Internet of Things Network Infrastructure for The Educational Purpose

1st Krzysztof Tokarz
Department of GCV&DS
Silesian University of Technology
Gliwice, Poland
krzysztof.tokarz@polsl.pl

3rd Gabriel Drabik
Department of GCV&DS
Silesian University of Technology
Gliwice, Poland
gabriel.drabik@polsl.pl

4th Jarosław Paduch
Department of GCV&DS
Silesian University of Technology
Gliwice, Poland
jaroslaw.paduch@polsl.pl

2nd Piotr Czekalski
Department of GCV&DS
Silesian University of Technology
Gliwice, Poland
piotr.czekalski@polsl.pl

5th Salvatore Distefano
Department of Computer Science and Engineering
University of Messina
Messina, Italy
sdistefano@unime.it

6th Riccardo Di Pietro
Department of Computer Science and Engineering
University of Messina
Messina, Italy
rdipietro@unime.it

7th Giovanni Merlino
Department of Computer Science and Engineering
University of Messina
Messina, Italy
gmarlino@unime.it

8th Carlo Scaffidi
Department of Computer Science and Engineering
University of Messina
Messina, Italy
cscaffidi@unime.it

9th Raivo Sell
Department of Mechanical and Industrial Engineering
Tallinn University of Technology
Tallinn, Estonia
raivo.sell@taltech.ee

10th Godlove Suila Kuaban
Institute of Theoretical and Applied Informatics
Polish Academy of Sciences
Gliwice, Poland
gskuaban@iitis.pl

***Abstract*—In this innovative practice full paper we present the implementation of the distant laboratory for the Internet of Things teaching and training. The recent outbreak of the SARS-COV-2 virus and related COVID-19 pandemic throughout the world has caused governments across the world to shut down schools and universities, to slow down the spread of the coronavirus that is causing the disease. As a result, some universities and schools have switched from physical classrooms to virtual or online classrooms. This approach is working well for theoretical subjects and courses, but it is not straight forward in the case of laboratory subjects and courses that require access to hardware resources. The IOT-OPEN.EU remote laboratory infrastructure presented in this paper is a timely solution. In this paper, we present current advances in distant learning, distant laboratory models, and the IOT-OPEN.EU remote laboratory implemented as part of the IOT-OPEN.EU ERASMUS+ project, along with short analysis on current advances in distant learning, where students are interacting with physical hardware remote way.**

***Index Terms*—Internet of Things, IoT, Distance Laboratories, Remote Laboratories, Distant Education**

I. Introduction

Internet of Things (IoT) became one of the key branches of the modern digital era. Without a doubt, we observe a vast number of opening positions related to the IoT on the professional market in both hardware and software, research and development and implementations. Gartner's report dated 2019 predicts 5.8 bln IoT end nodes by the end of 2020 [1] while IoT impact on the global business was estimated at 11.1 trillion USD by 2025 [2]. There is an observable need for qualified engineers and technical staff related to the IoT, including hardware and software developers, IoT network, energy efficiency, and IoT security specialists as well as IoT solution designers. As we IOT-OPEN.EU was started to provide standardized IoT training for bachelor's level, masters level, professionals who are already beyond their regular education but are about to dive into the IoT world because they're willing to or are required by their commercial

needs. Parallel and independently of the IoT development, we observe how classical teaching changes, from classical lectures, classes and laboratory exercises towards self-paced learning, using online resources.

This process was suddenly sped-up along with the outbreak of the SARS-COV-2 virus and related COVID-19 pandemic that forced universities, school teachers and trainers to rapidly switch from classical into online learning. Also, from the social point of view, distant learning is no longer the domain of amateurs, enthusiasts and hobbyists providing some information on their blogs, and vlogs: development of the massive online learning platforms (MOOCs) like, i.e. Coursera, EDX or Instructables, shows future development of training and teaching methodologies.

Nowadays it is not unusual to use, i.e. Youtube, Github or Wiki (i.e. Dokuwiki) for authoring and delivery of the teaching material. Of course, their credibility can be in doubt, so selecting trustworthy, up-to-date and credible material is a challenge. Interestingly, thanks to the WEB 2.0 development, and the possibility to comment on the content, one can find early symptoms of incredible ones.

In the paper, we summarise the results of our IOT-OPEN.EU, an Erasmus+ funded project, that was intended to deliver high-quality study materials within the IoT scope. In particular, we focus only on one aspect of the project: VREL - virtual, remote access IoT laboratory nodes that everyone can access using the web browser only, however, we also present briefly other components of the project to present how VREL IoT laboratory relates to it.

II. Current Advances in Distant Learning

Distance learning became a popular approach to deliver knowledge in modern university education. In addition to primary teaching aids such as e-books and other electronic teaching materials, video lectures, tests and quizzes that are available on most e-learning platforms laboratories with remote access are particularly helpful in teaching technical subjects. In the literature, we can find descriptions of many examples of distance laboratories created to support teaching in many various areas of technical study.

