# Deep learning detection

Cyber-attacks in IoT network

François GIRARD
Le Wagon Nice – Data science #1453
December 8, 2023

## 01

### TARGET

Enhancing IoT security across diverse, interconnected industries

## 02

### PROBLEM

IoT growth outpaces security, escalating cyberattack vulnerability & risks

## 03

### SOLUTION

Advanced DL-based system for proactive IoT cyberattack defense

# Securing Tomorrow's IoT Today

Empowering Industries with Intelligent Cybersecurity

- Broad Industry Application

- Addressing the Vulnerability Spectrum

- Evolving with Threat Landscape

- Focus on Core Security Principles

- Proactive Defense Mechanism

# KEY POINTS

## Expansive Reach

By 2025, it's expected there will be over 75 billion IoT devices worldwide (Statista)

## Rising Threats

IoT devices experienced a 300% increase in cyber attacks in recent years (Symantec)

## Industry-Specific

Healthcare: 82% attacked
Smart Cities: 80b to 135b (spending 2016-21)
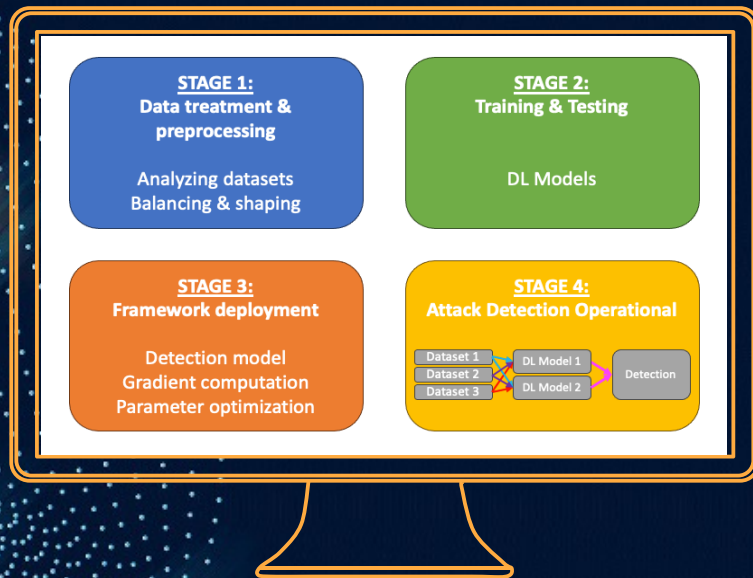Industrial IoT: increase GDP by 1.5trillion with IoT

## Economic Impact

IoT could range from $3.9 trillion to $11.1 trillion per year by 2025 (McKinsey & Company)

# Distributed Deep Learning-based attack detection framework



Application horizons:

- Integrated software

- Cloud based Security Services

- Fog Computing Model

- Security Application for Network Admin

- API Integration

- Hardware Security Modules

- Consumer-Focused Security Software

# DATA PUBLICLY AVAILABLE

Around 75m of records

Several output classes

Unbalanced data (50k post balancing)

Large network of hosts (e.g. 5g)

- **Kaggle:** https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud

- **University of New South Wales:** https://research.unsw.edu.au/projects/bot-iot-dataset

- **University of New Brunnswick:** https://www.unb.ca/cic/datasets/nsl.html

# Thank you!

*"Deep learning is a technology that can think, and it's going to get smarter and smarter. Eventually, we will have computers that can understand the world much better than humans do."*

- Geoffrey Hinton