Cyber Physical Systems Security Limitations, Issues and Future Trends

American University of Beirut

Cybersecurity Research Group

Cybersecurity Research Group

Professor Ali Chehab

Associate Professor Rouwaida Kanj

Research Scientist and Lecturer Dr. Hassan Noura

Biography: Rouwaida Kanj

<u>2012-present</u>
American University of Beirut (Lebanon), Associate Professor of Electrical and Computer Engineering

<u>Research Interests and Projects:</u> *Advanced algorithmic research and smart Analytics for Design for reliability and yield, Machine learning for VLSI, Smart Grid Security, and Medical Devices.*

<u>2004-2012</u>
IBM Austin Research Labs, Research Staff Member

<u>1998-2004</u>
UIUC (PhD 2004, MSc 2000)
SOI Circuit Design Styles and High-Level Circuit Modeling Techniques, *Adviser: Prof. Elyse Rosenbaum (recipient of 3 IBM PhD fellowships)*
High Level Design Exploration and Optimization, *Adviser: Prof. Farid Najm (now @ UToronto)*

<u>1994-1998</u>
American University of Beirut, (BEng, 1998)

<u>Awards:</u> *holder of 6 invention plateau awards, outstanding technical achievement award, 3 best paper awards*

A Glimpse on Cyber Physical Systems

Rapidly Changing World

- World's population is growing: 7 billion and counting
- Resource consumption is increasing dramatically: Annual per capita energy consumption at about 20 MWh/year
- At the same time, advances in the communication and computation infrastructures are happening at a fast rate
- ***<u>Need to leverage advances in science and technology to help us influence the world for better sustainability and growth</u>***

http://bit.ly/LNCPS-2014

ztrela.com/images/nnc.png

https://grist.org/population/2011-05-03-world-population-projected-to-hit-7-billion-on-oct-31-says-un/

Cybernetics: Science for Military Purposes

- During WWII, Norbert Wiener pioneered technology for the “automatic aiming and firing of anti-aircraft guns”
- The term ***“Cybernetics”*** was coined by Wiener who had significant impact on control theory

"cybernetics" = kybernetes (greek)= Pilot

Amazon.com

- Although he had no computers, the principles involved are similar to those used today in a huge variety of computer-based feedback control systems
- Considered as the beginnings for Cyber Physical Systems

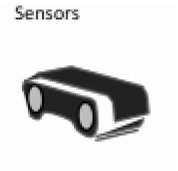
Lee and Seshia, *Introduction to Embedded Systems - A Cyber-Physical Systems Approach*, LeeSeshia.org, 2011

Cyber Physical Systems

- Introduced in 2006 by Helen Gill at the National Science Foundation

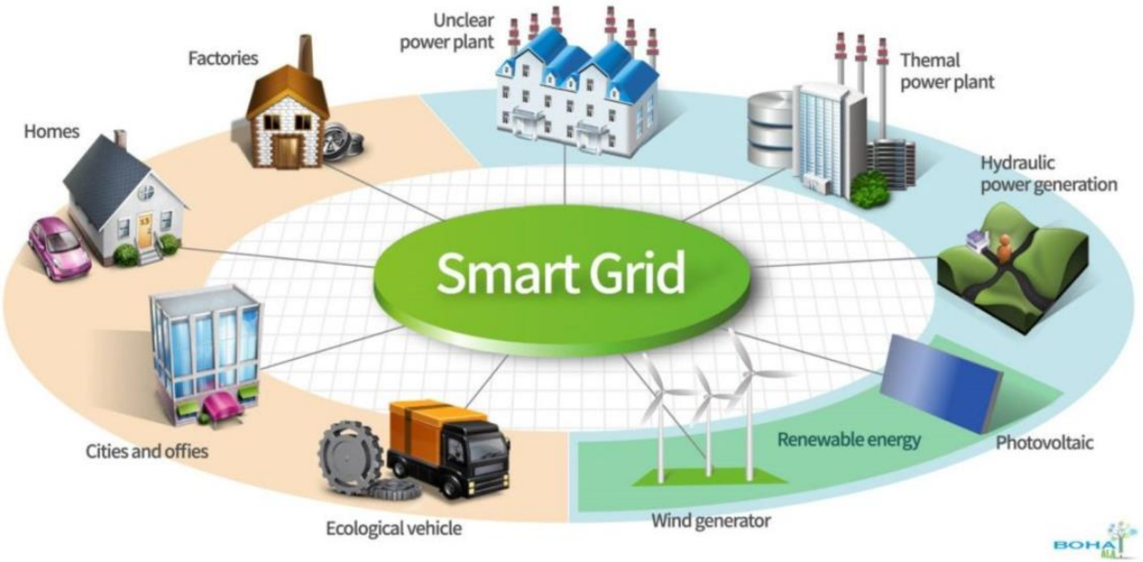
- CPS is about the integration of ***physical*** $\cap$ ***cyber*** for enhanced control and operation
    - **Cyber components =** computation and communication

    - **Physical components =** sensing and actuation



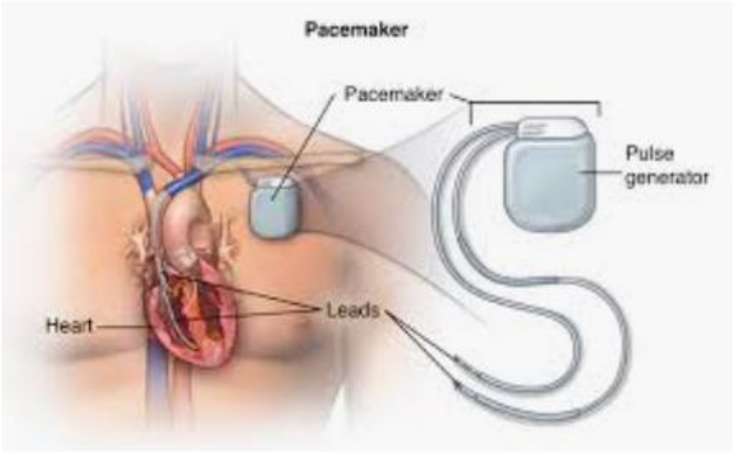
- It's all about understanding the ***joint dynamics*** of computers, software, networks, and physical processes

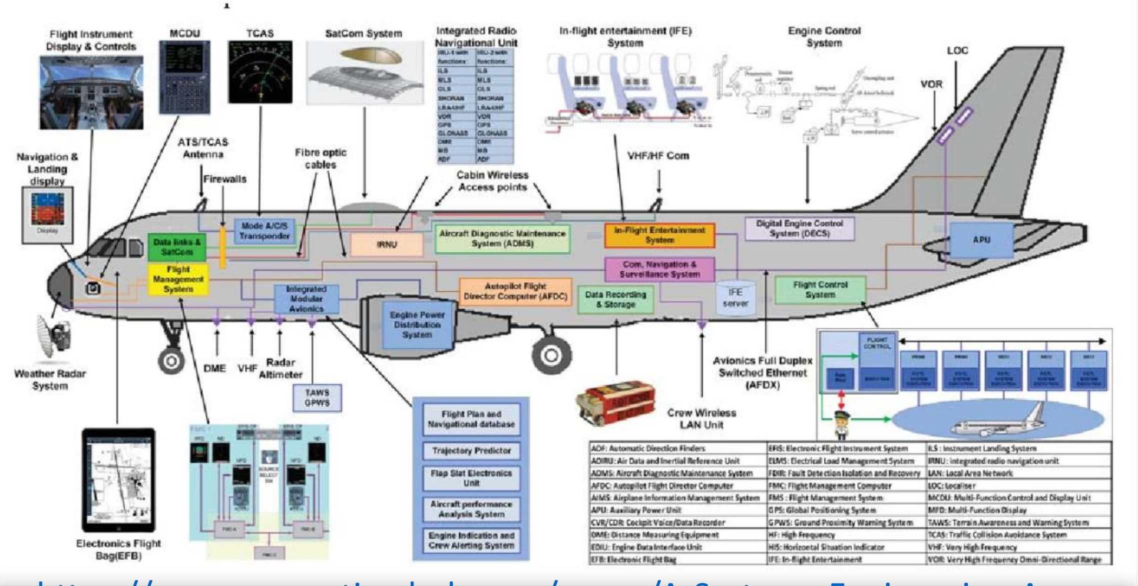
Lee and Seshia, *Introduction to Embedded Systems - A Cyber-Physical Systems Approach*, LeeSeshia.org, 2011



https://ecowarriorprincess.net/2019/11/smart-grid-technology-us-sustainability-social-justice/

http://bit.ly/LNCPS-2014





https://www.hackensackumc.org/wellness/health-information/article/adult-diseases-and-conditions-v0/overview-of-pacemakers-and-implantable-cardioverter-defibrillators-icds/

https://www.semanticscholar.org/paper/A-Systems-Engineering-Approach-To-Appraise-Risks-Of-Bogoda-Mo/1e54a67a176a1cbcf62b6ff35f8699d817f58307

CPS applications

- CPS affects various aspects in people's way of life and enables a wider range of services and applicat
- Cyber-physical systen
  - Industrial automatio
  - Vehicular systems (e driving),
  - Transportation syste s, etc.),
  - Medical systems (e.g ion, remote surgery)
  - Power systems (e.g.: nd and supply)
  - Smart cities, building cess)

"Entire planet as a single, massive Cyber-Physical System"

Cyber Physical Systems (CPSs)

- Heterogeneous and require novel methods and tools to function
- Operate in a ***dynamic environment***
- ***Adaptation*** and ***self-learning*** are necessary features to ensure reliable and fault tolerant operation
- ***Control critical infrastructures***
- **Therefore, they entail incredibly *high security requirements***

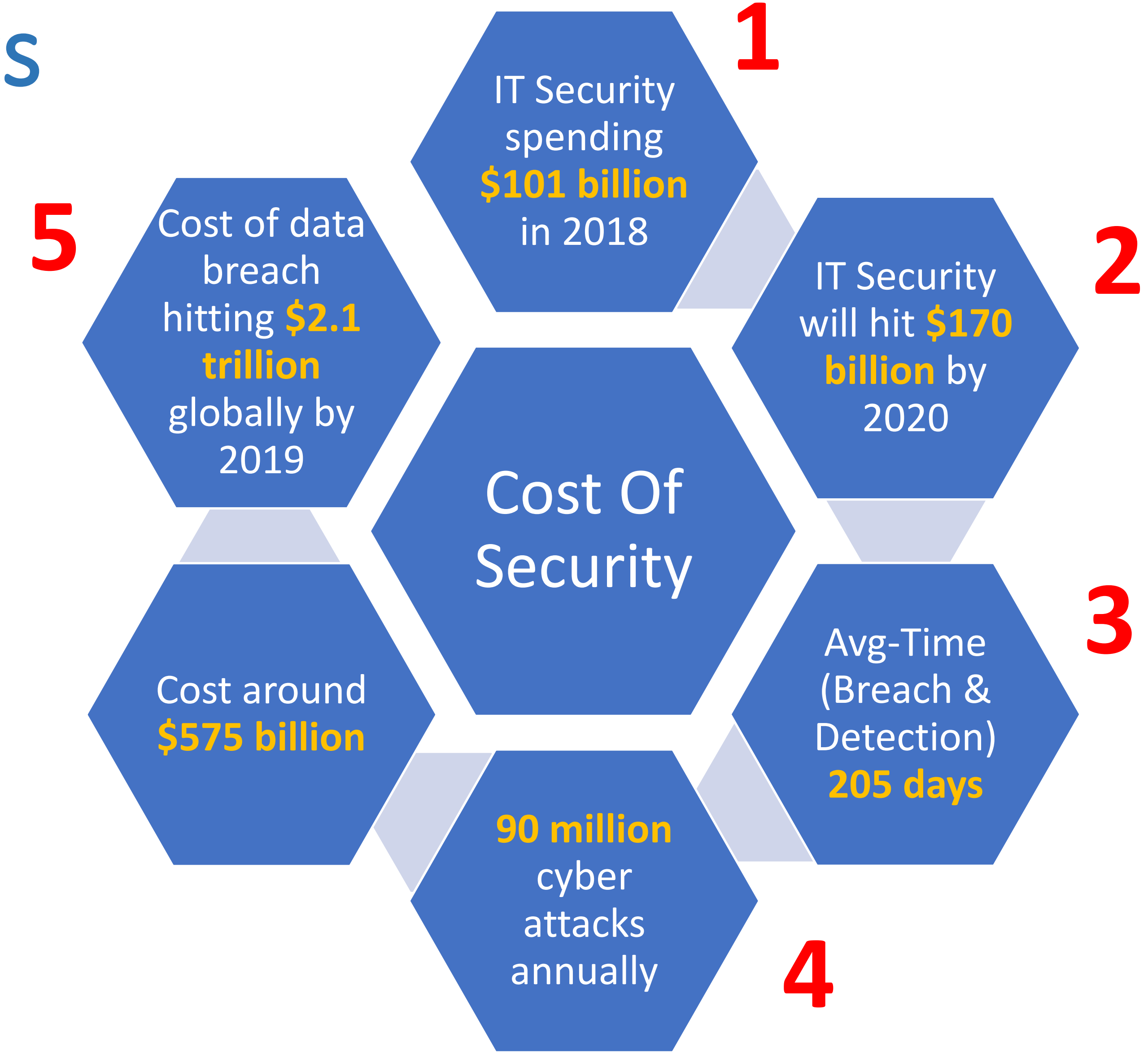
http://www.cerbero-h2020.eu/cpsweek2018-tutorial/