In [3], the authors presented some real cases in distance learning courses in the Industrial Engineering School at the Universidad Nacional de Educación (The Spanish Open University), Madrid, Spain. Their approach combines individual and collaborative learning in remote and local laboratories, in a distance learning context, and proposes the use of a Web-based experimental environment called Active Document [4] to improve the development of reasoning skills in practical work. The learning environment they proposed is used to organize and invoke the different computer tools that make up a virtual chemistry lab. Experiments may be structured in a way that enables students to perform lab work with colleagues, which is both more motivating than doing it alone and also allows students to learn to collaborate.

In [5], the authors described their Practical Experimentation by Accessible Remote Learning (PEARL) system, which allows students to work together while at a distance from the laboratory site, using a range of synchronous and asynchronous communications tools. They illustrated some experiments as a demonstration of the potential and validity of their approach. Experiments developed include an implementation of a remote electron microscope, a spectrometer, visual inspection of printed circuit boards and a digital electronic bench.

In [6], the authors present IoT Rapid Proto labs designed as authentic, productive learning environments. Their approach is based on three design principles: 1) Realistic, complex task situations, 2) Multidisciplinarity, and 3) Social interaction. The laboratory settings proposed by the authors is not a pure remote lab, however, rather blended (virtual as well as real), user-driven, and productive learning environment, supported also by Project Arena (a web-platform), which enables learners to effectively collaborate on rapid-prototyping of IoT products/services stimulating the flow of knowledge and innovation between higher education, enterprises, and other stakeholders.

In the paper [7] the authors present an approach that aims to transform traditional computer labs into virtual lab environments. The work recognizes two categories of experimental setups, where slightly different approaches are needed. The first category is software-based experimentation. The second category is hybrid experimentation, where software and hardware experimentation need to be conducted within the same experience. The proposed design relies on the concept of "virtual presence" whereby the students and their home computers appear as if located inside the lab.

In [8], the authors discuss the disadvantages of software simulation. They claim that while simulation packages have a significant place in Distance Learning (DL), they can never replace the need for real labs where students can construct their knowledge and put their theory and practice to a real test. Therefore, they argue that a Remote Laboratory (RL) expands the efficacy of a DL. Moreover, they present an alternative to simulation as developed two prototype laboratories for electrical engineering and physics.

In [9], the authors present a study, carried out in a Higher Education Institution in Brazil, where a remote lab (VISIR), addressing electric and electronic topics, was implemented, yielding 471 students' academic results and opinions. The results reveal some factors teachers may tackle to foster student learning and motivation. Teachers' involvement plus their ability to brief students on VISIR's usefulness have a significant influence not only on students' performance but also on their perception of learning and satisfaction with the tool.

In the paper, [10] the authors present remote access for a laboratory experiment that involves measurement of a volt-ampere characteristic of a semiconductor diode. The remote laboratory assumes using real equipment with setup controlled over the Internet, and with a video camera to display readings from real instruments to the learner. Paper [11] presents the description of some examples of remote laboratories created in Australia and some European countries. They are mainly

electric, microelectronic, control or computer laboratories but there are also realizations in the disciplines of physics, mechanical and mechatronic engineering including gasoline motors, pneumatics, material testing, plasma diagnostics, and radio-physics.

An IoT remote access laboratory idea appears in [12] in a context of the resource sharing between rich and poor schools in South Africa. In this particular example, the authors present a closed system with a remote interface to manipulate a robotic arm (controlled with the Arduino) to perform various chemical experiments. The distant student can remotely manipulate the physical device and observe results through the Internet with means of the video stream and sensor outputs.

In the paper [13], the authors present a RAL (Remote Access Laboratory) for the purpose of the Queensland (Australia) primary school where approximately 76% of pupils study remotely. It is because of the specific inhabiting conditions in Australia, where many people (including children) live in distant locations and cannot send children to school daily. The project applied to children aged between 7 and 12. In this laboratory, Meccano SpyKee robots were used (a humanoid form) that were controlled using PCs and connected wireless using WiFi. In particular, relating to the aforementioned Queensland case, the authors in the paper [11] present in-depth analysis of more, selected cases, where they tell a short story of RALs in various regions and universities across the world. The authors pay attention to the different reasons for driving RAL development in various regions of the world. In the case of large countries with small populations like Canada, Australia and Russia, development of RALs according to the authors, was driven mostly by physical distances and lack of access to the educational resources. In case of Europe, this one was technology-driven and introduced with various EU funded grants, to lower differences between developing and developed countries by providing access to the research and educational infrastructure across educational bodies and also to optimise setup and maintenance costs.

An interesting case study of the distant learning process using remote access laboratories is presented in the paper [14]. The authors point out differences between classical (on-site) and on-line, distant learning and propose a pedagogical approach with the goal-oriented approach and three-phase educational process including ”pre-lab”, ”lab-phase” and ”post-lab” steps to achieve best results.

In the paper [15], the authors start from the same conclusion as the authors of the IOT-OPEN.EU project, where students entering STEM education on any level face lack of IoT courses. The authors propose a learning framework on IoT, integrating hardware, software and communication, however mostly using available components (i.e. ThingSpeak, Google Cloud Web Services) and base on existing embedded systems course, extending it towards IoT education.

