Hackathon/Assignment - On 2-nd February, Current Year, upload in Sakai

MSc. Students from ISM – ICT | Cyber-Security Master program, who want to participate and start the Dev Hackthon on IoT & Security are engcouraged. Single student or teams of two/three candidates are accepted.

Deadline for the hack-days projects by sending the source code for the solution/challenge: on 2nd February, Current YEAR, 20:00 GMT to SAKAI (the submission must contain the source code, configuration files and compile/running info; also, the submission is flexible in terms of receiving the source code via public repositories GitHub, SVN, etc., although GitHub is preferred). The challenge for this Software Development Hackathon is to provide a solution into two parts for connecting a device to various IoT Clouds:

- Part 1 (MANDATORY – 2 out of 4 IoT Clouds) – connect a laptop or PC or Dev board (e.g. Raspberry Pi) to all this Internet of Things (IoT) Clouds by using directly the communications protocols (e.g. REST API – HTTP, MQTT, etc.) or the device client libraries (e.g. Java, C/C++, node.js – ECMAScript/JavaScript, Python, etc.):
  - Amazon AWS IoT: https://aws.amazon.com/iot/
  - Microsoft Azure IoT: https://azure.microsoft.com/en-gb/overview/iot/ (Get free account: https://azure.microsoft.com/en-gb/free/)
  - IBM Watson IoT: https://www.ibm.com/internet-of-things / https://www.ibm.com/us-en/marketplace/internet-of-things-cloud
  - Alibaba IoT Cloud
- Part 2 (OPTIONAL) – Try to separate the cryptographic security execution from the host/device client library into Java Card simulator or real Java Card – card / token / element for creating an Java Card applet and host client side (for APDUs exchange) in order to externalize parts of the cryptographic secure algorithms used for signing the registration/authentication messages to the IoT Clouds. in order to externalize and implement in the JavaCard applet various cryptographic functions which are used in the process of sending messages into the Cloud (e.g. oracle is using RSAwithSHA256 with asymmetric key on 2048 bits / other IoT Clouds need for the device authentication, another cryptographic algorithm such as ECDSA on 256 bits).

Architecture – partial copyright Oracle / partial www.ism.ase.ro done with draw.io tool: