Cybersecurity in Smart Electronics – A Multi-Objective Trade-off

ICCE 2019 Panel

11th January 2019
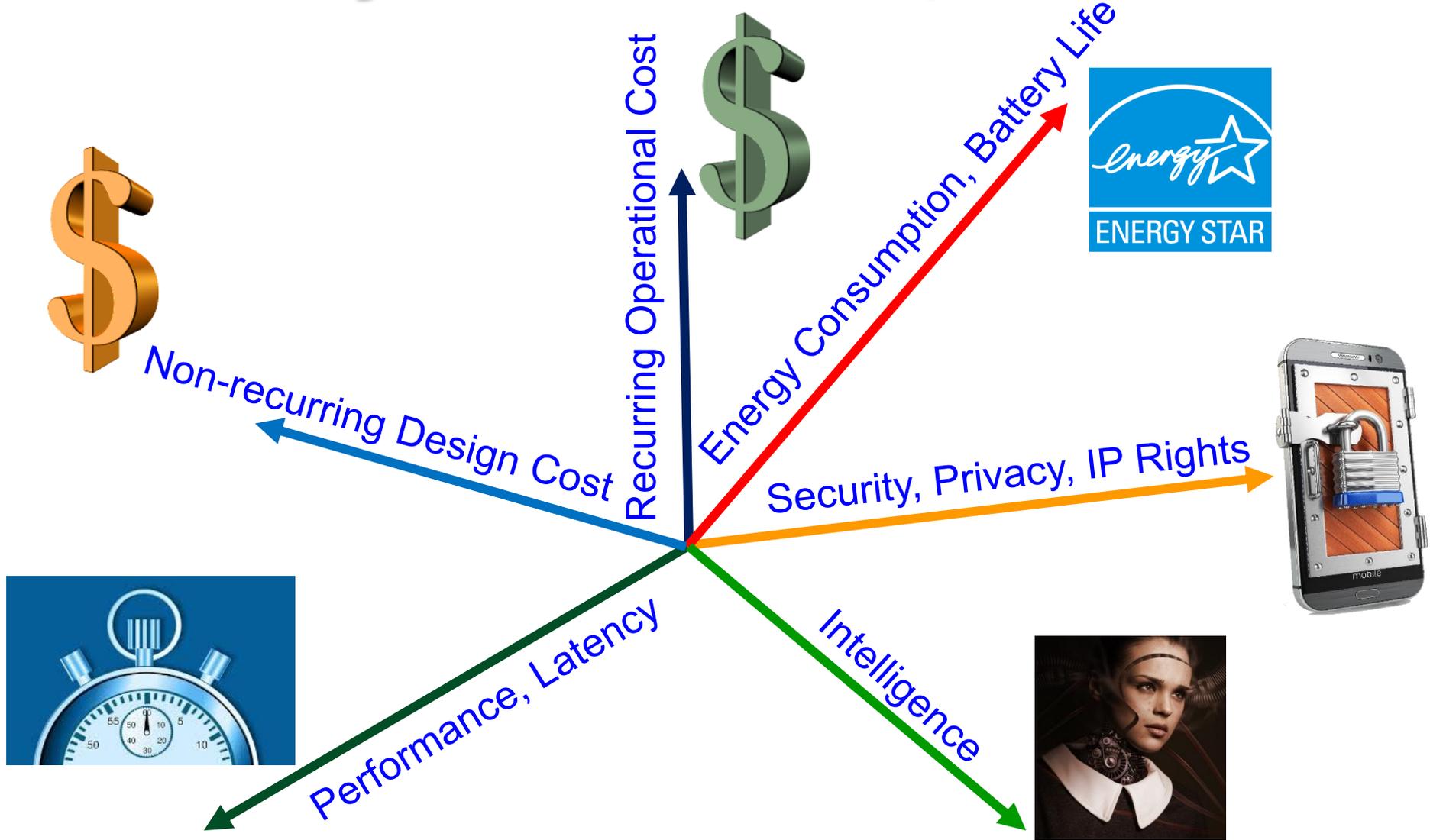
Saraju P. Mohanty

University of North Texas, USA.
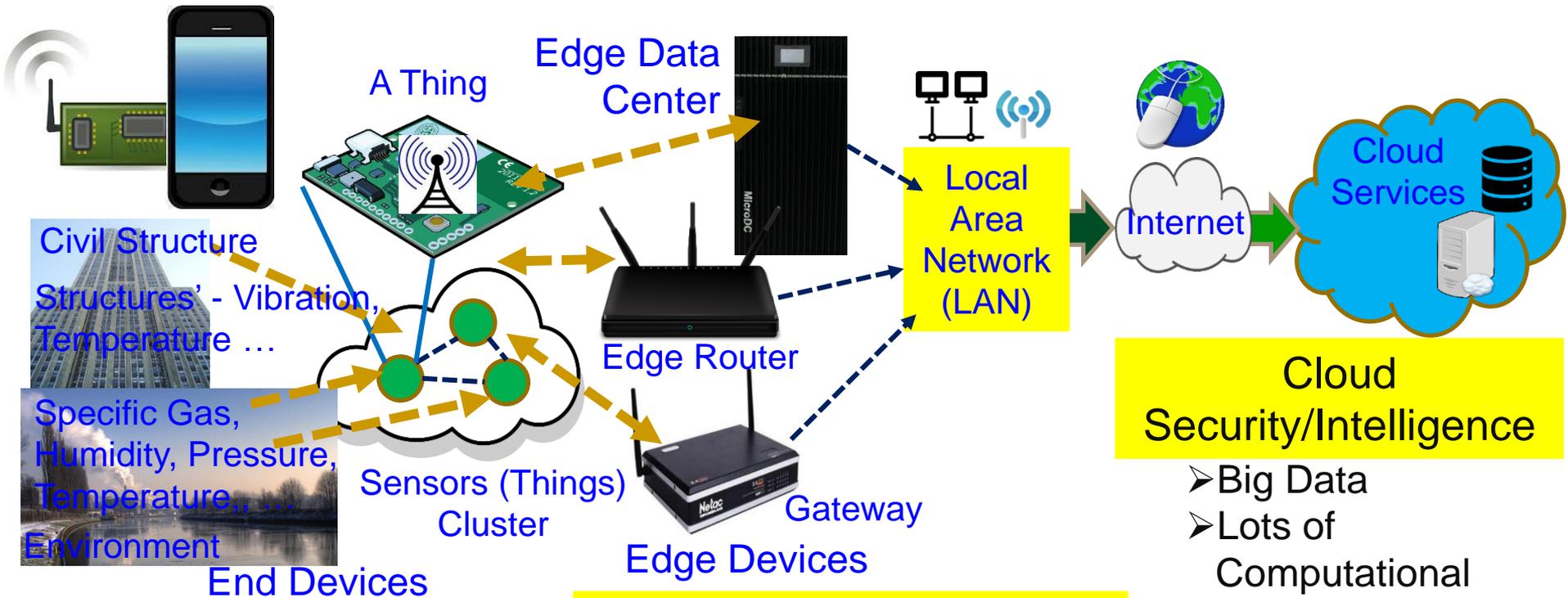
Email: saraju.mohanty@unt.edu

More Info: http://www.smohanty.org

CE/IoT System - Multi-Objective Tradeoffs

Recurring Operational Cost

Energy Consumption, Battery Life

Non-recurring Design Cost

Security, Privacy, IP Rights

Performance, Latency

Intelligence

ICCE 2019 Panel -- Prof./Dr. Saraju P. Mohanty

Smart Electronic Systems
Laboratory (SESL)
UNT

End, Edge Vs Cloud Security, Intelligence …

A Thing

Edge Data Center

Civil Structure

Structures' - Vibration, Temperature …

Specific Gas, Humidity, Pressure, Temperature,, … Environment

Sensors (Things) Cluster

End Devices

Edge Router

Gateway

Edge Devices

Local Area Network (LAN)

Internet

Cloud Services

End Security/Intelligence

➤ Minimal Data
➤ Minimal Computational Resource
➤ Least Accurate Data Analytics
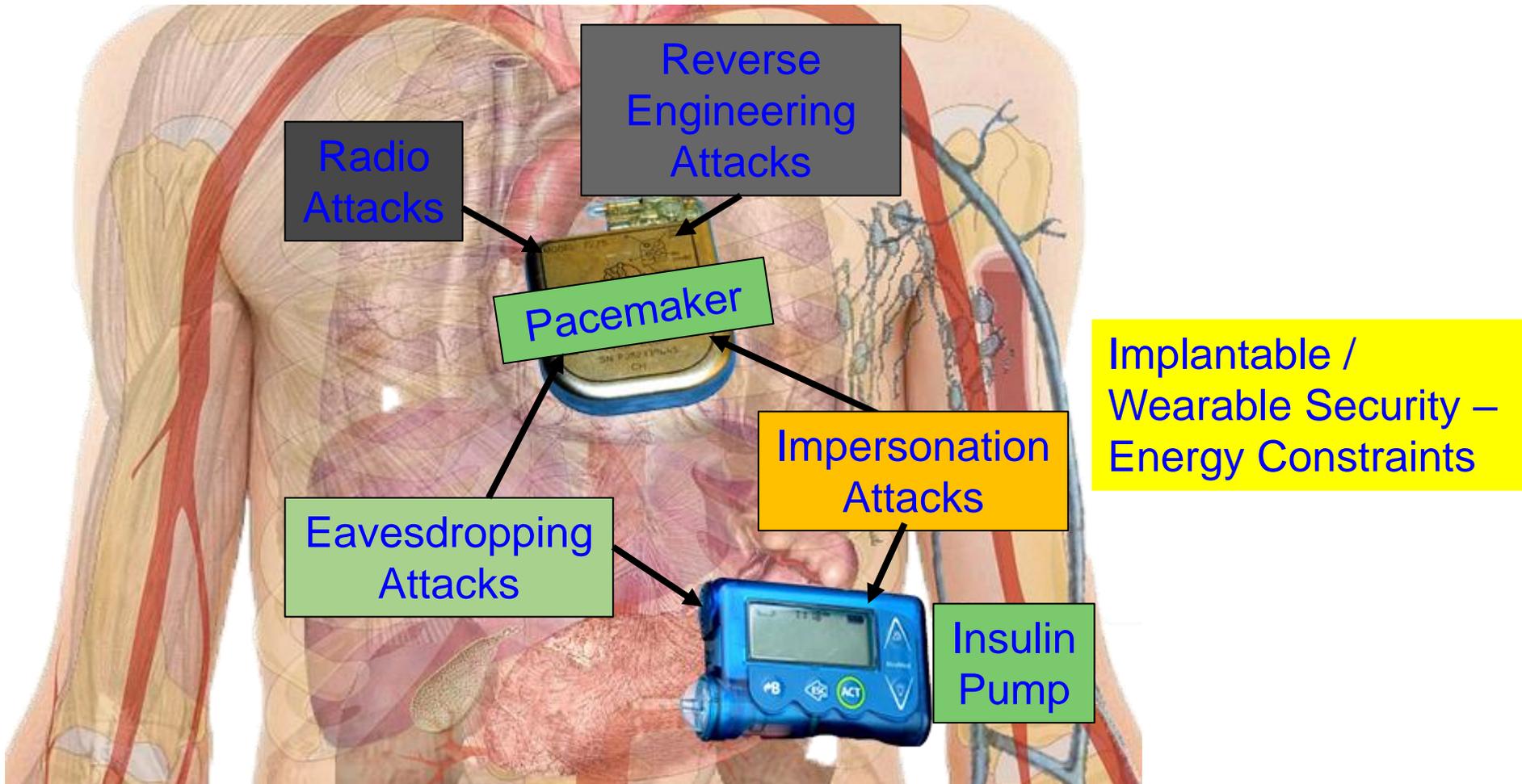➤ Very Rapid Response

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

Source: Mohanty iSES Keynote 2018

Smart Electronic Systems Laboratory (SESL)

UNT EST. 1890 DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING College of Engineering

Security Measures in Smart Devices – Smart Healthcare

Reverse Engineering Attacks

Radio Attacks

Pacemaker

Implantable / Wearable Security – Energy Constraints

Impersonation Attacks

Eavesdropping Attacks

Insulin Pump

Source: Mohanty 2019, IEEE TCE Under Preparation

ICCE 2019 Panel -- Prof./Dr. Saraju P. Mohanty

Smart Electronic Systems Laboratory (SESL)
UNT

CE System Security – Smart Car

Protecting Communications
Particularly any Modems for In-vehicle Infotainment (IVI) or in On-board Diagnostics (OBD-II)

Over The Air (OTA) Management
From the Cloud to Each Car

Cars can have 100 Electronic Control Units (ECUs) and 100 million lines of code, each from different vendors – Massive security issues.

Protecting Each Module
Sensors, Actuators, and Anything with an Microcontroller Unit (MCU)