One of the key assumptions of the IOT-OPEN.EU project was the placement of laboratory equipment among different partners. A similar approach is presented in the paper [16], where the HVAC laboratory has been created in the cooperation between the US and Switzerland universities. The authors created a laboratory in which US students could make research on a heat recovery system that was physically located in Switzerland. Swiss students also had access to a variety of equipment located in the US. The authors of the paper [17] describe a virtual laboratory designed for teaching the Internet of Things course. Students can create a model of the IoT system using provided sensors and actuators. Components of the system are created with the use of popular Arduino and Raspberry PI microcomputers; students can use them only with API provided. In our approach, students can not only utilize functions for reading or sending data to the IoT nodes but can reprogram the firmware using C language remotely. The base environment that our distance laboratory uses has been created at Tallinn University of Technology. It is described in the paper [18] in details, and possible outcomes of the approach where we use distant labs, along with the case study and impact on the teaching results is presented in the paper [19]. This teaching tool is created as a rich Internet platform, where different remote and virtual labs are integrated. The DistanceLab is designed to enable programming and controlling the connected devices via the web interface. It is done with a web-based programming environment: an automatically invoked compiling process and possibility of flashing programs directly to the connected devices. In the publication [20], the authors present an extension of this lab towards robotic applications.

III. IoT Devices and Platforms Towards Education

As the Internet of Things emerged rapidly, many STEM (Science, Technology, Engineering and Mathematics) educators found themselves with a lack of curriculum on the IoT. On the other hand, technical universities, VETs (Vocational Education and Training) and professional training centres had already vast experience in automation control trainings, usually homogeneous technology/manufacturer oriented courses for professionals to earn a certificate on some technology; embedded system courses for university students; digital circuits and electronics courses, networking and mobile devices programming curriculum and modules and others, related to the fundamentals of the IoT. All that composes solid and concrete fundamentals for introducing IoT into education.

A common challenge in case of the IoT courses is a need to provide to the audience an experimental part like, i.e. laboratory. It can be a form of laboratory activities or project, and this need is growing with the introduction of project-based and experiential-based learning. Many vendors currently deliver environments for the IoT labs in a form of the development toolkits that are usually bound to some particular software development kit, proprietary software and closed solutions. Training centres usually are offered with a free or discounted solution (including hardware and software samples and even full sets) and are unable to implement their own laboratory environments from scratch, because of lack of resources. This kind of approach follows the schematics where vendors want to “bind” trainers and students to their technology solely, and finally causes tailoring of the curriculum to fit one, specific

IoT solution provider. While this is acceptable in the case of the VETs training willing to obtain education and certification for specific product or system, it is rather unacceptable for universities and comprehensive STEM education.

In any case, implementation of the laboratory rooms on its own is costly, time-consuming and of low flexibility. Additionally, large market players provide free (or limited) services like, i.e. Azure, Watson, Google IoT services, delivering defacto flexible, yet, software-only IoT frameworks. Surely, those are useful in the education process as access is virtual, and it is pretty easy to use any of them, but without IoT hardware, it is only just a piece of the IoT puzzles needed for comprehensive engineering education nowadays. In many cases, IoT systems are provided to the students with means of simulators. While it is an essential part of the teaching and training, simulation cannot replace interfacing the real hardware with their vulnerabilities, failures, timings and other physical phenomena, usually not simulated.

An ideal approach to the IoT devices and platforms should then promote IoT laboratory solutions that are:

- easy to implement and maintain;
- provide touch with real hardware (not simulated one);
- include a variety of devices (platforms, sensors, actuators);
- integrate easily with other services;
- provide the ability to set up heterogeneous IoT networks;
- simplify user access, possibly over the web, without the need (or with scope) of software installation and configuration;
- ensure security for both users and infrastructure;

IV. IOT-OPEN.EU Project

IOT-OPEN.EU is an educational project within the Erasmus+ Key Action 2 framework, oriented towards Strategic Partnership between Higher Education (HE) and also commercial bodies. In 2015, once the project idea was born, there was no standardization in IoT teaching, and training and not so many universities had courses related to the IoT. On the other hand, the IoT idea was rapidly accepted by the industry, along with Industry 4.0 and "Smart" devices development. The commercial market expected universities to provide IoT courses to their students to let them become well-trained engineers, ideally with practical experience in the IoT systems and devices. This situation presented a gap between HE and European digital market expectations.

Those key facts lead to the shape of the grant, where 6 partners: 5 HE bodies and one SME (Small-Medium Enterprise company) decided to prepare a standardized solution for IoT teaching and training on various levels of education, starting from those who never heard about IoT, finishing on R&D opportunists, seeking for research ideas. Moreover, materials prepared within the IOT-OPEN.EU was classified, and a track for non-HE was identified, as, i.e. for hobbyists that are willing to play with IoT and VETS, on their professional careers, willing to extend or adapt their positions to the labour market requirements.

