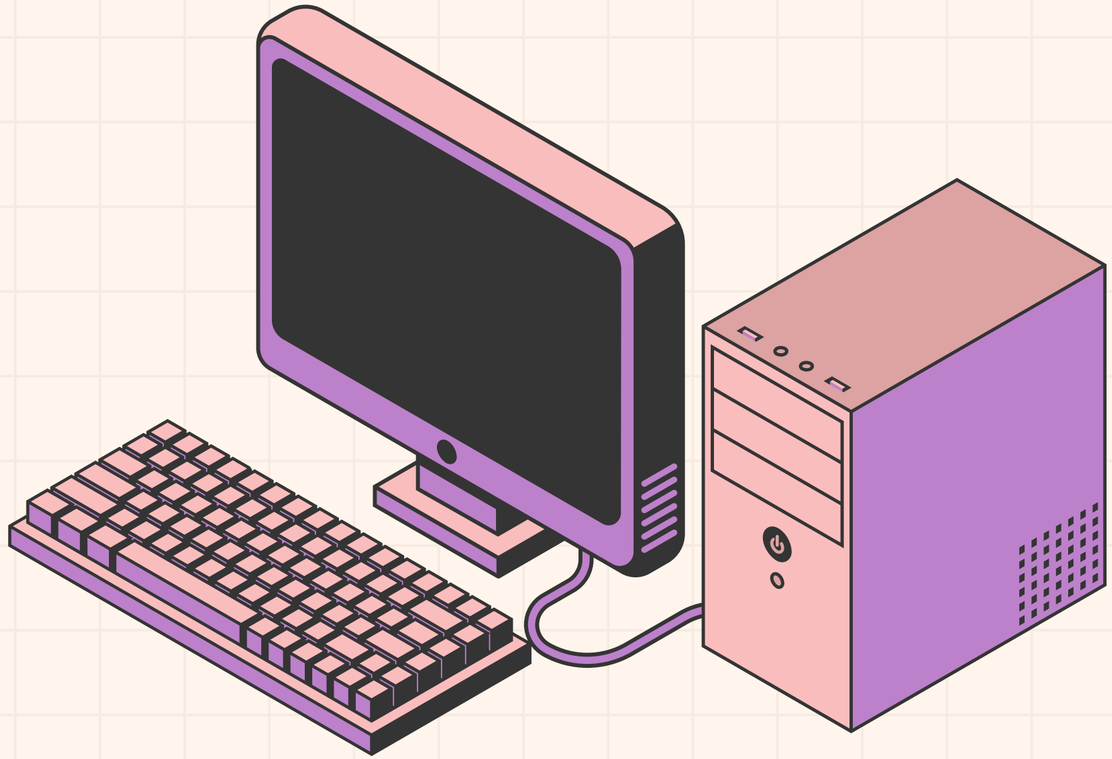
CYBERSECURITY SOCIETY
UNIVERSITY OF GALWAY

CYBER THREAT INTELLIGENCE

@ EDGE COMPUTING

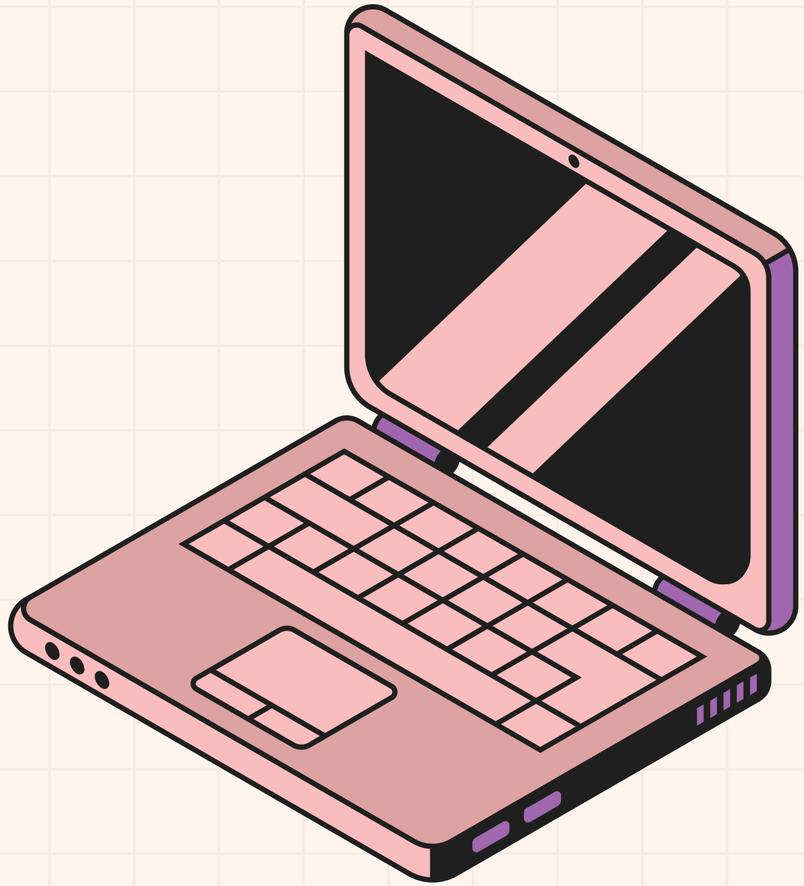


Muhammad Murtuza Hussain
MSc Cybersecurity Risk Management
Auditor of Cybersecurity Society

CYBERSECURITY SOCIETY
UNIVERSITY OF GALWAY

AGENDA

- What is Cyber Threat Intelligence?
- Security Threat Landscape
- Vulnerabilities & Attack Surfaces
- A Mitigation Strategy that involves LLM
- Conclusion

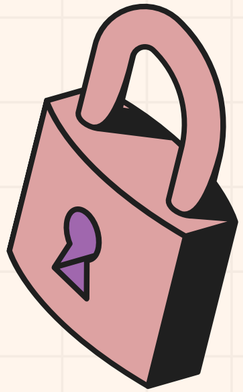


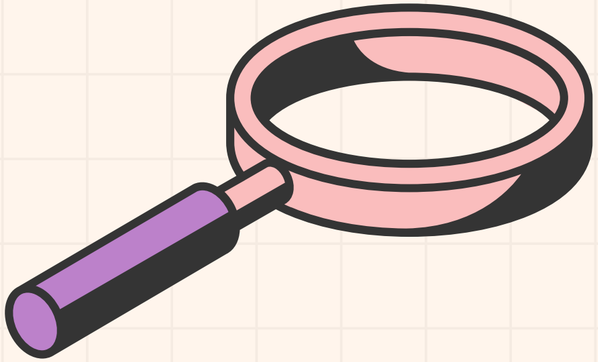
CYBERSECURITY SOCIETY
UNIVERSITY OF GALWAY

WHICH PART OF YOUR CURRENT TECHNOLOGY SETUP DO YOU SUSPECT IS MOST VULNERABLE TO CYBER THREATS TODAY?

CYBERSECURITY SOCIETY
UNIVERSITY OF GALWAY

CTI (CYBER THREAT INTELLIGENCE)





TYPES OF CTI

- Tactical
- Operational
- Strategic

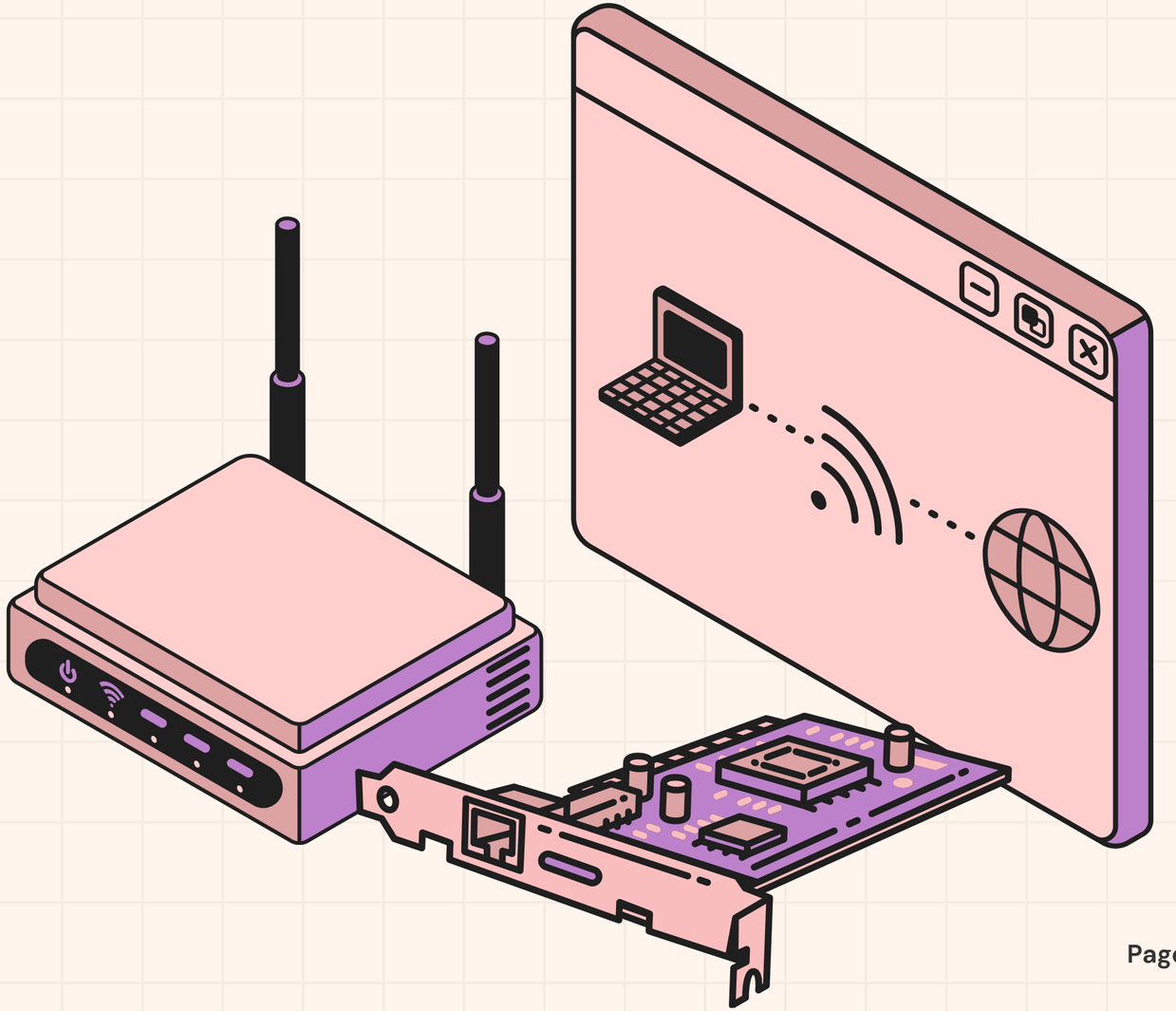
and many more...

KEY BENEFITS

- Real time detection
- Proactive approach (Prevention)
- Risk Mitigation

SECURITY THREAT LANDSCAPE

- **DATA POISONING ATTACKS,**
  MISCLASSIFYING IMAGES OR SENSOR READINGS
- **MODEL POISONING (PARAMETER TAMPERING)**
  DURING MODEL TRAINING/UPDATES
- **EVASION ATTACKS**
- **SIDE-CHANNEL ATTACKS**



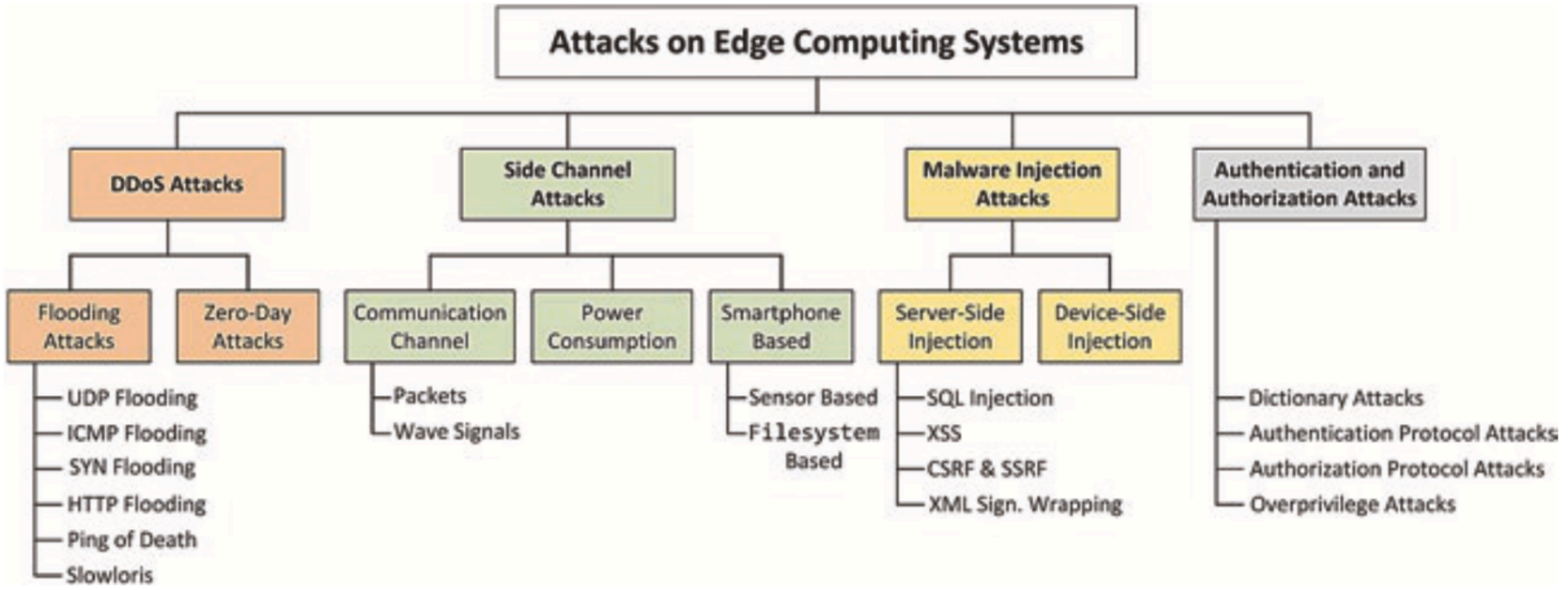
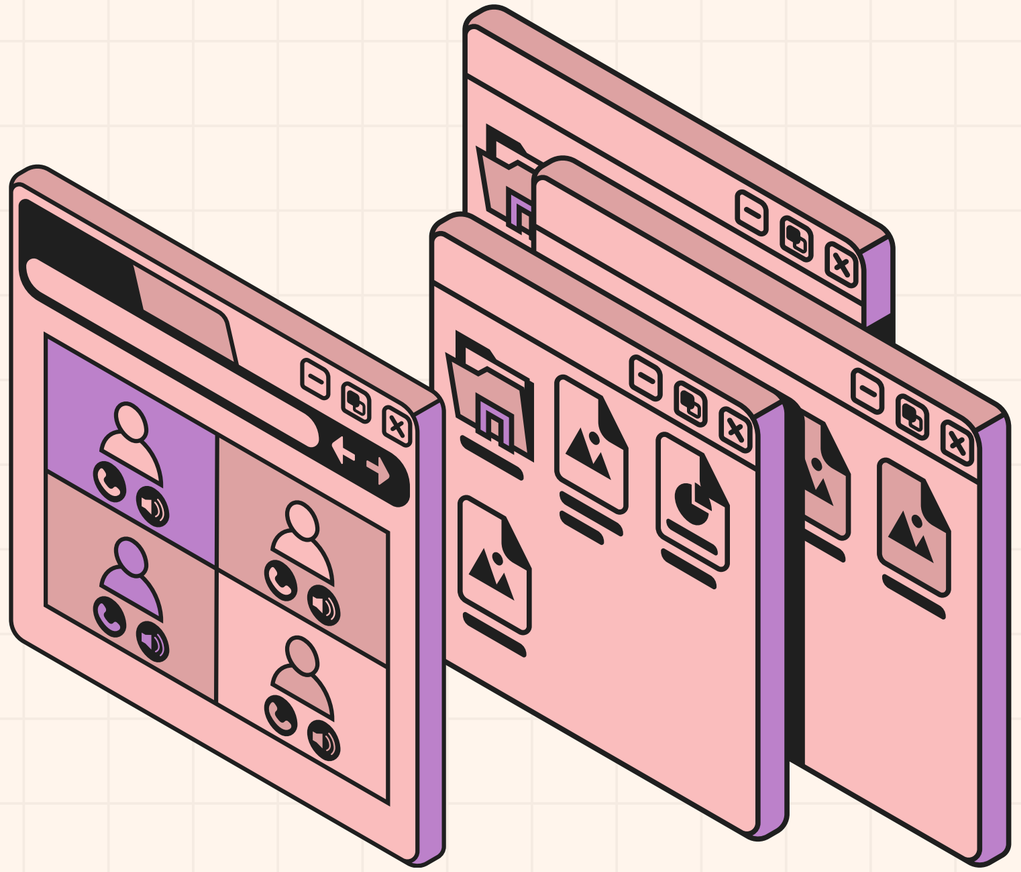


