YAKSHA: Trends and challenges in EU-ASEAN cybersecurity

A. Kostopoulos, I. Chochliouros

Fixed Network R&D Programs Section,
Hellenic Telecommunications Organization S.A. (OTE)

Scope

- **YAKSHA will build an ecosystem of partners** around its solutions **that will contribute to enhancing cybersecurity skills in Europe and creating new positions for cybersecurity specialists in ASEAN.**

- Moreover, the **direct access to the important ASEAN market will positively impact the competitiveness of European security industry**.

- **The YAKSHA software solution will be validated in real-world pilot projects in both EU and ASEAN**, ***initially focusing on Vietnam and Greece,*** *and with plans to expand the deployments to other countries*.

Objectives

1. **To assess the Cyber Security state-of-the-art in the ASEAN area and future developments**

   i. To **describe** in detail the **cybersecurity ecosystem in ASEAN region** (***complete assessment of the cybersecurity environment*** *and actors in the ASEAN region and comparison with EU*).

   ii. To **identify future trends and opportunities in EU-ASEAN cybersecurity.**

2. **To develop and validate a distributed, flexible, cybersecurity solution:**

   i. Develop innovative methods for malware detection, collection and analysis.

   ii. Validate the final product and YAKSHA service **in real pilot projects by testing the YAKSHA software suite in real-world test cases,** *represented by complex end-user organisations with articulated cybersecurity risks.*

Objectives (cont.)

3. To enable the *sustainable* uptake of scientific, technical and economic results and foster cooperation and partnerships between EU-ASEAN:

i. To **design and deploy** a **comprehensive communication and dissemination strategy**, *in order to increase the visibility of the results to all the relevant stakeholders, and contribute to an overall increased impact of the project.*

ii. To **develop a sustainable business model for the commercial exploitation** and **propose scenarios of the operationalisation** of the cybersecurity software.

iii. To **survey and develop possible areas of collaboration between European and ASEAN stakeholders**, *both in the academic sharing of knowledge and know-how and possible business partnerships.*

