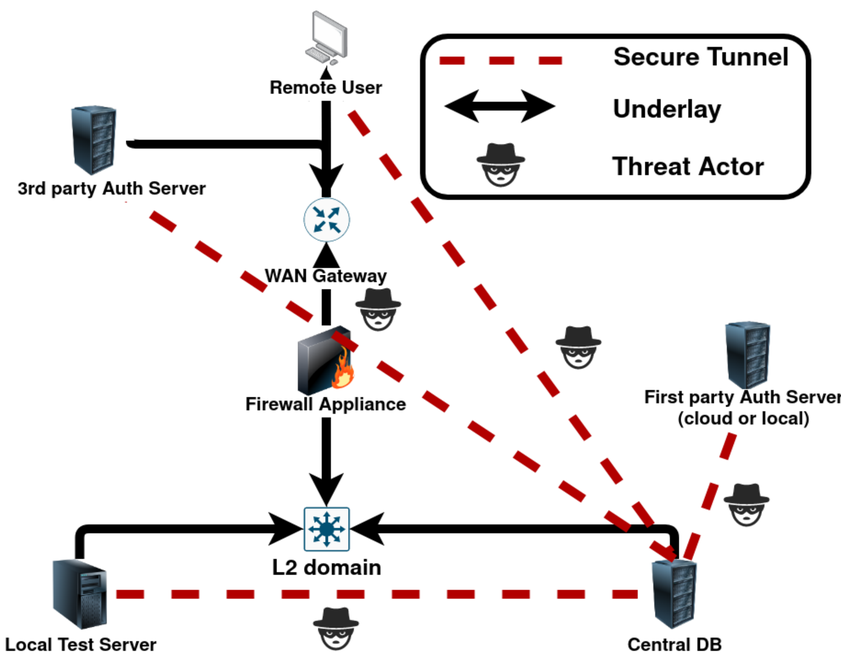


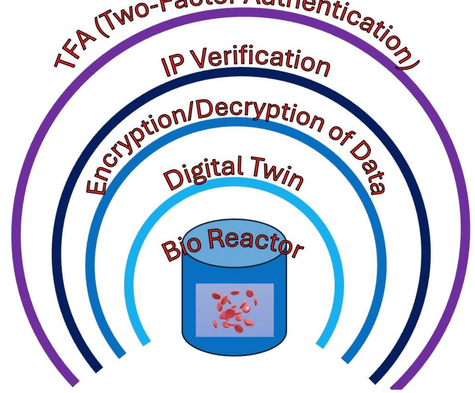
METHODS

- Bioreactor produces two signals as a function of cell quantity: glucose and oxygen concentration
- Simulated physical reactor (SPR) produces sensor signals with emulated noise in MATLAB Simulink
- Digital twin reactor (DTR) processes reactor data to determine process control decisions and detect faults
- Signals sent via MQTT protocol between SPR and DTR
- Performed vulnerability assessment on digital twin reactor system to help understand adversary incentives and methods
- Created a model for a production overlay network using zero-trust principles

RESULTS

- Designed cybersecure information flow system to transmit MQTT signals
- Developed Python script using 'qrcode' and 'pyotp' libraries for 2FA using Google Authenticator
- Ip verification Python script using SHA2 encryption of crucial information files
- Log data from experiments into a secure central server
- Simulated the effects of sensor and actuator faults and attacks within SPR
- Developed process control-side fault and cyberattack detection methods within DTR (Fraser-Hevlin et al.)
- Gained insight into this SCADA system's vulnerabilities, attacks, and consequences of attacks





FUTURE WORK

- Replace simulated physical reactor with actual bioreactor
- Implement ML to better detect both faults and cybersecurity threats
- Make hub and spoke VPN VLAN system

ACKNOWLEGEMENTS & FUNDING

- The authors are grateful for funding from The Griffiss Institute under contract no. SAA 10012021MM0336, a VICEROY Project entitled Northwest Virtual Institute for Cybersecurity Education & Research (CySER)
- We would like to acknowledge funding and support from NSF Grant #1645249, the WSU Voiland College Shop, and the following organizations.

REFERENCES

Fraser-Hevlin, Brenden; Schuler, Alec W.; Gozen, B. Arda; and Van Wie, Bernard J. (2024) "Using Digital Twins to Protect Biomanufacturing from Cyberattacks," *Military Cyber Affairs*: Vol. 7 : Iss. 1 , Article 7.
Available at: https://digitalcommons.usf.edu/mca/vol7/iss1/7