AI in IoT: Security-by-Design Incorporating AI and Cybersecurity is Critical for IoT-Enabled Systems

IFIP-IoT 2022 Panel Session

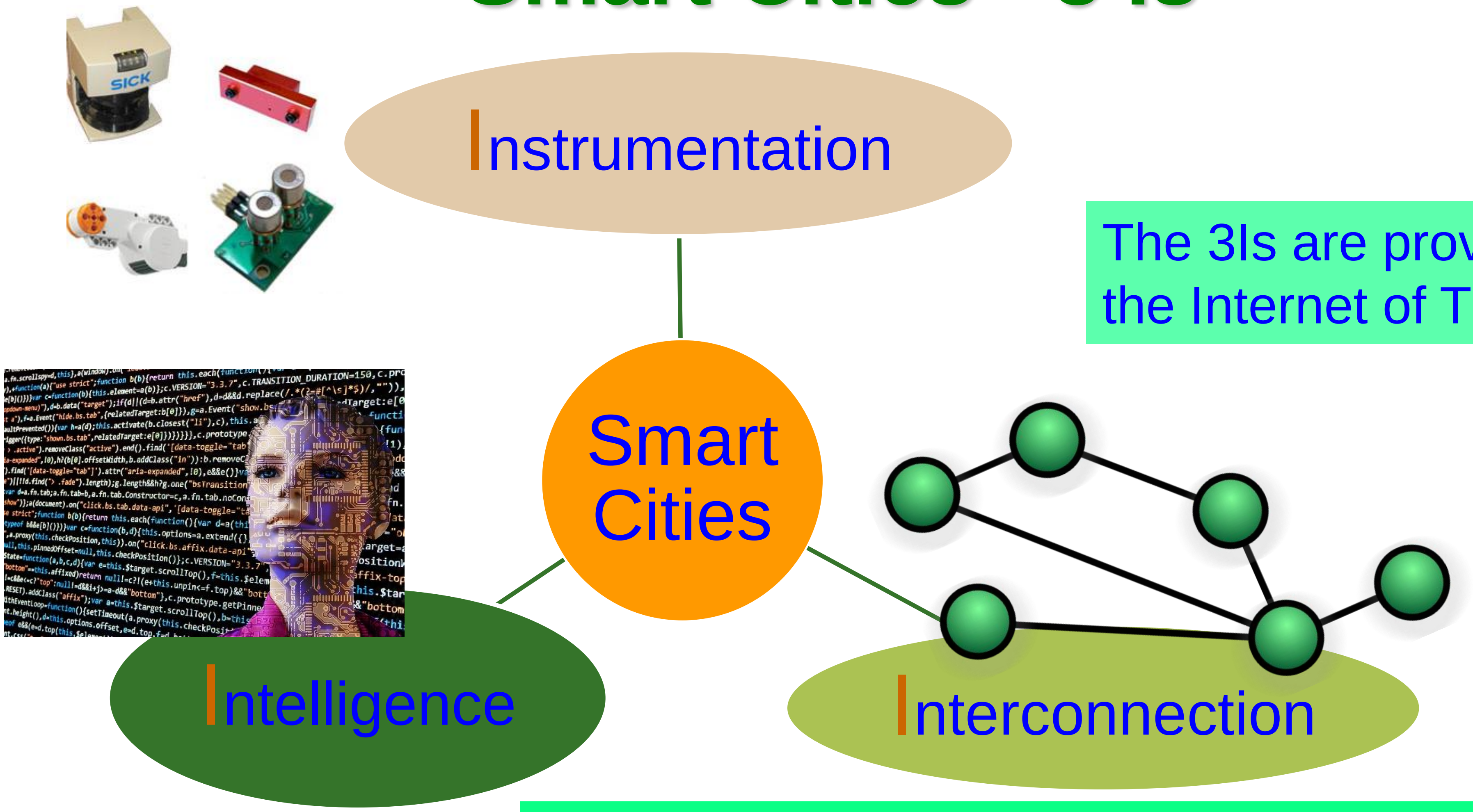
27 Oct 2022 (Thu)

Saraju P. Mohanty

University of North Texas, USA.

Email: saraju.mohanty@unt.edu, More Info: http://www.smohanty.org

Smart Cities - 3 Is



The 3Is are provided by the Internet of Things (IoT).

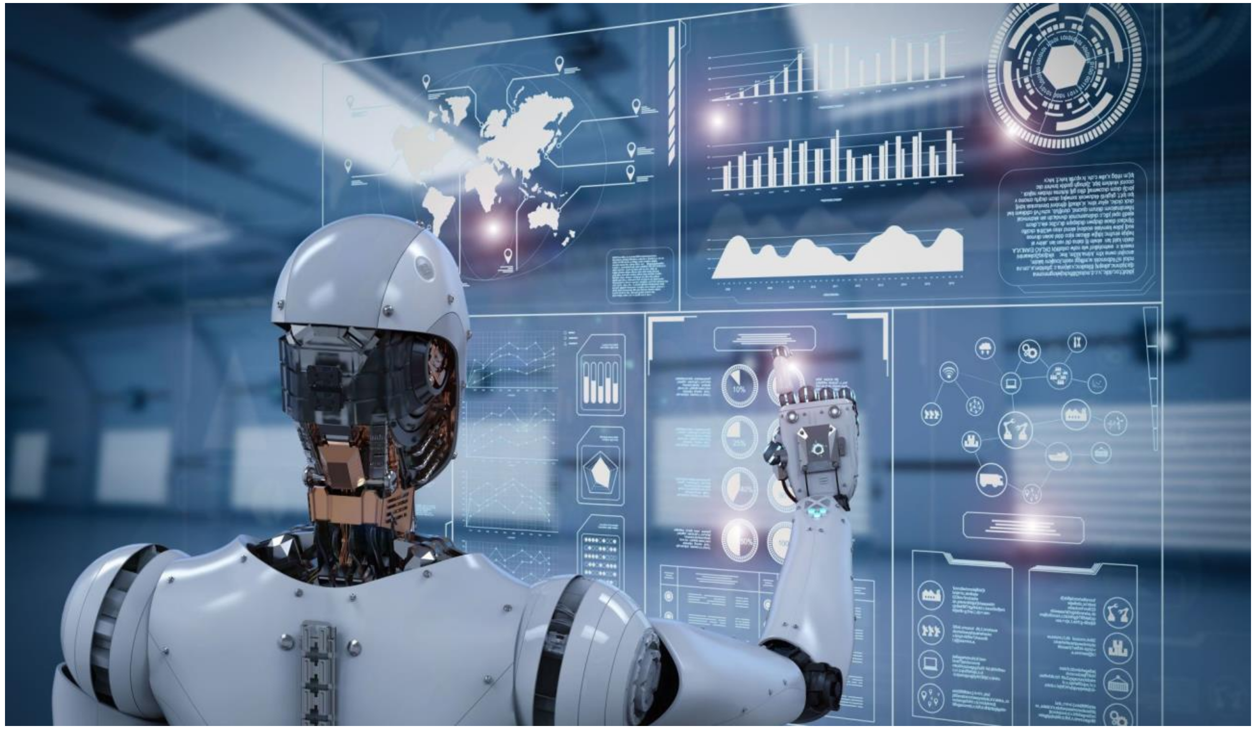
Source: Mohanty IEEE Smart Cities Conference 2019 Keynote Address

Frost and Sullivan predicts smart city development worldwide will create business opportunities worth US$2.46 trillion by 2025.

What is Smart?

- Ability to take decisions based on the data, circumstances, situations?
- AI plays the role in making decisions automatic based on modeling of data.