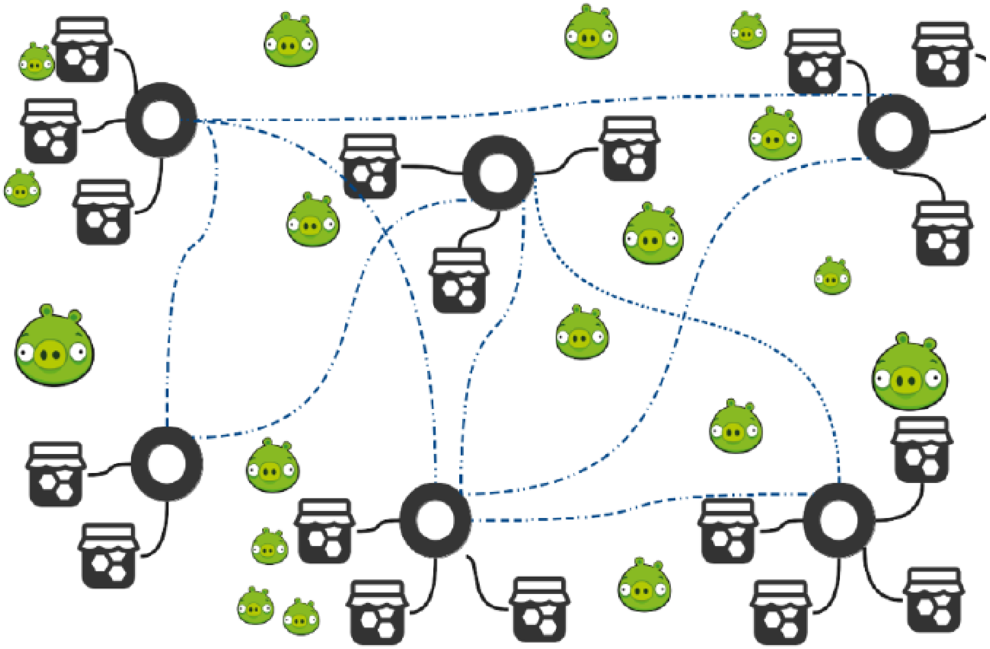
Challenges

- **Automated Honeypot Deployment**
  - *Create custom honeypots* with the integrated sensors properly configured.
- **Automated Attack & Malware Analysis**
  - *Extract knowledge from logs* in a human readable format
    → *attack analysis* can be *simplified* and partially *automated.*
  - Provide *ML tools and AI algorithms*
    malware detection, information correlation, attack patterns extraction.
- **Architecture and Scalability**
  - *Inherently distributed architecture.*
  - *The nodes already contain powerful analytical capabilities*
    → easier to collect information in a single place if needed.
  - *Leverage information gathered by nodes outside of one's organisation*
    → improving its readiness and defensive capabilities.
- **Global-scale Honeypots**
  - *Facilitate end-users to exploit their capabilities, selectively share their collected samples, tools and knowledge.*

YAKSHA Architecture

- **A YAKSHA Node:** *On top, the installed honeypots which are exposed to the Internet so that attackers will try to penetrate them.*

  Not only typical Linux and Windows honeypots, but also hooks for IoT devices, Android and SCADA systems.



Architectural Components

- **Maintenance and Integration Engine:** ***configuration of a new honeypot, uploading and exposing it to the Internet and data wipe.***

- **Monitoring Engine:** ***sanity checks to determine whether the honeypot is properly working*** (records changes in memory, processes, filesystem, network connections to detect anomalies during an attack).

- **Correlation Engine:** ***find how significant is the penetration and propagation of the sample, and it correlates the attack patterns with input from older samples.***

- **Reporting Engine:** **presenting the information in a readable form** *(issuing alerts and aggregating information for technical personnel, providing input on the organisation's cybersecurity risk levels).*

- **Connectivity and Sharing Engine:** ***information exchange with other YAKSHA nodes (e.g., malware samples).***

Use Cases

- ***End-users of YAKSHA operate critical infrastructures and have very high security standards*** → *honeypot deployment is a crucial procedure.*

- **YAKSHA trials will be conducted in both Europe and ASEAN countries** → *each end-user will deploy his custom honeypots*.

- ***The partners will cooperate in finding common configurations to selectively share findings and test these features.***

- **Use of real data** *(not simulated attacks).*

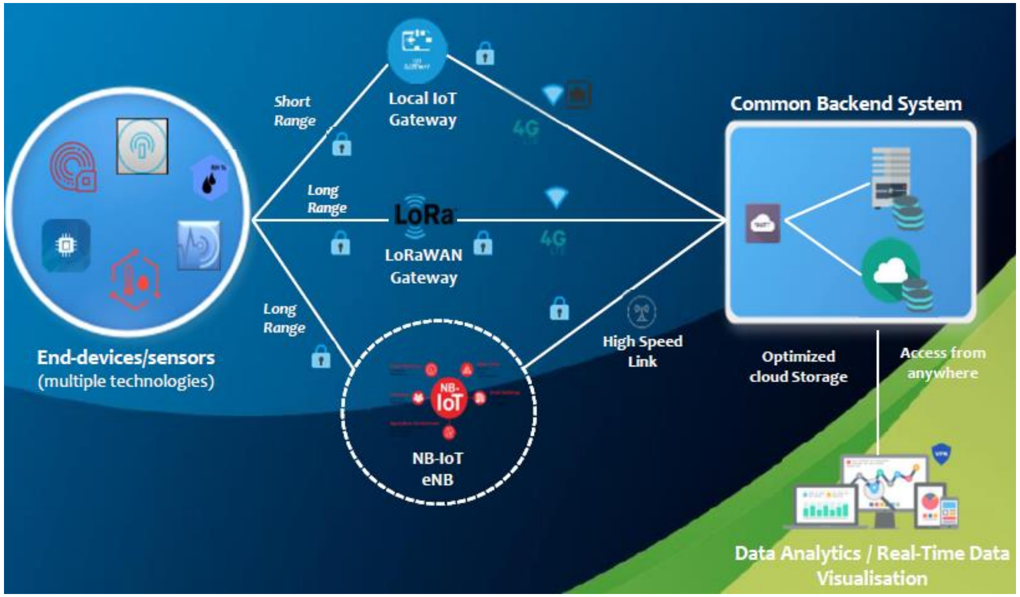
- **Evaluate with the experts how well it clusters** *the attacks, the quality of collected information, the reports, etc.*