Within the scope of the project, there were 3 major results planned and implemented:

- A set of materials for classical courses held at the university within the IoT fields, composed of IoT coursebook, number of DLP (Digital Light Processing projector) presentations to be provided for students with classical, auditory based lectures and on-site laboratories accompanied with hand-on labs manual.
- A purely online, self-paced courses in the form of MOOCs, available via edX.org and local platforms, kept by HE consortium participants.
- Several heterogeneous IoT laboratory nodes with remote access (VRELs): virtual and distant access laboratory nodes, implemented in different countries yet able to integrate additional services and cross-cooperate between different, physical locations. Nodes present different hardware and provide an opportunity to implement different IoT scenarios. Classical course and online one can be treated as stand-alone or supplemental. In any case, VRELs bring the practical, laboratory opportunities to interact with real, physical hardware, whether students choose to study on-site or online.

The components mentioned above compose the IoT educational framework, introduced and implemented within the scope of the IOT-OPEN.EU. In this paper and the following sections, we focus on the VREL part. VRELs constitute a key component in the IoT training enabling students to be able to interact with real devices during their study track even if they're unable to access them physically because they have no technical background or cannot afford to buy one. MOOCs and VRELs together provide a robust solution for all those that are unable to attend university for the regular course, whether because of lack of resources, living in a remote area, being disabled or because of any other reason, but are still willing to participate in the IoT revolution.

V. Distant Laboratories Model

Concluding requirements presented in chapter [IV], it was identified, that the most problematic part in introducing IoT modules into the curriculum are laboratories using end nodes layer and fog layer devices, that will provide additional services, merging IoT network and the Internet, mostly with means of routing (but not limited to). Other resources are usually readily available as a variety of them is already present on the Internet or can be provided with this way without any particular obstacles. Our VREL laboratory solution provides IoT infrastructure, that tackles IoT end nodes and fog layer services.

VREL laboratory implemented within the frame of IOT-OPEN.EU project has distributed hardware and software resources across 3 European countries: Estonia, Poland, and Italy. Usually, laboratories with remote access provide limited API that end-users (here students and supervisors) can use, implementing a closed number of scenarios. In the case of VRELs, there is low-level programming support that enables

a virtually unlimited number of scenarios, that can be implemented. This approach, however, requires that all components of the VREL infrastructure are safe to operate on this level of access thus require detailed and careful design, in particular regarding hardware and mechanical parts as real IoT solutions virtual laboratory nodes should contain both sensors and actuators.

Users should be able to access the system with means of a single, universal and standardized interface, regardless of their location and physical location of the laboratory infrastructure. Moreover, all tasks should be implementable using a web interface; thus, users only need an Internet connection and a web browser to use it. System interface for one of the VREL nodes is presented in Fig. 2.

Users should have the ability to book (reserve) a device(s) in an exclusive mode. Low-level programming usually also means that development requires dedicated libraries to interface hardware. Seamless library management is a complex challenge, as there are usually many libraries supporting particular hardware. Because of it, library management should be simplified and consistent across all laboratory components, constituting a solution that includes versatile possibilities like automatic updates or locking on a particular library version. Last but not least, users implementing networking should be able to create consistent communication solutions among nodes located in different locations (even countries), access other components like, i.e. cloud resources. On the other hand, users using in particular wireless interfaces should be limited to access hosting infrastructure, to limit vulnerabilities, implemented either voluntary or involuntary while performing exercises.

VI. VREL Implementation

Distant, remote access IoT laboratories implemented within the scope of the IOT-OPEN.EU project was settled in three European countries: Estonia, Poland and Italy. Other grant partners performed their end nodes tests and integration with the IOT-OPEN.EU VREL Central Server platform successfully and are awaiting future integration, possibly during the following extension of the grant. Locations of the system components across Europe and grant partners are presented in the Fig. 1.

On the hardware level, two platforms were chosen as presenting current trends for popular end node MCUs:

- Arduino Uno (Atmel) MCUs: ATmega328P;
- Espressif NodeMCUs: ESP 8266 (ESP-12E);

Additionally, RPi (Raspberry Pi) v.2 and v.3 boards were used to implement router/MCU remote programming interfaces and video streaming for the laboratory nodes. The software of choice for video streaming was open source Motion server. RPi platforms were also used to implement some of the integrated networking services along with PC computers. We used regular IP networking (IPv4); however, other radio interfaces may be connected to the laboratory platforms with ease, to extend networking capabilities and to implement pure IoT networking, like, i.e. 6LowPAN.

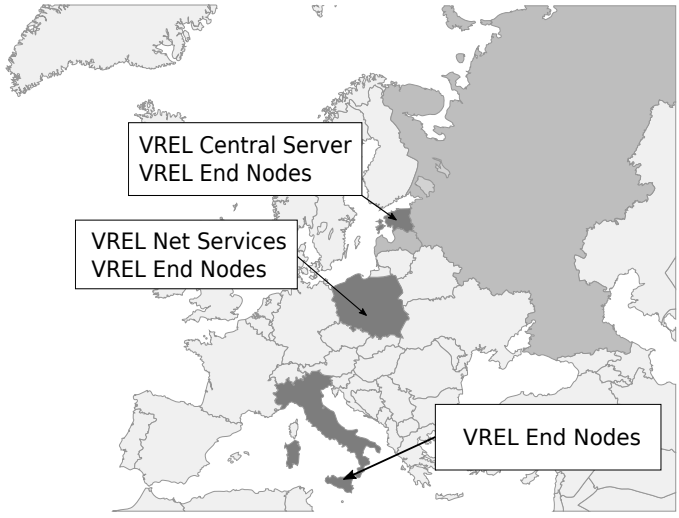

Fig. 1. IOT-OPEN.EU VREL infrastructure across Europe

The user interacts with the system using a web browser and receives feedback via text messages (regarding compilation, upload and flashing) and visual feedback from the integrated web cameras. Each end node contains at least one web camera while some of them are equipped with more, i.e. to present precise visual effect like, i.e. LCD display. The sample user interface is presented in Fig. 2.