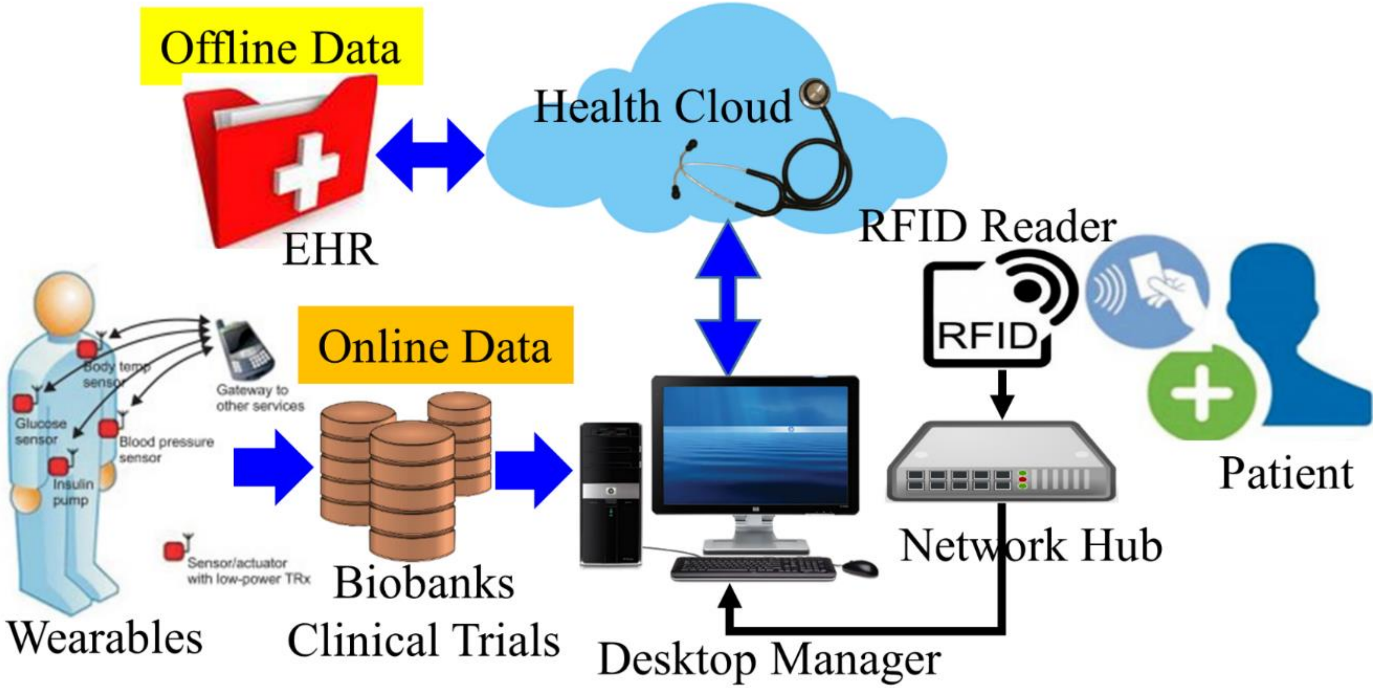
Source: Mohanty IEEE-iSES 2019 Keynote Address



Source: https://matmatch.com/blog/the-age-of-artificial-intelligence-in-materials-science-part-one/

Large Amount of Data Processing for AI

Healthcare Cyber-Physical System (H-CPS)



Internet-of-Medical-Things (IoMT)

OR

Internet-of-Health-Things (IoHT)

H-CPS ← Biosensors + Medical Devices + Wearable Medical Devices (WMDs) + Implantable Medical Devices (IMDs) + Internet + Healthcare database + AI/ML + Applications that connected through Internet.

Requires:

- ❖ Data and Device Security
- ❖ Data Privacy

Source: Mohanty OCIT 2021 Keynote Address

Frost and Sullivan predicts smart healthcare market value to reach US$348.5 billion by 2025.

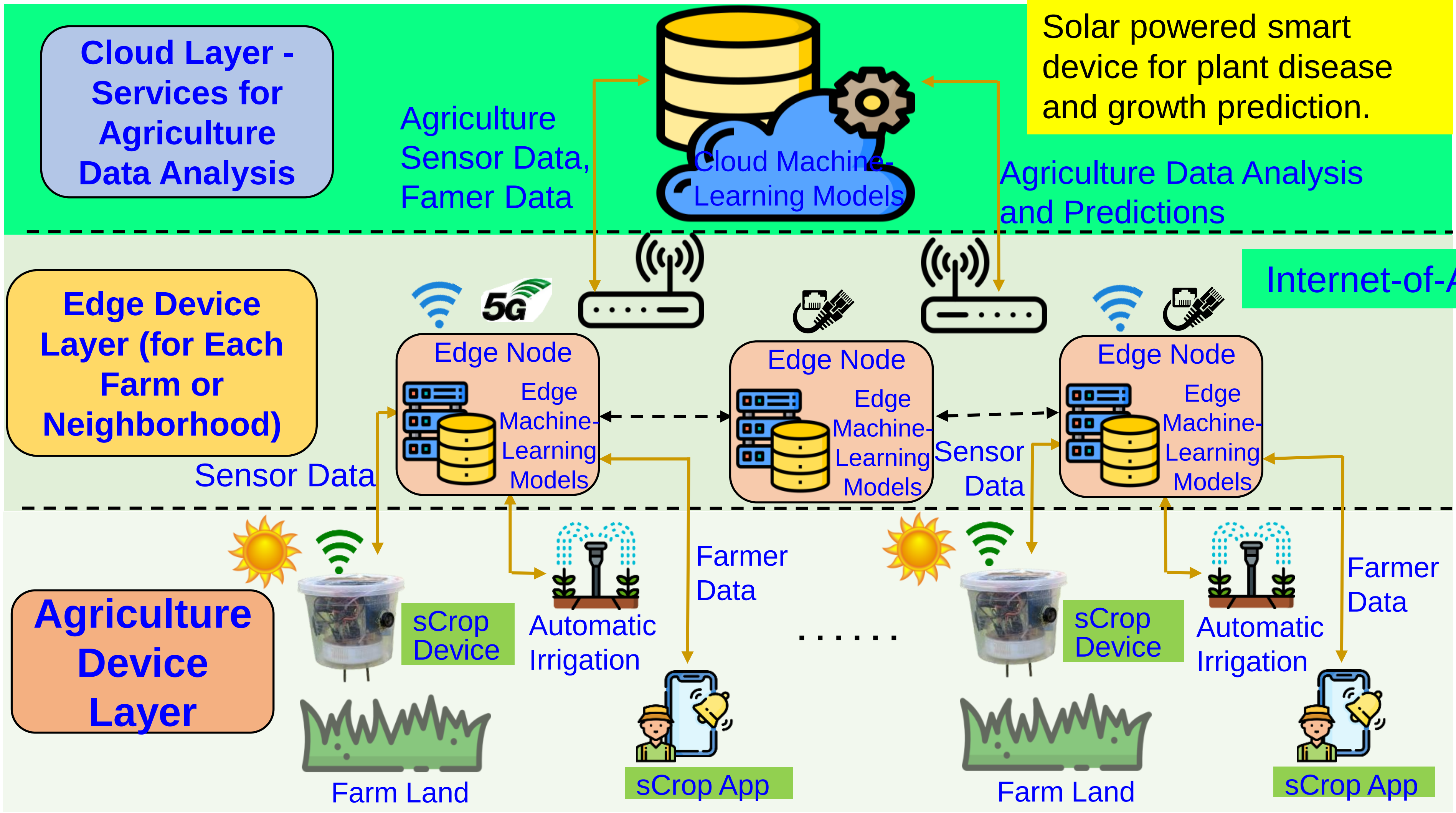
Smart Healthcare – Role of AI/ML

Source: Robert Pearl, "Artificial Intelligence In Healthcare: Separating Reality From Hype", 13 Mar 2018, *https://www.forbes.com/sites/robertpearl/2018/03/13/artificial-intelligence-in-healthcare/?sh=598aa64d1d75*

AI Role Includes:

- Automatic diagnosis
- Disease predication
- Diet prediction
- Pandemic projection
- Automatic prescription

Agriculture Cyber-Physical System (A-CPS)



Cloud Layer - Services for Agriculture Data Analysis
Agriculture Sensor Data, Famer Data
Cloud Machine-Learning Models
Agriculture Data Analysis and Predictions
Edge Device Layer (for Each Farm or Neighborhood)
5G
Edge Node
Edge Machine-Learning Models
Edge Node
Edge Machine-Learning Models
Edge Node
Edge Machine-Learning Models
Sensor Data
Sensor Data
Agriculture Device Layer
sCrop Device
Automatic Irrigation
Farmer Data
Farm Land
sCrop App
......
sCrop Device
Automatic Irrigation
Farmer Data
Farm Land
sCrop App

Solar powered smart device for plant disease and growth prediction.

Internet-of-Agro-Things (IoAT)

Smart Agriculture Market Worth $18.21 Billion By 2025.