Risks of Complex Cyber Physical Systems

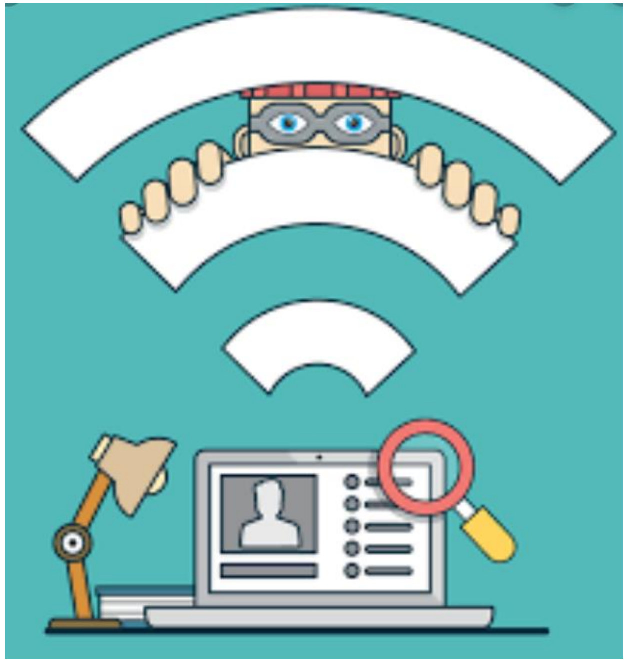
- CPSs are subject to serious risks
- The use of complex cyber-physical systems in today's airplanes has redefined "*the aerospace cybersecurity paradigm*"
- There is a need to
  - Mitigate or prevent cyber attacks on communication and navigation systems
  - Enhance passengers' safety

https://www.semanticscholar.org/paper/A-Systems-Engineering-Approach-To-Appraise-Risks-Of-Bogoda-Mo/1e54a67a176a1cbcf62b6ff35f8699d817f58307

Security Costs



Too much to Gain, Too much at stake!



https://whatismyipaddress.com/wireless-hacking

Let’s connect the dots…

https://www.tap.io/app/2176

Outline

1. CPS – Background
- CPS Layers
- CPS Use & Classification
- CPS Components

2. CPS Security Alert
- CPS Threats
- CPS Vulnerabilities
- CPS Attacks
- CPS Challenges

3. CPS Security Measures
- CPS Risk Management
- Cryptographic Solutions
- Non-Cryptographic Solutions

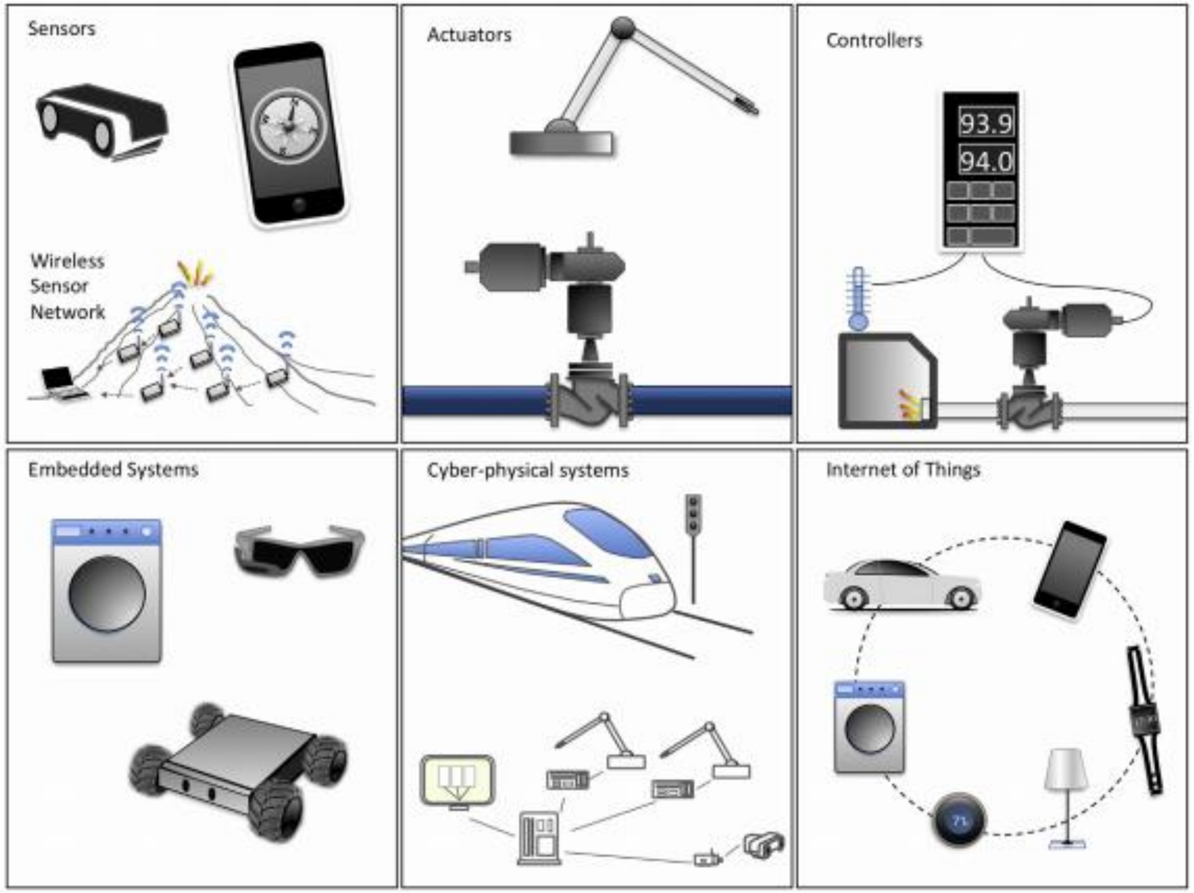
4. Lessons Learnt

5. Trending: Cyber Security and AI

Introduction

- Cyber-Physical Systems include:
  - Real-time, embedded and/or transactional services systems
  - Possible communication between system components
- Cyber and physical processes collaborate with each other to often form a distributed system
  - Increases the overall complexity of the resulting architecture over traditional real-time, embedded or services systems
- Cyber-physical systems include physical or virtual environments where people live, work and play that are instrumented and controlled by some form of computer system

Cyber-physical systems vs Internet of Things



- **Sensors**: gather information
- **Actuators**: initiate a physical action
- **Controllers**: monitor and adjust operating conditions of dynamical systems
- **Embedded Systems**: small computers with dedicated functions
- **Cyber-physical system**: computation, communications and physical processes depend on each other
- **Internet of Things**: computing paradigm where objects are intelligent and networked

[1], Loukas, G., 2015. *Cyber-physical attacks: A growing invisible threat*. Butterworth-Heinemann.

CPS-Background: CPS and the 4th Industrial Revolution

"industry 4.0 is the trend towards automation and data exchange in manufacturing technologies and processes" https://en.wikipedia.org/wiki/Industry_4.0

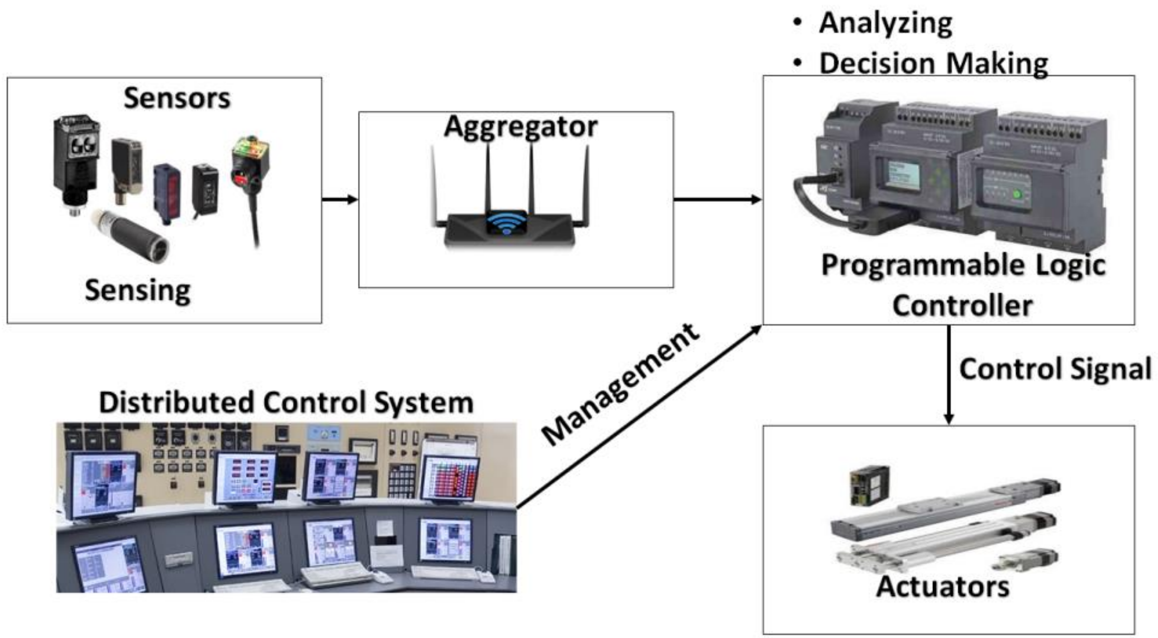
CPS supposed to play a key role in Industry v4.0.

CPS enables smart applications and services to operate accurately and in real-time.

CPS and Industry v4.0 offer a significant economic potential: the German gross value will be boosted by a cumulative of 267 billion euros by 2025

Cyber and physical systems are integrated: monitor, collect and exchange data and sensitive information in a real-time manner.

CPS Central Components



CPS can **sense the surrounding environment**, with the ability to **adapt and control the physical world**.

This is mainly attributed to their flexibility and capability to change the operation of system(s) process(es) through the use of real-time computing.

Sensors: record real-world data and make them available to other network nodes.