Use Cases: *IoT Platform Testbed*

- **Pre-commercial environment** (infrastructure and settings) **to collect real data** of potential attacks against the smart home IoT platform product.

- **YAKSHA analytics capability will be used to raise awareness and provide decision support** *in strengthening the cybersecurity posture of the product.*

- **Awareness of potential attacks in the wild, against ICT products and services.**

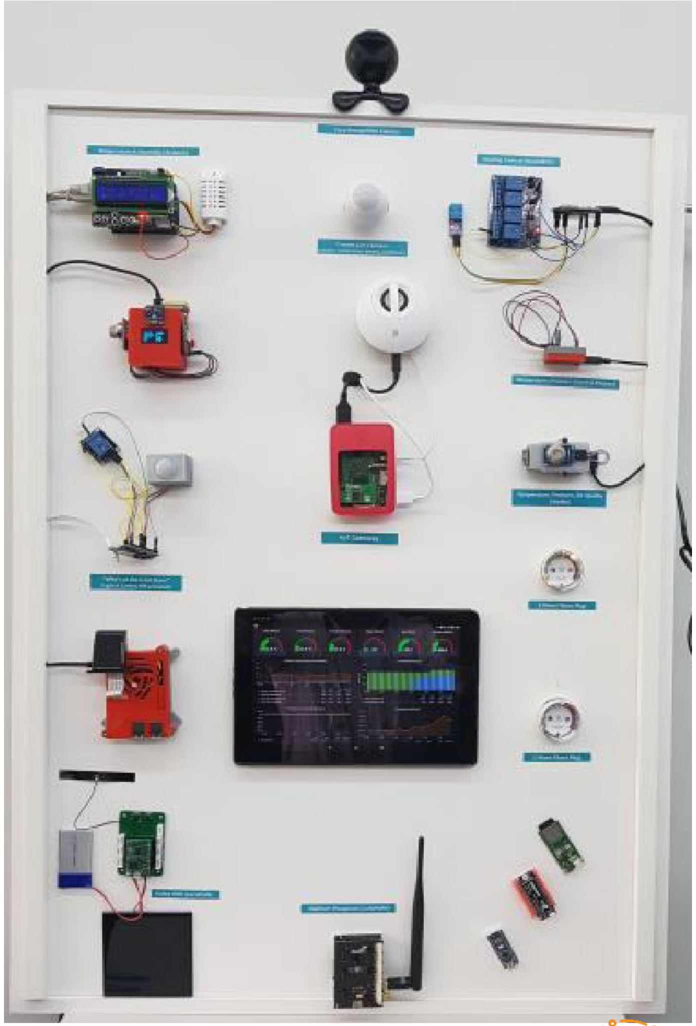


Use Cases: IoT Platform Testbed

