Panel on Digital Services in Cyber Environments

Theme: Protecting Systems Based on Internet of Things and Big Data

Panelists

Jaime Lloret, Universitat Politecnica de Valencia, Spain

Joshua Chukwuere, North-West University, South Africa

Petre Dini, IARIA, USA

Moderator

Jorge Cobb, The University of Texas at Dallas, USA

SoftNet 2019
The Fourteenth International Conference on Systems and Networks Communications

Artificial Intelligence in Internet of Things data traffic for real time monitoring of critical situations in Smart Cities.

Jaime Lloret Mauri

Professor

Department of Communications
Polytechnic University of Valencia
Camino de Vera 46022, Valencia - Spain

SoftNet 2019
The Fourteenth International Conference on Systems and Networks Communications

Joshua Ebere Chukwuere

Assistant Professor

Computer Sciences and Information Systems Group

North West University South Africa

SoftNet 2019

The Fourteenth International Conference on Systems and Networks Communications

Cyber-Protection Grows along with the Population Growth

Petre Dini

Fellow

IARIA

SoftNet 2019
The Fourteenth International Conference on Systems and Networks Communications

SoftNet 2019
ISBN: 978-1-61208-096-3
November 24-28, 2019 - Valencia, Spain

Using Artificial Intelligence in Network Data to improve Critical Services in Smart Cities

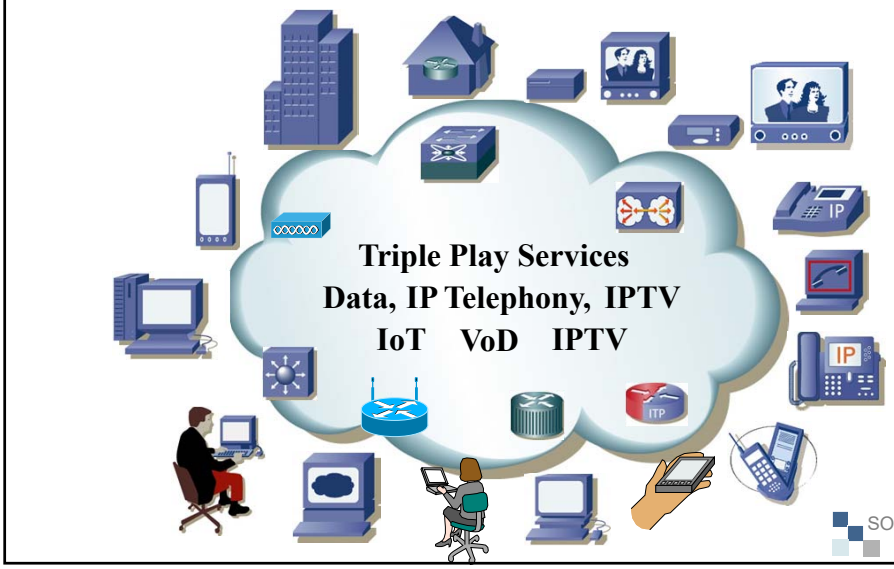
By Jaime Lloret

UNIVERSIDAD POLITECNICA DE VALENCIA

IGIC Instituto de investigación para la gestión integrada de zonas costeras

Departamento de Comunicaciones

Using Artificial Intelligence in Network Data to improve Critical Services in Smart Cities