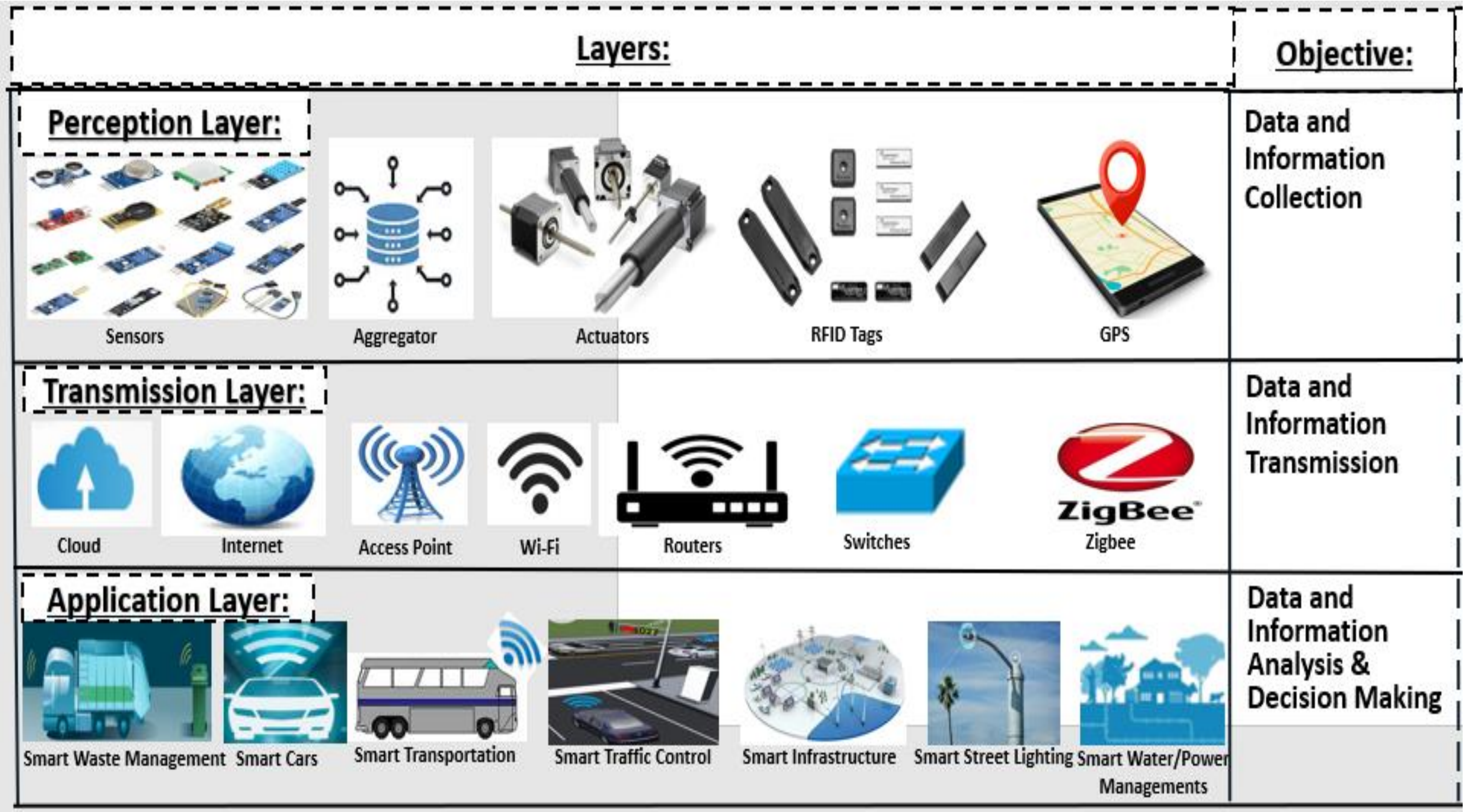
Aggregators: receive and process the sensed data before issuing the corresponding decisions.

Actuators: make the decisions made visible to the surrounding environment.

Programmable Logic Controllers: classified as industrial digital computers that control the manufacturing processes including robotic devices or fault diagnosis processes.

Distributed Control Systems: are computerized control systems that allow autonomous controllers to be distributed throughout the system with a central operator supervisory control.

CPS Layers


Layers:
Objective:
Perception Layer:
Sensors
Aggregator
Actuators
RFID Tags
GPS
Data and Information Collection
Transmission Layer:
Cloud
Internet
Access Point
Wi-Fi
Routers
Switches
ZigBee
Zigbee
Data and Information Transmission
Application Layer:
Smart Waste Management
Smart Cars
Smart Transportation
Smart Traffic Control
Smart Infrastructure
Smart Street Lighting
Smart Water/Power Managements
Data and Information Analysis & Decision Making

1. CPS – Background

- CPS Layers
- CPS Use & Classification
- CPS Components

2. CPS Security Alert

- CPS Threats
- CPS Vulnerabilities
- CPS Attacks
- CPS Challenges

3. CPS Security Measures

- CPS Risk Management
- Cryptographic Solutions
- Non-Cryptographic Solutions

4. Lessons Learnt

5. Trending: Cyber Security and AI

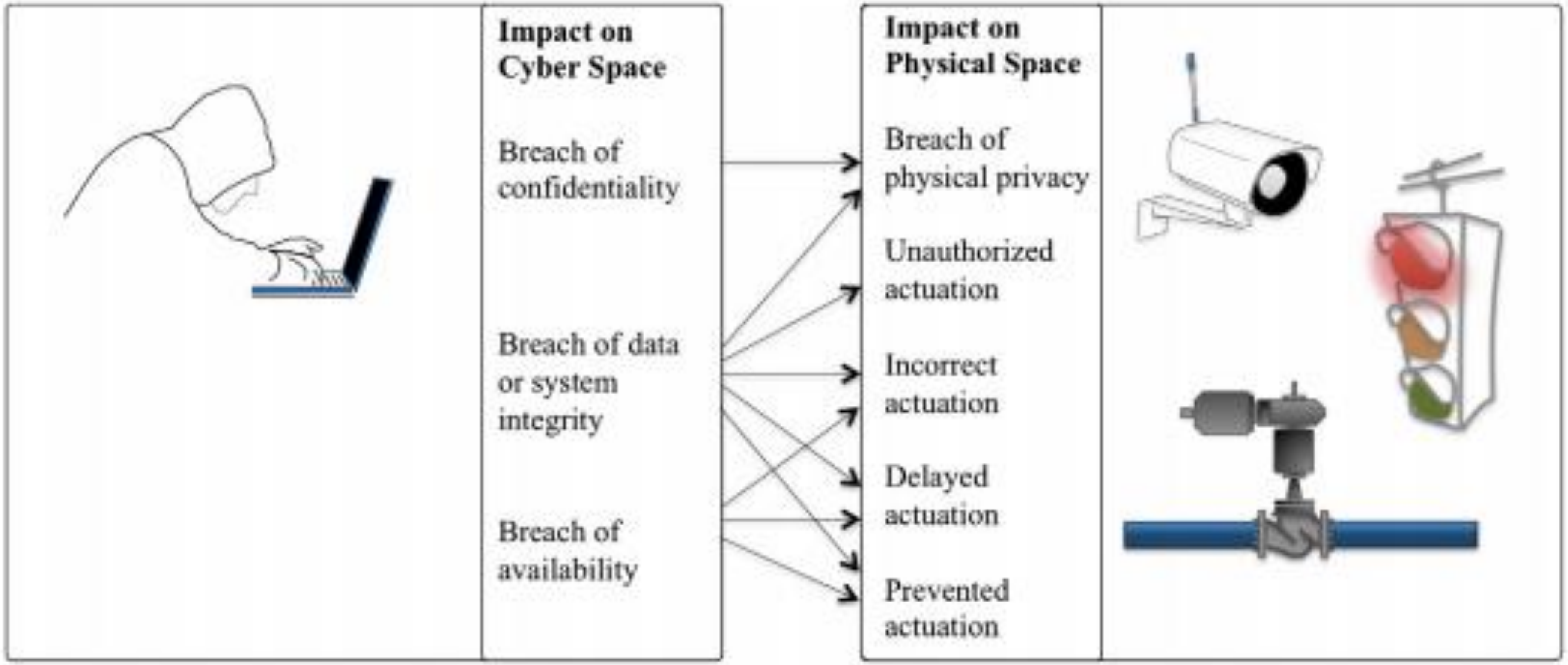
CPS Layers and Associated Attack Vectors

Layers:	Objective:	Threat/Attack:	Target:	Security Measure:
Perception Layer:  Sensors, Aggregator, Actuators, RFID Tags, GPS	Data and Information Collection	• Eavesdropping • Port Scan • Passive Replay	• Confidentiality • Privacy • Authentication	• Trust Management • Source Authentication • Secure Data/Systems • Data Protection
Transmission Layer:  Cloud, Internet, Access Point, Wi-Fi, Routers, Switches, Zigbee	Data and Information Transmission	• Man-in-the-Middle • Meet-in-the-Middle • DoS/ D-DoS • Repudiation • Replay –	• Confidentiality • Integrity • Availability • Authentication	• Strong Password Policy • Strong Authentication • Lightweight Dynamic Symmetric Encryption • Secure Tunnelling
Application Layer:  Smart Waste Management, Smart Cars, Smart Transportation, Smart Traffic Control, Smart Infrastructure, Smart Street Lighting, Smart Water/Power Managements	Data and Information Analysis & Decision Making	• Malicious Code Injection • Botnets - malware • Trojans • Worms • Buffer Overflow	• Privacy • Security • Safety • Authentication	• IDS/IPS • Firewalls • Strong Authentication • Strong Authorisation • Trust Management

Cyber-physical attacks

- Cyber-physical attacks can be characterized by their impact in cyberspace and the corresponding impact in physical space.

[1], Loukas, G., 2015. *Cyber-physical attacks: A growing invisible threat*. Butterworth-Heinemann.



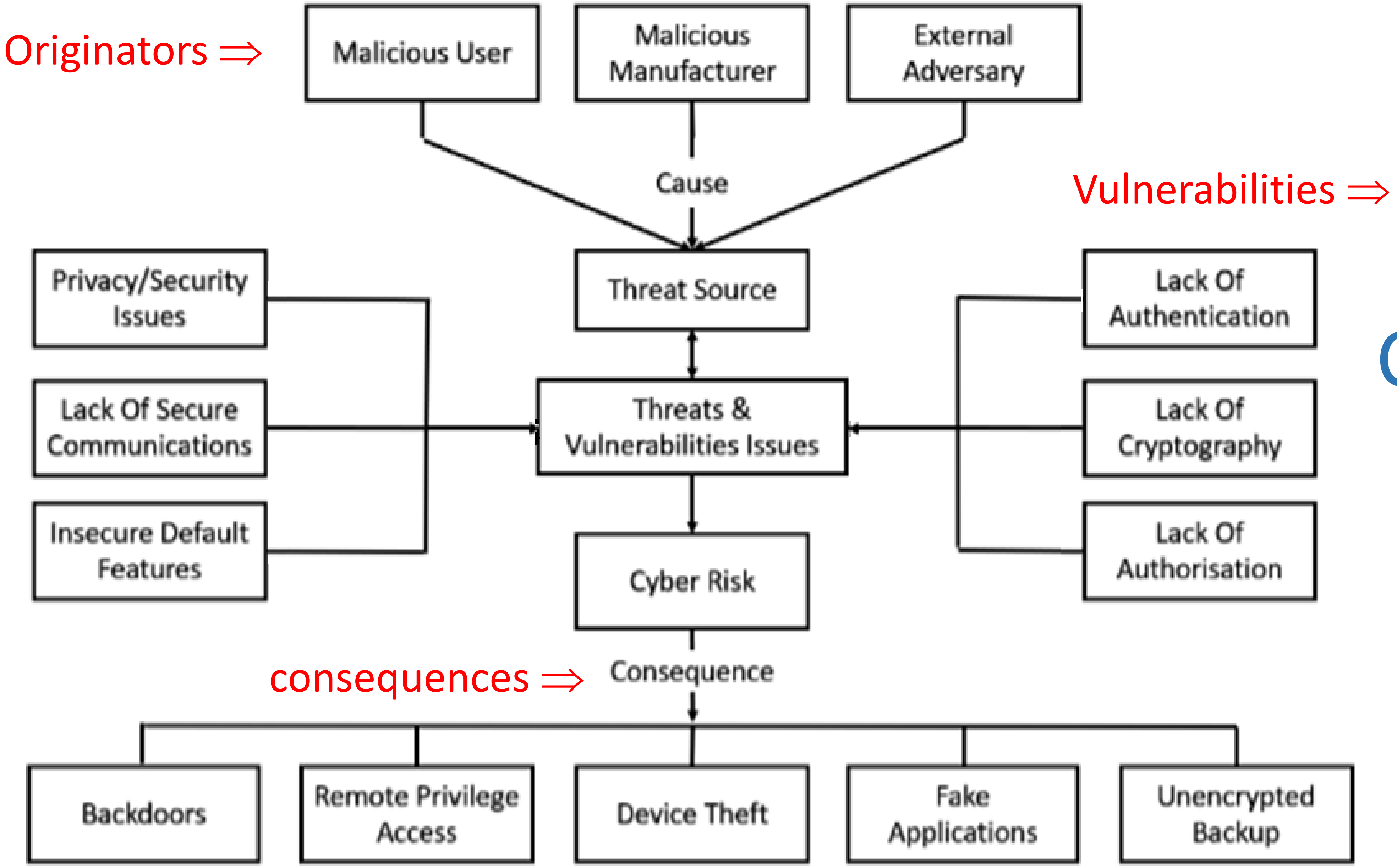
Cyber-physical attacks

- **Breach of physical privacy**
  - Confidentiality of people’s real-time blood sugar level
  - The number of occupants in a house
  - Other private information collected from sensors
- **Unauthorized actuation**
  - Unauthorized user initiates actuation by breaching the integrity of a computer system that controls an actuator
- **Incorrect actuation**
  - The adversary aims to affect an actuator’s operation by breaching the integrity or availability of the instructions sent to it, the sensor data on which it relies, or its controller’s operation
  - Example: an attack that would consistently lower the speed values reported by a car’s sensors, so as to cause its cruise control system to keep accelerating.

