

# Privacy Aware Multi-agents for System of Systems

*Nathalia Nascimento, Thao Min Le, and Nil Ergin*

*Presenter: Nil Ergin*

AI4SE & SE4AI Workshop

September 22, 2026



**PennState**

# The Research Problem

## AI-agents in collaborative SoS

- Increased use of AI-agents in SoS operations: supply chain management, insurance contracting, algorithmic trading, smart contracts

## Trade-off

- Organizations need to coordinate decisions while protecting local operational information

## Lack of effective Coordination

- Unintended coordination and planning consequences:
  - Low-capacity utilization, shortage gaming, bull-whip effect

## Problem

Address the collaboration tradeoff between protecting local system interests and maintaining SoS level system operational performance



**PennState**

# Illustrative Scenario: The Supply Chain Planning Problem

## Multi-agent Studies

- Reinforcement learning-based multi-agent model for aerospace manufacturing
- Distributed surrogate model for learning effective policies in supplier networks to maintain model privacy while reducing communication time
- LLM-based agents for sequential supply chain problems with partial observability

Gap

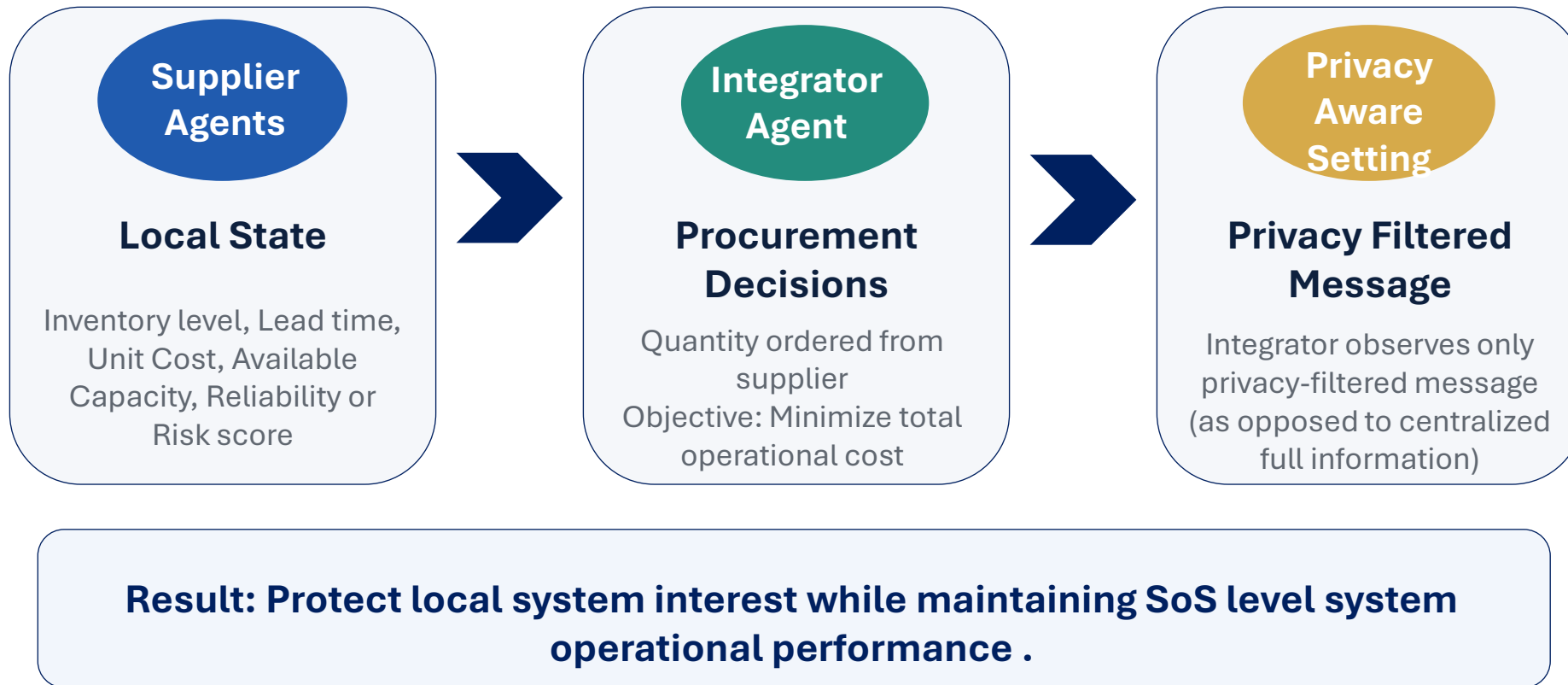
## This Research

- Challenges remain in evaluating how different supplier disclosure policies affect system-level performance and supplier exposure
- Minimize operational cost using only the information allowed by each supplier's privacy policy