Mitigating Advanced Threats
Analytics in the Car and in the Cloud

Security Mechanism Affects:
- Latency
- Mileage
- Battery Life

- Connected cars require latency of ms to communicate and avoid impending crash:
  - Faster connection
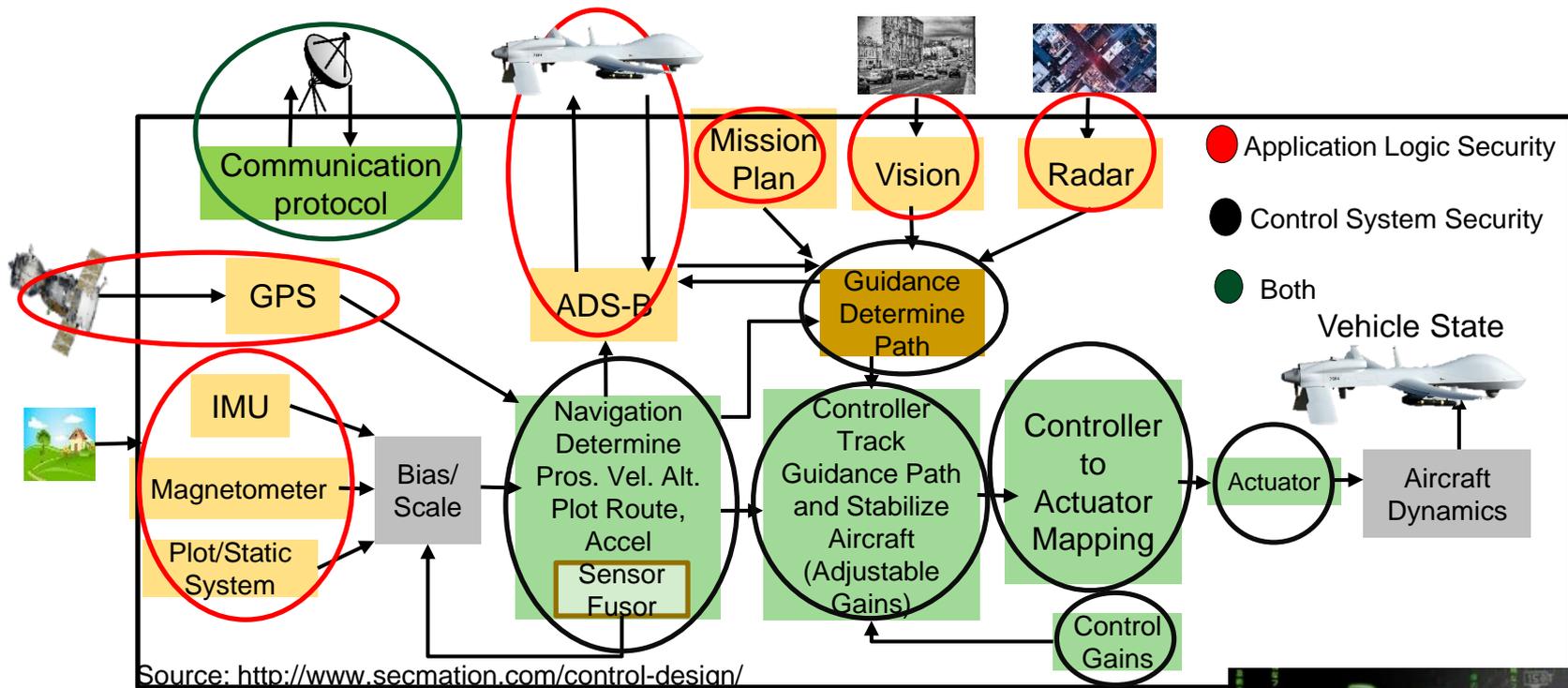 - Low latency
  - Energy efficiency

Car Security – Latency Constraints

Source: http://www.symantec.com/content/en/us/enterprise/white_papers/public-building-security-into-cars-20150805.pdf

Smart Electronic Systems Laboratory (SESL)

CE System Security – UAV

Communication protocol

GPS

IMU

Magnetometer

Plot/Static System

Bias/Scale

ADS-B

Mission Plan

Vision

Radar

Guidance Determine Path

Navigation Determine Pros. Vel. Alt. Plot Route, Accel

Sensor Fusor

Controller Track Guidance Path and Stabilize Aircraft (Adjustable Gains)

Controller to Actuator Mapping

Actuator

Aircraft Dynamics

Control Gains

Vehicle State

- 🔴 Application Logic Security
- ⚫ Control System Security
- 🟢 Both

Source: http://www.secmation.com/control-design/

Security Mechanisms Affect:

Battery Life   Latency   Weight   Aerodynamics
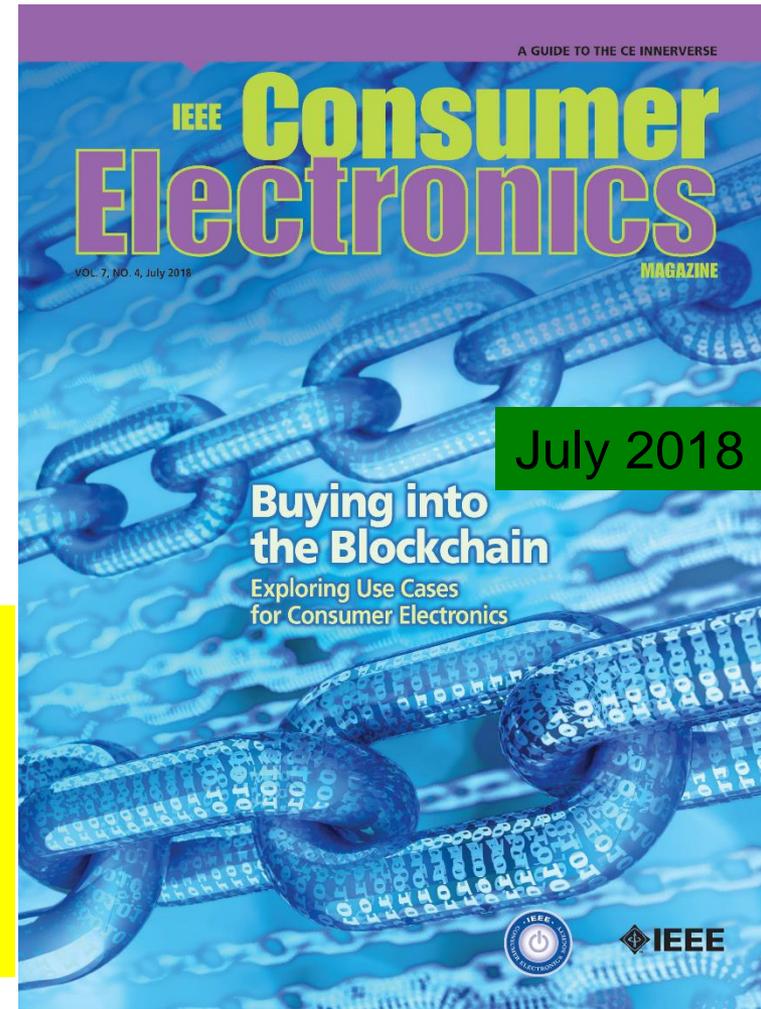
UAV Security – Energy and Latency Constraints