Cyber-physical attacks

- **Delayed actuation**
  - The adversary delays actuation by breaching the integrity or availability of the data and systems involved. Suppression of warnings can also be included in this category
  - Example: denial of service attack to delay measurements on dangerous pressures to be reported to a gas pipeline’s safety valve controllers
- **Prevented actuation**
  - The adversary blocks actuation altogether by breaching the integrity or availability of the data and systems involved
  - **EX-1**: Sleep deprivation attack that exhausts the battery of a surveillance robot or a medical implant until it can no longer function
  - **EX-2**: Malware infection that suppresses the operation of a car window by injecting a “close” command every time an “open” command is received.

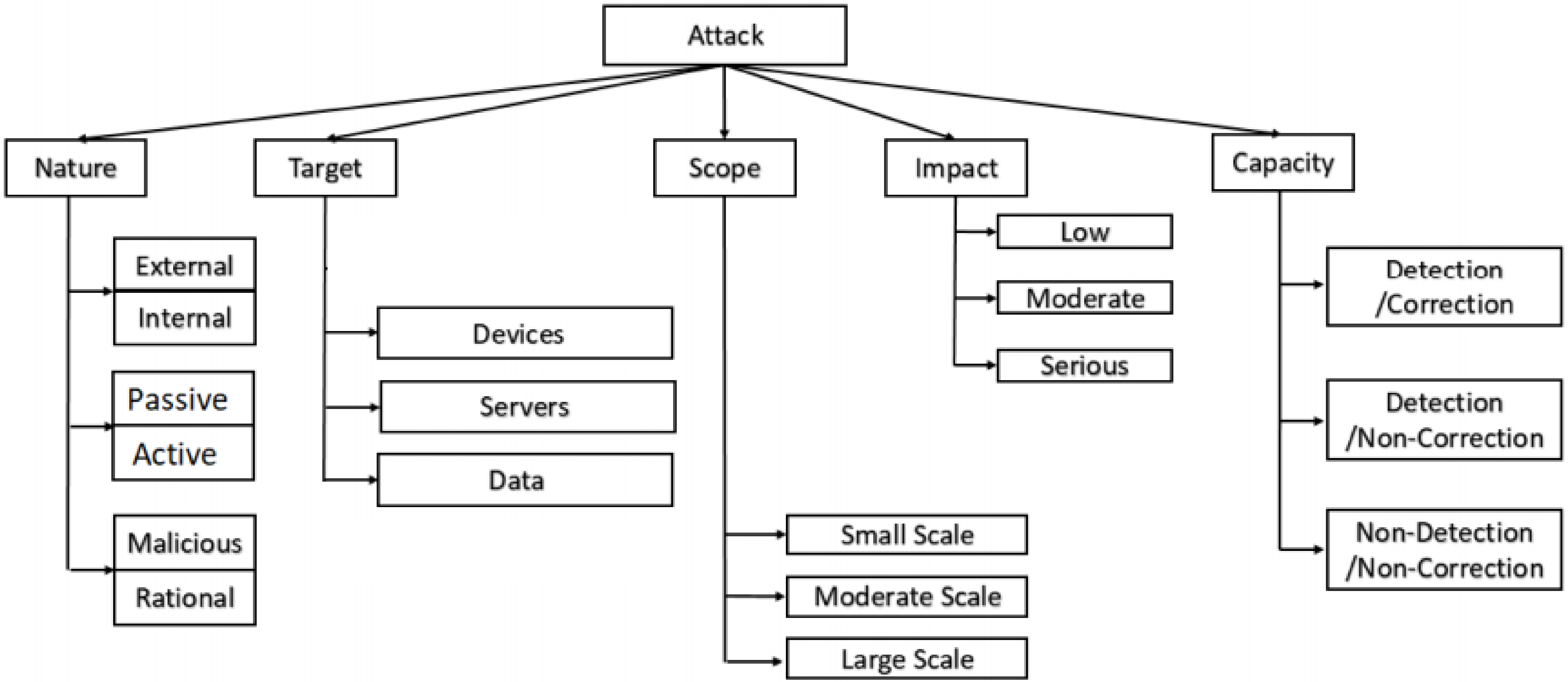
CPS Risks



Originators ⇒
Malicious User
Malicious Manufacturer
External Adversary
Cause
Vulnerabilities ⇒
Threat Source
Privacy/Security Issues
Lack Of Secure Communications
Insecure Default Features
Threats & Vulnerabilities Issues
Lack Of Authentication
Lack Of Cryptography
Lack Of Authorisation
Cyber Risk
consequences ⇒
Consequence
Backdoors
Remote Privilege Access
Device Theft
Fake Applications
Unencrypted Backup

Attackers Profile

A cyber-physical attack is a security breach in cyberspace that adversely affects physical space