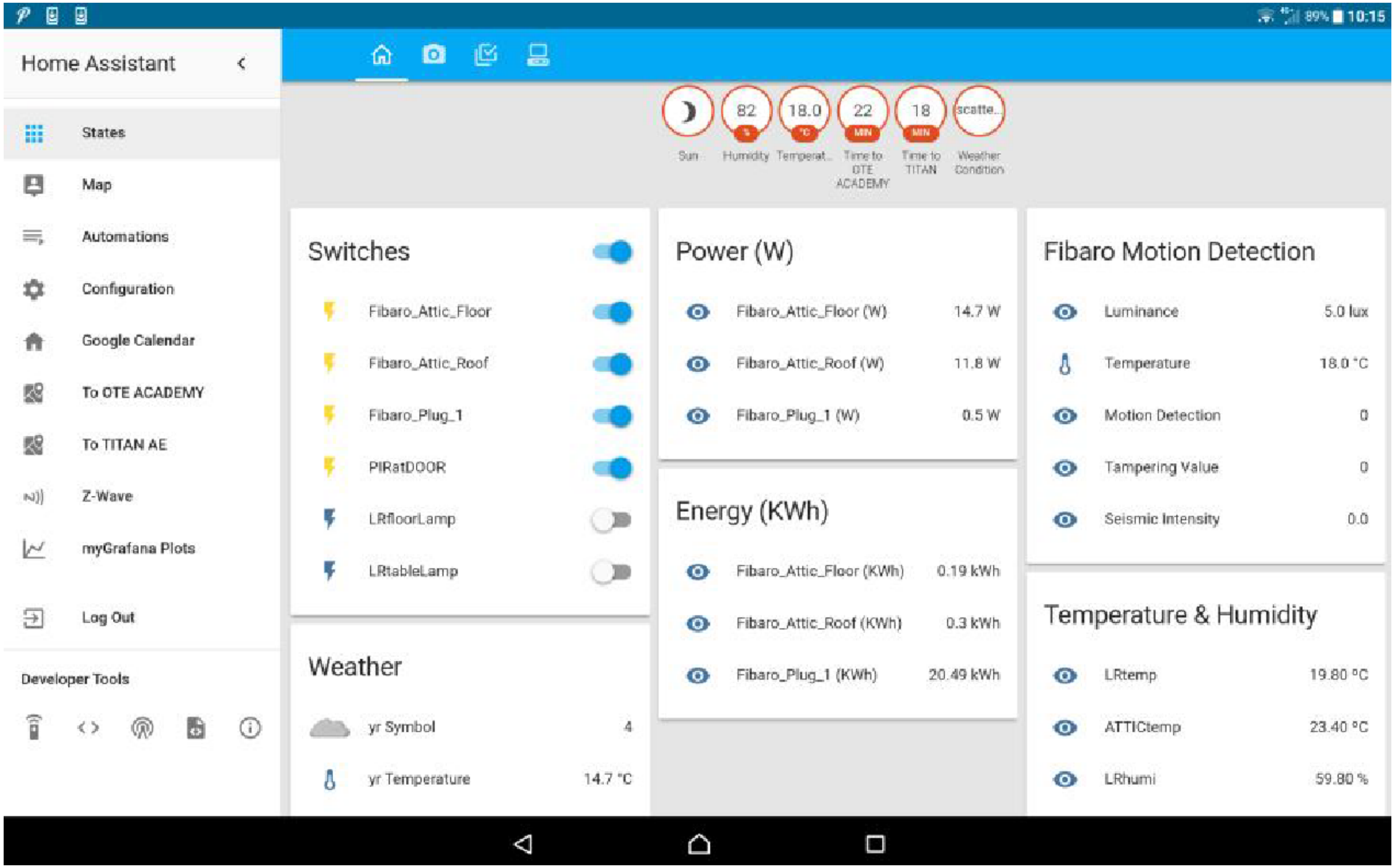
- A wide range of **end-devices and sensors** are integrated on the IoT platform
  - Cameras
  - Microphones
  - Motion sensors
  - Temperature / humidity sensors
  - Energy consumption monitoring devices

- The end-devices use multiple technologies for communicating with the IoT platform
  - WiFi
  - 4G
  - High speed links

- Via LoRaWAN gateway, monitoring data are sent to a common backend system, with optimized cloud storage.