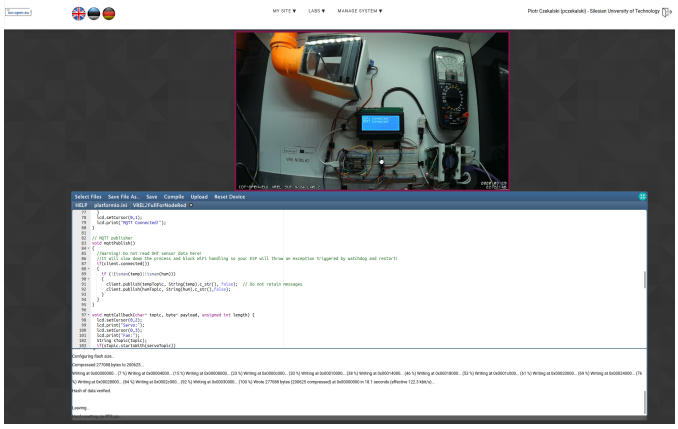

Fig. 2. User interface for the end node programming in C++

The general schema of the VREL infrastructure is visualised in Fig. 3. End nodes are grouped physically in remote destinations related to the grant partners, however within the scope of the local resources they are or may be distributed among different locations, i.e. SUT (Silesian University of Technology) uses devices (end nodes) located in various locations, including i.e. building roof for environmental measures, simulating heating and cooling of the smart house (Fig. 4) but also nodes located indoors (Fig. 5).

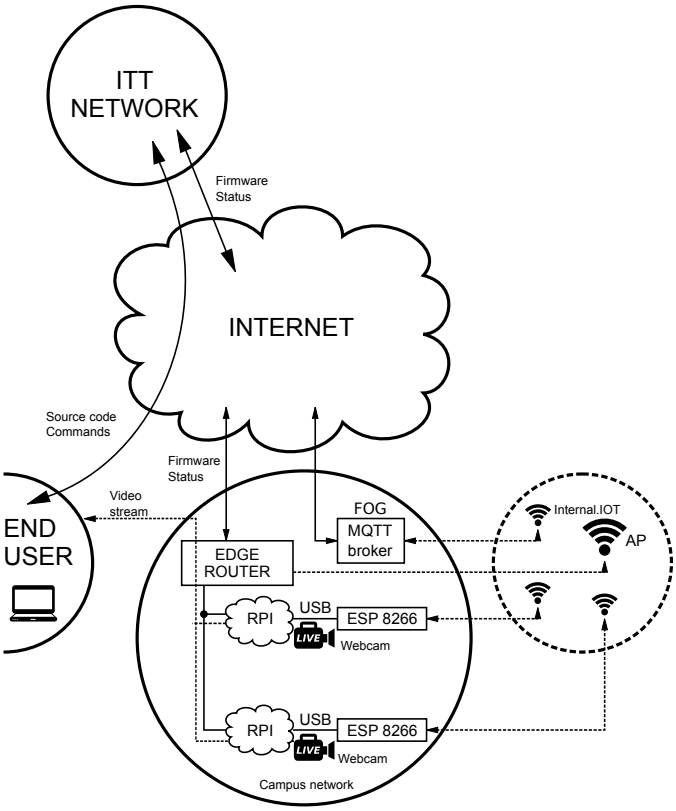

Fig. 3. VREL infrastructure

Fig. 4. VREL SUT roof top thermal smart house laboratory end node

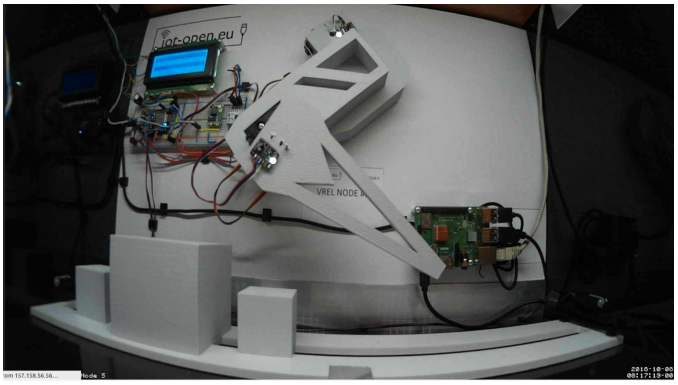

Fig. 5. VREL SUT indoor laboratory end node

A. VREL Management System and Front-side Services

The primary services for the solution are located in Tallinn/Estonia, implementing user front-side with rich web interface that includes source code editor and file manager, user management system with roles, device booking features and remote communication centre. This services also integrate source code storage, source code compilation tool-chain for various platforms (including two aforementioned) and development library management services. Part of those features is implemented with means of popular PlatformIO framework, that in details is being used for library management and for source compilation. PlatformIO also handles libraries and framework/compiler tool-chain updates, performed on demand (not automatically).