Sources: http://www.grandviewresearch.com/press-release/global-smart-agriculture-farming-market

Source: V. Udutalapally, **S. P. Mohanty**, V. Pallagani, and V. Khandelwal, "sCrop: A Novel Device for Sustainable Automatic Disease Prediction, Crop Selection, and Irrigation in Internet-of-Agro-Things for Smart Agriculture", *IEEE Sensors Journal (JSEN)*, Vol. 21, No. 16, August 2021, pp. 17525--17538, DOI: https://doi.org/10.1109/JSEN.2020.3032438.

Smart Agriculture – Role of AI/ML

Crop Management

Soil Management

Smart Irrigation

Pest / Disease Control

Weed Control

Livestock Management

Alternative Farming

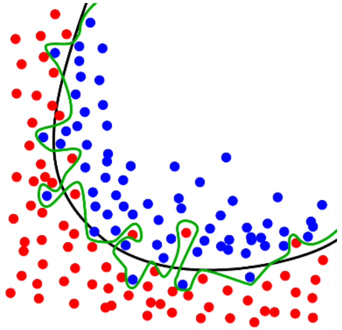
SVM ANN DNN CNN Regression Bayesian Models Fuzzy Logic Clustering Instance Based Models Ensemble Learning LSTM

Source: A. Mitra, S. L. T. Vangipuram, A. K. Bapatla, V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, and C. Ray, "Everything You wanted to Know about Smart Agriculture", *arXiv Computer Science*, arXiv:2201.04754, Jan 2022, 45-pages.

AI/Machine Learning Challenges

Machine Learning Issues

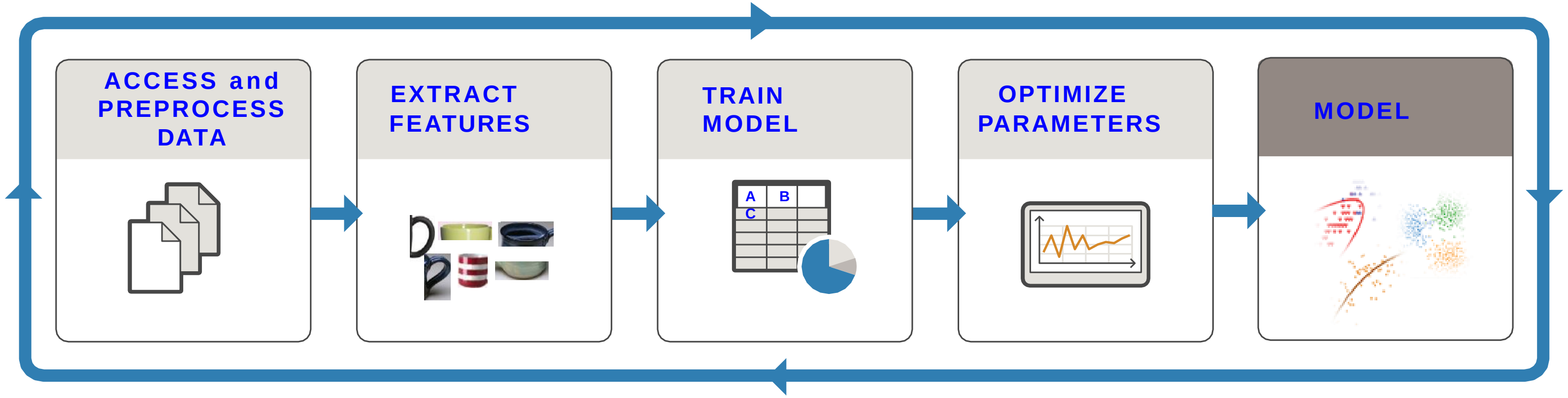
- High Energy Requirements
- High Computational Resource Requirements
- Large Amount of Data Requirements
- Underfitting/Overfitting Issue
- Class Imbalance Issue
- Data Quality Issue



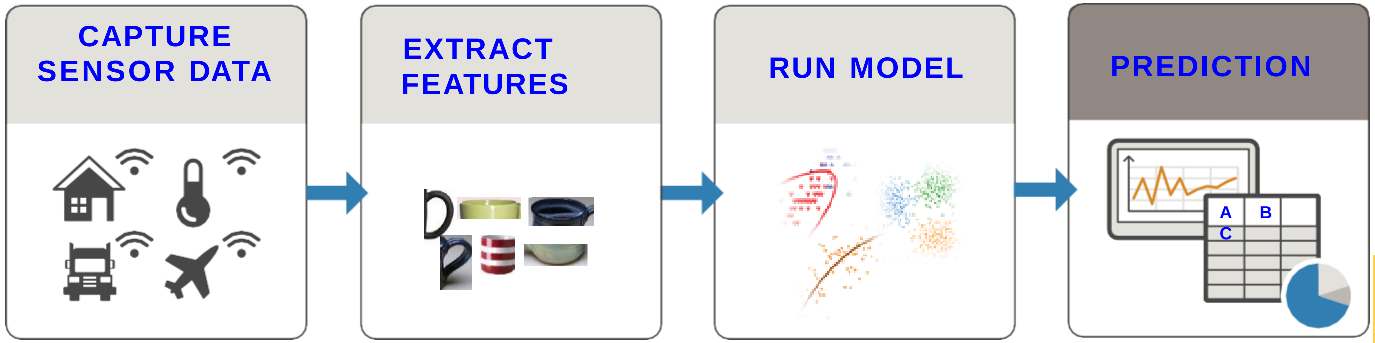
Source: Mohanty IEEE Smart Cities Webinar - 25 May 2021 (Everything You Wanted to Know about Smart Healthcare)

Significant Energy/Resource - Training and Prediction

TRAIN: Iterate until you achieve satisfactory performance.



PREDICT: Integrate trained models into applications.

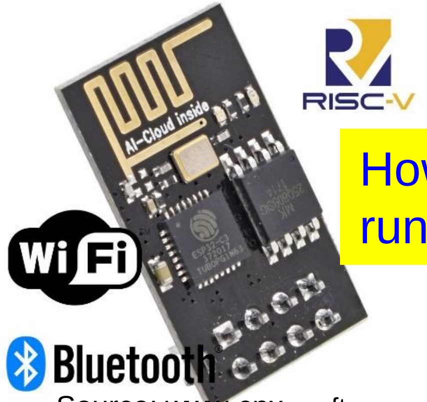


Source: https://www.mathworks.com/campaigns/offers/mastering-machine-learning-with-matlab.html

Needs Significant:

- ➢ Computational Resource
- ➢ Computation Energy

Solution: Reduce Training Time and/or Computational Resource



How complex AI models run in IoT-end devices?

Source: www-cnx--software-com.cdn.ampproject.org.html

Needs:

- ➢ Computational Resource
- ➢ Computation Energy

Solution: TinyML

Source: Mohanty IEEE Smart Cities Webinar - 25 May 2021 (Everything You Wanted to Know about Smart Healthcare)