Use Cases: *IoT Platform Testbed*



Switches	
Fibaro_Attic_Floor	on
Fibaro_Attic_Roof	on
Fibaro_Plug_1	on
PIRatDOOR	on
LRfloorLamp	off
LRtableLamp	off

Power (W)	
Fibaro_Attic_Floor (W)	14.7 W
Fibaro_Attic_Roof (W)	11.8 W
Fibaro_Plug_1 (W)	0.5 W

Fibaro Motion Detection	
Luminance	5.0 lux
Temperature	18.0 °C
Motion Detection	0
Tampering Value	0
Seismic Intensity	0.0

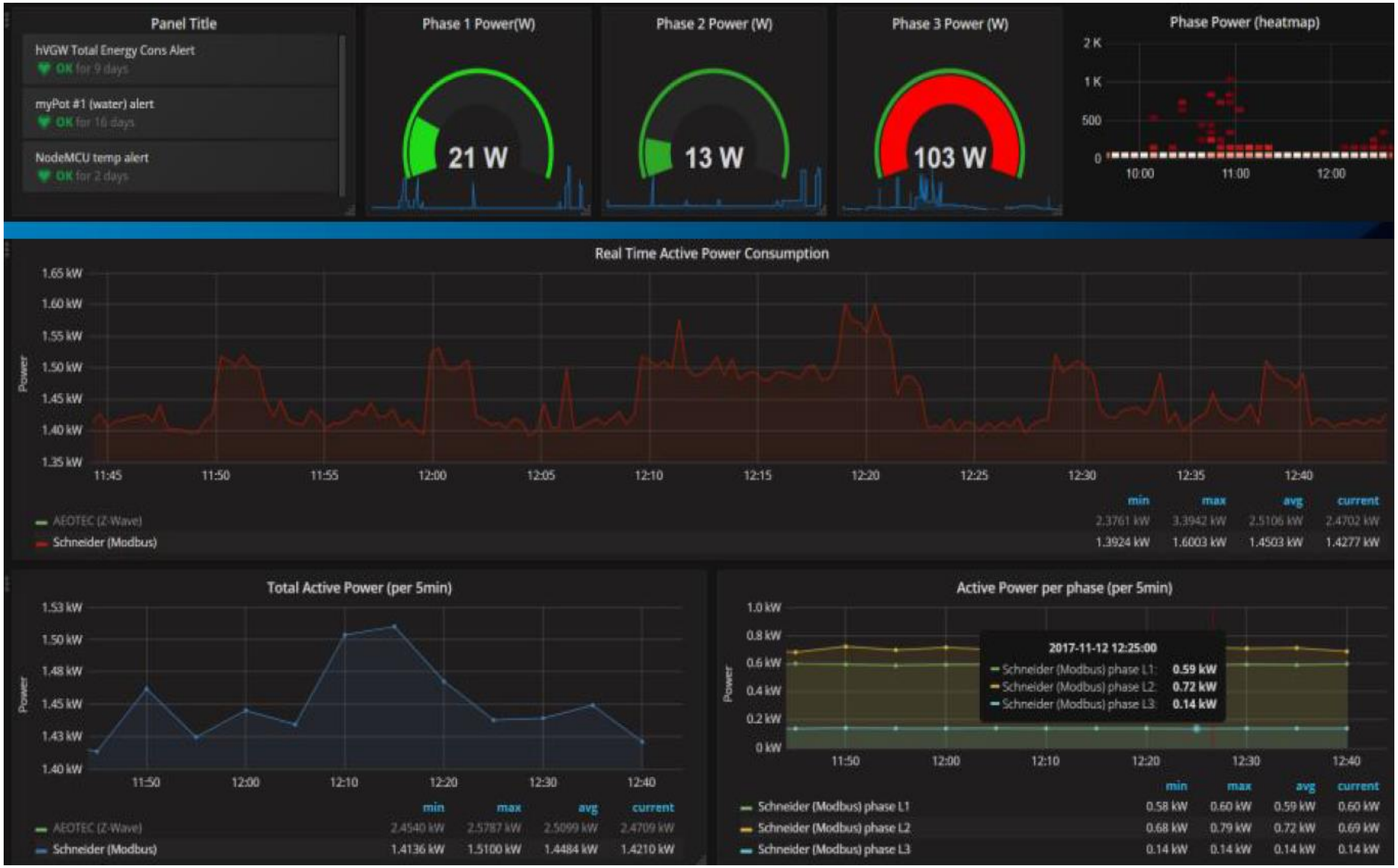
Energy (KWh)	
Fibaro_Attic_Floor (KWh)	0.19 kWh
Fibaro_Attic_Roof (KWh)	0.3 kWh
Fibaro_Plug_1 (KWh)	20.49 kWh