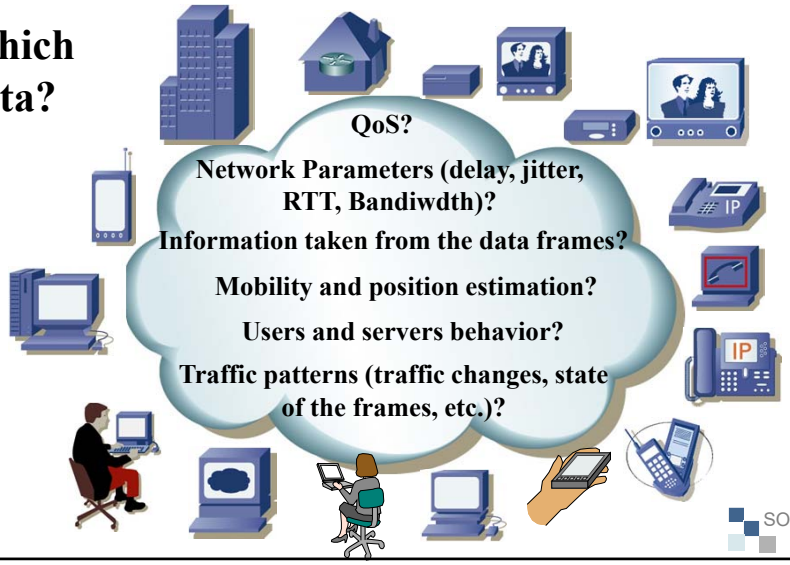


SOFTNET 2019

Using Artificial Intelligence in Network Data to improve Critical Services in Smart Cities

IGIC DCOM

Which data?

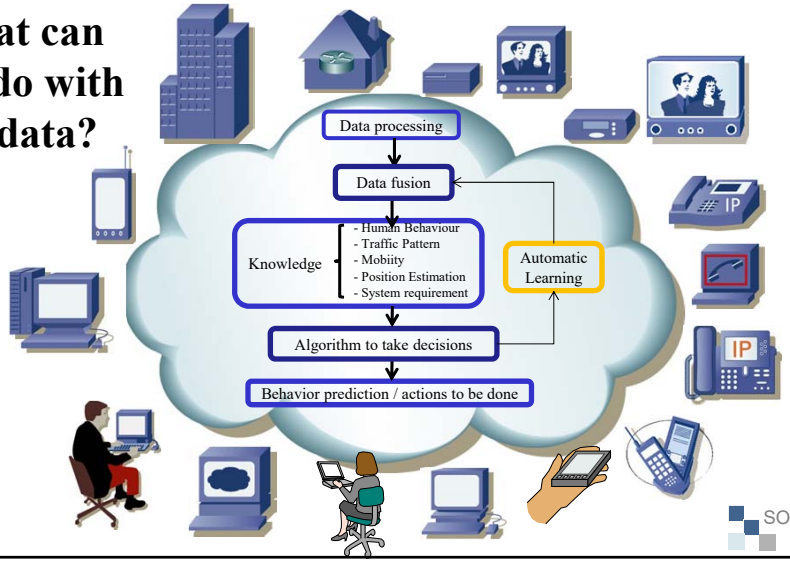


SOFTNET 2019

Using Artificial Intelligence in Network Data to improve Critical Services in Smart Cities

IGIC DCOM

What can we do with the data?

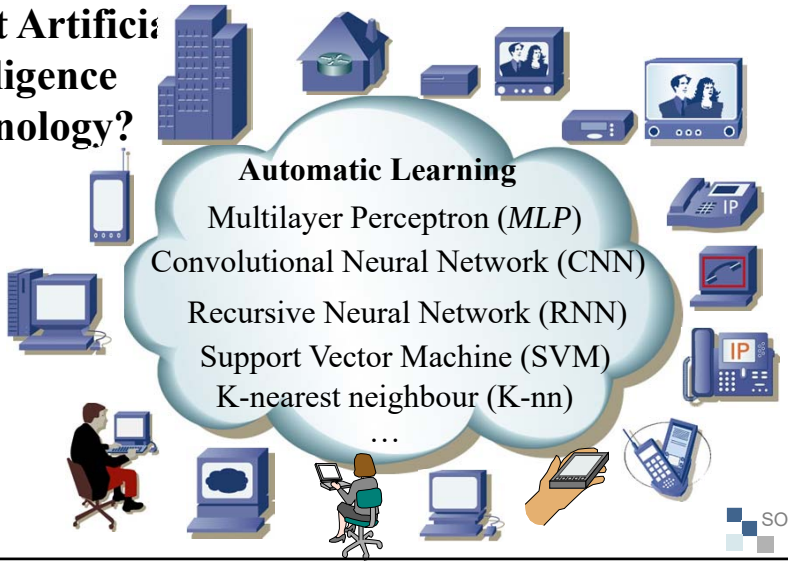


SOFTNET 2019

Using Artificial Intelligence in Network Data to improve Critical Services in Smart Cities

IGIC DCOM

What Artificia Intelligence Technology?