SYSTEM FAILURE

Source: http://politicalblindspot.com/u-s-drone-hacked-and-hijacked-with-ease/

Smart Electronic Systems Laboratory (SESL)
UNT EST. 1890 DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING College of Engineering

Blockchain – Energy Issue

Scalability

High Latency

Blockchain Challenges

Fake Block Generation

Energy Consumption
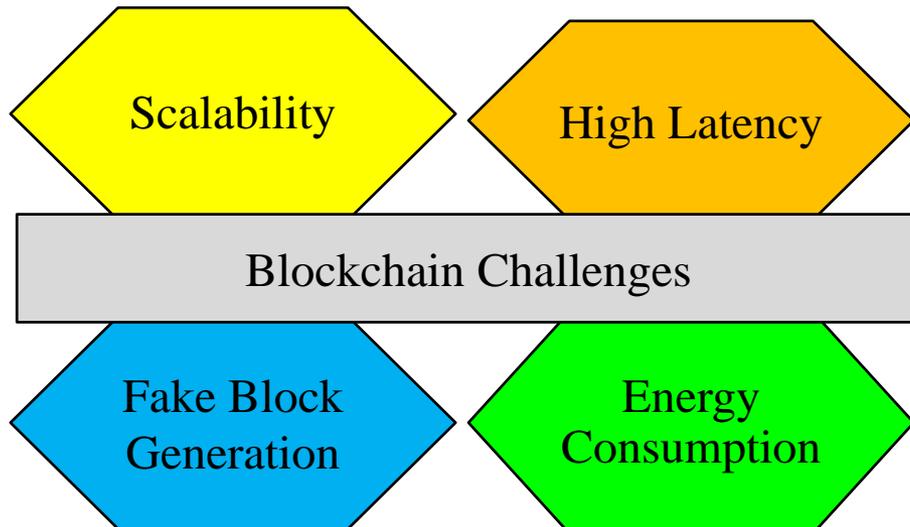
Source: Mohanty 2018, CE Magazine July 2018

A GUIDE TO THE CE INNERVERSE

IEEE **Consumer Electronics** MAGAZINE

VOL. 7, NO. 4, July 2018

July 2018

Buying into the Blockchain
Exploring Use Cases for Consumer Electronics

➢Energy for mining of 1 bitcoin → 2 years consumption of a US household.

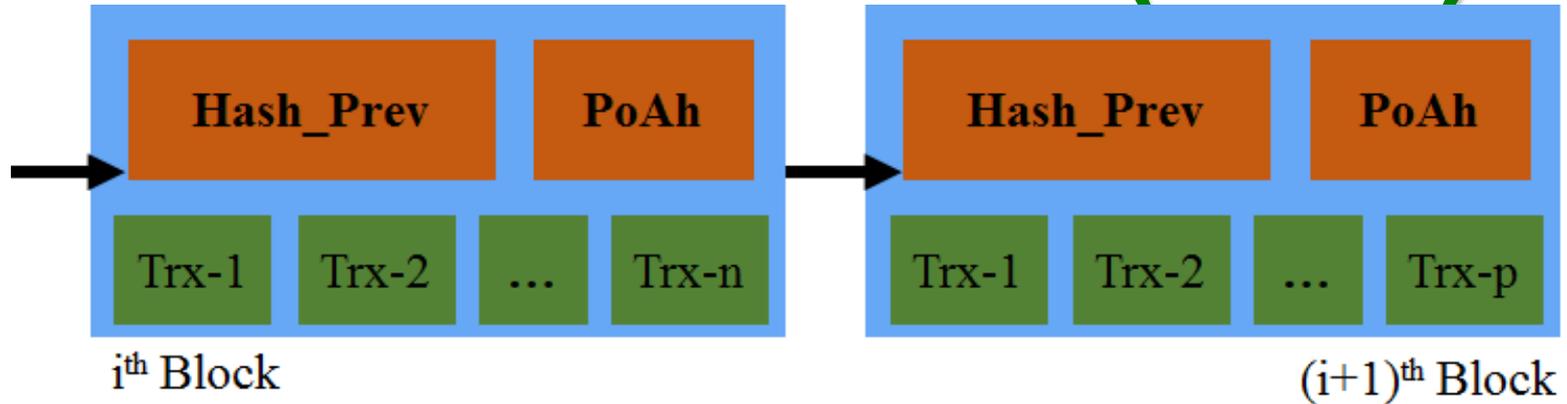➢Energy consumption for each bitcoin transaction → 80,000X of energy consumption of a credit card processing.

