YAKSHA

Realising Honeypot-as-a-Service for IoT Deployments

A. Kostopoulos, I. Chochliouros

Fixed Network R&D Programs Section,

Hellenic Telecommunications Organization S.A. (OTE)

INFOCOM World – Athens, *November 26, 2019*

Scope & objectives

- **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**
2. **To develop and validate a distributed, flexible, cybersecurity solution.**
3. **To enable the *sustainable* uptake of scientific, technical and economic results and foster cooperation and partnerships between EU-ASEAN.**

Architectural Components

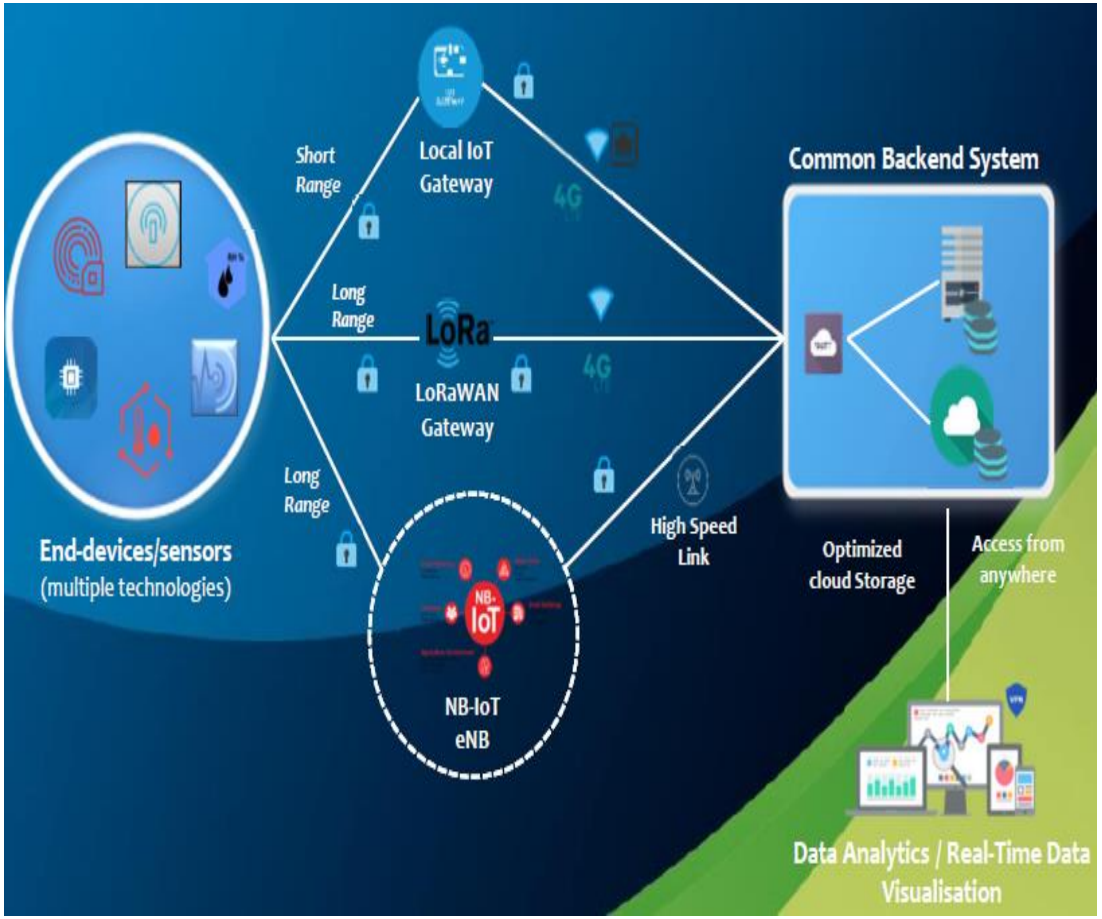
- **A YAKSHA Node:** *On top, the installed honeypots which are exposed to the Internet so that attackers will try to penetrate them.*
    - **Maintenance and Integration Engine:** *Configuration of a new honeypot, uploading and exposing it to the Internet and data wipe.*
    - **Monitoring Engine:** *Sanity checks* to determine whether the honeypot is *properly working*
    - **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**
    - **Connectivity and Sharing Engine:** *Information exchange* with other YAKSHA nodes (*e.g., malware samples*).

Use Case: *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.**



Physical location

The Research Labs of OTE are located in the OTE Academy building.

The physical address of OTE Academy building is:

- *1 Pelika & Spartis St., Marousi, PC 151 22, Athens, Greece.*

OTE's IoT testbed

The IoT testbed includes:

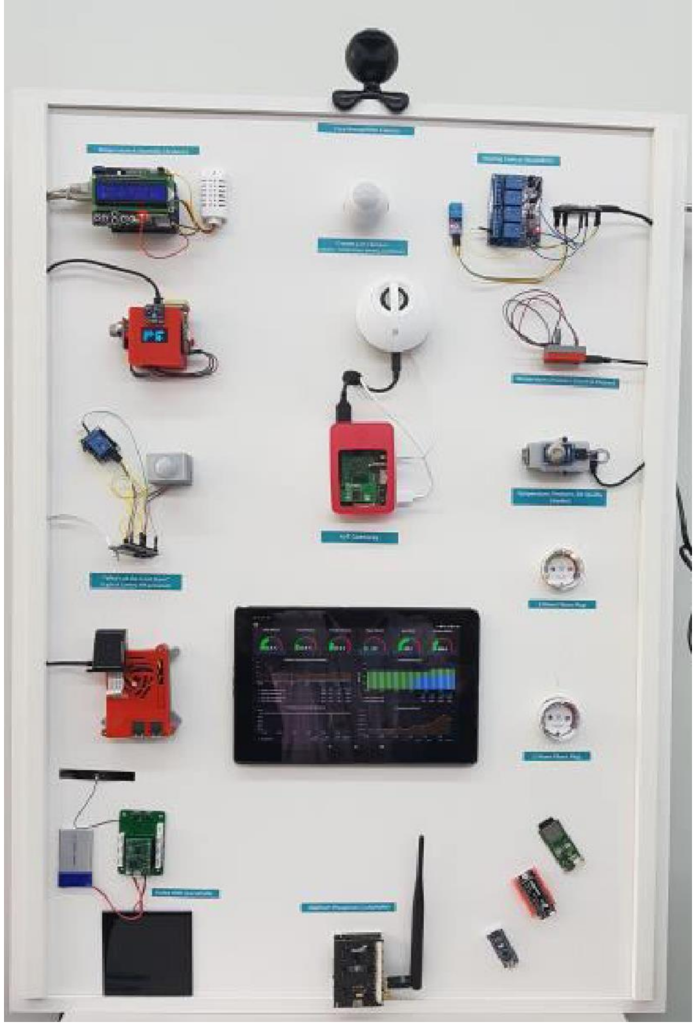
- **A flexible, scalable, end-to-end IoT platform, developed from scratch exclusively by OTE, including:**
  - **A wide range of end-devices/sensors** *such as, air-quality, temperature, humidity, pressure, activity, luminance, fire as well as power/energy ones,* ***communicate with the backend (cloud) infrastructure over a wide range of short/long range technologies*** *(Ethernet, Wi-Fi, z-wave, BLE, LoRaWAN, NB-IoT).*
  - ***IoT hubs/gateways*** *(local and remote – based on LoRaWAN) for facility automation and energy management/control (based on events/rules) supporting multiple HAN/BAN/LAN/WAN technologies/interfaces; over 150 Techs/protocols are currently supported.*
  - ***A (common) backend infrastructure*** *(incl., storage, monitoring/data visualization, command exchange, etc.).*

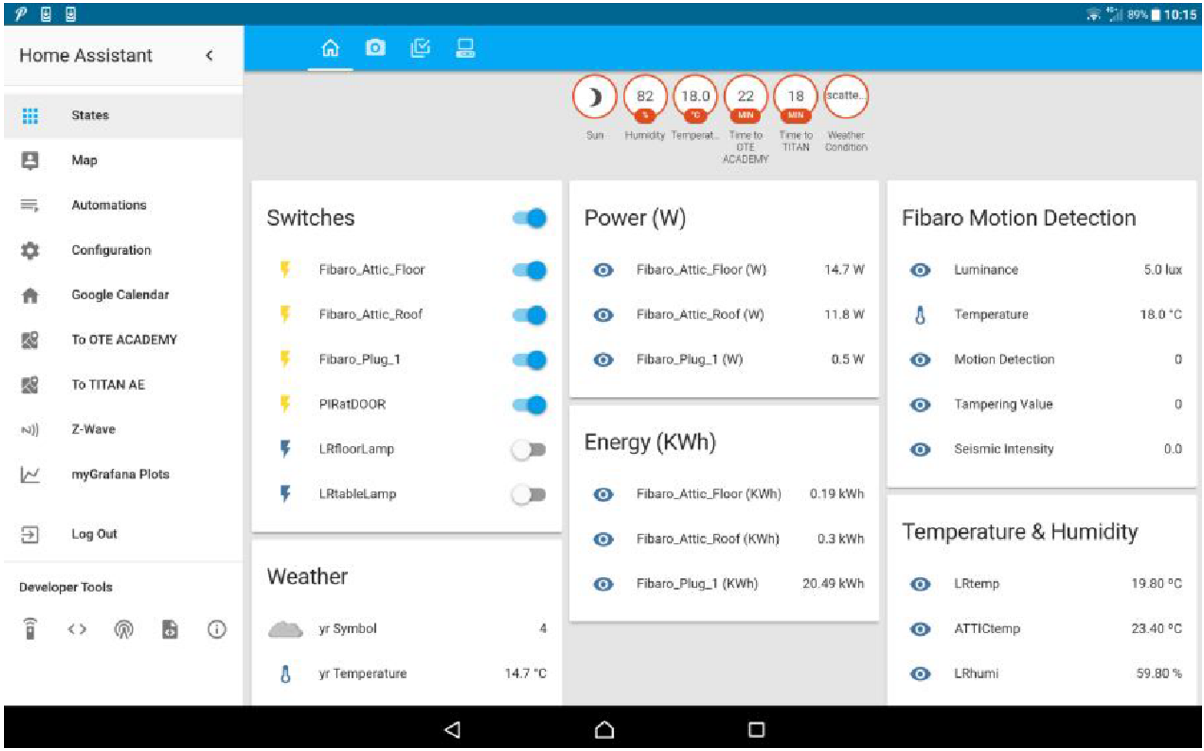
- **LoRaWAN (Long Range Wide Area Network) is a media access control (MAC) protocol for wide area networks.**

  It is designed to allow low-powered devices to communicate with Internet-connected applications over long range wireless connections.

  LoRaWAN can be mapped to the second and third layer of the OSI model.

OTE’s IoT testbed (cont.)





89% 10:15

Home Assistant

- States
- Map
- Automations
- Configuration
- Google Calendar
- To OTE ACADEMY
- To TITAN AE
- Z-Wave
- myGrafana Plots
- Log Out

Developer Tools

Sun	Humidity	Temperat...	Time to OTE ACADEMY	Time to TITAN	Weather Condition
☽	82 %	18.0 °C	22 MIN	18 MIN	scatte...