SOFTNET 2019

Using Artificial Intelligence in Network Data to improve Critical Services in Smart Cities

IGIC DCOM

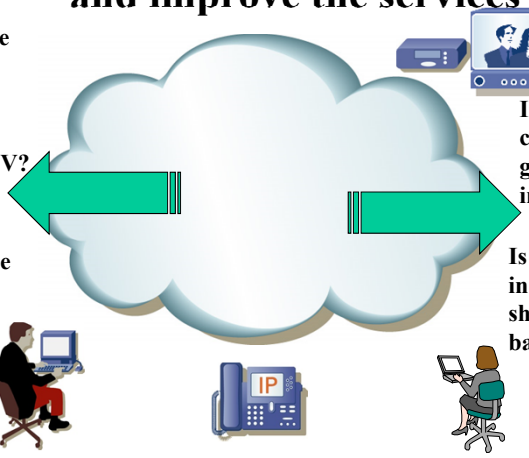
Take additional information from the network and improve the services

Do People like the football match?

Is there a nice program in the TV?

What places are most visited in the network?

Is it a good weather?



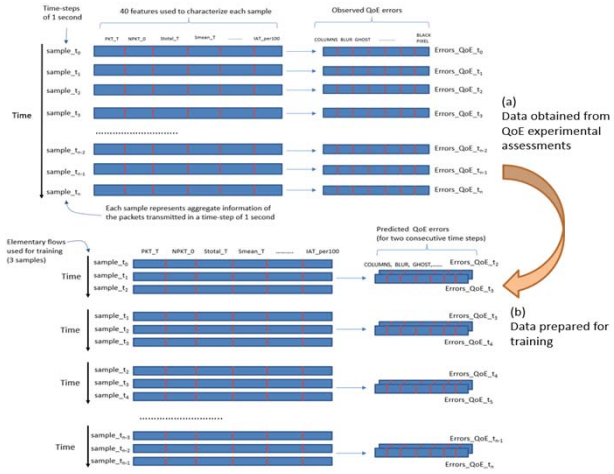
Is the QoE of the channel/VoD service good or should be improved?

Is something happening in critical services that should use the available bandwidth?

SOFTNET 2019

Using Artificial Intelligence in Network Data to improve Critical Services in Smart Cities

M Lopez-Martin, B Carro, J Lloret, S Egea, A Sanchez-Esguevillas, Deep learning model for multimedia quality of experience prediction based on network flow packets, IEEE Communications Magazine 56 (9), 110-117. 2018

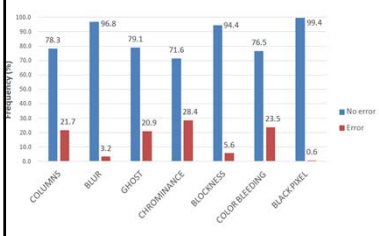


Training data formed by aggregate data samples (a) and final configuration of the training data (b)

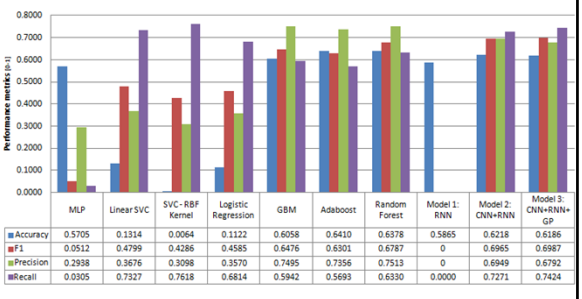
SOFTNET 2019

Using Artificial Intelligence in Network Data to improve Critical Services in Smart Cities

M Lopez-Martin, B Carro, J Lloret, S Egea, A Sanchez-Esguevillas, Deep learning model for multimedia quality of experience prediction based on network flow packets, IEEE Communications Magazine 56 (9), 110-117. 2018



Frequency distribution for QoE label values.