Source: N. Popper, "There is Nothing Virtual About Bitcoin's Energy Appetite", The New York Times, 21st Jan 2018, https://www.nytimes.com/2018/01/21/technology/bitcoin-mining-energy-consumption.html.

ICCE 2019 Panel -- Prof./Dr. Saraju P. Mohanty

Smart Electronic Systems Laboratory (SESL)
UNT DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING College of Engineering
EST. 1890

IoT-Friendly Blockchain – Proof-of-Authentication (PoAh)

Cloud

Edge Devices

Fog

Edge

Blockchain

Prev-Hash	PoAh

Trx-1	Trx-2	...	Trx-p

Blockchain

Prev-Hash	PoAh

Trx-1	Trx-2	...	Trx-p

Private/Permissioned Blockchain with Trusted or partially-trusted nodes

Hash	PoAh
T1	T2	T3

Hash	PoAh
T1	T2	T3

Hash	PoAh
T1	T2	T3

Hash	PoAh
T1	T2	T3

Hash	PoAh
T1	T2	T3

Hash	PoAh
T1	T2	T3

Hash	PoAh
T1	T2	T3

Hash	PoAh
T1	T2	T3

Hash	PoAh
T1	T2	T3

IoT

End Devices

Source: Puthal and Mohanty 2019, IEEE Potentials Jan 2019 and ICCE 2019

ICCE 2019 Panel -- Prof./Dr. Saraju P. Mohanty

Smart Electronic Systems Laboratory (SESL)

UNT EST. 1890 DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING College of Engineering

IoT-Friendly Blockchain – Proof-of-Authentication (PoAh)

	Proof-of-Work (PoW)	Proof-of-Stake (PoS)	Proof-of-Activity (PoA)	Proof-of-Authentication (PoAh)
Energy consumption	High	High	High	Low
Computation requirements	High	High	High	Low
Latency	High	High	High	Low
Search space	High	Low	NA	NA

PoW - 10 min in cloud	PoAh - 3 sec in Rasperry Pi	PoAh - 200X faster than PoW

Source: Puthal and Mohanty 2019, IEEE Potentials Jan 2019 and ICCE 2019

ICCE 2019 Panel -- Prof./Dr. Saraju P. Mohanty

Smart Electronic Systems Laboratory (SESL)

IoMT Security – A PUF a Device Authentication

End Devices

Edge Router

Internet

Local Area Network (LAN)