Switches

Switches	●
Fibaro_Attic_Floor	●
Fibaro_Attic_Roof	●
Fibaro_Plug_1	●
PIRatDOOR	●
LRfloorLamp	○
LRtableLamp	○

Weather

yr Symbol	4
yr Temperature	14.7 °C

Power (W)

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

Energy (KWh)

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

Fibaro Motion Detection

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

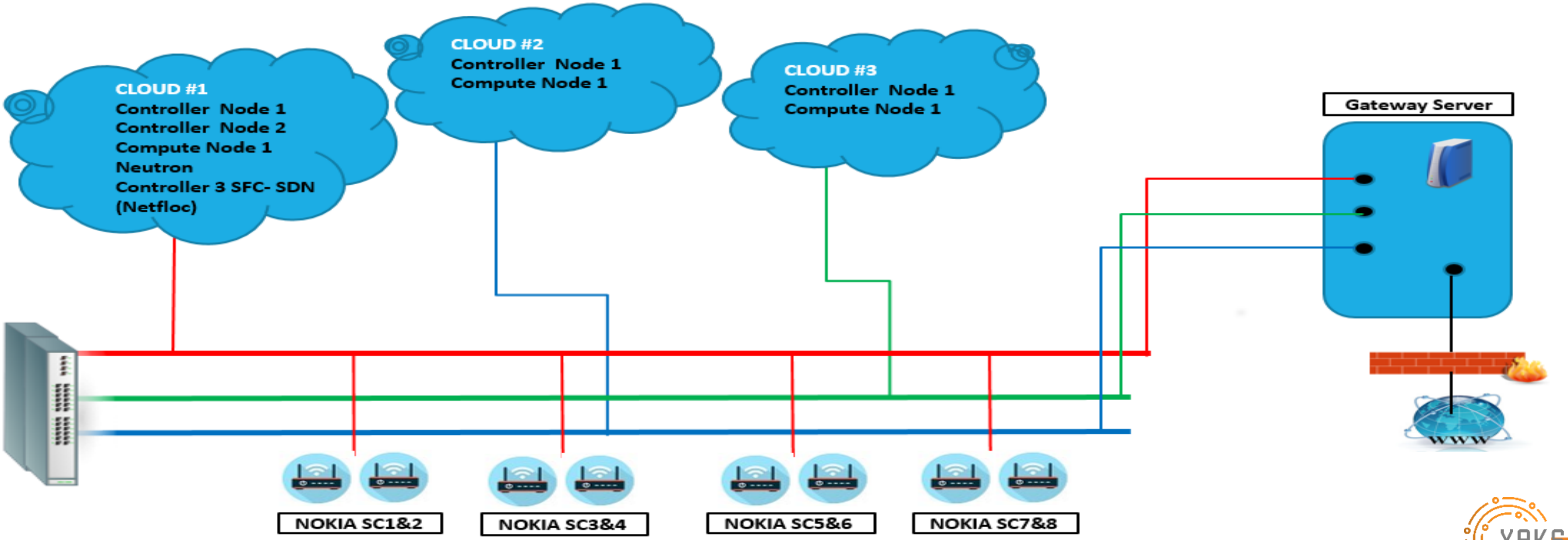
Temperature & Humidity

LRtemp	19.80 °C
ATTICtemp	23.40 °C
LRhumi	59.80 %

OTE's cloud testbed

The cloud testbed includes:

- **An OpenStack-*based* cloud infrastructure** (>220 CPU cores, >30 TB HDD, >340 GB RAM), consisting of 1 gateway, 5 controllers, 4 x86 + 2 ARM-*based* compute nodes, a VPN Server, a CISCO PIX FW, switches/routers, while being interconnected to OTE's Labs, *providing thus additional capabilities for testing new technologies either for PoC or for field trials.*
- **Eight Nokia 4G/4G+/Wi-Fi Small cells** distributed in two floors.
- **A broadband connection over GRNET**, serving as backhaul link.