	MLP	Linear SVC	SVC - RBF Kernel	Logistic Regression	GBM	Adaboost	Random Forest	Model 1: RNN	Model 2: CNN+RNN	Model 3: CNN+RNN+ GP
Accuracy	0.5705	0.1314	0.0064	0.1122	0.6058	0.6410	0.6378	0.5865	0.6218	0.6186
F1	0.0512	0.4799	0.4286	0.4585	0.6476	0.6301	0.6787	0	0.6965	0.6987
Precision	0.2938	0.3676	0.3098	0.3570	0.7495	0.7356	0.7513	0	0.6949	0.6792
Recall	0.0305	0.7327	0.7618	0.6814	0.5942	0.5693	0.6330	0.0000	0.7271	0.7424

Performance metrics (aggregated) for QoE classification for all models

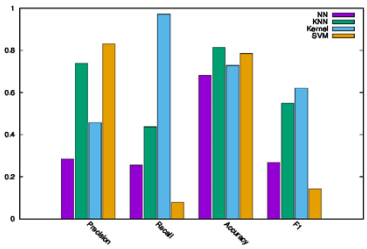
SOFTNET 2019

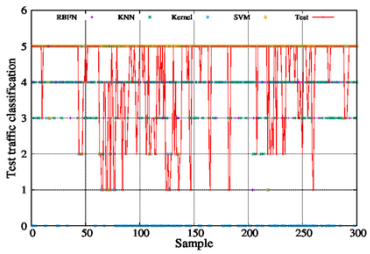
Using Artificial Intelligence in Network Data to improve Critical Services in Smart Cities

A Canovas, JM Jimenez, O Romero, J Lloret, Multimedia Data Flow Traffic Classification Using Intelligent Models Based on Traffic Patterns, IEEE Network 32 (6), 100-107. 2018

There are 5 labels that represent the type of traffic during the video transmission:

Non critical
Low critical
Some critical
Critical
Very critical



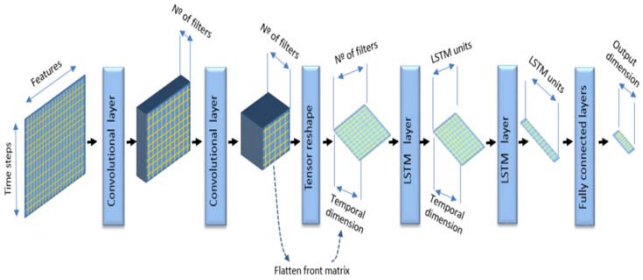


Results of classification based on the different methods. Top, (a), Accuracy level. Bottom, (b), Traffic Classification.

SOFTNET 2019

Using Artificial Intelligence in Network Data to improve Critical Services in Smart Cities

M Lopez-Martin, B Carro, A Sanchez-Esguevillas, J Lloret, Network traffic classifier with convolutional and recurrent neural networks for Internet of Things, IEEE Access 5, 18042-18050. 2017

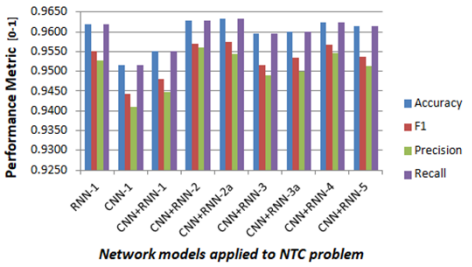


Combination of CNN and two-layer RNN

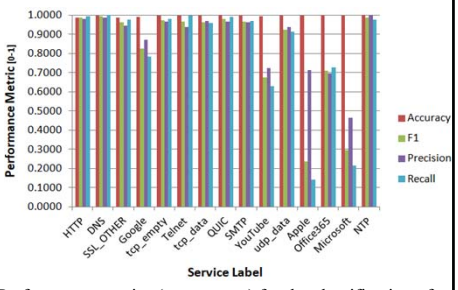
SOFTNET 2019

Using Artificial Intelligence in Network Data to improve Critical Services in Smart Cities