1. CPS – Background

- CPS Layers
- CPS Use & Classification
- CPS Components

2. CPS Security Alert

- CPS Threats
- CPS Vulnerabilities
- CPS Attacks
- CPS Challenges

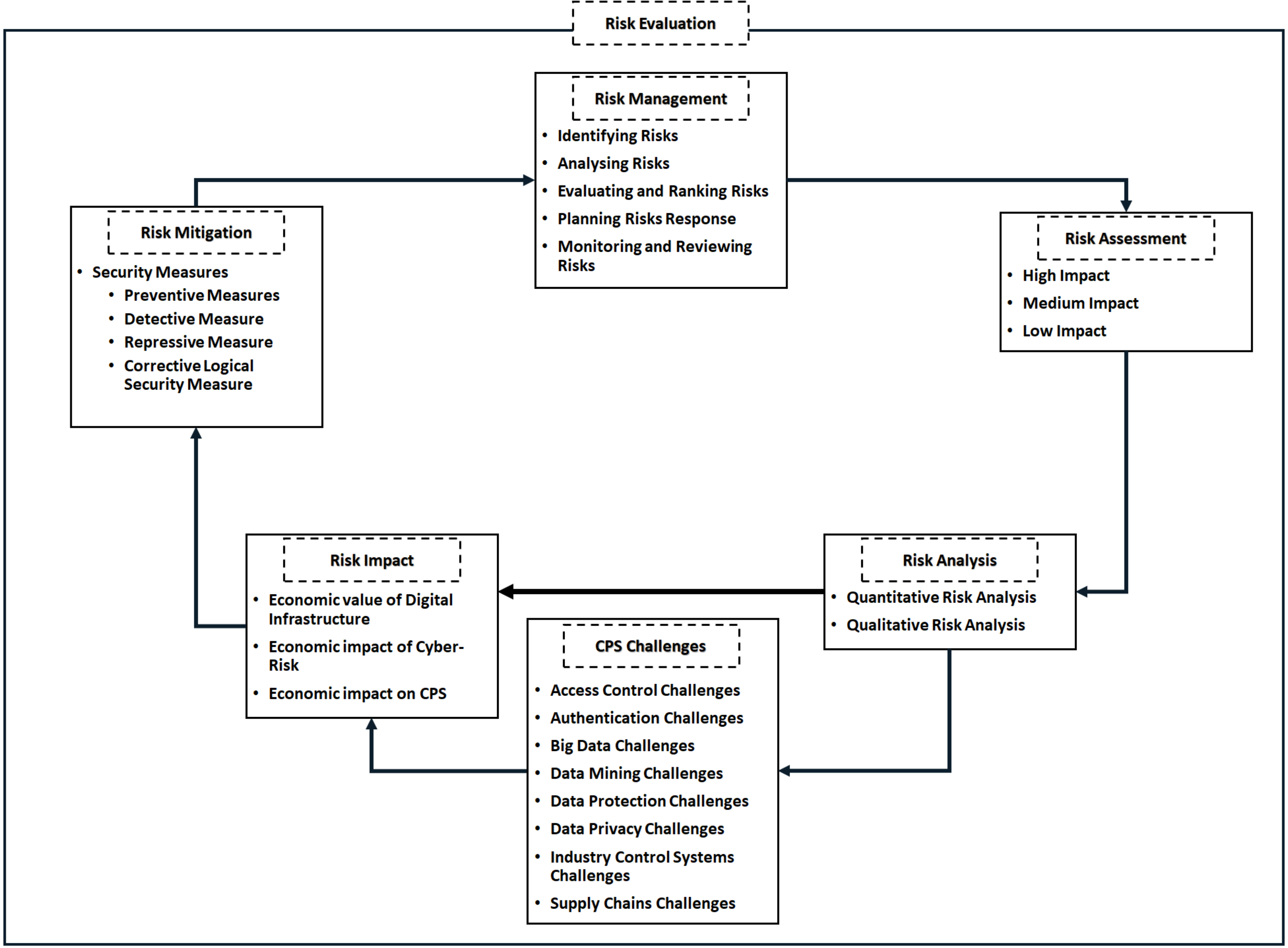
3. CPS Security Measures

- CPS Risk Management
- Cryptographic Solutions
- Non-Cryptographic Solutions

4. Lessons Learnt

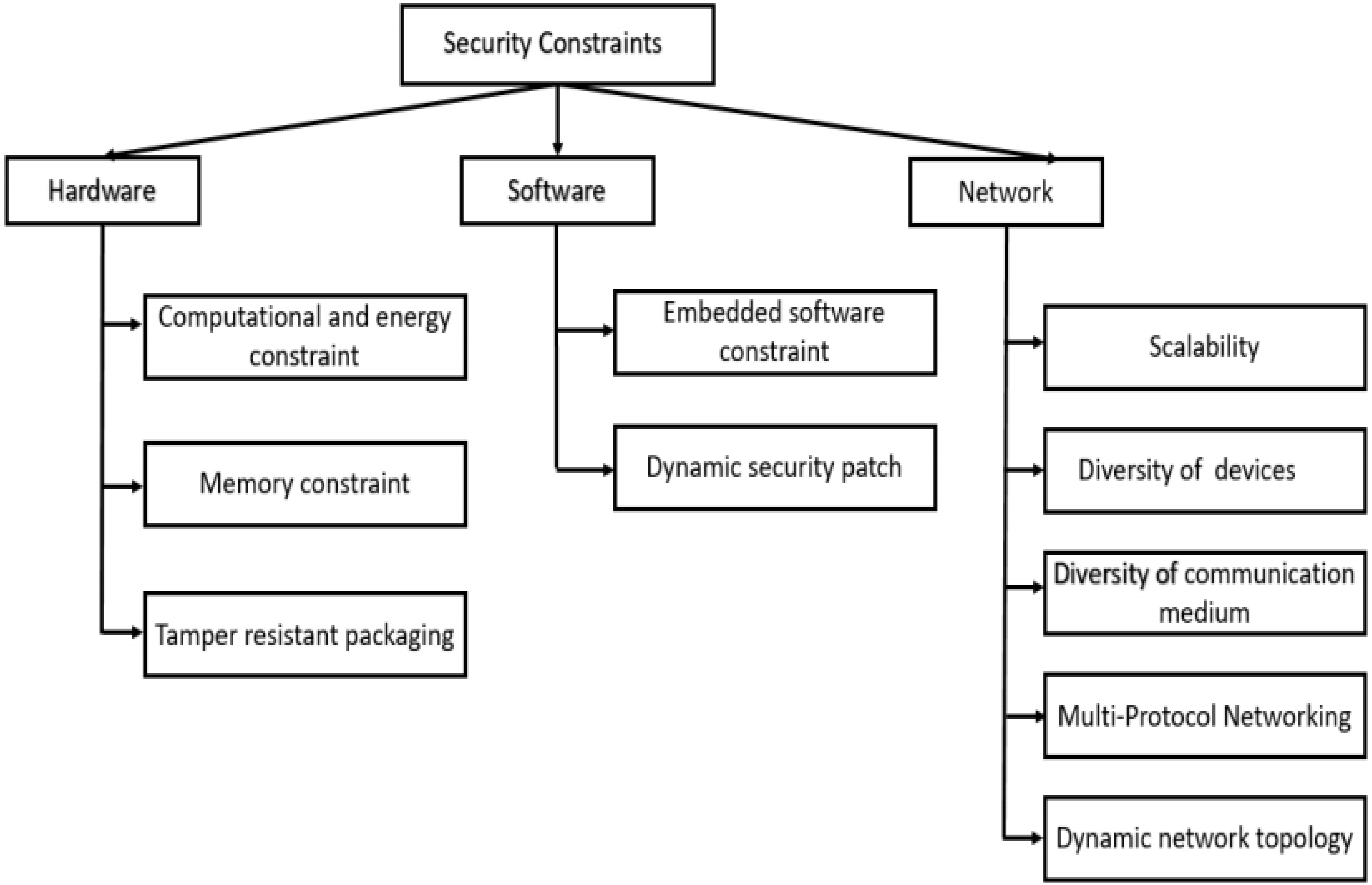
5. Trending: Cyber Security and AI

CPS Risk Management



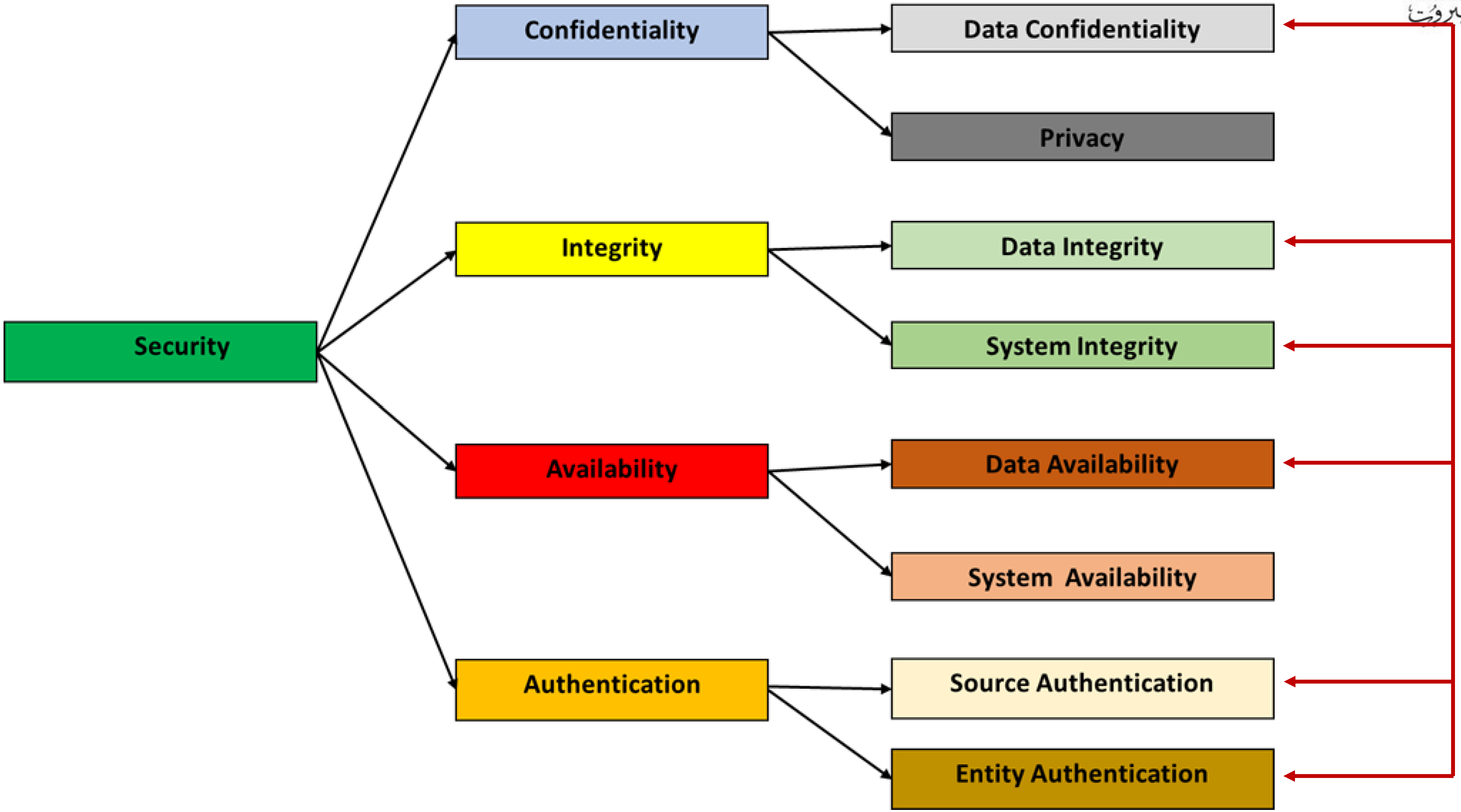
CPS Security Constraints and Challenges

There constraints that limit secure operations, and solutions must take these constraints into consideration



- **Authentication Challenges**
  - **Weak Authentication Practices**
  - **Single/Two Factor Authentication**
  - **Lack of Biometric Use**
- **Big Data Challenges**
  - **Huge Data Amount**
  - **Lack of Real-Time Processing**
  - **Lack of Accountability**
  - **Lack of Real-Time Data Protection**
  - **Privacy Breaches**
  - **Trade-Off Issues**
- **Access Control Challenges**
  - **Single Sign On**
  - **Abuse of Privileges**
  - **Lack of Employee Screening**
  - **Access Control Issues**
- **Supply Chains Challenges**
  - **Real-Time Management Issues**
  - **Traffic Issues**
  - **Scheduling Issues**

Research Goals



The secret: is in how to generate secrets!

What is Cryptography (www.m-w.com)

cryptography noun

Save Word

cryp·tog·ra·phy | \ krip-ˈtä-grə-fē \

Definition of *cryptography*

1 : secret writing

2 : the enciphering and deciphering of messages in secret code or cipher
also : the computerized encoding and decoding of information

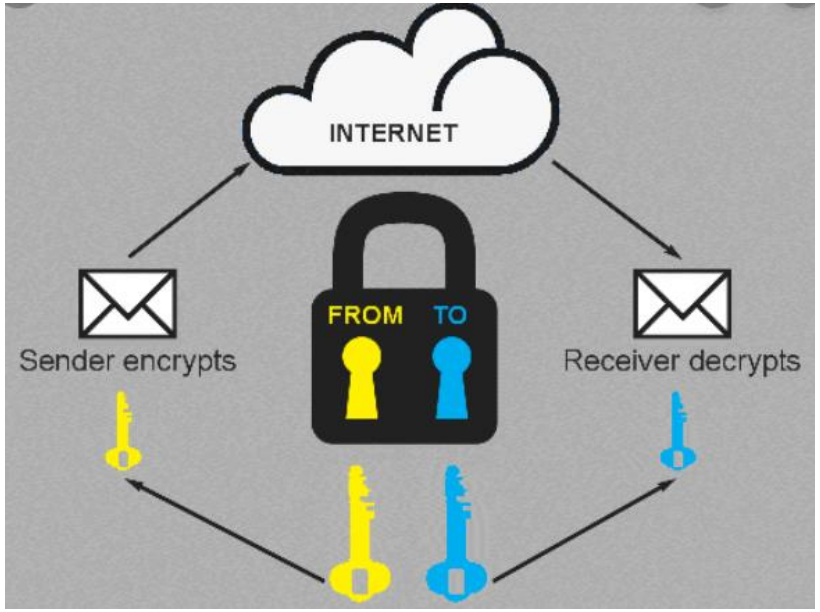
3 : CRYPTANALYSIS

Security Solutions: A bit more Technical

- Security Solutions
  - Cryptographic approach
    - Cryptographic Algorithms
    - Cryptographic Protocols
  - Non cryptographic approach
    - Logical Protection:
      - Intrusion Detection /Prevention System
      - Honeypot
      - Firewall
    - Physical Protection

Cryptographic Solutions (mainly data protection)

