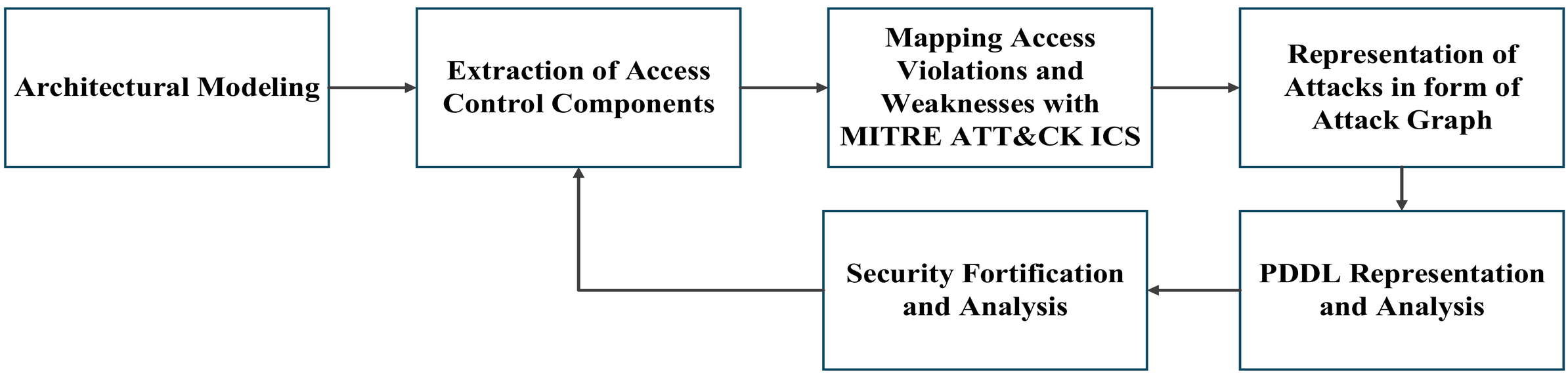
AI Based Dynamic Threat Modeling for Assessing Access Control Posture in Cyber Physical Systems

Indrakshi Ray, Shwetha Gowdanakatte
Colorado State University, Fort Collins

Problem Statement

- Access control is a primary OT attack surface
- 88% of breaches are caused due to access control errors [1]
- Lateral movement after initial access [2]
- Classic ICS landmark attacks (Triton, Industroyer) leveraged legitimate access path [3]
- CPS systems induce cross- zone authorization risk
- Authorization attack paths are largely unmodeled
- Existing threat models overlook policy- induced lateral movement
- Static threat models lack adaptation to dynamic security posture

Proposed Methodology



Novel Contribution

- Authorization as a first-class attack surface
- Architecture modeling for structured information extraction
- Transformation of architecture modeling into AI-interpretable planning artifacts
- Bridging MITRE ATT&CK ICS with automated reasoning
- Enabling AI planners to generate and compare realistic multi-agent attacks
- Data-driven CPS security fortification
- Adaptive threat modeling with continuous planning refinement based on empirical analysis

Acknowledgement

Partially supported by the U.S. ONR under award #N000142612041

[1] R. Sobers "139 Cybersecurity Statistics and Trends" Varonis "139 Cybersecurity Statistics and Trends [updated 2025]" 2025
[2] NCSC "Preventing Lateral Movement" Preventing Lateral Movement | National Cyber Security Centre - NCSC.GOV.UK 2021
[3] CSIS "Significant Cybersecurity Incidents" Significant Cyber Incidents | Strategic Technologies Program | CSIS 2026