Value Creation Network
Internet of Things

Project presentation

ASSET - Adaptive Security for Smart Internet of Things in eHealth

Habtamu Abie, Dr. Scient., Principal Scientist

ASSET Project Manager

Norwegian Computing Center

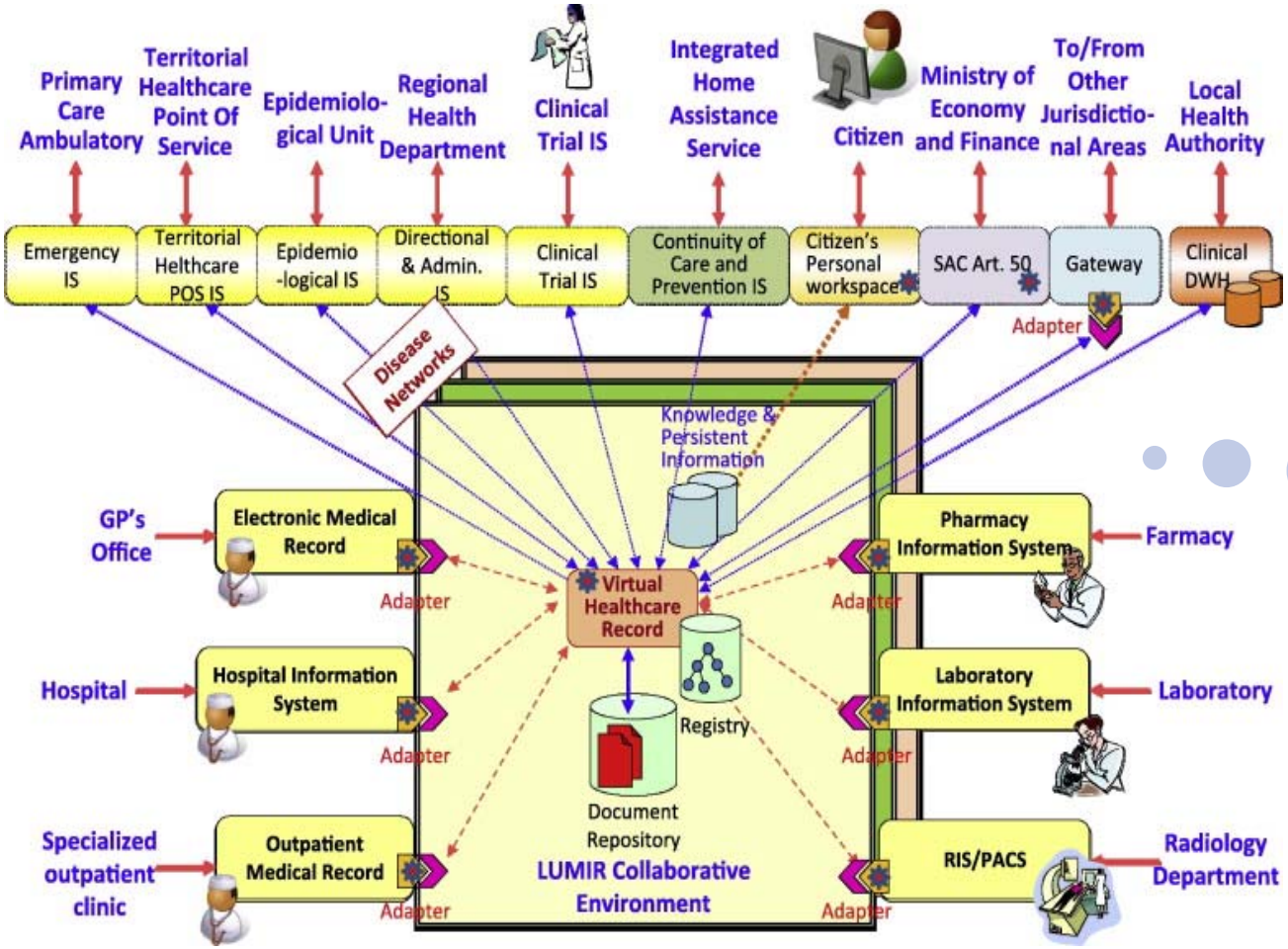
asset.nr.no

Tuesday 19th of March 2013,
09:30-17:00, Telenor, Oslo, Norway.