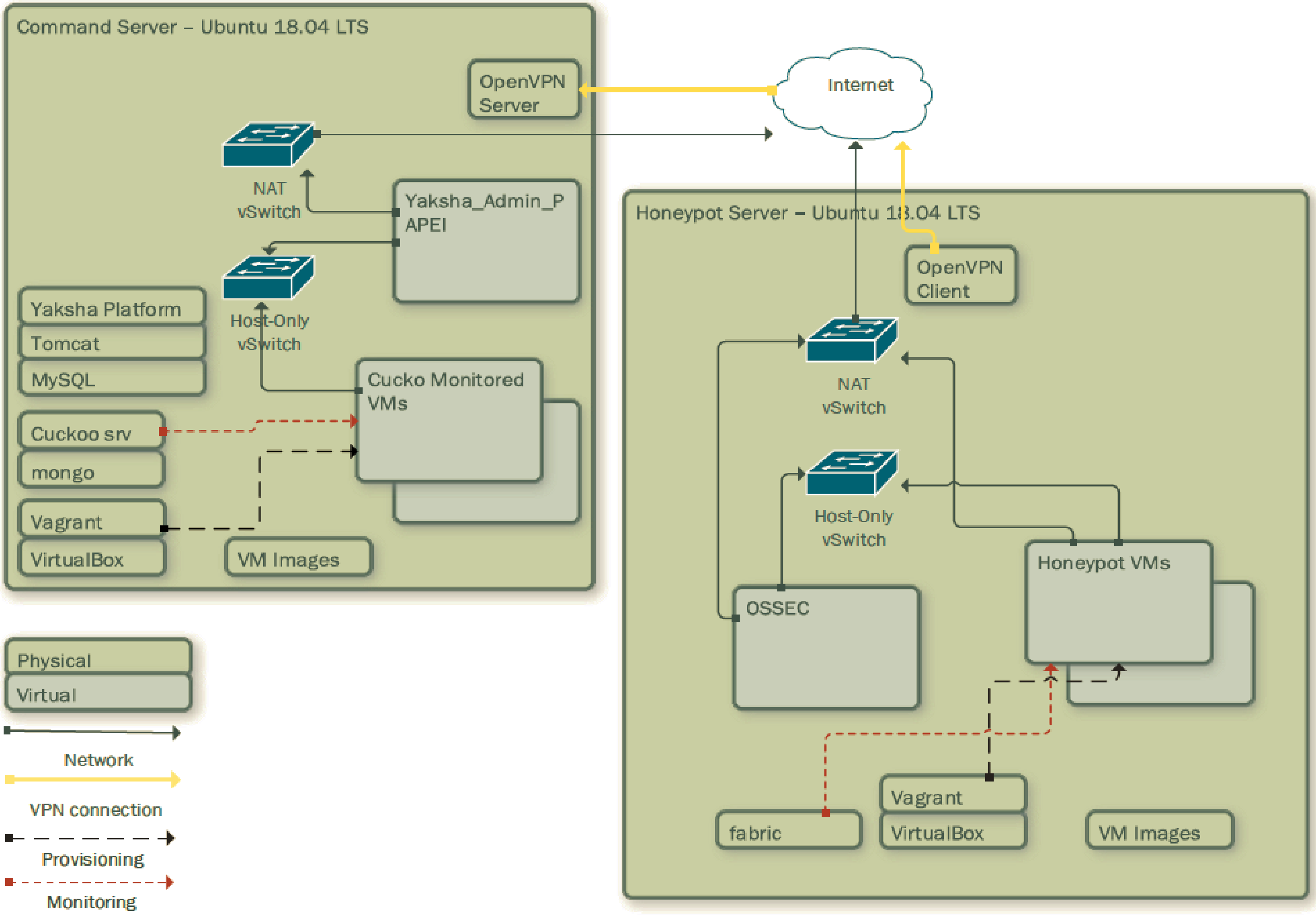


YAKSHA Architecture

The YAKSHA pilot project installation for Greece will handle one end-user node, at OTE premises.

The figure provides a scheme of a typical YAKSHA node, constituted by:

- ***a Command and Control Server,*** *and;*
- ***a Honeypot Server***



Hardware specifications

Server	***Type***	***Specifications***
Command and Control	**Physical**	▪ CPU: support for 4 running threads ▪ RAM: 4GB ▪ Disk: 128 GB ▪ OS: Ubuntu 18.04
Honeypot server	**Physical**	▪ CPU: support for 16 running threads at least ▪ RAM: 32GB or more ▪ Disk: 1T or more (SSD/nvram) ▪ OS: Ubuntu 16.04 or a more recent LTS version

IoT Gateway

In order to send the data generated by the sensors, a gateway is required.
For the YAKSHA pilot, an Up-Board gateway is used:

- *Intel® ATOM™ x5-Z8350 Processors,*
- *4GB DDR3L RAM*
- *16GB eMMC*

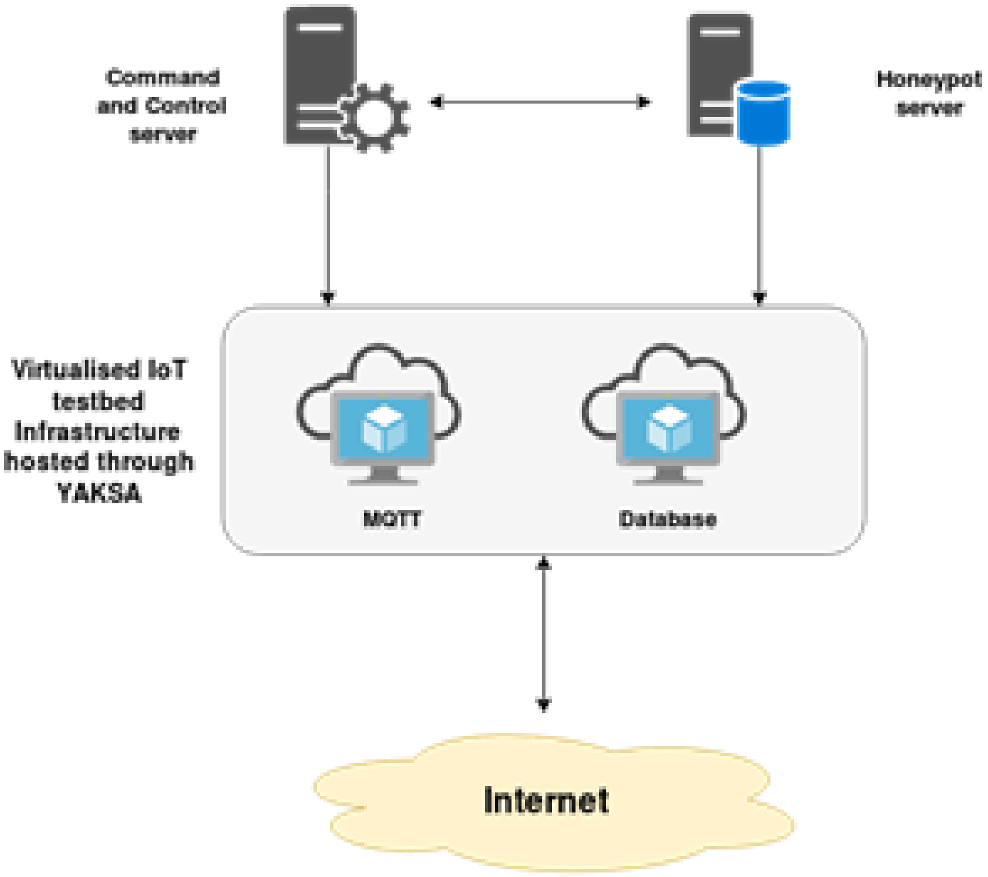
Installing YAKSHA in OTE’s lab testbed

After YAKSHA installation:

- **One physical machine for:**
  - *YAKSHA command and control server,*
  - *YAKSHA honeypot server.*