**PennState**

# Problem Formulation



# Methodology: Privacy-Aware MAS Architecture



**PennState**

# Experimental Setup

## Data Set

### Inventory Dataset for Complex Supply Chains

- Time-indexed records of
  - Demand
  - Inventory
  - Lead time and
  - Cost variables
- Each warehouse is a supplier-side entity

## Implementation

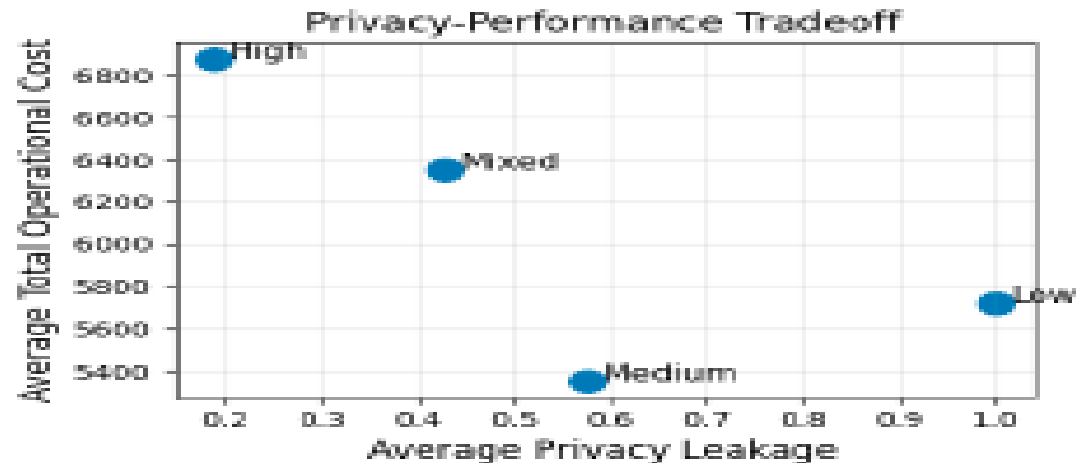
- Each supplier state constructed from available data set
  - Lead time in days, ordering cost
  - Approximate available capacity using current inventory
  - Heuristic risk proxy for supplier risk
- Privacy-policy layer scenarios:
  - Low
  - Medium
  - High
  - Mixed
- System integrator implemented through procurement decision logic and supplier scoring

# Preliminary Results

- Aggregate results for 100 procurement requests per privacy scenario

| Scenario | Leakage | Total Cost | Service | Shortage | Risk Pen. |
|----------|---------|------------|---------|----------|-----------|
| Low      | 1.000   | 5719.81    | 1.000   | 0.00     | 50.40     |
| Medium   | 0.575   | 5350.89    | 0.995   | 10.39    | 51.95     |
| Mixed    | 0.427   | 6355.43    | 1.000   | 0.00     | 50.34     |
| High     | 0.188   | 6879.08    | 1.000   | 0.00     | 49.48     |

- Privacy-performance tradeoff over 100 procurement requests



# Implications for Practice



## Collaborative SoS environments

Concerns for sharing internal data



## Applications

Supply chain management  
Federated Model Development  
System Design  
Distributed Surveillance Analysis



## Tradeoff Evaluation

System level performance and individual system privacy constraints



## Ai-agent Networks

Effectiveness of AI agent networks under a range of privacy scenarios



**PennState**

# Future Work

- Evaluate model on larger datasets
- Examine effects of alternative scoring weights, leakage weights, privacy-policy configurations
- Incorporate learning mechanism for SoS system integrator

# Q&A Thank you.

Nil Ergin: [nhe2@psu.edu](mailto:nhe2@psu.edu)



**PennState**