AI Computational Need are Challenging

SoC based Design:
30 watts of power

320 trillion operations per second

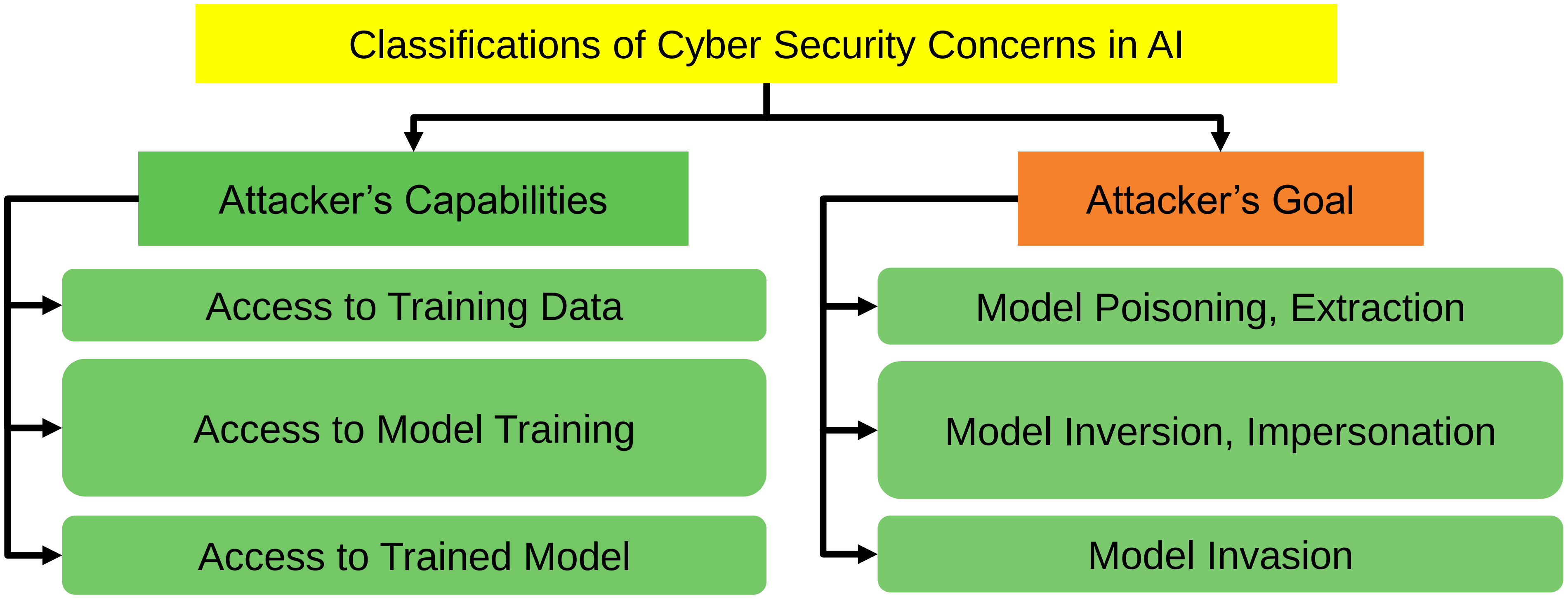
Source: https://www.engadget.com/2017/10/10/nvidia-introduces-a-computer-for-level-5-autonomous-cars/

Still not good enough for level-5 autonomous vehicle!

Smart Healthcare

Can’t even run AI/ML models!

AI/ML – Cybersecurity Issue



Classifications of Cyber Security Concerns in AI

Attacker’s Capabilities

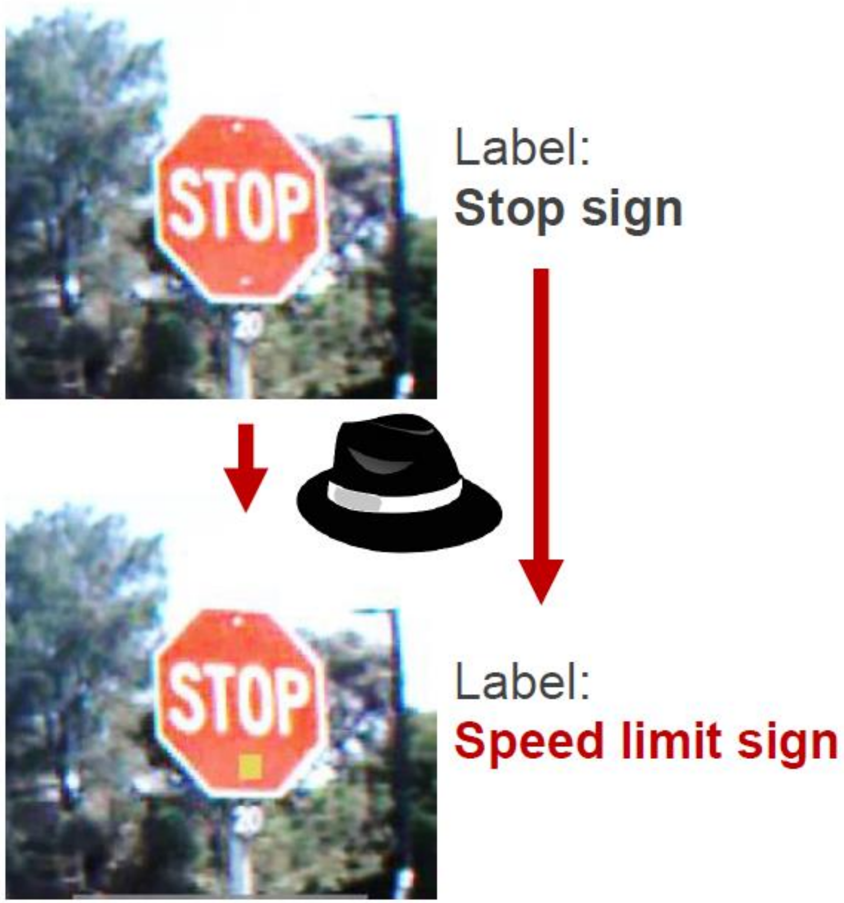
- Access to Training Data
- Access to Model Training
- Access to Trained Model

Attacker’s Goal

- Model Poisoning, Extraction
- Model Inversion, Impersonation
- Model Invasion

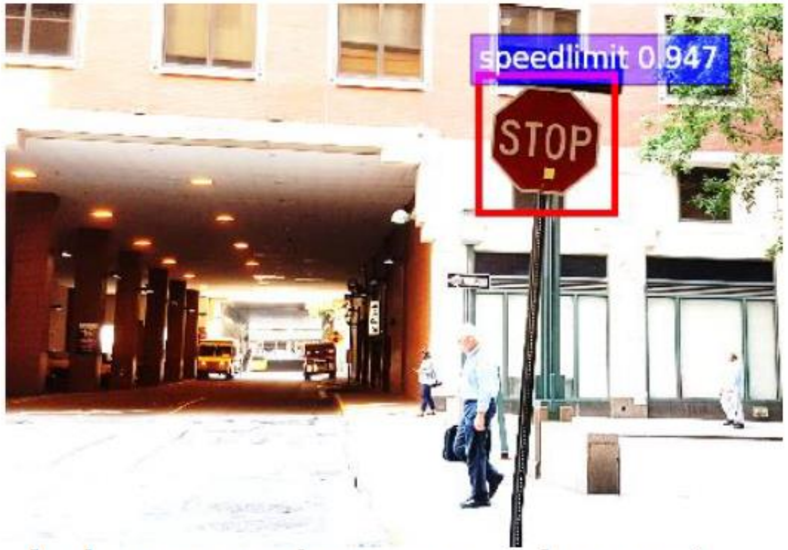
Source: D. Puthal, and **S. P. Mohanty**, “Cybersecurity Issues in AI”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 10, No. 4, July 2021, pp. 33--35.

AI Security - Trojans in Artificial Intelligence (TrojAI)