M Lopez-Martin, B Carro, A Sanchez-Esguevillas, J Lloret, Network traffic classifier with convolutional and recurrent neural networks for Internet of Things, IEEE Access 5, 18042-18050. 2017



Classification performance metrics (aggregated) vs. network models



Performance metrics (one vs. rest) for the classification of several service labels (15 more frequent)

SOFTNET 2019

Using Artificial Intelligence in Network Data to improve Critical Services in Smart Cities

Related papers

M Lopez-Martin, B Carro, A Sanchez-Esguevillas, J Lloret, Shallow neural network with kernel approximation for prediction problems in highly demanding data networks, Expert Systems with Applications 124, 196-208. 2019

S Egea, AR Mañez, B Carro, A Sánchez-Esguevillas, J Lloret, Intelligent IoT traffic classification using novel search strategy for fast-based-correlation feature selection in industrial environments, IEEE Internet of Things Journal 5 (3), 1616-1624. 2017

M Lopez-Martin, B Carro, A Sanchez-Esguevillas, J Lloret, Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in IoT, Sensors 17 (9), 1967. 2017

SOFTNET 2019

Using Artificial Intelligence in Network Data to improve Critical Services in Smart Cities

jlloret@dcom.upv.es

SOFTNET 2019

Petre Dini - Valencia

PANEL

Protecting the Systems based on Internet of Things and Big Data

Cyber-Protection Grows along with the Population Growth

Petre Dini
IARIA, USA
petre@iaria.org

2 Facts

1. Population Growth ~ 80 millions/year | 10 B (2040)

"Die Bildung wird täglich geringer, weil die Hast größer wird."

(Friedrich Wilhelm Nietzsche)

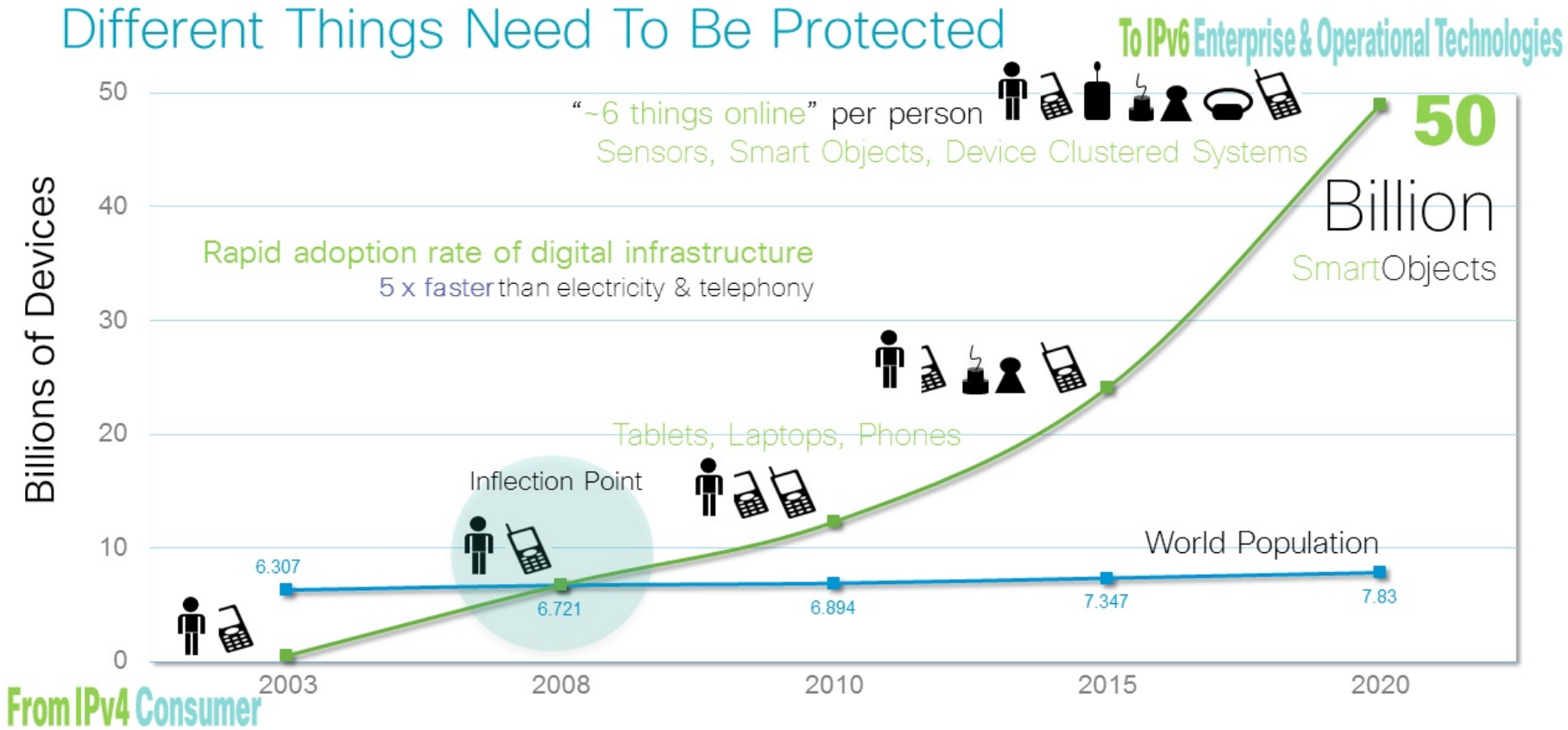
“Education is decreasing daily as the hurry grows.“