The ASSET Project

- IoTs can improve eHeath
  - Digital Health Ecosystems and IOT
  - IoTs simplify everyday life and improve quality of lives
  - IoTs are also vulnerable to attacks
- Goals and objectives
- Project partners
- Case study: Patient monitoring
- ASSET lab setup
- Summary

Digital Health Ecosystems create digital environments for networked health organizations



IoT is one of the building blocks of the digital health ecosystem

Source: L. D. Serbanati et al., Steps towards a digital health ecosystem, Journal of Biomedical Informatics, 44(4), August 2011, 621–636

IoTs can improve quality of lives

- at home, while travelling, when sick, at work, when jogging, and/or at gym

Source:
Digital Medicine

- Can be used to
  - track objects and people
  - identify and authenticate people
  - collect and sense data automatically

IoTs are also vulnerable to attacks

- Communication is wireless
- Limited physical security
- No centralized control
- Energy and computationally constrained operations
- Dynamic topology and behavior
- Unwanted side-effects of deployment in new context

Context-aware adaptive security for IoT

- from three related viewpoints:
  - from the Things that are connected
  - from the environments in which they are situated, and
  - from the interactions that occur between Things, their environments and their human users

- Some types of modern IoT applications
  - require instant adaptation of their security mechanisms due to their exposure to increasing situational dynamics

Motivating Projects

- FP7
  - GEMOM – Genetic message-oriented secure middleware
  - uTRUSTit - Usable TRUST in the Internet of Things
  - e-SENSE - Capturing Ambient Intelligence for Mobile Communications through Wireless Sensor Networks
  - UbiSec&Sens - Ubiquitous Security and Sensing in the European Homeland
- National
  - PETweb I & II – Privacy-respecting Identity Management for e-Norge
  - SAMPOS - Strategies for Seamless Deployment of Mobile Patient Monitoring Systems

Goals and objectives

- Goals
  - develop risk-based adaptive security methods and mechanisms for IoT in eHealth
  - adapt to dynamic changing conditions of IoT, including usability, threats, and diversity/heterogeneity
- Objectives
  - Build risk estimating and predicting models
  - Build methodology for security measurement and metrics
  - Prototype and validate the adaptive methods in patient monitoring scenarios in Oslo University Hospital
  - Build light-weight abilities in smart things

Project partners

- National Partners
  - Norwegian Computing Center
  - Gjøvik University College
  - Oslo University Hospital
- International partners
  - VTT Technical Research Center of Finland
  - Queen Mary University of London
- 2 PhD fellows and 2 Master's students
  - Risk estimation and prediction
  - Risk-based adaptive security
  - Adaptive lab and simulation testbed for IoT in eHealth
  - Adaptive intrusion detection for WBAN

Risk-based security adaptation

- Risk-based adaptation
  - access could be authorized according to the measured risk
  - measurable risk to strengthen the security of IoT systems
- Implements quantified risk adaptive security solutions
  - measuring risk
  - establishing an acceptable risk level
  - ensuring that the information is used, accessed and distributed all the way up to the acceptable risk level
- Self-adaptiive risk-based protection
  - Based on risk levels, automatically adjust the settings and actions to satisfy protection requirements of the new operating conditions