Encrypt = lock



Decrypt = unlock

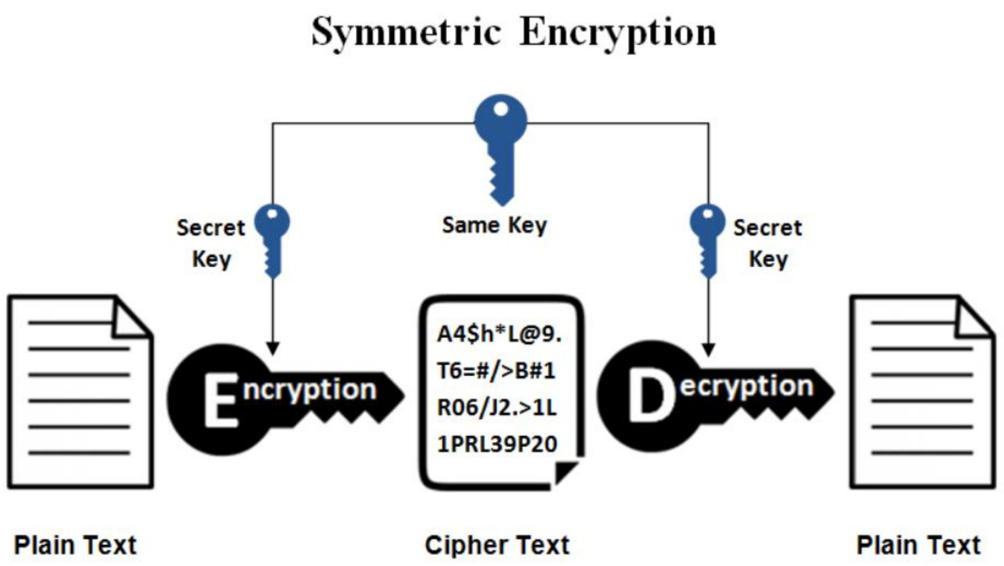
Key = password

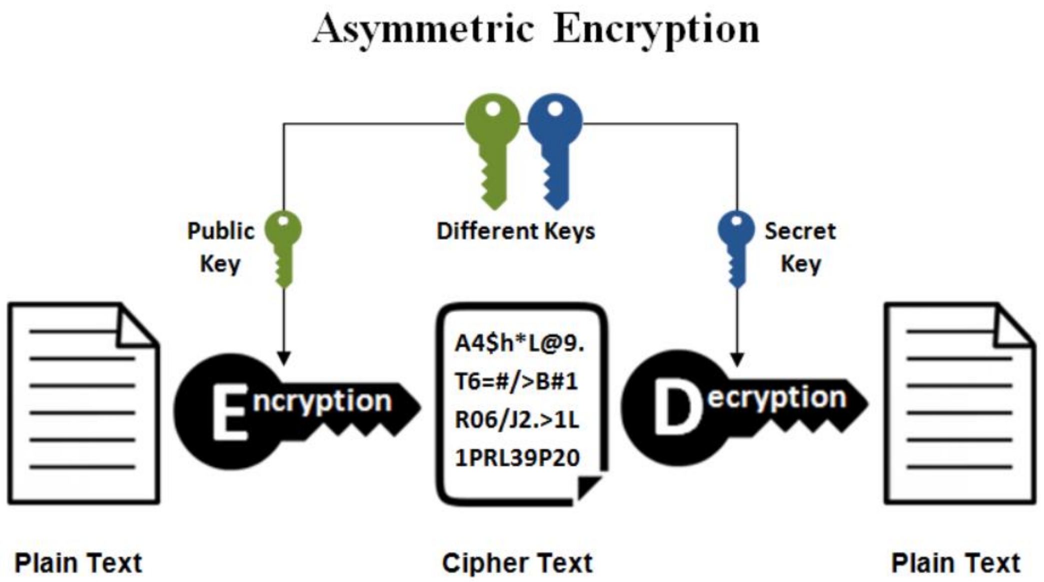
Encryption = Algorithm + Key

Algorithm: Known to all

Key: Secret

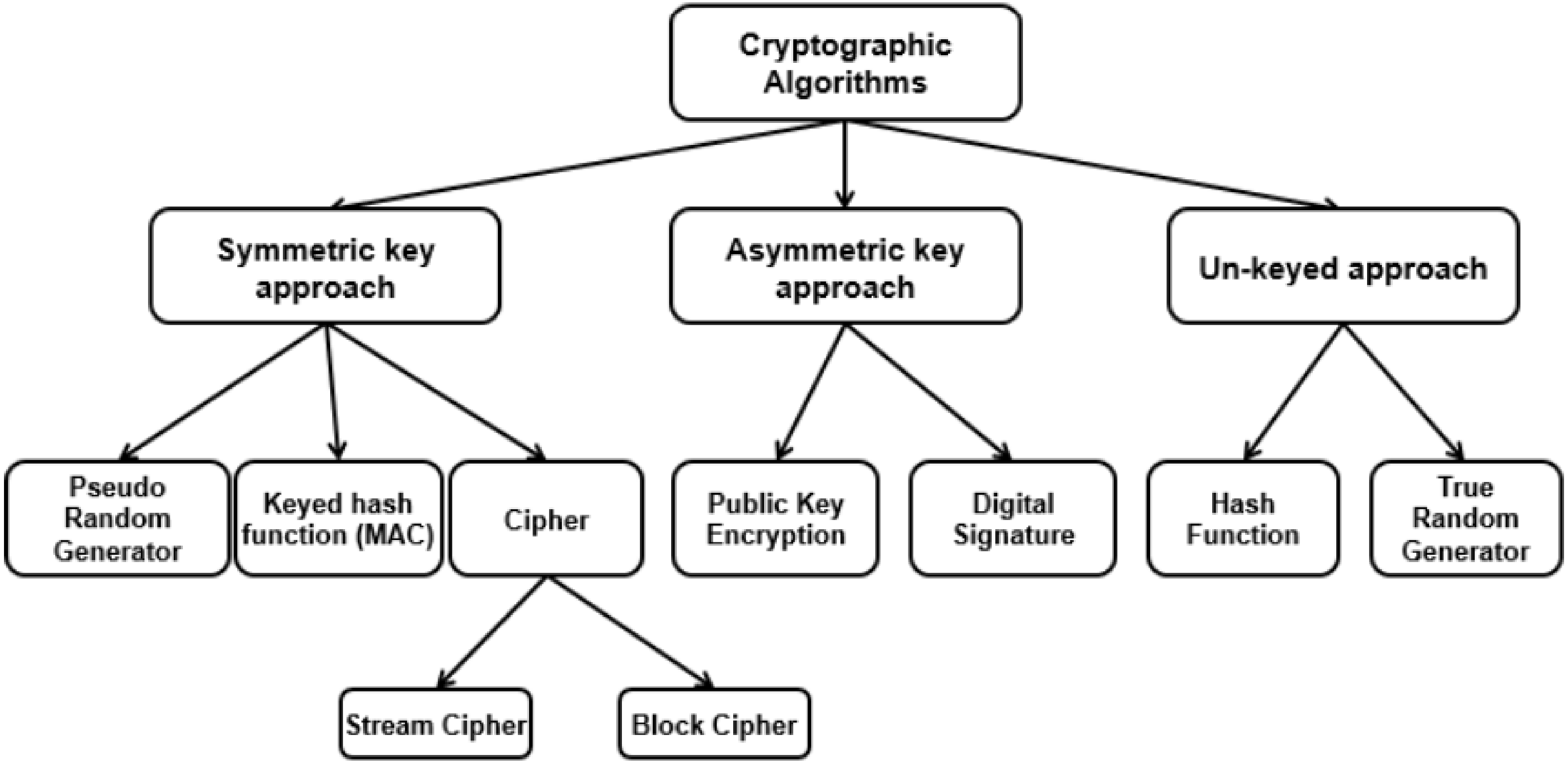
Cryptographic Solutions (mainly data protection)



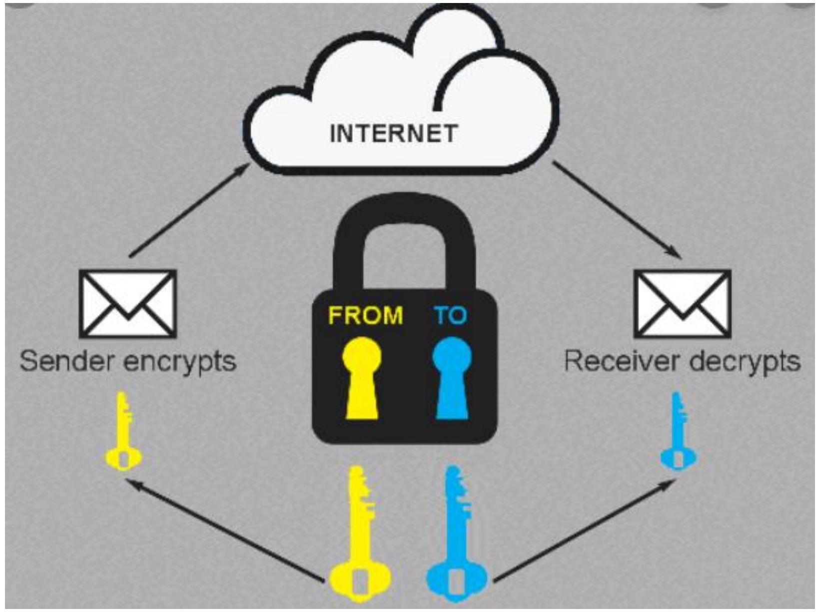


cipher: secret or disguised way of writing a code

Cryptographic Solutions (mainly data protection)



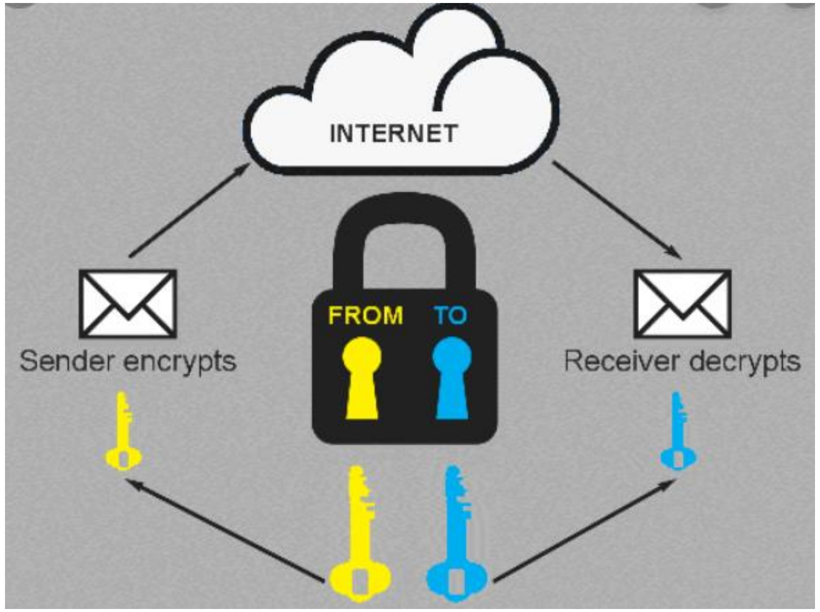
Cryptographic Solutions (mainly data protection)



Attackers Objectives:

1. Decrypt the message — Simpler
2. Recover Key — Tougher

Cryptographic Solutions (mainly data protection)



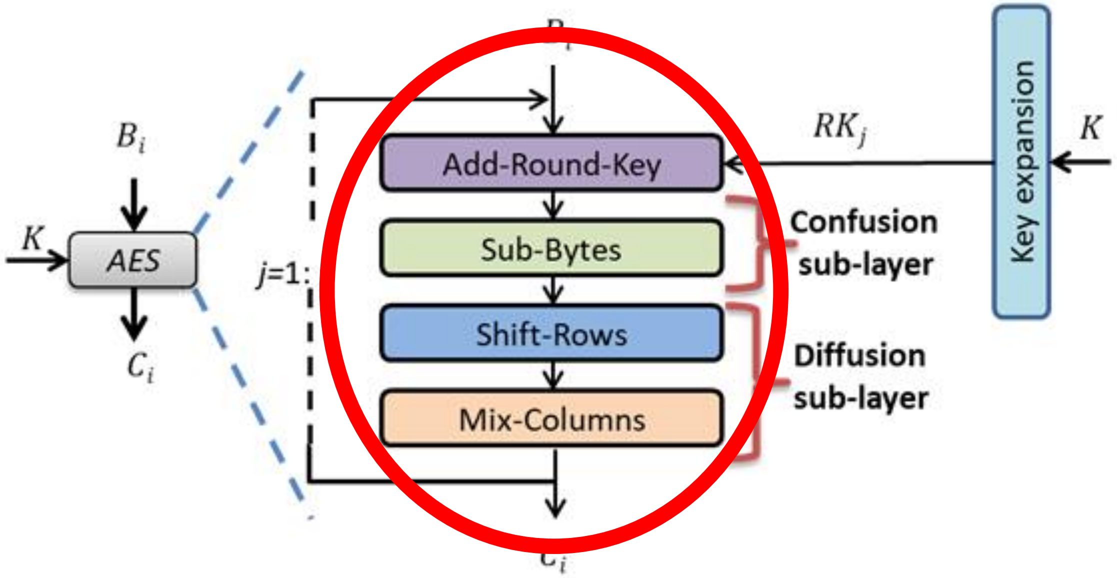
Attackers Objectives:
1. Decrypt the message
2. Recover Key

- Advanced technologies: attackers can break more codes
- Therefore we need
  1. Complex yet efficient encryption algorithms and
  2. Key generation and management systems

Security Solutions

- Typically, data confidentiality, data integrity, and data origin authentication are ensured by using symmetric cryptographic algorithms (require r rounds).

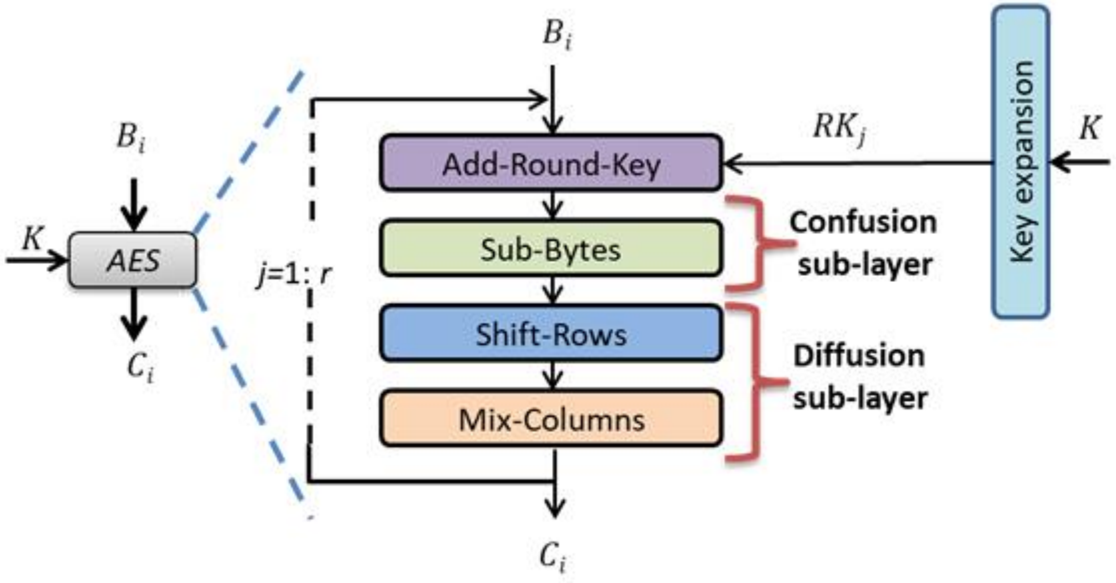
- AES for example
  - 4 primitives per round
  - Multiple rounds



|K|	*r*
128	10
196	12
256	14

Security Solutions

- Traditional solutions might have a negative impact on the CPS system performance:
  - Delay-sensitive and stringent QoS requirements
  - Devices with limited battery lifetime and limited computation

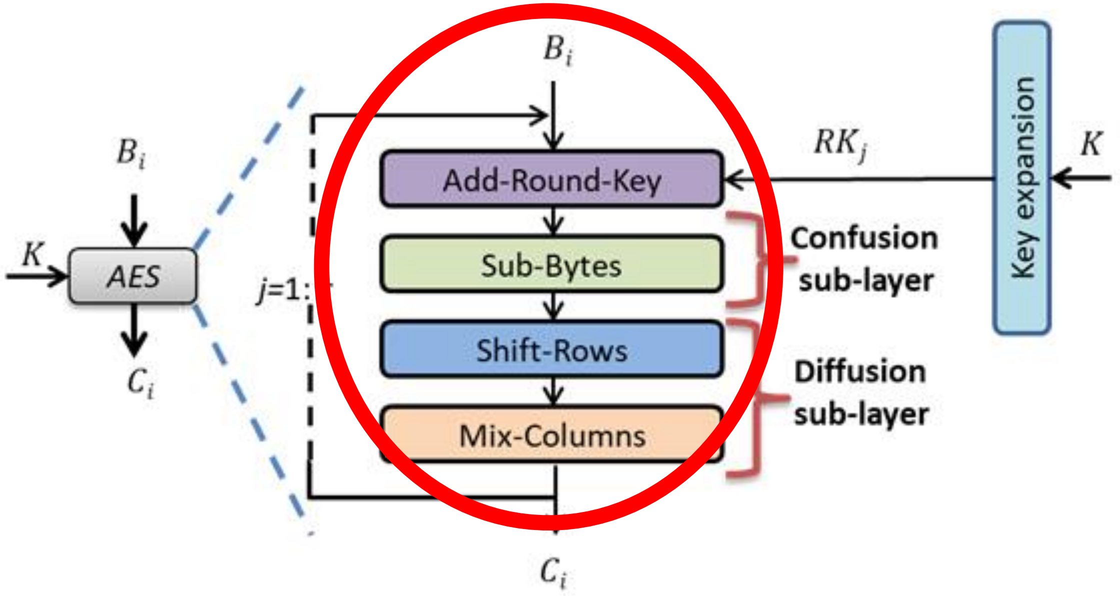


|K|	r
128	10
196	12
256	14

Security Solutions

- **Solution**: New lightweight symmetric cryptographic algorithms and protocols that use dynamic key-dependent cipher structure

