Available online at www.sciencedirect.com

ScienceDirect

IFAC-PapersOnLine 49-25 (2016) 419–424

Device Security Implementation Model based on Internet of Things for a Laboratory Environment

Pavel Blazek*, **, Ondrej Krejcar*, Daniel Jun, Kamil Kuca*, *****

** Center for Basic and Applied Research, Faculty of Informatics and Management, University of Hradec Kralove, Hradec Kralove, Czech Republic; (e-mail: {pavel.blazek, ondrej.krejcar, kamil.kuca}@ uhk.cz).*
*** Faculty of Military Health Sciences, University of Defence Hradec Kralove, Czech Republic (email: daniel.jun@unob.cz)*
**** Biomedical Research Centre, University Hospital Hradec Kralove, Czech Republic*

Abstract: Miniaturization of computer technology and its price drop have led to its spreading throughout all areas of human activities. Its application in research and labs is only one of many implementations. Labs are equipped with expensive devices in order to achieve first quality results, however, many of them with the use of autonomous equipment. Lab information systems enable, in connection with compatible equipment, to interpret information from different sensors. Internet of Things (IoT) phenomenon has a potential to exceed the mentioned standard. Implementation of IoT can upgrade many areas which we can encounter in laboratories. The aim of this article is to outline a part of these problems linked to this environment.

Keywords: Laboratory; IoT; Security; Automation

1. INTRODUCTION

The article should logically follow and extend the model of data security in the environment of laboratory research described in Blazek et al. (2015). A procedure of tasking lab workers by their supervisor is described here, where samples are labelled with the bar code in individual phases of the experiment. The aim was to make tracking a particular sample from in silico modelling through synthesis to pharmacological testing impossible, or at least most difficult in order to prevent undesirable collection of information which could be disclosed or misused. This procedure is feasible in many simultaneously processed tasks in the routine operation of the lab.

The next goal was to secure tracking and usage of sensitive chemical and biological substances in the course of experiments. A concurrent logistic view on material movement is considered subsidiary but not unimportant. It can be reached simply by extension of number of observed items. Simultaneously, their number and state is also observed.

2. PROBLEM DEFINITION

Protection of biomedical data does not only mean implementation of security functions in the lab information and management system (LIMS). The key philosophy of our security concept is based on use of technologies, which are used by majority of labs autonomously, however, at higher level and more effectively, Krejcar et al. (2013) and Roman et al. (2013). The whole concept involves elements of physical security, as well as application and system settings in LIMS, Lee et al. (2015). For enhanced comfort, there is an intention to equip the workplace with "smart gadgets" which would support and automatize selected routine activities, Behan et al. (2013) and Miorandi et al. (2012).

Only few workplaces have a complex security system. The reason is a lack of conception of equipment purchases, unknowingness of the problem, the lack of money or unwillingness of investments. The lab entry security system is usually based on radio frequency identification (RFID) technology, Ilie-Zudor et al. (2011). Only authorized persons, who have to identify themselves by touching their ID card or token on a reading device at the door, are permitted to enter the laboratory areas. After switching on the computer in their office, they are asked, according to the size of network environment, for verification of access to the operation system environment or working domain environment. This procedure is repeated for access to the PC which is connected to lab devices. Bioactive and inflammable substances are stored in refrigerators and special cabinets where the access is limited either at the level of building renovations in combination with the ID card or token entry verification or the cabinet itself is protected where the material is stored, Yang et al. (2013). There are different options starting with installing a pulley with a padlock, an electric lock with a push-button panel for inserting the entry code or RFID reader which could work with a different variant of cards than those used for the entry.

To sum up all mentioned above steps, we find out that

- A worker uses different types of identification elements
- He/she has to remember different codes and passwords

2405-8963 © 2016, IFAC (International Federation of Automatic Control) Hosting by Elsevier Ltd. All rights reserved.
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2016.12.086

- The applied system is so complicated that it leads to circumvention of security measures
- Efficiency of applied technologies does not reach appropriate values

Information systems for managing lab work comprise modules which allow communication with laboratory devices and monitoring of the defined variables in lab premises. Based on set values, they are able to react to deviations from the set limit values.