“La educación disminuye diariamente a medida que crece la prisa ."

2. The Amount of Data grows and the Number of IoT Devices grows

Cyber-protection becomes a challenging continuous activity, as User Education & Knowledge do not follow the Complexity of the Systems

~8B (2020) → ~10B (2040) → ~150B devices



Source: Cisco IBSG projections, UN Economic & Social Affairs http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf

https://tools.cisco.com/security/center/resources/secure_iot_proposed_framework

On the Data | Information Sharing, a Key

- "The IoT entities will generally not be a single-use, single-ownership solution. The devices and the control platform on which data may be consumed and shared could have different ownership, policy, managerial and connectivity domains.
- Devices will be required to have equal and open access to a number of data consumers and controllers concurrently, while still retaining privacy and exclusivity of data where that is required between those consumers. Information availability while providing data isolation between common customers is critical.
- There is a need for appropriate identity controls and build trust relationships between entities to share the right information."

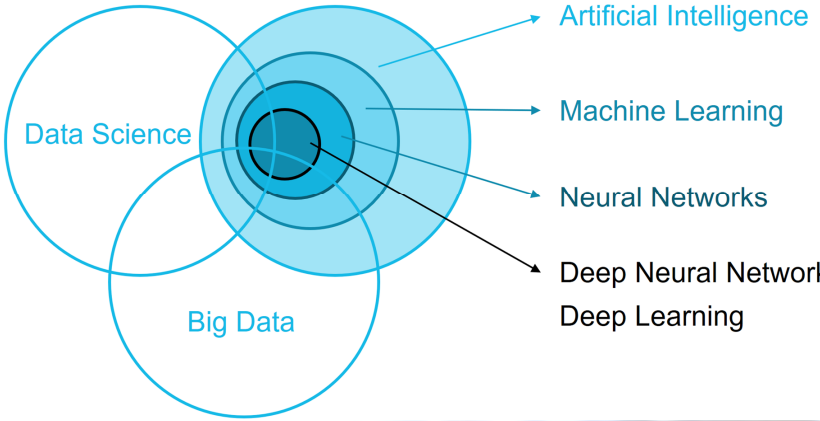
- Yet, 'Things':
- Limited security computing capabilities
- Encryption algorithms need higher processing power
- Low CPU cycles vs. effective encryption