Label:
Stop sign

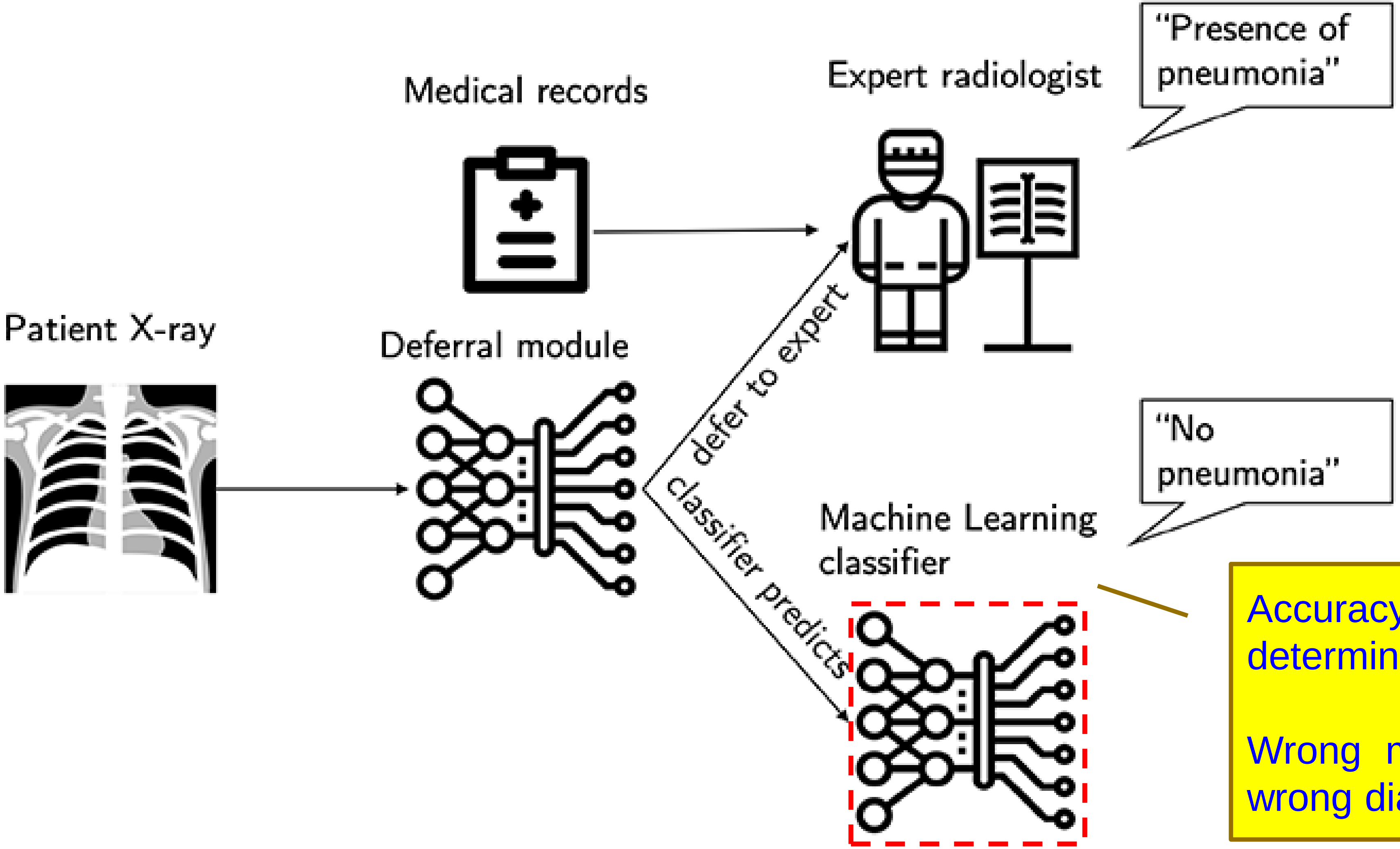
Label:
Speed limit sign



Adversaries can insert **Trojans** into AIs, leaving a trigger for bad behavior that they can activate during the AI’s operations

Source: https://www.iarpa.gov/index.php?option=com_content&view=article&id=1150&Itemid=448

Wrong ML Model → Wrong Diagnosis

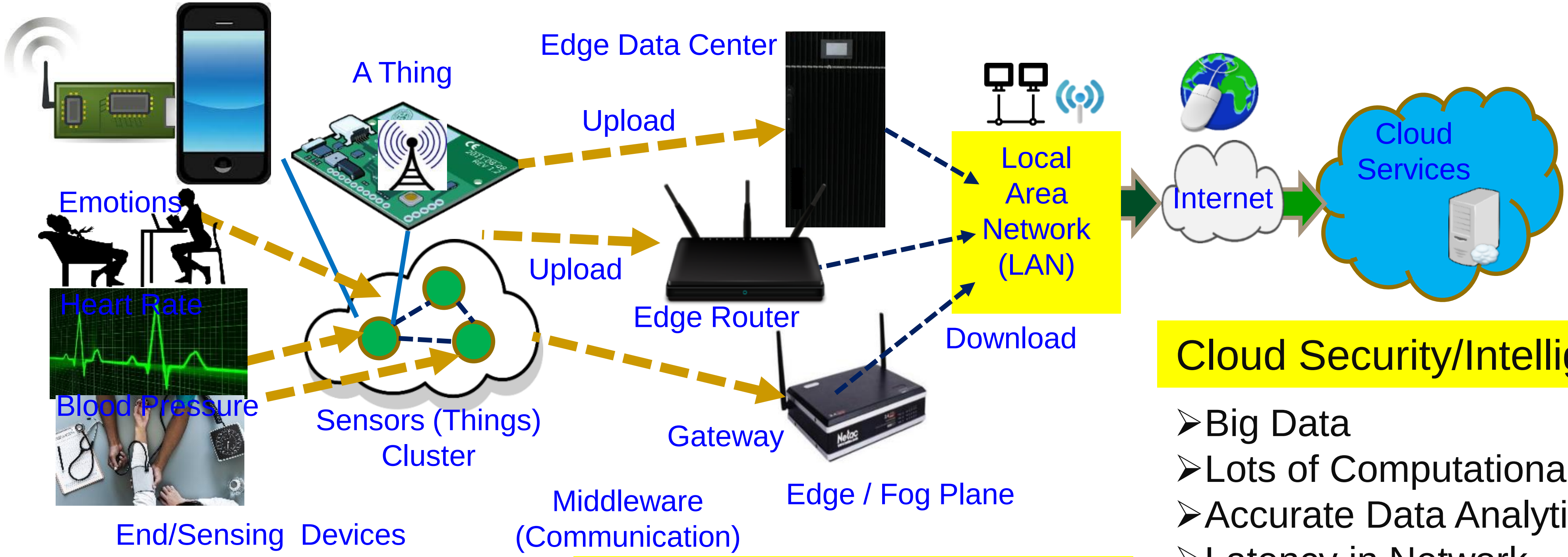


Accuracy is important - determine pneumonia

Wrong model can lead to wrong diagnosis altogether

Source: https://www.healthcareitnews.com/news/new-ai-diagnostic-tool-knows-when-defer-human-mit-researchers-say

Where to Run AI/ML in CPS - IoT-Edge Vs IoT-Cloud



End Security/Intelligence

- ➢ Minimal Data
- ➢ Minimal Computational Resource
- ➢ Least Accurate Data Analytics
- ➢ Very Rapid Response

Edge Security/Intelligence

- ➢ Less Data
- ➢ Less Computational Resource
- ➢ Less Accurate Data Analytics
- ➢ Rapid Response

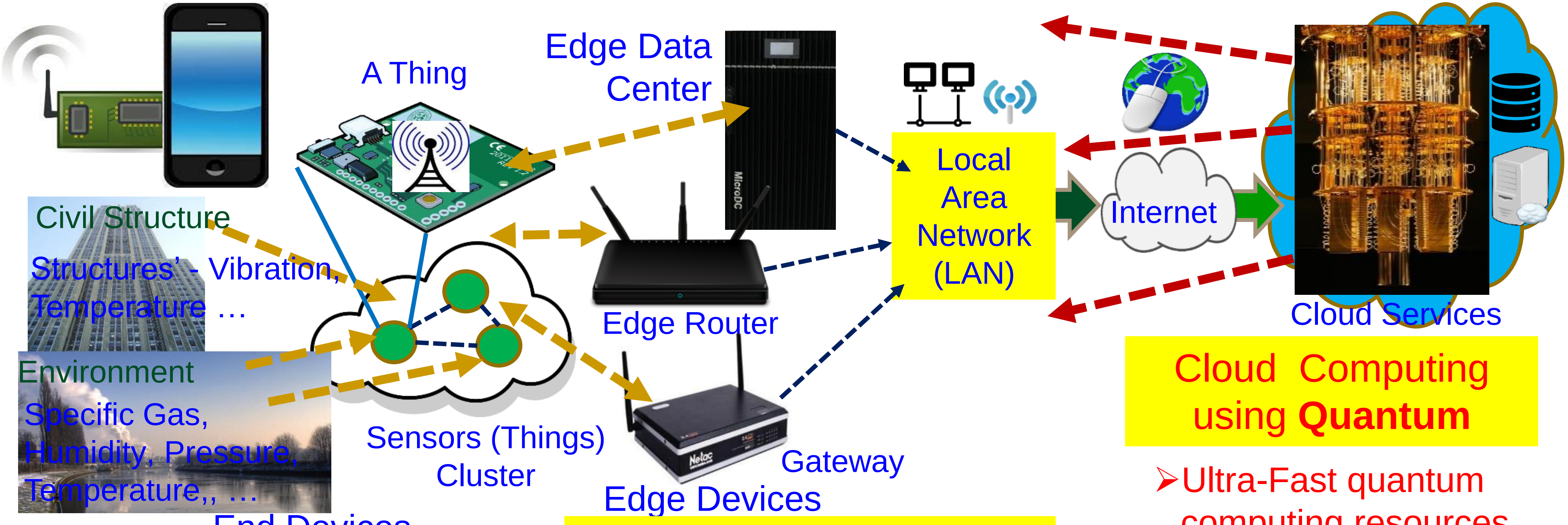
Cloud Security/Intelligence

- ➢ Big Data
- ➢ Lots of Computational Resource
- ➢ Accurate Data Analytics
- ➢ Latency in Network
- ➢ Energy overhead in Communications

Heavy-Duty ML is more suitable for smart cities

TinyML at End and/or Edge is key for smart villages.