The concept involves recording in the log and sending an email or SMS to the authorized person. To get information on the last person who handled samples in the fridge, did not close the door and caused the damage, appears to be either a hard problem to solve or it means going through records in the system of entry logs or viewing cameras recordings.

3. LABIS BASIC MODULES

The proposed protected LIMS marked LabIS, Blazek et al. (2015), works with modules which meet demands of lab technicians in different stages of the running experiment. It is based on the environment with a central authority for verification of the user´s access to the system, with a database where the data and metadata for forthcoming and running experiments are stored and also with an applied layer which modifies amount of displayed information according to assigned authorizations.

The subsequent extension follows up the given models and technically extends protection of manipulation with lab samples as sources of sensitive data. LIMS becomes the system not only with functions for lab management and the place for storage, Sobeslav et al. (2016), of subsequently processed data but also the system for audit of incidents at physical and data levels, Zhou et al. (2004).

The central authentication module (CAM) is the center of proposed solution which comprises the list of all authorized persons. Both the lightweight directory access protocol (LDAP) database and the Active directory (AD) can be its ground. It is important to tie the user accounts data to the used identification codes e.g. RFID tokens, which are used for identification of persons in the given workplace. CAM becomes the real central authority for verification of persons´ authorization to enter the building and assigned premises as well as their log in the LIMS information system with defined authorizations.

Following is module of audit (MAUD) - the incidents audit database (Event log module). Information on incidents from surveillance system and on activities from LIMS is collected there. Stored data may be filtered, analysed and evaluated. We can easily track down frequency of unauthorized attempts to break into the system or premises, or on the contrary, monitored data access and movement of persons suspicious of sensitive data or material leak.

Not only LIMS and the registration system of entry to the workplace can be connected to both mentioned above modules. Additional devices, which are connected with lab activities and the outputs of which affect or immediately follow up LIMS data and security audit can be integrated into the given assembly, Chin et al. (2015) and Xu et al. (2014).

4. IDEA OF IoT IMPLEMENTATION IN LABORATORY ENVIRONMENT

In order to get complete data, labs should be replenished by "smart gadgets" which can extend possibilities to protect and simultaneously to provide required data. Principally, that means not only implementation of Internet of Things (IoT) device which can support household, but also introduction of industrial applications in labs environment. The application layer can care for operation or monitoring of the place where these applications are integrated, and together with CAM can play the role of security elements and source of incidents audit. As far as the limited access to biologically active substances and their registration is concerned, these devices can be simply integrated for example into cheaper models of cabinets and refrigerators together with electric locks and sensors.

Basically, one module can be used as initial and can be completed according to a desired function by the required periphery, Borgia (2014). The universal module (UM) participates in lab incidents audit. If we use it on the entrance door to the building, to the restricted work area in the lab or on the door of the cabinet with observed material, it will always generate information on the usage of identification card which will be verified in CAM database, Papadopulos et al. (2013) and according to individual setting it will provide the desired operation. To degrade a computer to a gatekeeper would be waste of money. Cheaper commercially produced models which suit our purpose are available as well. If we connect to UM the RFID lock control readers, the door contact sensor and the temperature sensor, which will read the temperature of the internal protected areas, we are able to create higher variability of the output. Figure (Fig. 1) shows integration of IoT into LIMS.

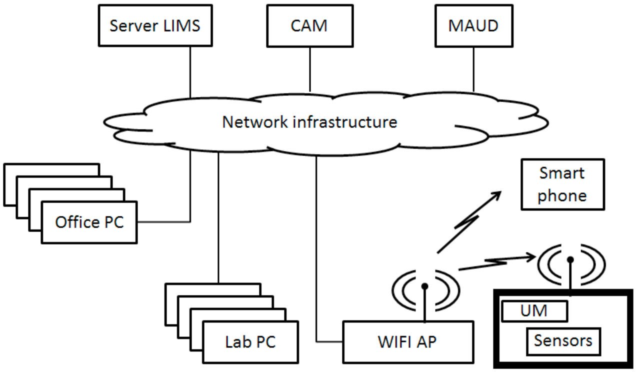

Fig.1. LIMS block network schema