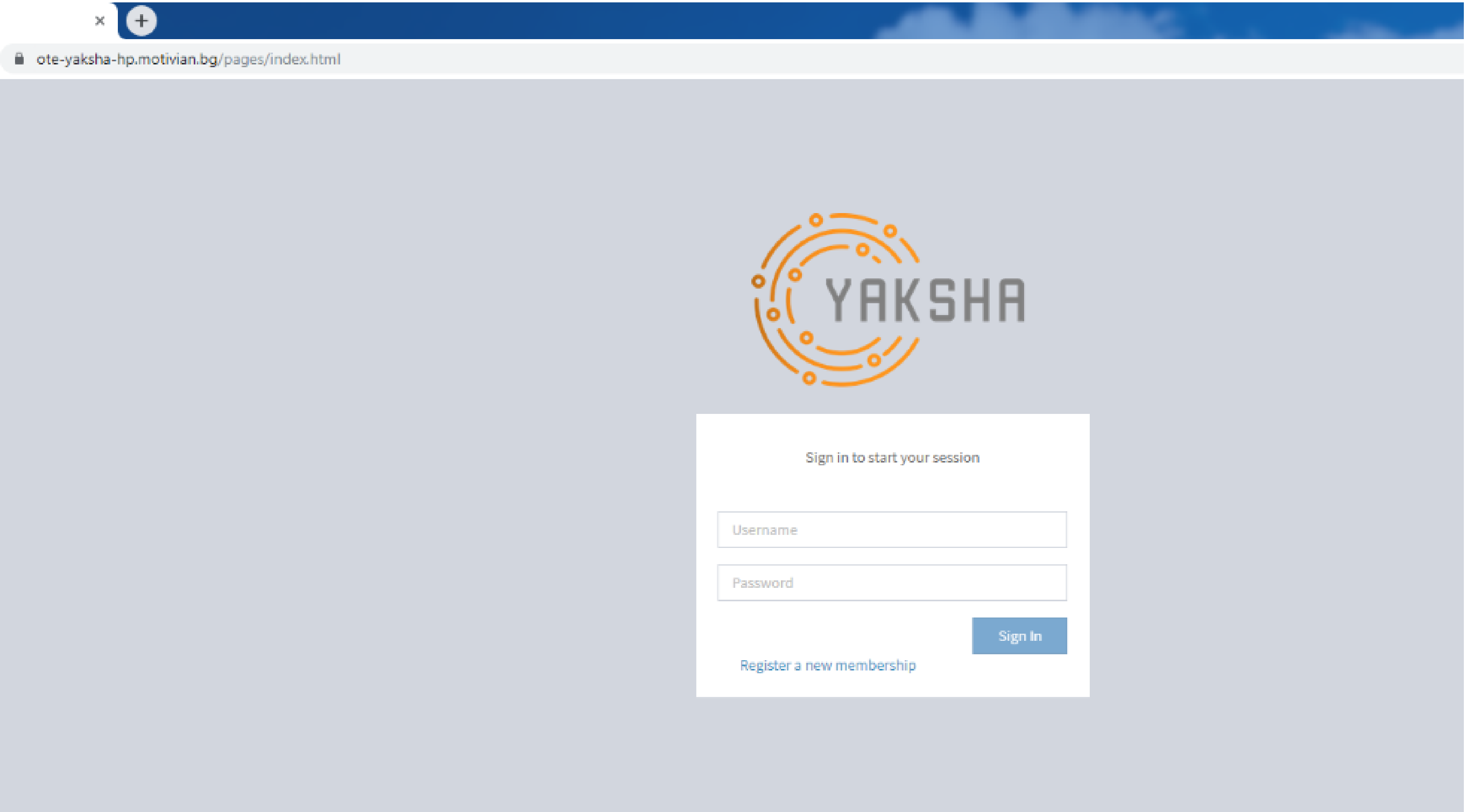
- **IoT testbest consists of:**
  - *MQTT (MQ Telemetry Transport) broker*
  - *Database.*

Each part is hosted on a dedicated virtual machine, which are part of OTE’s cloud infrastructure.


Command and Control server
Honeypot server
Virtualised IoT testbed Infrastructure hosted through YAKSA
MQTT
Database
Internet

MQTT is a machine-to-machine (M2M)/"Internet of Things" connectivity protocol)