Weather	
yr Symbol	4
yr Temperature	14.7 °C

Temperature & Humidity	
LRtemp	19.80 °C
ATTICtemp	23.40 °C
LRhumi	59.80 %

- ***End-users can connect remotely to the back-end system to have access to their data, as well as control their end-devices.***

Use Cases: *IoT Platform Testbed*



hVGW Total Energy Cons Alert
OK for 9 days

myPot #1 (water) alert
OK for 16 days

NodeMCU temp alert
OK for 2 days

Real Time Active Power Consumption

	min	max	avg	current
AEOTEC (Z-Wave)	2.3761 kW	3.3942 kW	2.5106 kW	2.4702 kW
Schneider (Modbus)	1.3924 kW	1.6003 kW	1.4503 kW	1.4277 kW

Total Active Power (per 5min)

	min	max	avg	current
AEOTEC (Z-Wave)	2.4540 kW	2.5787 kW	2.5099 kW	2.4709 kW
Schneider (Modbus)	1.4136 kW	1.5100 kW	1.4484 kW	1.4210 kW

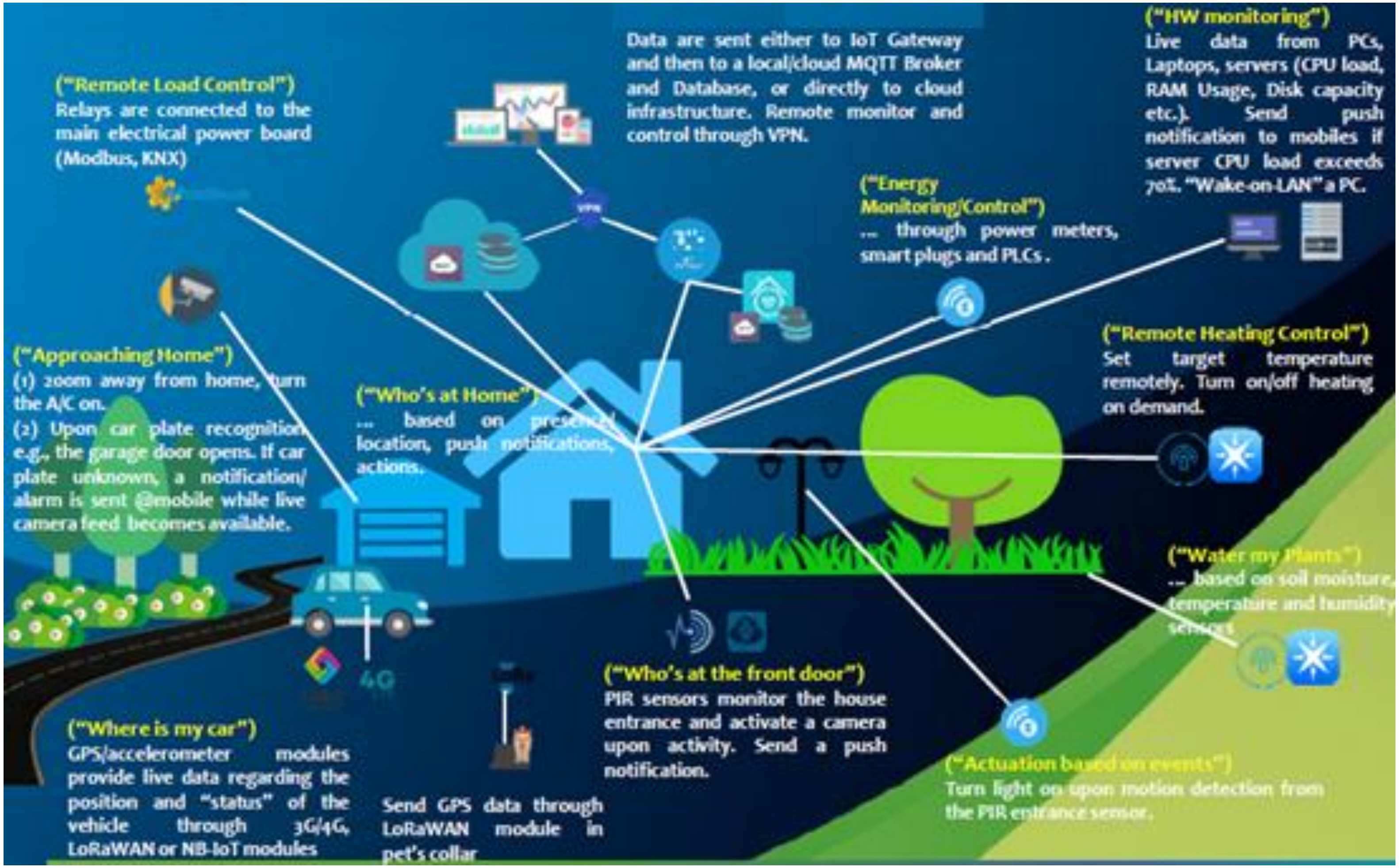
Active Power per phase (per 5min)