Alignment of ISMS, ISRM and ASSET

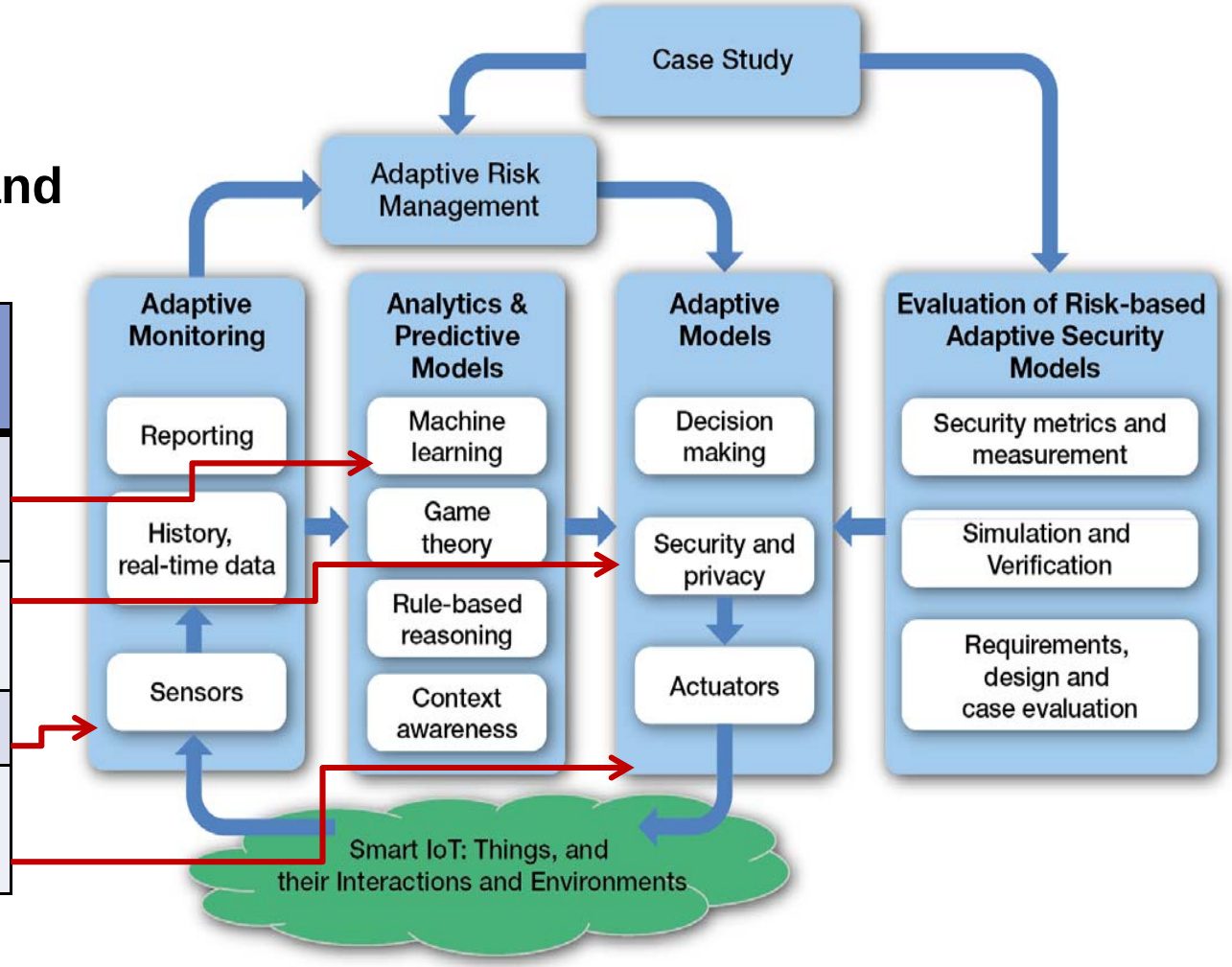
Information Security Management System (ISMS) Process	Information Security Risk Management (ISRM) Process	ASSET Adaptive Risk Management Process/Methodology
Plan	Establishing the context Risk assessment Risk treatment planning Risk acceptance	Analyze (Plan)
Do	Implementation of risk treatment plan	Adapt (Execute)
Check	Continual monitoring and reviewing of risks	Monitor
Act	Maintain and improve the Information Security Risk Management Process	Adapt (Learn)

ISO/IEC 27005:2007 **ASSET: Monitor-Analyze-Adapt (plan, learn, execute)**

Risk-based Adaptive Security Framework

Alignment of ISMS and ASSET Processes

ISMS Process	ASSET Process
Plan	Analyze (Plan)
Do	Adapt (Execute)
Check	Monitor
Act	Adapt (Learn)