- Introduce savings
  - **Round level**
  - **Number of Rounds**



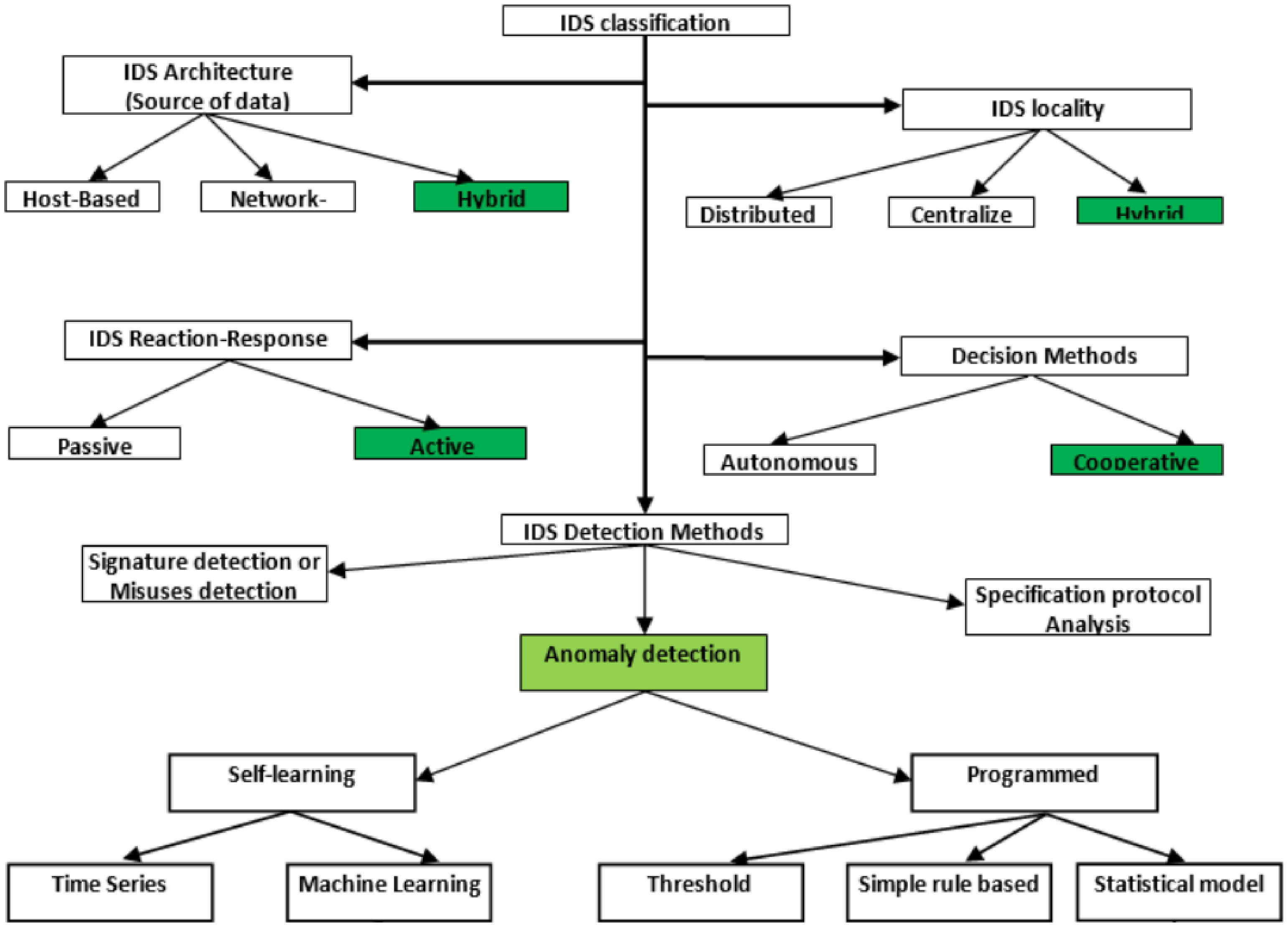
/K/	r
128	10
196	12
256	14

Future Work: Non-Cryptographic Solutions

- Cryptographic solutions need to be complemented with **non-cryptographic solutions**
- The latter **leverage AI to enable behavioral analysis of the network**
- The research group is currently **advancing the research** in the following areas

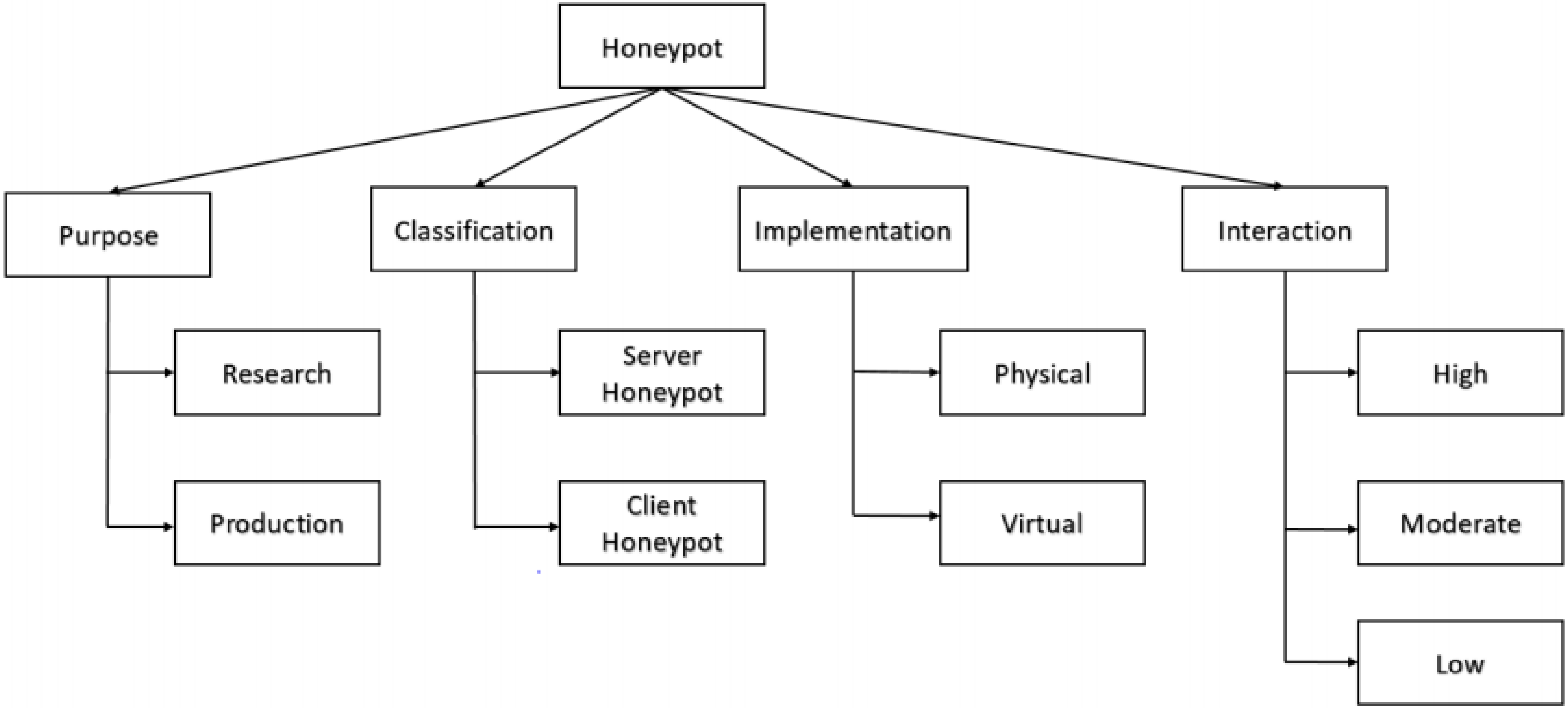
1. **IDS/IPS Systems**, based on either
    - Signature
    - Specification
    - **Anomaly detection**
    - Security Information and Event Management (SIEM) systems
2. **Honeypots and Deception techniques**

IDS Classification



Honeypot Classification

"a **decoy** system set up with deliberate weaknesses and a high profile to **attract attacks** for the purpose of analysis"



1. CPS – Background

- CPS Layers
- CPS Use & Classification
- CPS Components

2. CPS Security Alert

- CPS Threats
- CPS Vulnerabilities
- CPS Attacks
- CPS Challenges

3. CPS Security Measures

- CPS Risk Management
- Cryptographic Solutions
- Non-Cryptographic Solutions

4. Lessons Learnt

5. Trending: CyberSecurity and AI

Lessons learned

Maintaining Security Services: new lightweight cryptographic solutions to secure Cyber-Physical systems and IoCPT in real-time operations with minimum computational complexity.

Confidentiality: a new class of lightweight block or stream cipher algorithms to secure CPS resource-constrained real-time communications.

Protecting Digital Evidences: to overcome eliminating sources of evidence that trace back to the attack source, such as the case of Shamoon, Duqu, Flame and Stuxnet malware types.

Enforcing Compliance: respecting users' privacy by ensuring data access regulatory compliance, especially when stored by utility providers

Suggestions & Recommendations

Prevention Layer	

Authentication Sub-layer	• User/Device Authentication:
	  • Multi-factor Authentication
	  • Physical Protection
	  • Strong and Variable Password
	• Source Authentication and Message Integrity
	• Access Control

Privacy Sub-layer	• Patients Privacy • Anonymity (Pseudonymity) • Proxies VPN • Preserving Privacy at Cloud (Differential Privacy, Secret Sharing, Homomorphic Encryption)
Data Confidentiality Sub-layer	• Encryption Algorithm
Defensive Layer	
Detection Sub-layer	• Intrusion Detection Systems (Anti-malware) • SIEM • Honeypots • Data System Integrity
Correction Sub-layer	• Intrusion Prevention Systems • Firewalls • Data Backup • Alternative Devices and Configuration

1. CPS – Background

- CPS Layers
- CPS Use & Classification
- CPS Components

2. CPS Security Alert

- CPS Threats
- CPS Vulnerabilities
- CPS Attacks
- CPS Challenges

3. CPS Security Measures

- CPS Risk Management
- Cryptographic Solutions
- Non-Cryptographic Solutions

4. Lessons Learnt

5. Trending: Cyber Security and AI

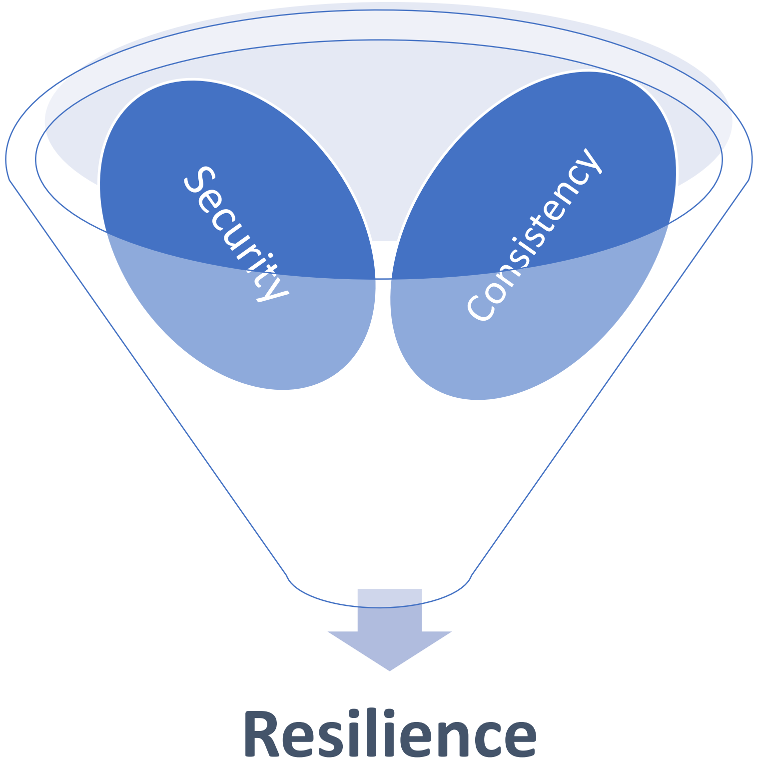
Cybersecurity and AI

1. AI for Network Resilience
2. IoT Device Identification
3. Abnormal Traffic Detection
4. Guarding against Traffic Analysis