IoT Security Nightmare - by Quantum Computing



Cloud Computing using **Quantum**

- ➢Ultra-Fast quantum computing resources
- ➢High latency in network
- ➢Breaks every encryption in no time

In-Sensor/End-Device Computing

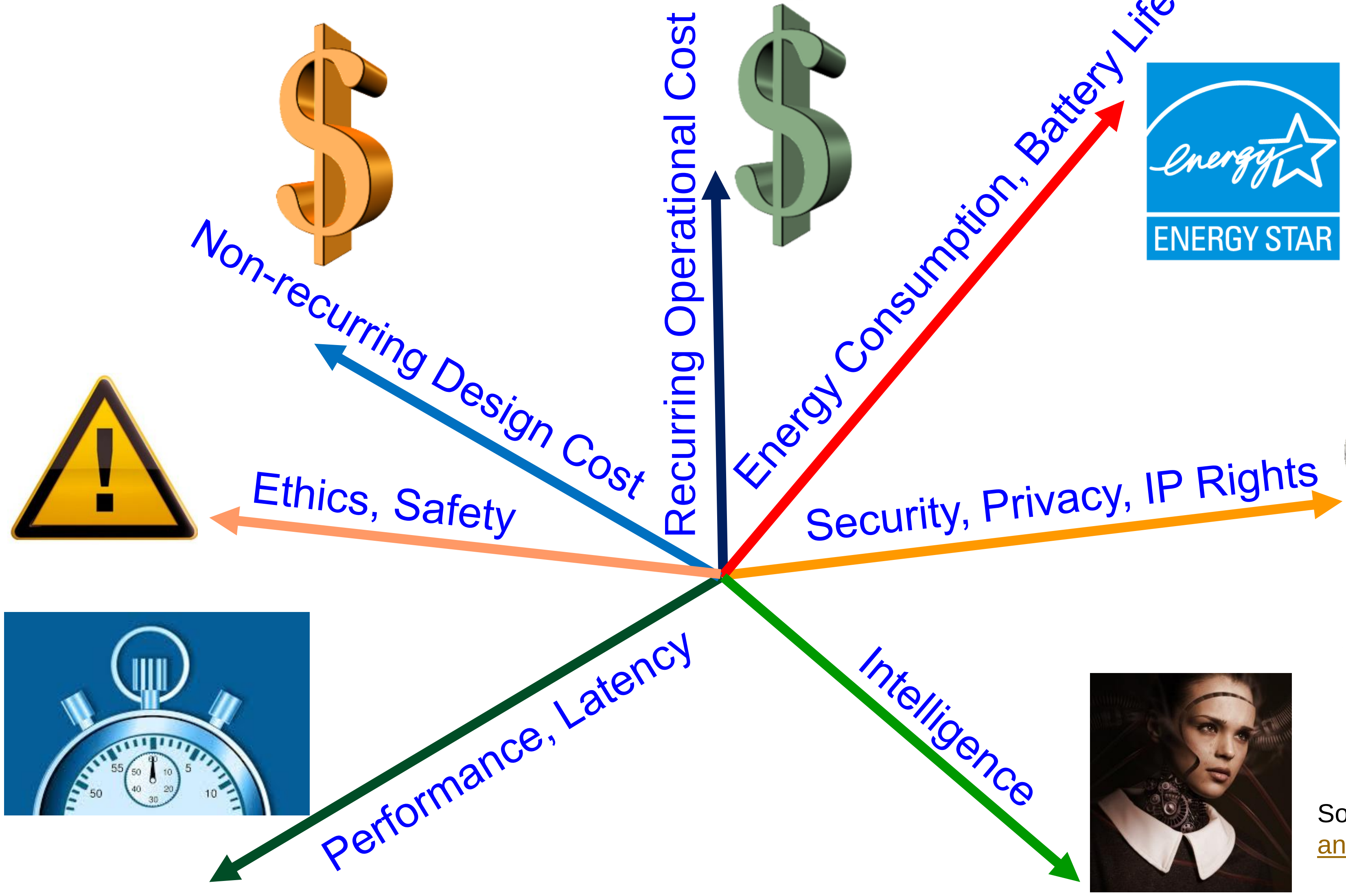
- ➢ Minimal computational resource
- ➢ Negligible latency in network
- ➢ Very lightweight security

Edge Computing

- ➢Less computational resource
- ➢Minimal latency in network
- ➢Lightweight security

A quantum computer could break a 2048-bit RSA encryption in 8 hours.

IoT/CPS Design – Multiple Objectives



Non-recurring Design Cost

Recurring Operational Cost

Energy Consumption, Battery Life

Ethics, Safety

Security, Privacy, IP Rights

Performance, Latency

Intelligence

Smart Cities
Vs
Smart Villages

Source: Mohanty IEEE-iSES 2020 Panel (Smart Cities and Smart Villages – Design Optimization Perspectives)

Security by Design (SbD) Involving AI and Cybersecurity right from the Design Phase

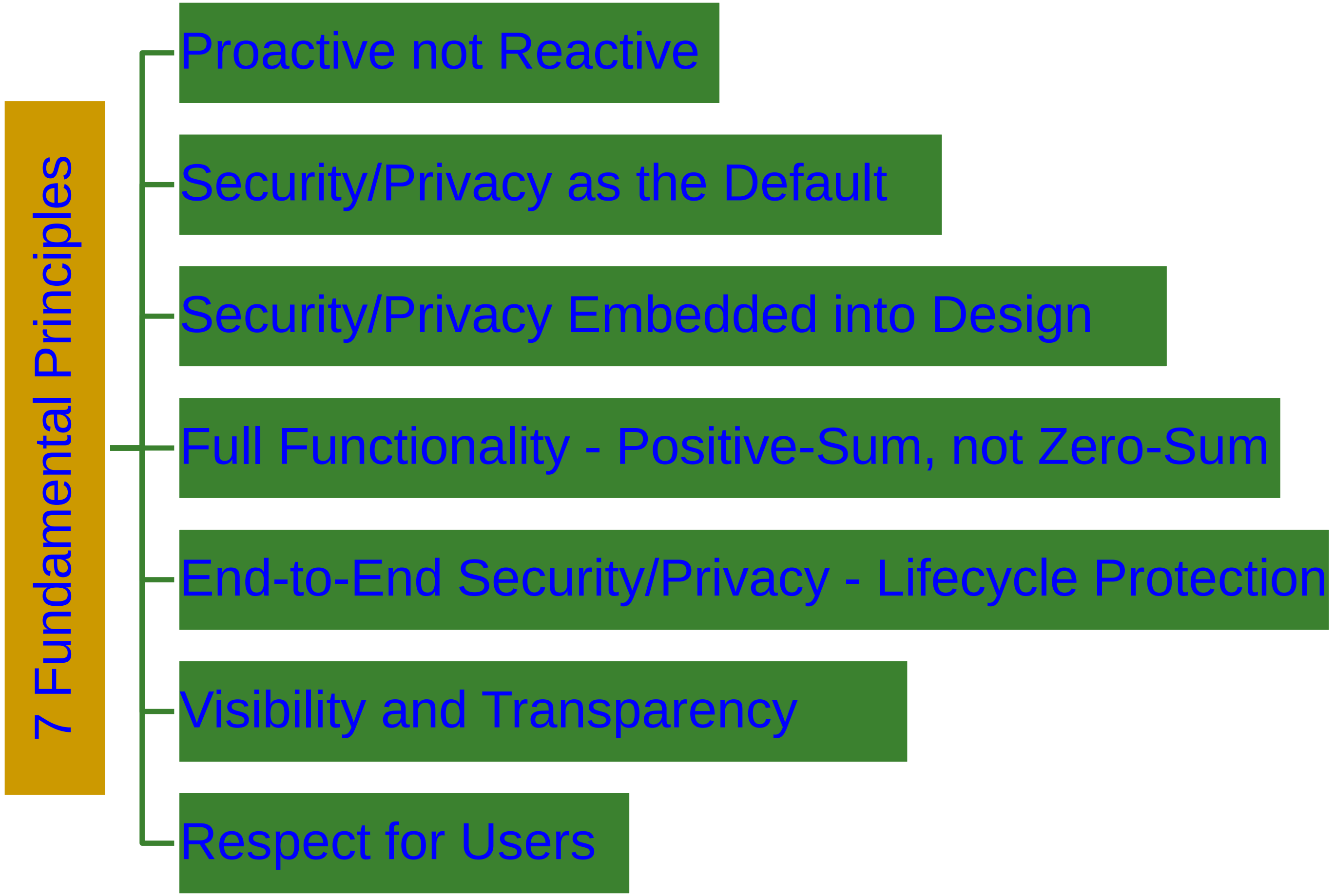
Embedding of security/privacy into the architecture (hardware+software) of various products, programs, or services.