As the VREL system is used by partner universities (users), a separate user management system was introduced and integrated: any user willing to use VREL laboratory nodes must register an account. That is a requirement to enable exclusive device booking to let users do not interrupt one another during experiments.

Users can book more than one device at a time, thus it can create complex networking solution itself or can cooperate with other users and services using local networking and Internet services. Central management system stores user files (per user) as well as templates (per end node), so users can temporarily suspend their work and return later. That enables teaching scenarios with continuous laboratory work, where students develop their solution over a number of meetings, implementing project-based learning model.

Finally, central VREL management server provides compiling features for C++ code, with respect to the specific requirements given by platforms, i.e. memory limits, memory mapping, and adding resources. Once the firmware package with source code is created, it is then injected through the SSH channel (additionally secured with a VPN connection) into the proxy/routing/programming devices (here RPi). Then RPi flashes MCU using integrated programmer, via USB interface. Use process is presented in Fig. 6.

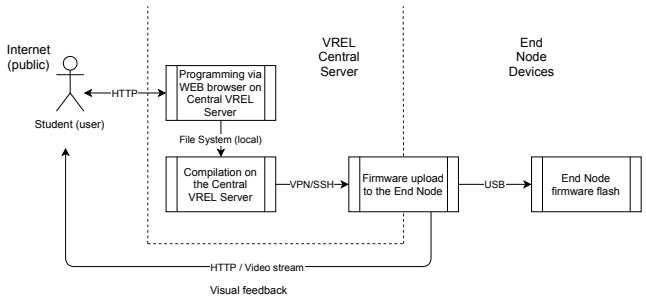

Fig. 6. User interaction

B. End Nodes

End nodes represent various hardware, including at the moment aforementioned: Arduino and ESP 8266 MCUs, temperature and humidity sensors, light level sensors (here for

measuring the reflection of the light to detect flap movement), 6DOF IMUs (Gyro + Accelerators), servos, stepper motors, high power LEDs, LCD displays and colour RGB sensors. It is assumed that every single end node should be able to access network directly or indirectly. Also, local network (among nodes) should present to limits to let students be able to implement various communication scenarios, even "dangerous ones", like i.e. IoT security related ones (i.e. hacking). Whilst devices are located in the separate network, this is not considered to be serious vulnerability. VREL nodes provide ability to let students practice interaction with various sensors and actuators using different, low level protocols. That covers in particular:

- digital inputs and outputs;
- analogue inputs using A/D converters (built in into the MCUs);
- communication with external sensors using SPI, I2C, OneWire and Serial protocols;
- simulating analogue output using PWM, directly over GPIO and indirectly through I2C expanders;
- controlling servos;
- controlling step motors;

Aforementioned list is non-exclusive, but presents core of the IoT technologies. It prepares students to implement IoT devices from scratch, in most real-live scenarios even if laboratory nodes seem to be synthetic.

C. Network Integration and Services

As experimentation with IoT systems requires network connectivity, natural choice to bind distributed laboratories is the Internet network. Because of the diversity of hardware platforms, there were two implementations of layer 1 and 2 chosen:

- IEEE 802.3 for Arduino Uno with Ethernet Shield (implemented in Italy and Estonia),
- IEEE 802.11 for Espressif ESP8266 with integrated WiFi 2.4 GHz (implemented in Poland and Estonia).

Arduino Uno based end nodes constituted de-facto a sensor network, so in most scenarios data are transferred from the end node to the Internet and cloud services thus devices are connected into the sub-networks, hidden behind NAT and firewall and physically connected to the Internet.

Similar way, ESP8266 based end nodes are provided with a dedicated, private, separated from the Internet (no packet routing), WiFi access point (AP), to implement various training scenarios. That also includes peer-to-peer communication among nodes as well as implementing mesh networks using ESPs' capability to act simultaneously in access point and station mode (AP+STA). Those devices include both sensors and actuators and require bi-directional data transfer.

As aforementioned AP network is physically separated from the Internet, to provide connectivity to the Internet and cloud services, there is an application-level MQTT (Message Queuing Telemetry Transport protocol) broker, binding AP and Internet, using two interfaces and Node-Red server. This service is implemented using the RPi 3B+ device, using it's Ethernet interface for Internet connectivity and wireless one to connect to the private AP.

D. Security considerations

During the design of the system, its security was one of the critical aspects. This kind of distributed solution with a number of devices spread across Europe and different networks, if misused or compromised due to the vulnerabilities, would rise hard to track and trace cases.

Access to the system requires account registration and exclusive booking of the device. That enables tracking of the voluntary acts of attacks and identification of the attacker. Access to the system is logged; thus backwards identification is possible.

The system uses secure VPN connections among distant laboratory nodes, and central management server and firmware is injected to the end node via proxies (RPi devices, located on the end node side) using SSH connections (over VPN) with authorisation using certificates. We consider this channel is secure and along with best practices.