1. AI for Network Resilience: Motivation

- There is no security without verifying network consistency

AI helps enforce security



AI helps guarantee security measures <u>don't affect proper functionality</u>

Proposed Architecture

- **Solution**: we propose a Neural Network overlay on top of Software Defined Networks (SDN)

Distributed Extraction + Distributed Processing + Centralized Management

- **Key Contributions**:
  - Edge Feature extraction
  - AI based overlay network over the data plane
  - Distributed processing over different nodes
  - Decision making at the data plane level
  - SDN Controller optimizes and monitors the distribution process

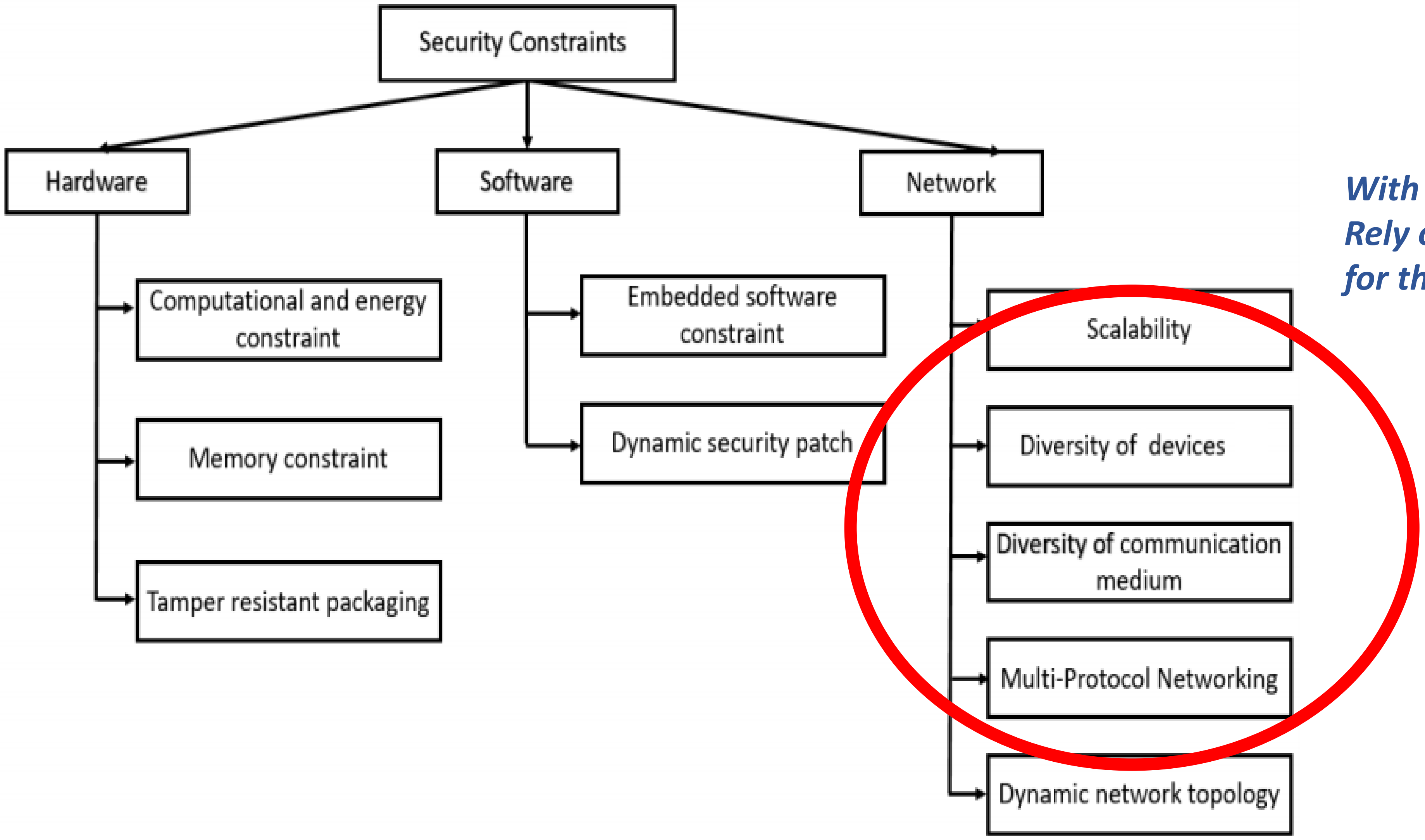
SDN: Security Results

Technique	Anomaly Detection (Balanced Data)	Anomaly Detection (Unbalanced Data)	Attack Identification (Balanced Data)	Attack Identification (Unbalanced Data)
Random Forest	99.2%	99.3%	98.3%	99.61%
SVM	96.74%	96.93%	90.64%	93.6%
KNN	94.5%	96.4%	90.19%	90.5%
DT	95.76%	96.4%	89.5%	90.89%
MLP	97.5%	97.0%	94.3%	92.73%
BPNN	98.7%	98.6%	77.2%	75.8%
DNN	96.11%	96.13%	95.03%	93.67%

SDN: Consistency Results

Technique	Accuracy	Precision	Recall	F1-score
ConvNet	**96%**	**96%**	**93%**	**90%**
RNN	96%	83.4%	78.3%	78.5%
DNN	95.5%	93%	81.6%	77.5%

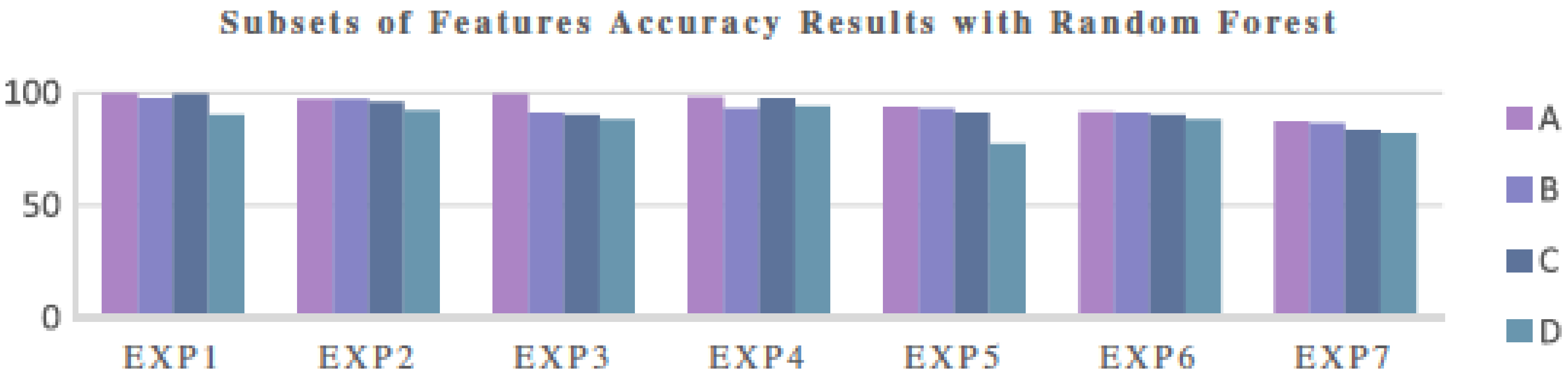
Flashback: CPS challenges



With IoT and IoCPS:
Rely on AI to classify malicious traffic for the variety of devices onboard

2. AI for IoT Traffic Classification (IoT Device Identification)

Model– Accuracy



AI for IoT Traffic Classification
Random Forest - Accuracy

	Accuracy	Precision	Recall	F1-score
RF	99.93%	0.999	0.999	0.9985
DT	99.85%	0.9977	0.9977	0.9977
RNN	99.77%	0.9965	0.9966	0.9965
ConvNet	99.78%	0.9971	0.9962	0.9966
ResNet	0.9978	0.997	0.9965	0.9967

3. AI for IoT Traffic Classification

Normal vs Attack Traffic - Accuracy

	Accuracy	Precision	Recall	F1-score
RF	***97.14%***	***0.8581***	***0.8628***	***0.8601***
DT	*96.28%*	*0.8299*	*0.8034*	*0.8157*
RNN	*95.35%*	*0.7925*	*0.9459*	*0.8469*
ConvNet	*95.16%*	*0.7872*	*0.9394*	*0.8410*
ResNet	*94.77%*	*0.7777*	*0.9533*	*0.8363*

This covered few of the interesting topics the group is tackling

Selected Contributions

- New lightweight symmetric cryptographic algorithms and protocols that use dynamic key-dependent cipher structure
    - Achieving required cryptographic performance with reduced latency and resources
    - Efficiency, flexibility and robustness make the proposed solutions good candidates IoT systems

    - *Noura, H.N., Salman, O., Chehab, A. and Couturier, R., "Preserving data security in distributed fog computing". Ad Hoc Networks, 94, 2019.*
    - *Noura, H.N., Salman, O., Chehab, A. and Couturier, R., " DistLog: A Distributed Logging Scheme for IoT Forensics". Ad Hoc Networks, 2019.*
    - *Melki, R., Noura, H.N. and Chehab, A., 2019. Lightweight multi-factor mutual authentication protocol for IoT devices. International Journal of Information Security, pp.1-16, 2019.*
    - *Noura, H.N., Chehab, A. and Couturier, R., "Efficient & secure cipher scheme with dynamic key-dependent mode of operation". Signal Processing: Image Communication, 78, 2019.*
    - *Noura, H.N., Melki, R., Chehab, A. and Mansour, M.M., "A Physical Encryption Scheme for Low-Power Wireless M2M Devices: a Dynamic Key Approach". Mobile Networks and Applications, 24(2), pp.447-463, 2019.*
    - *Noura, H.N., Chehab, A., Sleem, L., Noura, M., Couturier, R. and Mansour, M.M. One round cipher algorithm for multimedia IoT devices. Multimedia tools and applications, 77(14), pp.18383-18413, 2018.*
    - *Yaacoub, J.P.A., Noura, M., Noura, H.N., Salman, O., Yaacoub, E., Couturier, R. and Chehab, A.,. Securing internet of medical things systems: Limitations, issues and recommendations. Future Generation Computer Systems, 2019.*

- *Physical Unclonable functions and ID-based key distribution framework for smart grid security*

    - *Seferian, V., Kanj, R., Chehab, A. and Kayssi, A., 2017. Identity Based Key Distribution Framework for Link Layer Security of AMI Networks. IEEE Transactions on Smart Grid.*
    - *Seferian, V., Kanj, R., Chehab, A. and Kayssi, A., 2014, November. PUF and ID-based key distribution security framework for advanced metering infrastructures. In Smart grid communications (smartgridcomm), 2014 IEEE international conference on (pp. 933-938). IEEE.*

- *AI for reliability, modeling and statistical analysis of systems designs*

    - *Shaer, Lama, R. Kanj, A. Chehab, R. Joshi "Regularized logistic regression for fast importance sampling based SRAM yield analysis." Quality Electronic Design (ISQED), 2017 18th International Symposium on. IEEE, 2017.*
    - *Shaer, L., Kanj, R., & Joshi, R. (2019, May). Data Imbalance Handling Approaches for Accurate Statistical Modeling and Yield Analysis of Memory Designs. In 2019 IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 1-5). IEEE.*
    - *Kanj, R., Joshi, R., & Nassif, S. (2006, July). Mixture importance sampling and its application to the analysis of SRAM designs in the presence of rare failure events. In 2006 43rd ACM/IEEE Design Automation Conference (pp. 69-72). IEEE.*

Conclusions

- CPS part of 4^{th} industrial revolution
- Privacy and Security key functional requirements
- Lightweight cryptography and non-cryptographic defensive/preventive measures are needed
- AI plays key role in cybersecurity of CPS

Thank You