2017-11-12 12:25:00
- Schneider (Modbus) phase L1: 0.59 kW
- Schneider (Modbus) phase L2: 0.72 kW
- Schneider (Modbus) phase L3: 0.14 kW

	min	max	avg	current
Schneider (Modbus) phase L1	0.58 kW	0.60 kW	0.59 kW	0.60 kW
Schneider (Modbus) phase L2	0.68 kW	0.79 kW	0.72 kW	0.69 kW
Schneider (Modbus) phase L3	0.14 kW	0.14 kW	0.14 kW	0.14 kW

- ***The back-end system is also enabled to provide data analytics, as well as real-time data visualisation to the end-users,***

Use Cases: *IoT Platform Testbed*



("Remote Load Control")
Relays are connected to the main electrical power board (Modbus, KNX)

Data are sent either to IoT Gateway and then to a local/cloud MQTT Broker and Database, or directly to cloud infrastructure. Remote monitor and control through VPN.

("HW monitoring")
Live data from PCs, Laptops, servers (CPU load, RAM Usage, Disk capacity etc.). Send push notification to mobiles if server CPU load exceeds 70%. "Wake-on-LAN" a PC.

("Energy Monitoring/Control")
... through power meters, smart plugs and PLCs.

("Approaching Home")
(1) 200m away from home, turn the A/C on.
(2) Upon car plate recognition e.g., the garage door opens. If car plate unknown, a notification/ alarm is sent @mobile while live camera feed becomes available.

("Who's at Home")
... based on presence/ location, push notifications, actions.

("Remote Heating Control")
Set target temperature remotely. Turn on/off heating on demand.

("Water my Plants")
... based on soil moisture, temperature and humidity sensors

("Who's at the front door")
PIR sensors monitor the house entrance and activate a camera upon activity. Send a push notification.

("Actuation based on events")
Turn light on upon motion detection from the PIR entrance sensor.