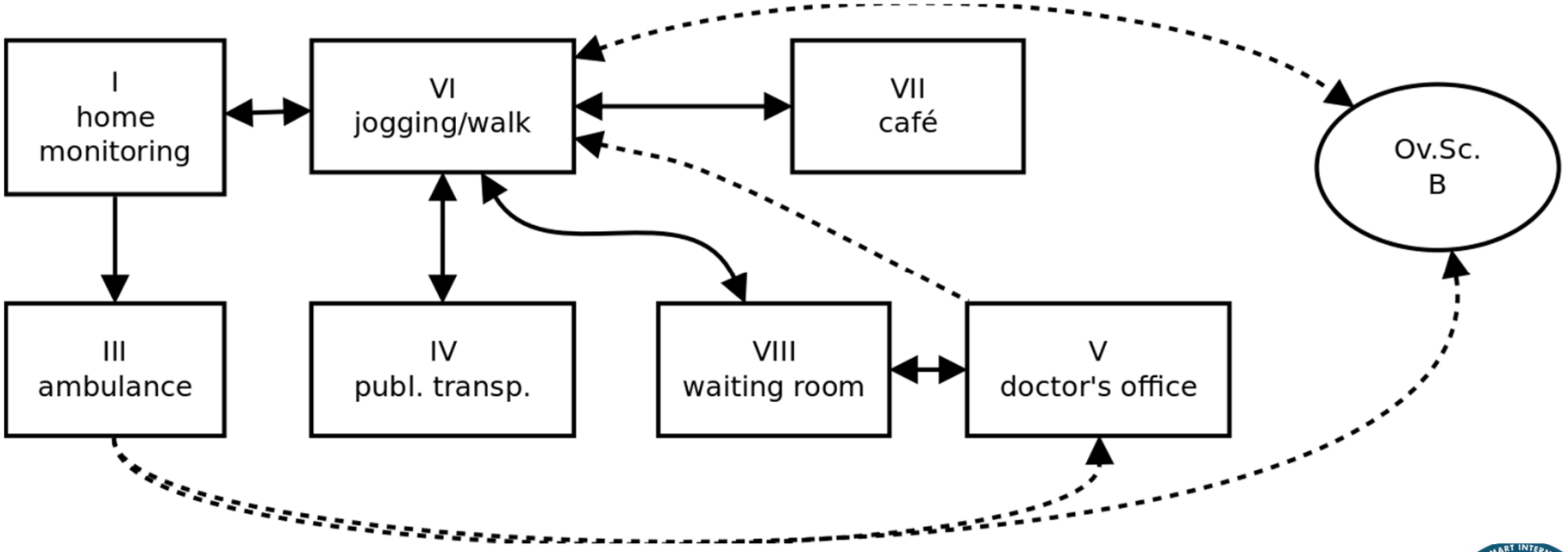
H. Abie and I. Balasingham, Risk-Based Adaptive Security for Smart IoT in eHealth, 7th International Conference on Body Area Networks (BODYNETS 2012)

Case Study: Patient Monitoring

- Patient monitoring systems
  - major data source in healthcare environments
- maintain a certain level
  - availability
  - quality of service (QoS)
  - security and privacy of the patient
- Two different scenarios
  - home environments
  - hospital environments

