Tampere University

Risks of Employing AI Agents in Smart Environments

Aygün Varol

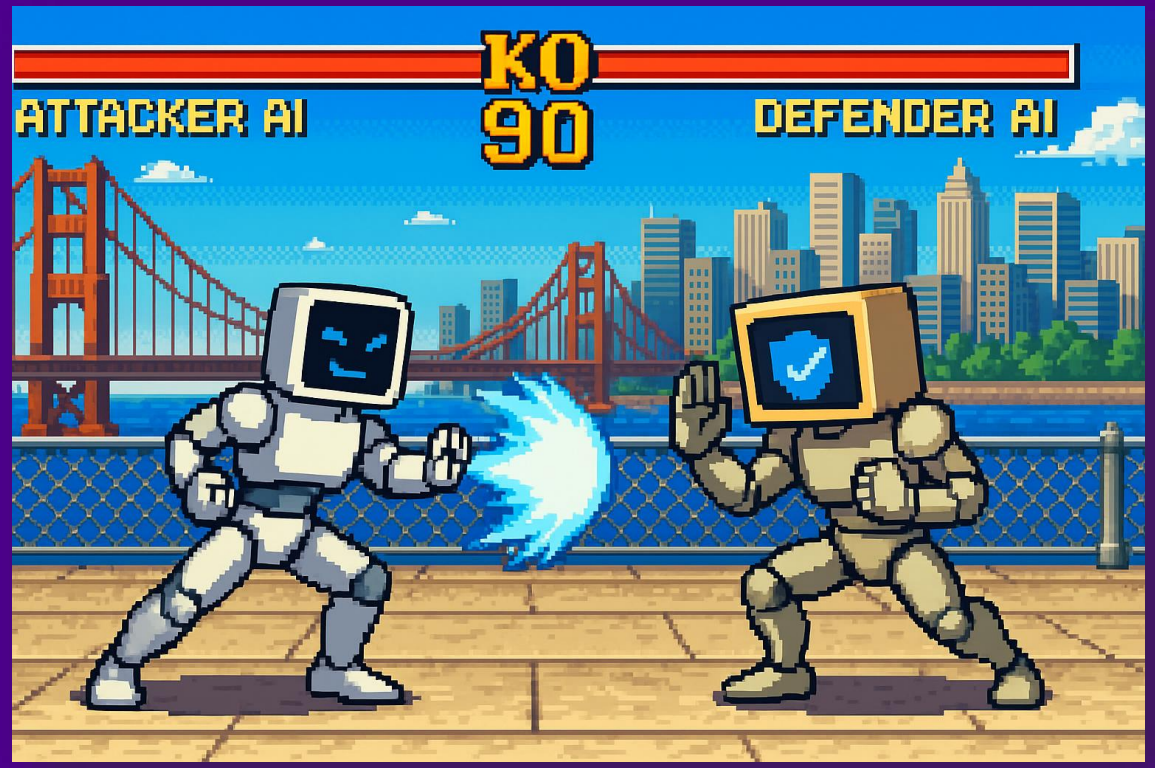
Doctoral Researcher
Augmentative Technology Group

Why This Matters

- AI agents are everywhere in smart environments
- Benefits are huge, so are the risks
- **Goal:** map the top risks and the fixes

Cybersecurity

- Adversarial & data-poisoning attacks
- Model inversion / extraction & backdoors
- DoS can cripple critical infrastructure
- Weak data protection ⇒ breaches & automated attacks



Ethics, Privacy & Human Rights

- Algorithmic bias → unfair outcomes
- Black-box opacity erodes accountability
- Massive personal-data collection
- Surveillance, vulnerable groups

Conclusion

- Risks are interconnected
- Trustworthy AI = lawful, ethical & robust
- Invest now: secure design, control mechanisms

Tampere University

Risks of Employing AI Agents in Smart Environments

Thank you!

Questions?

Aygün Varol
Doctoral Researcher
Faculty of ITC
aygun.varol@tuni.fi