("Where is my car")
GPS/accelerometer modules provide live data regarding the position and "status" of the vehicle through 3G/4G, LoRaWAN or NB-IoT modules

Send GPS data through LoRaWAN module in pet's collar

Use Cases: *IoT Platform Testbed*

Threat category	Threat	Component affected
Malicious code /software/ activity	Virus, worms/trojans, botnets, backdoors	Gateways
Malicious code /software/ activity	Privilege escalation	Gateway
Malicious code /software/ activity	Code injection	Database server
Denial of service	Denial of service	Analystics Server
Distributed Denial of Service	Distributed DoS	External targets (botnet)
Miners	Privilege escalation	Gateway
Execution of arbitrary code in IoT devices	Remote code execution	IoT devices
Leakage of private data	Data leakage	IoT devices

Use Cases: IoT Platform Testbed

The considered OTE IoT platform supports the following capabilities:

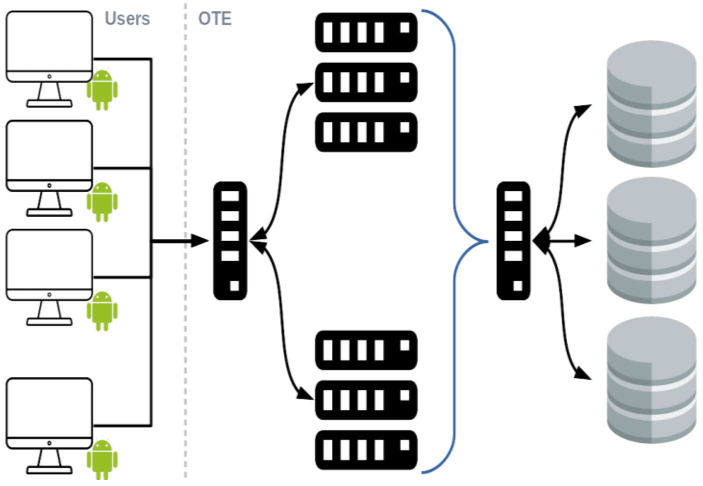
- **Monitoring (power/energy/voltage)**
- **Energy management/Control (remotely, on-demand)**
- **Facility automation (based on predefined events/rules)**
- **Push notifications at end-users' mobile devices**
- **Enhanced security and data privacy (VPN, SSL Certificates)**
- **Data visualization**

Use Cases: *Streaming box*

- **Pre-commercial environment** (infrastructure and settings) **to collect real data** *of potential attacks against the smart home IoT platform product.*

- **YAKSHA analytics capability will be used to raise awareness and provide decision support** *in strengthening the cybersecurity posture of the product.*

- **Awareness of potential attacks in the wild against ICT products and services.**



Use Cases: *Streaming box*

Threat category	***Threat***	***Component affected***
Malicious code /software/ activity	Virus, worms/Trojans, botnets, backdoors	Streambox
Malicious code /software/ activity	Privilege escalation	Streambox
Malicious code /software/ activity	Code injection	Streaming server
Denial of service	Denial of service	Streaming Server
Distributed Denial of Service	Distributed DoS	External targets (botnet)
Miners	Privilege escalation	Streambox
Execution of arbitrary code in Streambox	Remote code execution	Home network devices
Leakage of private data	Data leakage	Home network devices

spi

UNIVERSITY OF PIRAEUS

OTE
GROUP OF COMPANIES

inno

MOTIVIAN

VTT

Atos

vinasa

CyberSecurity
MALAYSIA

NECTEC
a member of NSTDA

ACICA
ASEAN Chief Information Officer Association

DISE

Thank you for your attention!

https://project-yaksha.eu/

For more information:

Dr. Ioannis P. Chochliouros
Head of Fixed Network R&D Programs Section
Research and Development Dept., Fixed & Mobile
Core Network DevOps & Technology Strategy Division, Fixed & Mobile
E-Mail: ichochliouros@oteresearch.gr; ic152369@ote.gr;

Dr. Alexandros Kostopoulos
Fixed Network R&D Programs Section
Research and Development Dept., Fixed & Mobile
Core Network DevOps & Technology Strategy Division, Fixed & Mobile
E-Mail: alexkosto@oteresearch.gr;