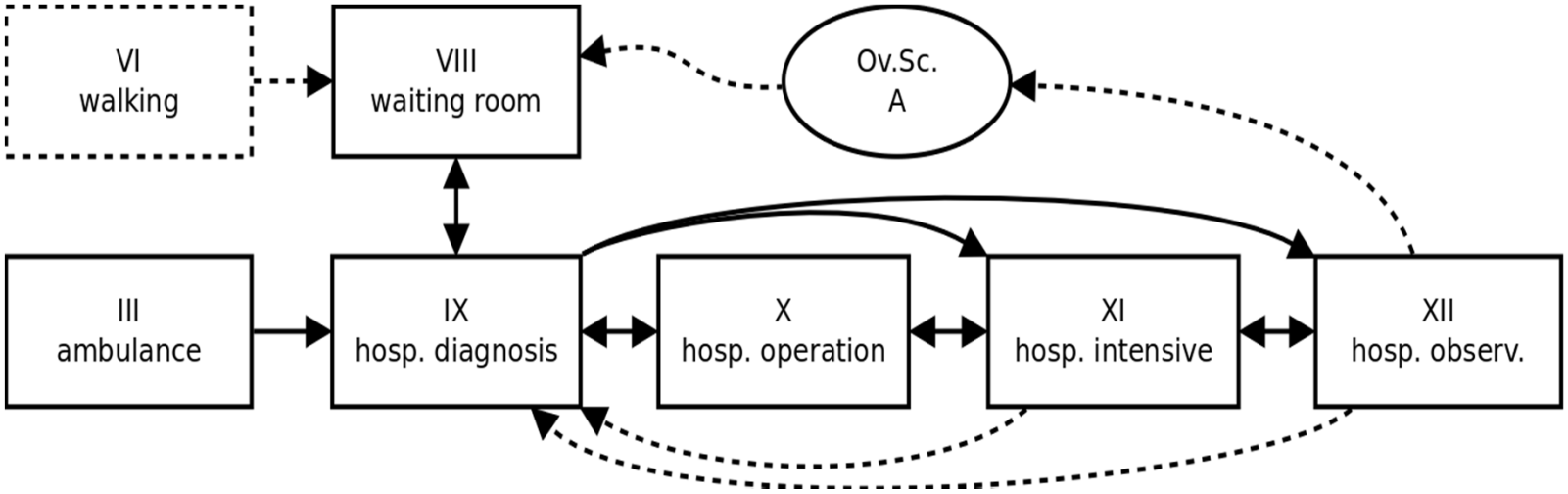
The Home Scenario and its Core Scenarios

core scenario	core scenario name	ov. sc. A	ov. sc. B	transition to core scenario
I	home monitoring	•		VI, III
II	accident			III
III	ambulance	•	•	IX, (V)
IV	public transport	•		VI
V	doctor's office	•		VI, III
VI	jogging, walking	•		IV, I, VIII, (III)
VII	café	•		VI, (III)
VIII	waiting room	•	•	V, IX, VI
IX	hospital diagnosis		•	X, XI, XII, VI, (VIII)
X	hospital operation		•	XI, (IX)
XI	hospital intensive		•	XII, X
XII	hospital observation		•	VI, XI, IX