Fig. 6.1 Different types of attacks against edge computing systems (Xiao et al. 2019)

ARCHITECTURE CHALLENGES

& ATTACK SURFACES

- Hardware Heterogenerity
- Network Protocols
- Resource Constraints
- Physical Access



CYBERSECURITY SOCIETY
UNIVERSITY OF GALWAY

DECENTRALIZED THREAT INTELLIGENCE

LIGHTWEIGHT MACHINE LEARNING (ML) MODELS

EDGE SERVER

CENTRAL LARGE LANGUAGE MODEL (LLM) SERVER

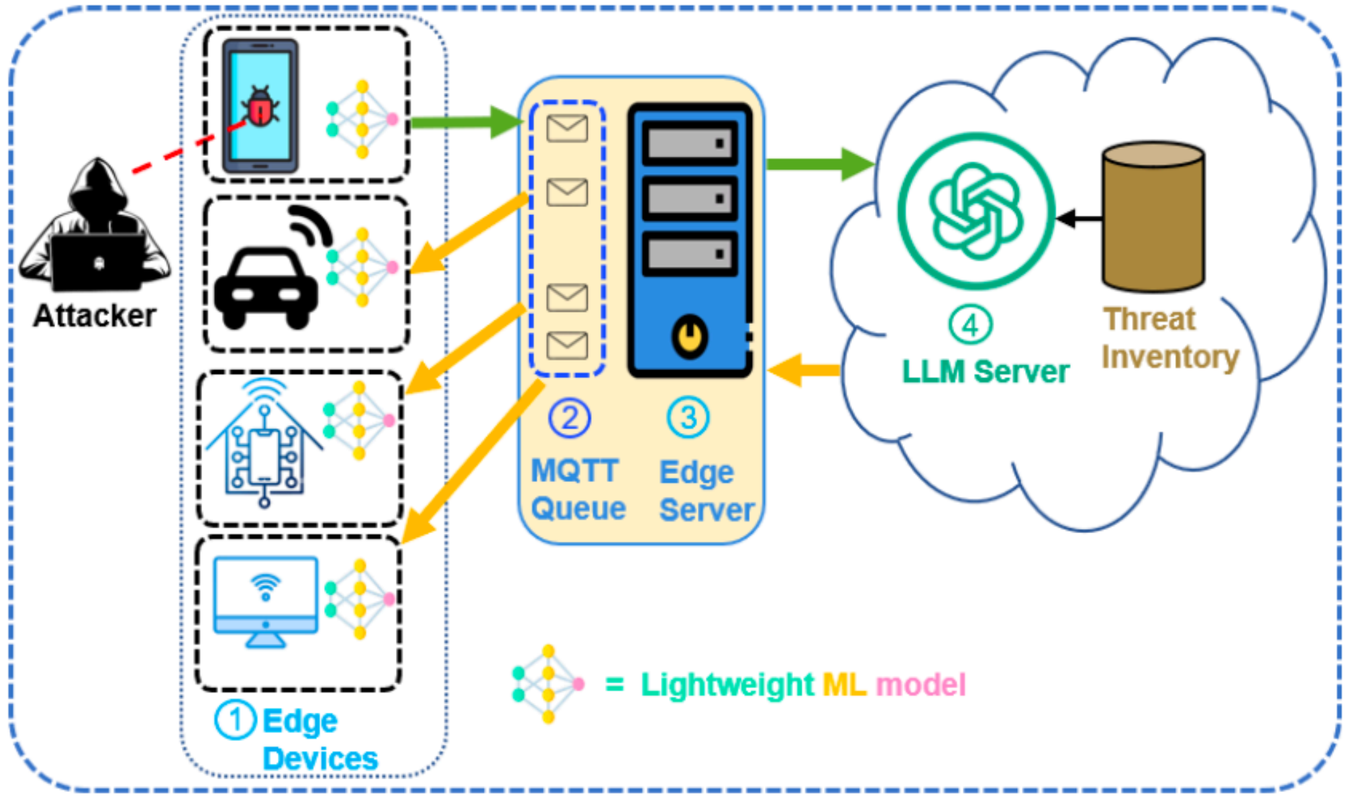
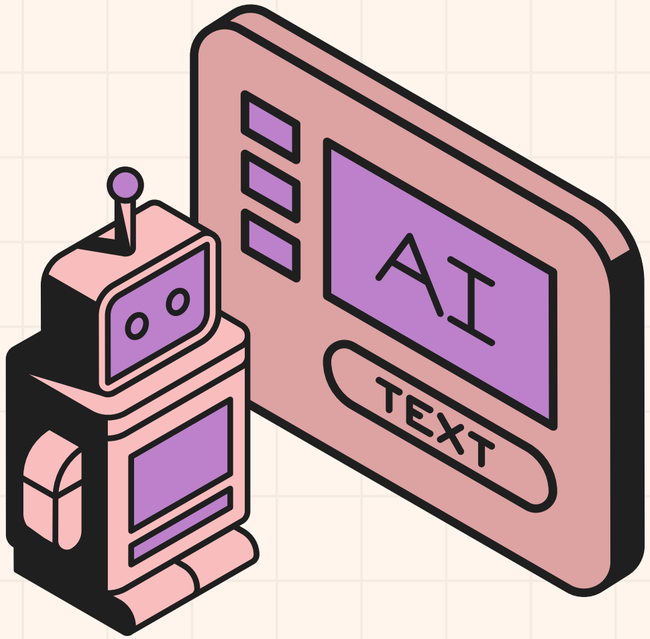