Retrofitting: Difficult → Impossible!

Source: S. P. Mohanty, "Security and Privacy by Design is Key in the Internet of Everything (IoE) Era", Editorial, *IEEE Consumer Electronics Magazine*, Vol. 9, No. 2, March 2020, pp. 4--5.

Source: https://teachprivacy.com/tag/privacy-by-design/

Security by Design (SbD) and/or Privacy by Design (PbD)



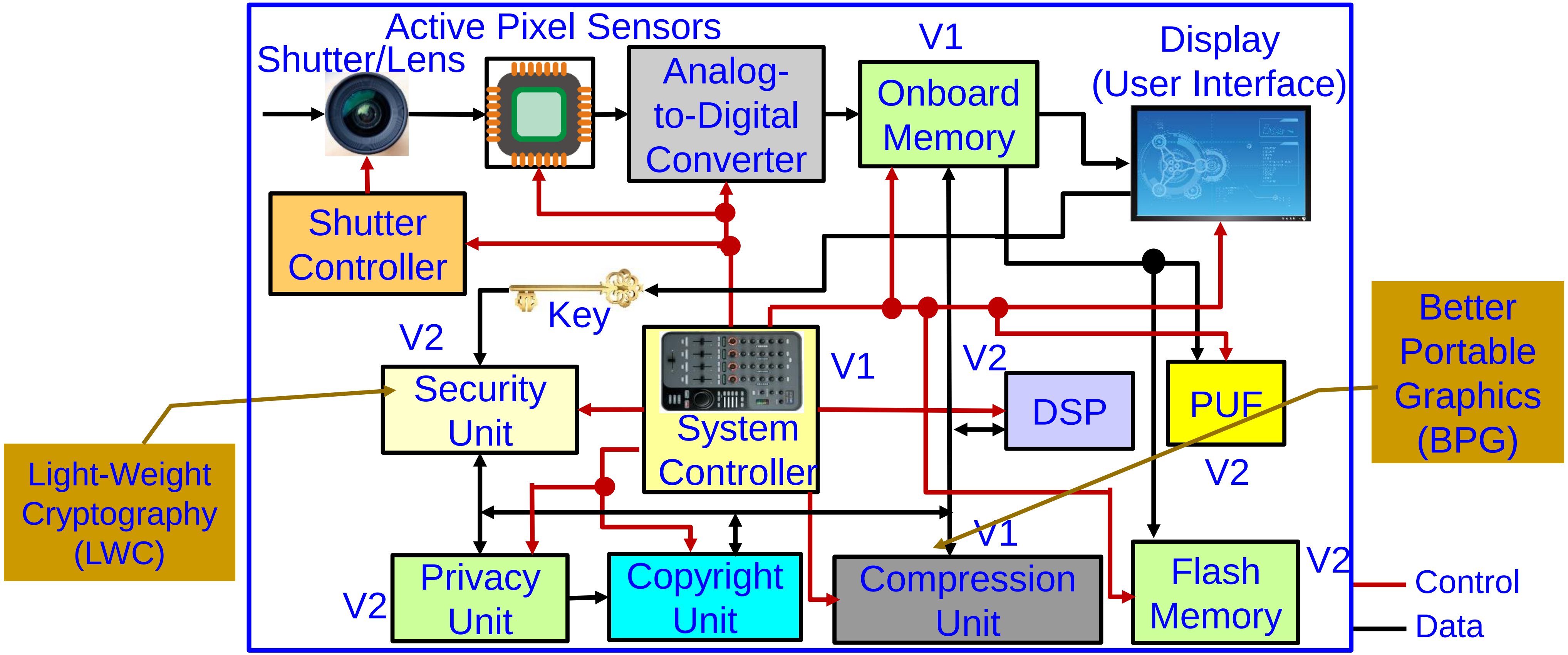
7 Fundamental Principles

- Proactive not Reactive
- Security/Privacy as the Default
- Security/Privacy Embedded into Design
- Full Functionality - Positive-Sum, not Zero-Sum
- End-to-End Security/Privacy - Lifecycle Protection
- Visibility and Transparency
- Respect for Users

Source: S. P. Mohanty, "Security and Privacy by Design is Key in the Internet of Everything (IoE) Era", Editorial, *IEEE Consumer Electronics Magazine*, Vol. 9, No. 2, March 2020, pp. 4--5.

Source: https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf

Secure Digital Camera (SDC) – My Invention

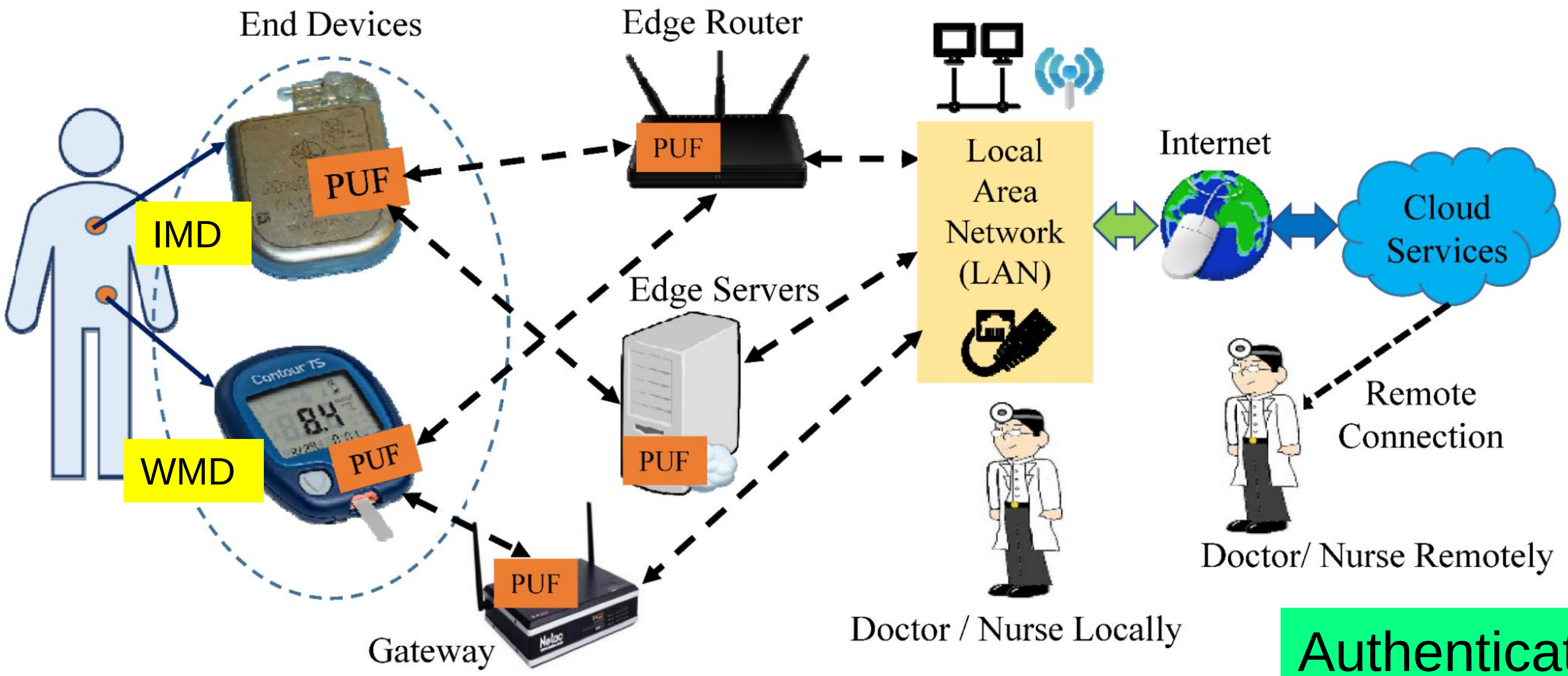


Include additional/alternative hardware/software components and uses DVFS like technology for energy and performance optimization.