On the other hand, a model where users are enabled to have access to the network-connected devices on the low, programming level (firmware) like in case of our VREL nodes, raises serious considerations and possibly of a virtually unlimited number of vulnerabilities, i.e. DoS/DDoS attacks using VREL devices, MAC address fooling, etc. In the case of the open development environment, it is impossible to create a fully secure solution, yet the riskiest is enabling users to connect to the Internet network in an unrestricted way. In such a case, the common approach is to create an internal, separate wireless network that when compromised, won't impact public network nor affect many resources. On the other hand, separating devices from the web critically limits the number of actors participating in scenarios, i.e. students won't be able to send their data to the cloud, analyse, store nor visualise it using external tools. That also breaks the idea of a distributed system which integrates devices across their physical locations (across participating countries). Here comes a solution with fog layer devices that act as application protocol level routers. In the case of VREL labs, an MQTT (Message Query Telemetry Transport) protocol broker was used. Access to the broker requires providing credentials that are distributed in the publicly available documentation. This approach raises the question about implemented security model (de-facto "security by obscurity") however our tests show that for over 2 years if running, we didn't note a single issue regarding miss-use of the broker, nor unauthorised access, thus proving that chosen approach is keeping this vulnerability on the reasonable and acceptable level.

The idea of the separated network with message-level routing is presented in Fig. 7.

VII. Summary

The recent outbreak of the SARS-COV-2 virus and related COVID-19 pandemic throughout the world has caused governments across the world to shut down schools and universities

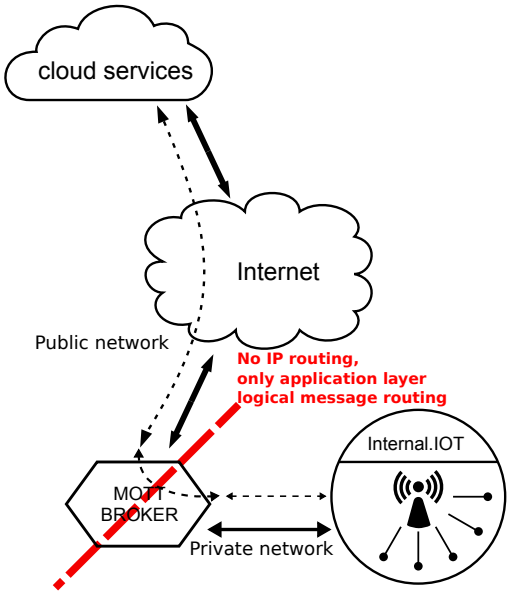

Fig. 7. VREL Security: MQTT routing model

within a week, to slow down the spread of the coronavirus that is causing the disease which has forced a lot of universities and schools to switch from the usual physical classrooms to virtual or online classrooms. However, this mode of learning is not working well for laboratory subjects and courses as it is not straight forward to handle laboratory subjects and courses that require access to hardware resources remotely.

We have presented current advances in distant learning and have discussed distant laboratory models. We have also presented the IoT-OPEN.EU remote laboratory infrastructure and IoT courses which were designed and implemented as part of the IoT-OPEN.EU ERASMUS+ project. We have discussed IoT related technologies and platforms that can be leveraged for IoT training. The presented solution has been introduced into the participating universities curriculum on the Internet of Things. Pilots performed in the Silesian University of Technology, covering classical, online courses and use of VREL labs and IOT-OPEN.EU project-created content in years 2017-2020, present and prove usability and reasonable approach to the distance learning with this kind of tools, as well as indicate the growing popularity of the mixed learning model, where students use on-site and online materials parallel.

At the moment of writing this article, over 500 students are studying or already studied using IOT-OPEN.EU materials and tools on-site and close to 8000 students enrolled for IOT-OPEN.EU online courses, including use of VREL nodes. Suddenly, the COVID-19 outbreak forced rapid switch from classical courses to the on-line version. As the current study semester is still running, we're collecting details on the impact of the presented infrastructure and laboratory use statistics. This data set is to be processed, once the semester is finished in September 2020 and there is a chance to provide comparable characteristics of on-line and on-site versions of the course.

In our future work, we intend to develop a framework for remote laboratory courses in IoT, AI, Big data, and automation where the data captured by the IoT nodes will be analyzed and the results used to control cyber-physical systems.

When other grant partners, than those that were involved in the VREL infrastructure implementation, successfully performed their integration tests, we also expect dynamic growth in the number of end nodes, platforms and IoT services constituting educational IoT framework.

ACKNOWLEDGMENT

This material is based upon work supported by the European Union under the Erasmus+ Key Action 2 (Strategic Partnership) project IOT-OPEN.EU (Innovative Open Education on IoT: improving higher education for European digital global competitiveness), reference no. 2016-1-PL01-KA203-026471.

The European Commission support for the production of this publication does not constitute the endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

This work was partially supported by the research project (RAU-6, 2020) of the Silesian University of Technology (Gliwice, Poland), via Statutory Research funds of Faculty of Automatic Control, Electronics and Computer Science, Silesian University of Technology, Gliwice, Poland.