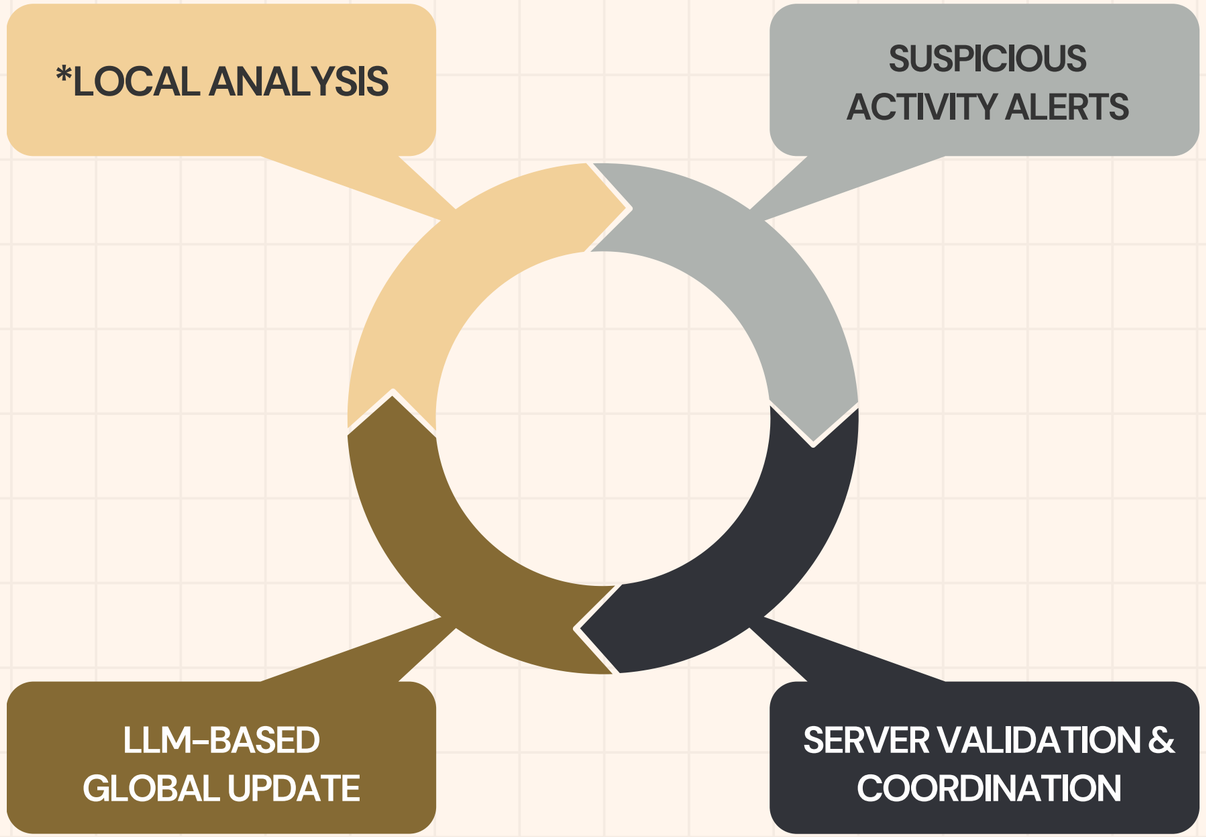
Fig. 1. Configuration of the lightweight ML model at Edge devices with Edge server and Central LLM with trained with a large inventory of threat intelligence