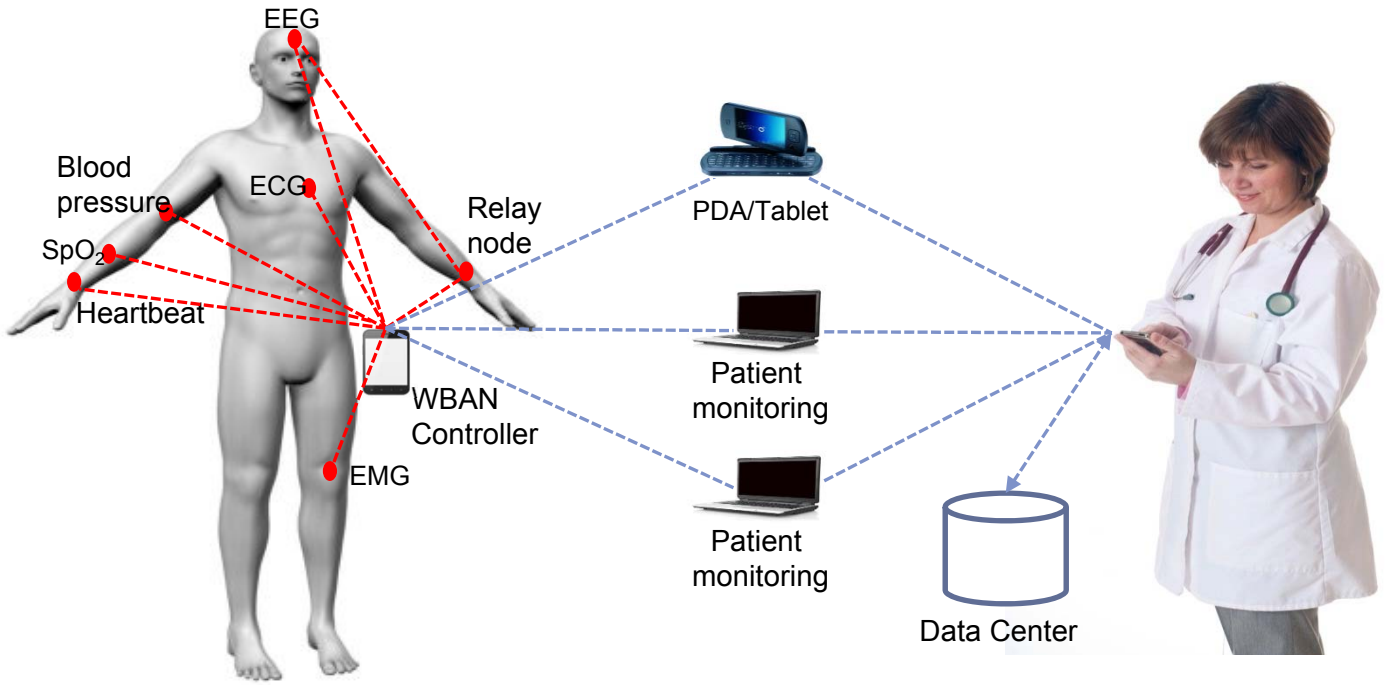


The Hospital Scenario and its Core Scenarios

core scenario	core scenario name	ov. sc. A	ov. sc. B	transition to core scenario
I	home monitoring	•		VI, III
II	accident			III
III	ambulance	•	•	IX, (V)
IV	public transport	•		VI
V	doctor's office	•		VI, III
VI	jogging, walking	•		IV, I, VIII, (III)
VII	café	•		VI, (III)
VIII	waiting room	•	•	V, IX, VI
IX	hospital diagnosis		•	X, XI, XII, VI, (VIII)
X	hospital operation		•	XI, (IX)
XI	hospital intensive		•	XII, X
XII	hospital observation		•	VI, XI, IX



ASSET Lab Set Up



Acronyms
- ECG (Electrocardiography)
- EEG (Electroencephalography)
- SpO2 (Oxygen Saturation)
- EMG (Electromyography)
- WBAN (Wireless Body Area Network)

Devices in use:
- Smartphones: Sony Xperia, Galaxy Nexus
- Motes: Shimmer kit
- Dash7: Wizzikit
- Tablet Samsung Galaxy 10
- PCs: Laptops

Radio types:
- IEEE 802.15.4
- Wifi
- Bluetooth
- ZigBee
- NFC
- GPRS/ GSM

Sensor types:
- Heartbeat, blood pressure, blood sugar level
- EEG, ECG, EMG, temperature, light, humidity
- Accelerometer, Gyro, Magnetometer, GSR
- Strain Gauge, GPS, Barometric Pressure , SpO2
- Vibration switch, NFC, proximity sensor, etc.

Summary

- Challenges
  - models for accurately predicting future and unknown events and adapting accordingly
  - adaptation causing minimal deviations from normal operation
  - enabling adaptation across multiple time scales
  - where and how much risk to take
  - how could risk damages be controlled
  - optimize algorithms for different IoT processing capabilities
  - improve the light-weight abilities of smart things by improving their context-awareness and self-abilities

Summary…

- An innovative risk-based adaptive security for IoT in eHealth
  - identify unknown threats to IoT eHealth systems
  - estimate and predict risk damages and future benefits
  - adapt security decisions upon those predictions
- Goals
  - increase understanding of, and thus ability to develop, techniques and algorithms for predicting unknown risk
  - contribute to the IoT vision to become secure Internet of anything, anywhere, connected, anyhow

Thanks!

The Research Council of Norway

The End!

asset.nr.no