YAKSHA Dashboard



ote-yaksha-hp.motivian.bg/pages/index.html

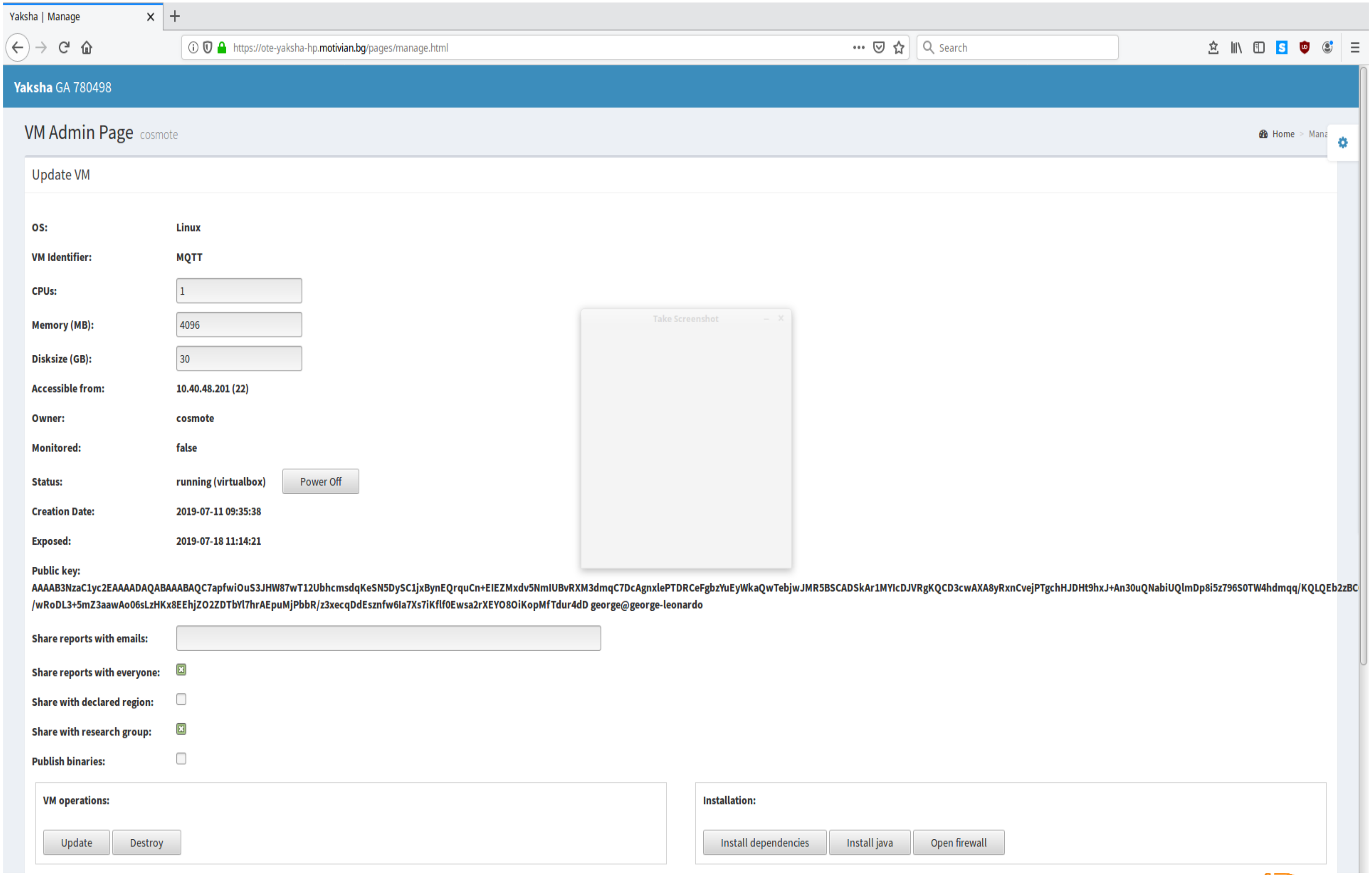
Sign in to start your session

Username

Password

Virtual infrastructure

The virtual machine, which is deployed for the MQTT broker, for OTE's IoT platform.



Yaksha GA 780498

VM Admin Page cosmote

Update VM

OS: Linux

VM Identifier: MQTT

CPUs: 1

Memory (MB): 4096

Disksize (GB): 30

Accessible from: 10.40.48.201 (22)

Owner: cosmote

Monitored: false

Status: running (virtualbox) [Power Off]

Creation Date: 2019-07-11 09:35:38

Exposed: 2019-07-18 11:14:21

Public key:
AAAAB3NzaC1yc2EAAAADAQABAAABAQC7apfwiOuS3JHW87wT12UbhcmsdqKeSN5DySC1jxBynEQrquCn+EIEZMxdv5NmIUBvRXM3dmqC7DcAgnxlePTDRCeFgbzYuEyWkaQwTebjwJMR5BSCADSkAr1MYIcDJVRgKQCD3cwAXA8yRxnCvejPTgchHJDHt9hxJ+An30uQNabiUQlmDp8i5z796S0TW4hdmqq/KQLQEb2zBC
/wRoDL3+5mZ3aawAo06sLzHKx8EEhjZO2ZDTbYl7hrAEpuMjPbbR/z3xecqDdEsznfw6Ia7Xs7iKflf0Ewsa2rXEYO8OiKopMfTdur4dD george@george-leonardo

Share reports with emails:

Share reports with everyone: ☒

Share with declared region: □

Share with research group: ☒

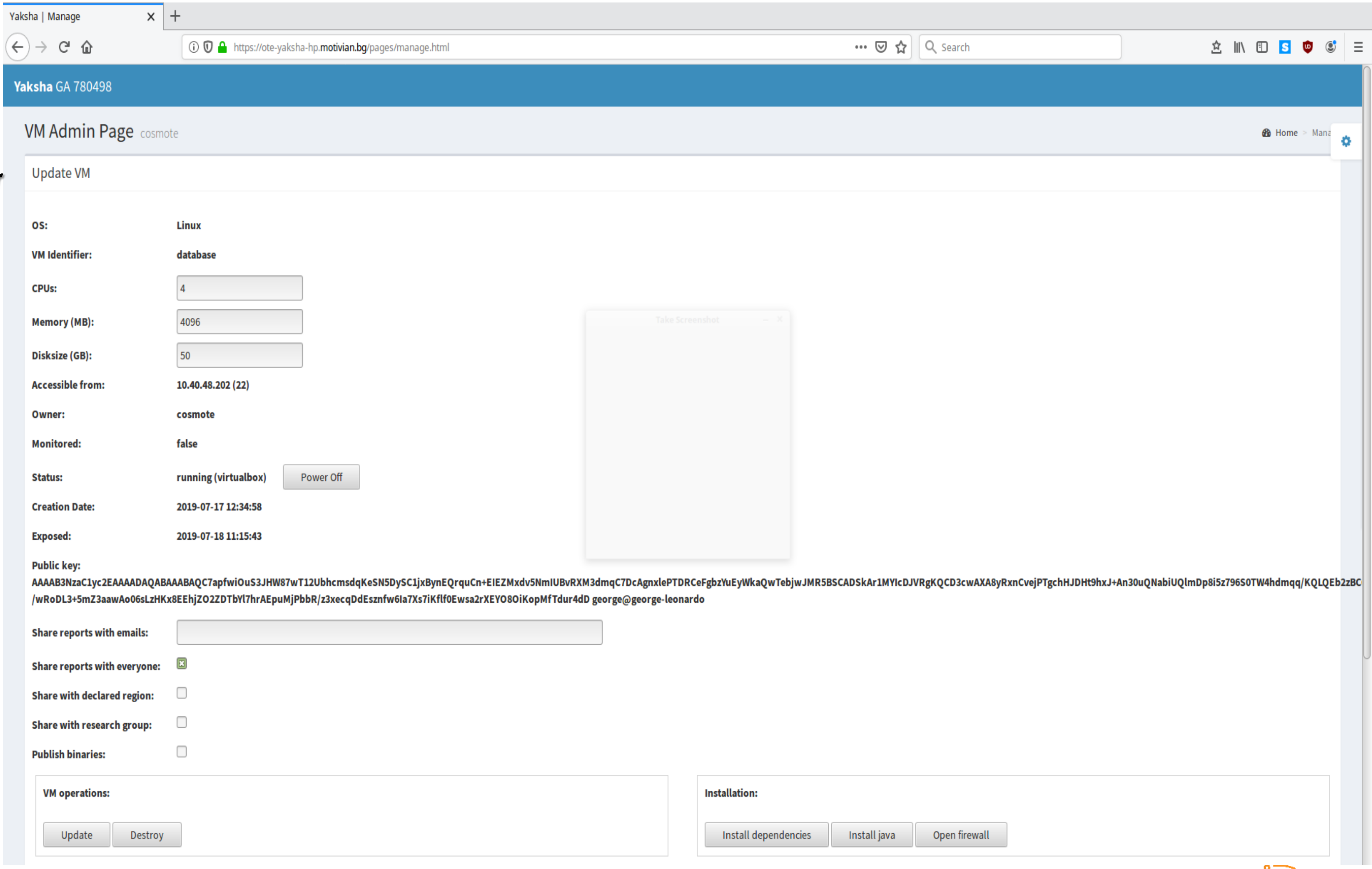
Publish binaries: □

VM operations: [Update] [Destroy]

Installation: [Install dependencies] [Install java] [Open firewall]

Virtual infrastructure (cont.)

The virtual machine, which is deployed for the database, for OTE's IoT platform.



VM Admin Page cosmote

Update VM

OS:	Linux
VM Identifier:	database
CPUs:	4
Memory (MB):	4096
Disksize (GB):	50
Accessible from:	10.40.48.202 (22)
Owner:	cosmote
Monitored:	false
Status:	running (virtualbox) Power Off
Creation Date:	2019-07-17 12:34:58
Exposed:	2019-07-18 11:15:43

Public key:
AAAAB3NzaC1yc2EAAAADAQABAAABAQC7apfwiOuS3JHW87wT12UbhcmsdqKeSN5DySC1jxBynEQrquCn+EIEZMxdv5NmIUBvRXM3dmqC7DcAgnxlePTDRCeFgbzYuEyWkaQwTebjwJMR5BSCADSkAr1MYIcDJVRgKQCD3cwAXA8yRxnCvejPTgchHJDHt9hxJ+An30uQNabiUQlmDp8i5z796S0TW4hdmqq/KQLQEb2zBC
/wRoDL3+5mZ3aawAo06sLzHKx8EEhjZO2ZDTbYl7hrAEpuMjPbbR/z3xecqDdEsznfw6Ia7Xs7iKflf0Ewsa2rXEYO8OiKopMfTdur4dD george@george-leonardo

Share reports with emails:	
Share reports with everyone:	☒
Share with declared region:	☐
Share with research group:	☐
Publish binaries:	☐

VM operations:

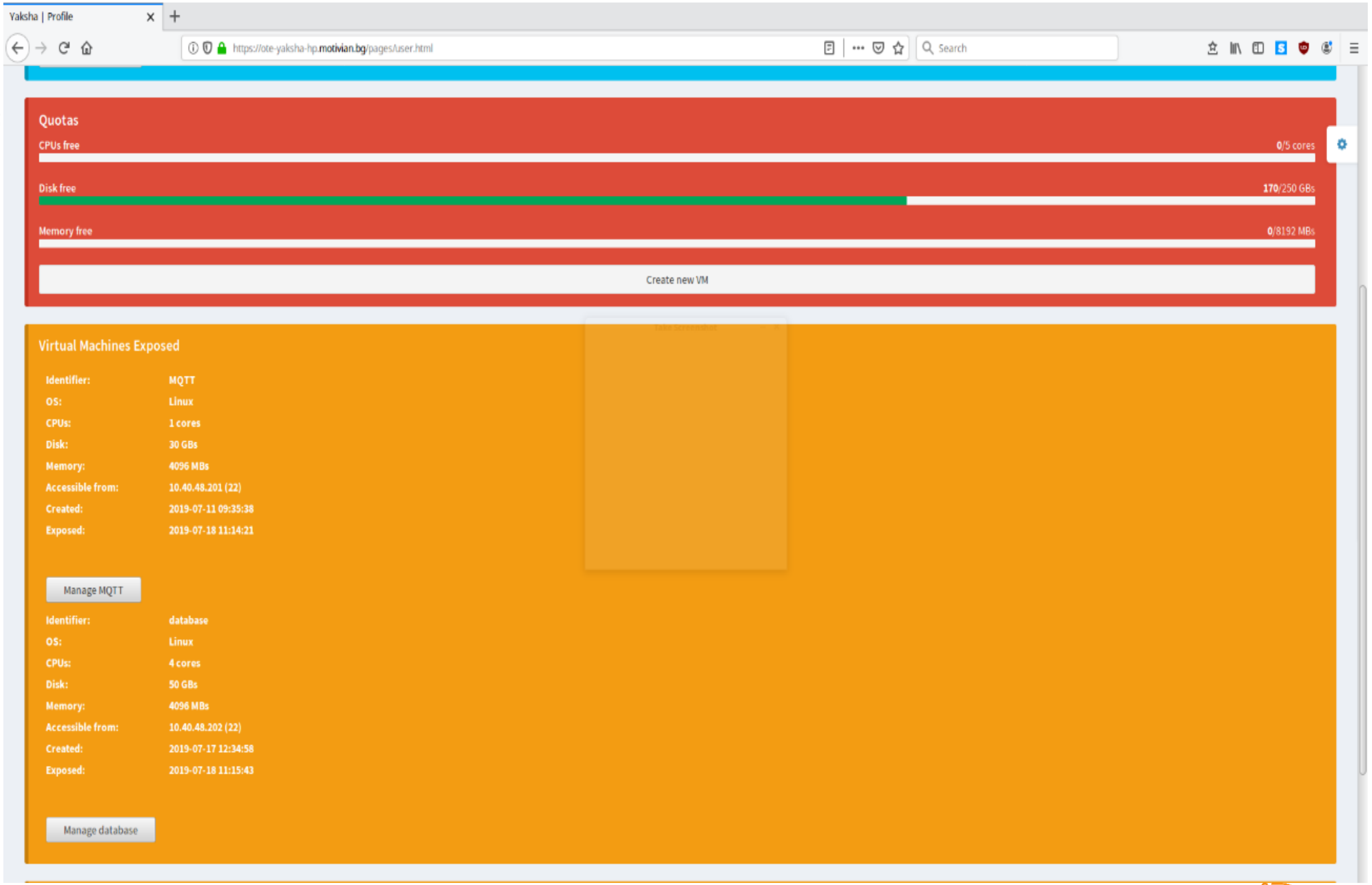
Update Destroy

Installation:

Install dependencies Install java Open firewall

Virtual infrastructure (cont.)