REFERENCES

[1] Gartner, "Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020," 2019. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io

[2] McKinsey and Company, "The Internet of Things: Mapping the Value Beyond the Hype," McKinsey Global Institute, Tech. Rep., 2016.

[3] B. Barros, T. Read, and M. F. Verdejo, "Virtual collaborative experimentation: An approach combining remote and local labs," *IEEE Transactions on Education*, vol. 51, no. 2, pp. 242–250, may 2008.

[4] M. F. Verdejo, B. Barros, T. Read, and M. Rodriguez-Artacho, "Designing a CSCL environment for experimental learning in a distance learning context," in *The Role of Technology in CSCL*. Springer US, 2007, pp. 139–153.

[5] C. Colwell, E. Scanlon, and M. Cooper, "Using remote laboratories to extend access to science and engineering," in *Computers and Education*, vol. 38, no. 1-3. Elsevier Ltd, 2002, pp. 65–76.

[6] W. Admiraal, L. Post, P. Guo, N. Saab, S. Makinen, O. Rainio, J. Vuori, J. Bourgeois, G. Kortuem, and G. Danford, "Students as future workers: Cross-border multidisciplinary learning labs in higher education," *IJTES*, vol. 3, no. 2, 2019.

[7] G. Gercek and N. Saleem, "Transforming traditional labs into virtual computing labs for Distance Education," *iJOE*, pp. 46–51, 2008.

[8] B. Alhalabi, D. Marcovitz, K. Hamza, and S. Hsu, "Remote Labs : An Innovative Leap in the World of Distance Education Remote Labs : An Innovative Leap in the World of Distance Education," in *Proceedings of The 4th World Multiconference on Systemics, Cybernetics and Informatics (SCI 2000) and The 6th International Conference on Information Systems, Analysis and Synthesis (ISAS 2000)*, Orlando, FL, 2000.

[9] C. Viegas, A. Pavani, N. Lima, A. Marques, I. Pozzo, E. Dobboletta, V. Atencia, D. Barreto, F. Calliari, A. Fidalgo, D. Lima, G. Temporão, and G. Alves, "Impact of a remote lab on teaching practices and student learning," *Computers and Education*, vol. 126, pp. 201–216, nov 2018.

[10] E. Otoakhia, T. Jenmanachaiyakun, A. Afaneh, S. Alzebda, M. Mani, O. Sonbul, and A. N. Kalashnikov, "Embedded web server for remote laboratory access for undergraduate students studying electronic engineering," in *Proceedings - IEEE International Symposium on Circuits and Systems*, 2011, pp. 337–340.

[11] H. Ku, T. Ahfock, and T. Yusaf, "Remote access laboratories in Australia and Europe," *European Journal of Engineering Education*, vol. 36, no. 3, pp. 253–268, jun 2011.

[12] N. Dlodlo and A. C. Smith, "The Internet-of-things in remote-controlled laboratories," in *Proceedings of the 13th Annual Conference on World wide Web Applications ZA WWW 2013*, Johannesburg, 2011, pp. 14–16.

[13] A. A. Kist, A. Maxwell, P. Gibbings, R. Fogarty, W. Midgley, and K. Noble, "Engineering for primary school children: Learning with robots in a remote access laboratory," in *SEFI Annual Conference 2011*, 2011, pp. 586–591.

[14] M. F. Verdejo, B. Barros, R. G. Antón, and T. Read, "The design and implementation of experimental collaborative learning in a Distance Learning context," in *ITHET03 "4th international conference on Information Technology Based Higher Education"*.

[15] J. He, D. C. T. Lo, Y. Xie, and J. Lartigue, "Integrating Internet of things (IoT) into STEM undergraduate education: Case study of a modern technology infused courseware for embedded system course," in *Proceedings - Frontiers in Education Conference, FIE*. Erie, PA, USA: Institute of Electrical and Electronics Engineers Inc., 2016.

[16] W. Hutzel and R. Furter, "International partnership using remotely accessed labs," in *Proceedings - Frontiers in Education Conference, FIE*, vol. 2005, 2005.

[17] M. Despotović-Zrakić, A. Labus, Z. Bogdanović, M. Labus, and S. Milinović, "A Virtual Laboratory for Teaching Internet of Things," *Proceedings of the 10th International Conference on Virtual Learning ICVL 2015*, vol. 2, no. 1, pp. 259–264, 2015.

[18] R. Sell and S. Seiler, "Improvements of multi-disciplinary engineering study by exploiting design-centric approach, supported by remote and virtual labs," *International Journal of Engineering Education*, vol. 28, no. 4, pp. 759–766, 2012.

[19] S. Seiler, R. Sell, and D. Ptasik, "Embedded System and Robotic Education in a Blended Learning Environment Utilizing Remote and Virtual Labs in the Cloud, Accompanied by â??Robotic HomeLab Kitâ??" *International Journal of Emerging Technologies in Learning (iJET)*, vol. 7, no. 4, pp. 26–33, 2012.

[20] R. Sell, T. Rüütmann, and S. Seiler, "Inductive principles in engineering pedagogy on the example of remote labs," in *Proceedings - 2013 2nd Experiment@ International Conference, exp.at 2013*, 2013, pp. 68–71.