Cloud Services

Edge Servers

Remote Connection

Gateway

Doctor / Nurse Locally

Doctor/ Nurse Remotely
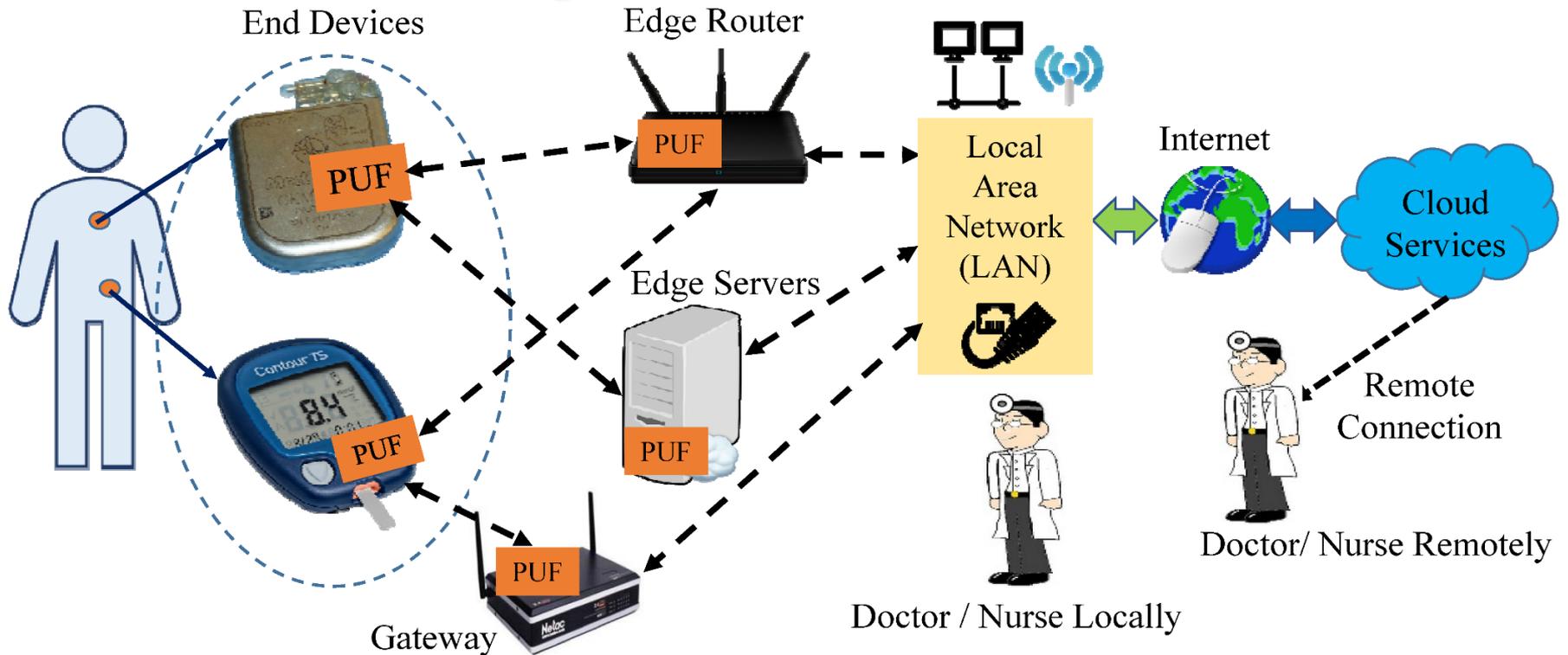
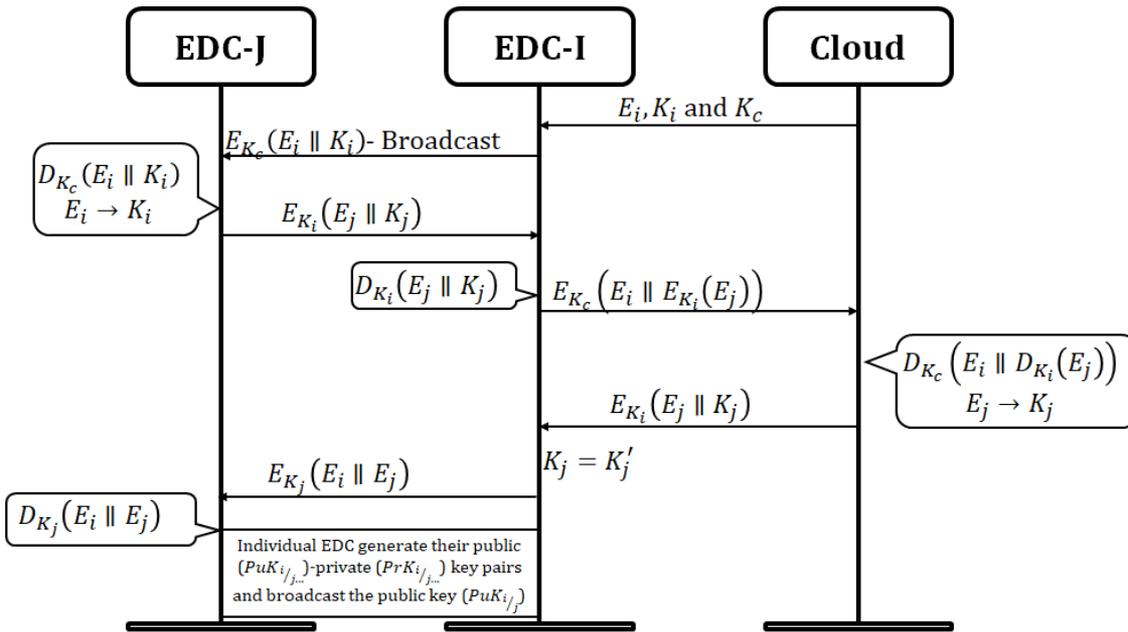| Proposed Approach Characteristics	Value (in a FPGA / Raspberry Pi platform)
Time to Generate the Key at Server	800 ms
Time to Generate the Key at IoMT Device	800 ms
Time to Authenticate the Device	1.2 sec - 1.5 sec