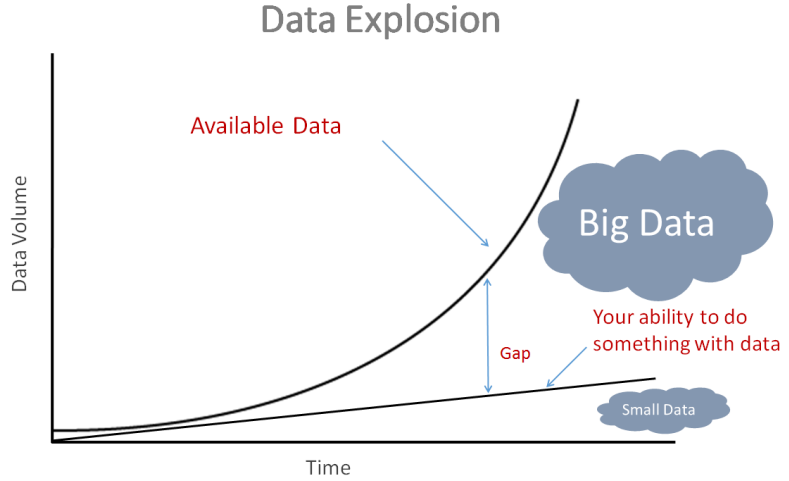
- Vulnerability
- Physical Protection
  - Mobile devices can be stolen
  - Fixed devices can be moved

https://tools.cisco.com/security/center/resources/secure_iot_proposed_framework

Huge Data, Event Patterns, Machine Learning

- **Huge Data | Volume, Time**
- **Event Patterns | Status Situations | Plans of Actions**
- **Machine Learning**

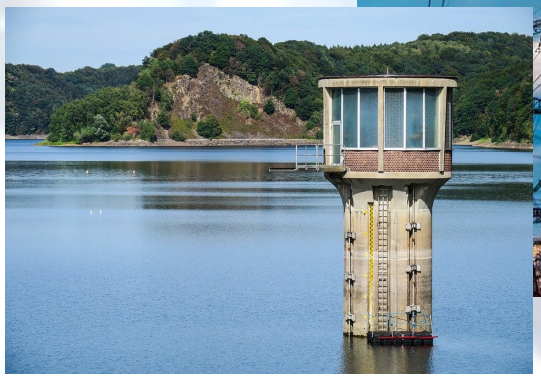


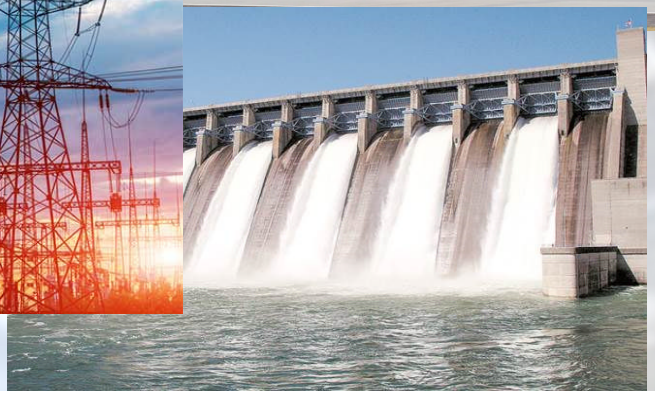


Fraunhofer – FOKUS - Fraunhofer Gesselschaft

Complexity

- Decisional: Deep understanding
- Using: Shallow
- Designing: Both
- Updating: Both
- Integrating: Both
- Protection:
  - Both +
  - Threats +
  - Solutions +
  - Priorities +





Humans | The Weakest Link

- **Humans | End-users**
  - **Education (at (~) the technology speed)**
  - **Awareness (incentives and penalties for access/use)**
- **Strategic critical systems**
  - **Governmental strategies**
  - **Self-protecting mechanisms**
- **University curricula**

Thanks

WWW.IARIA.ORG