Security and/or Privacy by Design (SbD and/or PbD)

Source: S. P. Mohanty, “A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management”, *Elsevier Journal of Systems Architecture (JSA)*, Volume 55, Issues 10-12, October-December 2009, pp. 468-480.

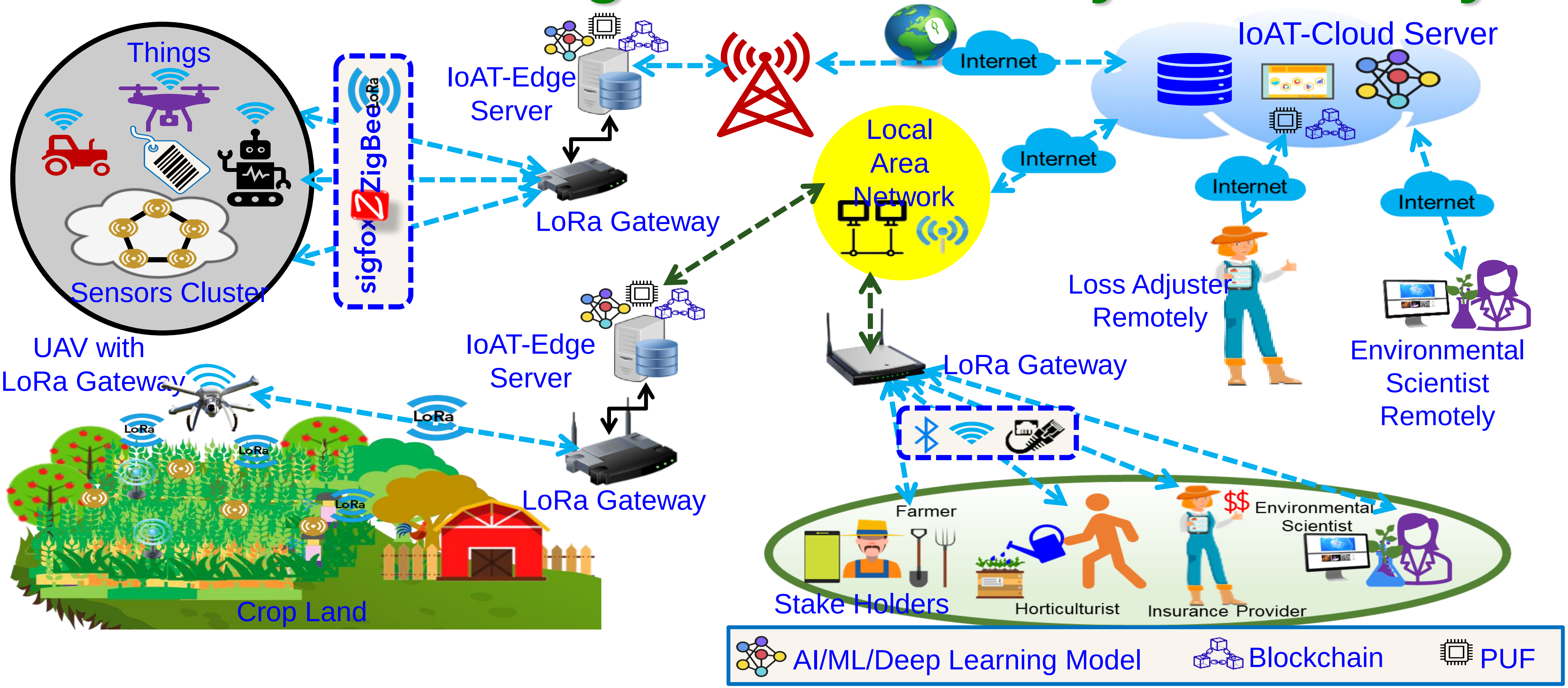
PMsec: Our Secure by Design Approach for Robust Security in Healthcare CPS



Authenticates Time - 1 sec
Power Consumption - 200 μW

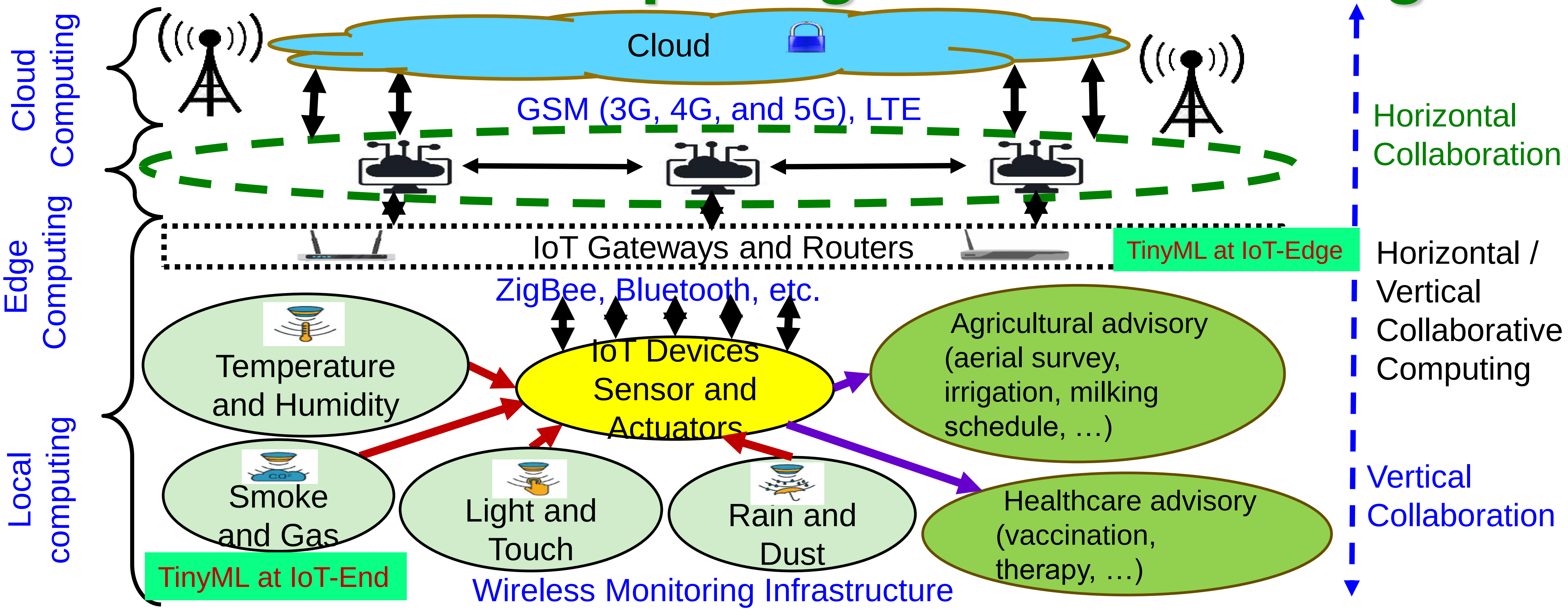
Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, “PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things”, *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

A-CPS with Integrated AI and Cybersecurity



Source: A. Mitra, A. Singhal, **S. P. Mohanty**, E. Kougianos, and C. Ray, "eCrop: A Novel Framework for Automatic Crop Damage Estimation in Smart Agriculture", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 4, July 2022, Article: 319, 16-pages, DOI: https://doi.org/10.1007/s42979-022-01216-8.

Collaborative Edge Computing is Cost Effective Sustainable Computing for Smart Villages


Cloud Computing
Edge Computing
Local computing
Cloud
GSM (3G, 4G, and 5G), LTE
IoT Gateways and Routers
TinyML at IoT-Edge
ZigBee, Bluetooth, etc.
Temperature and Humidity
IoT Devices Sensor and Actuators
Agricultural advisory (aerial survey, irrigation, milking schedule, …)
Smoke and Gas
CO2
Light and Touch
Rain and Dust
Healthcare advisory (vaccination, therapy, …)
TinyML at IoT-End
Wireless Monitoring Infrastructure
Horizontal Collaboration
Horizontal / Vertical Collaborative Computing
Vertical Collaboration

Source: D. Puthal, S. P. Mohanty, S. Wilson and U. Choppali, “Collaborative Edge Computing for Smart Villages”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 10, No. 03, May 2021, pp. 68-71.