***The characteristics of the deployed VMs** (e.g., CPU, disk, memory, etc.).*



Quotas

CPUs free 0/5 cores

Disk free 170/250 GBs

Memory free 0/8192 MBs

Create new VM

Virtual Machines Exposed

Identifier:	MQTT
OS:	Linux
CPUs:	1 cores
Disk:	30 GBs
Memory:	4096 MBs
Accessible from:	10.40.48.201 (22)
Created:	2019-07-11 09:35:38
Exposed:	2019-07-18 11:14:21

Manage MQTT

Identifier:	database
OS:	Linux
CPUs:	4 cores
Disk:	50 GBs
Memory:	4096 MBs
Accessible from:	10.40.48.202 (22)
Created:	2019-07-17 12:34:58
Exposed:	2019-07-18 11:15:43

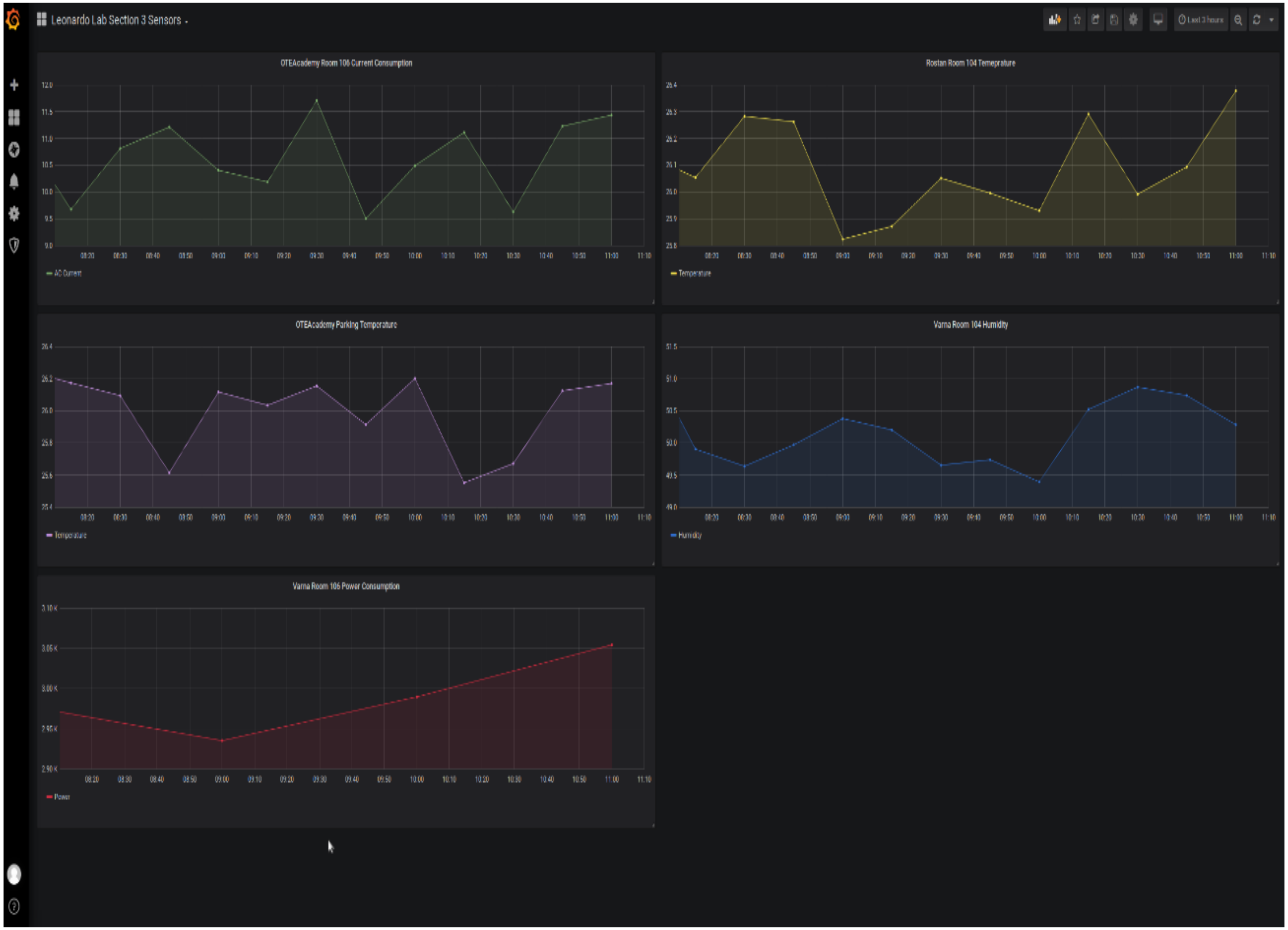
Manage database

Sensors’ data

***All measurements are received from five different sensors, all connected to OTE’s IoT testbed platform*:**

- ***power consumption,***
- ***humidity,***
- ***temperature,***
- ***base stations sites,***
- ***parking area.***

The measurements are visualised by using the Grafana software.



YAKSHA

spi
UNIVERSITY OF PIRAEUS
OTE
GROUP OF COMPANIES
inno
MOTIVIAN
VTT
Atos
vinasa
CyberSecurity
MALAYSIA
NECTEC
a member of NSTDA
ACICIA
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
E-Mail: ichochliouros@oteresearch.gr; ic152369@ote.gr;

Dr. Alexandros Kostopoulos
Research and Development Dept., Fixed & Mobile
E-Mail: alexkosto@oteresearch.gr;