Source: Mohanty 2019, IEEE TCE Under Preparation

Smart Electronic Systems Laboratory (SESL)

Secure Edge Datacenter

Algorithm 1. Load Balancing Technique

1. If (EDC-I is overloaded)
2. EDC-I broadcast (E_i, L_i)
3. EDC-J (neighbor EDC) verifies:
4. If (E_i is in database) & ($p \leq 0.6$ & $L_i << (n-m)$)
5.   Response $E_{Kpu_i}(E_j||K_j||p)$
6. EDC-I perform $D_{Kpr_i}(E_j||K_j||p)$
7. $k_j' \leftarrow E_j$
8. If ($k_j' = k_j$)
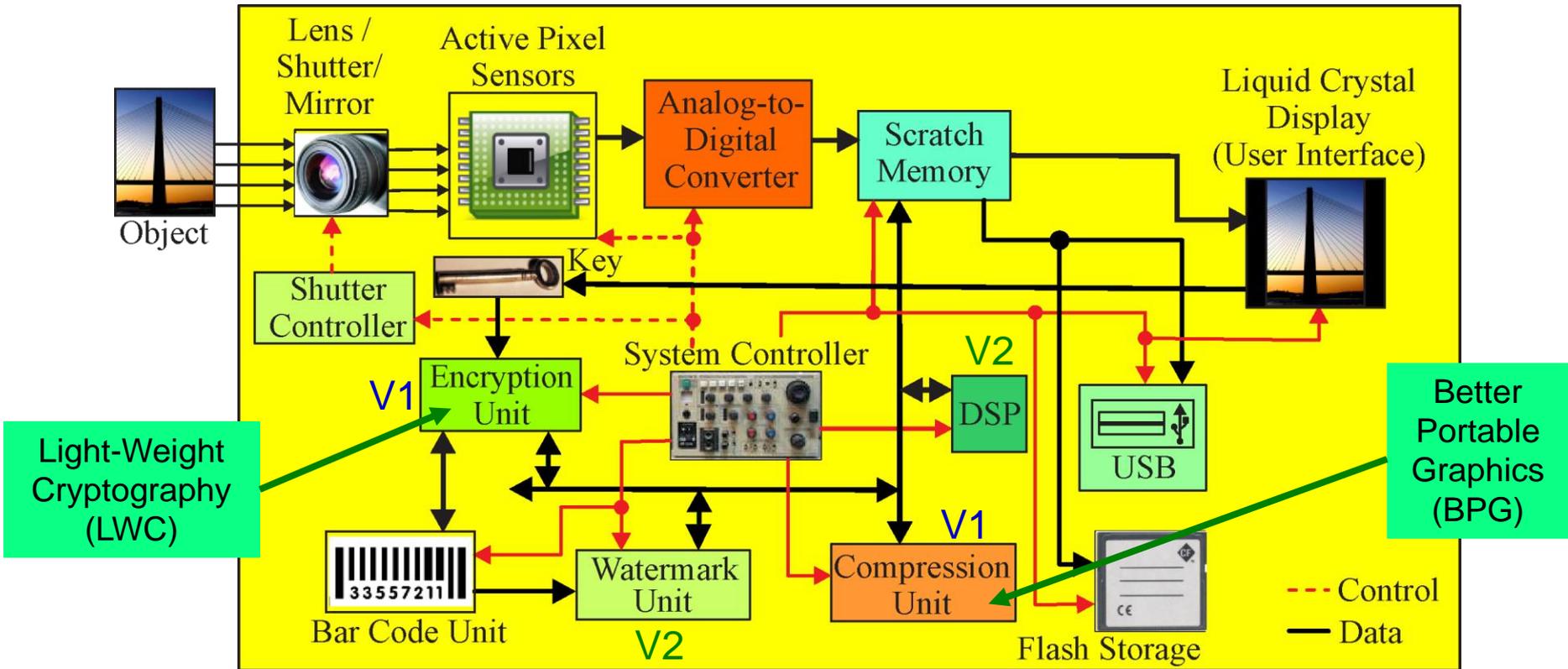9.   EDC-I select EDC-J for load balancing.

Secure edge datacenter –
➢ Balances load among the EDCs
➢ Authenticates EDCs

Response time of the destination EDC has reduced by 20-30 % using the proposed allocation approach.

Source: Puthal, Mohanty 2018, IEEE Communications Magazine May 2018

Smart Electronic Systems Laboratory (SESL)

ESR-Smart – End-Device Optimization

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

Source: Mohanty 2006, TCAS-II May 2006; Mohanty 2009, JSA Oct 2009; Mohanty 2016, Access 2016

ICCE 2019 Panel -- Prof./Dr. Saraju P. Mohanty

Thank You !!!

Slides Available at: http://www.smohanty.org

Hardwares are the drivers of the civilization, even softwares need them.