CYBERSECURITY SOCIETY
UNIVERSITY OF GALWAY

METHODOLOGY

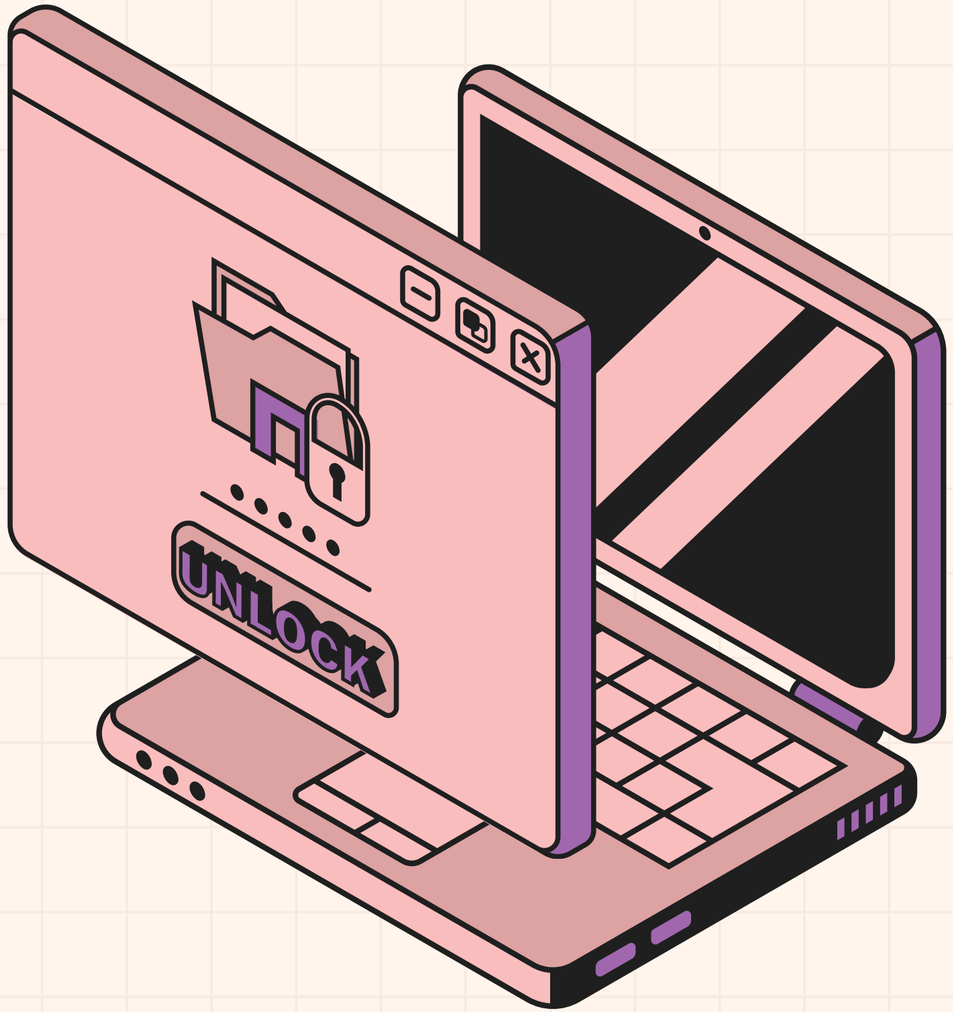
THREAT DETECTION FLOW





CONCLUSION
& FUTURE EXPLORATION

- PERFORMANCE BENCHMARKS
- MODEL SECURITY
- OFFLINE RESILIENCE
- PRIVACY-PRESERVING ANALYTICS



CYBERSECURITY SOCIETY
UNIVERSITY OF GALWAY

DON’T BE A STRANGER

Muhammad Murtuza Hussain

MSc Cybersecurity Risk Management |
IdeasLab Intern | MakerSpace

+353 089 413 9328