****

**Collection of Good Examples of Setting up Various Projects**

**Systematically Described and Evaluated**

An important part of the EPIC project is to collect experiences with different ways of creating collaborative student projects. In this document, we present the experiences gained from the first year EPIC projects as an inspiration for others. In 2018, there have been seven project carried by 22 students selected from 6 universities. At the beginning of the first year, the possible project themes, project definitions given by different companies are announced in the EPIC webpage. In each university, EPIC project is announced and applications from students together with their theme preferences are collected. In each university, student recruiting is done through an open, fair and transparent process. Supervisors come together and assign students t o projects according to the preferences and background of students and project requirements. For each project, an EPIC supervisor is assigned in order to make the communication between company and students from different universities. The supervisor is selected from the same country of the company if possible. The students/company/supervisor matching is announced so that before companies and students come together in the student meeting, they can start talking about the details of projects via conference calls.

The list of the projects is given in Table 1 together with the company defining the project and names of supervisors and students working on the project. In the following sections, project proposals, learning objectives, final project report submitted by students and supervisor evaluations are presented for each project.

Table : Projects of 2018

|  |  |  |  |
| --- | --- | --- | --- |
| **Project Name** | **Company** | **Supervisor** | **Students** |
| Energy Dashboard | Saxion research chair, Sustainable Energy Systems | Cees van Keulen , Saxion  Edmund Schaefer, Saxion | Şamil Nart AGU  Alisher Djalilov RTU |
| Facility Management | NOKIA | Lukasz Zabludowski UTP | Krzysztof Pałczyński UTP  Santa Zvirbule RTU  Hamdi Burak Usul AGU |
| e-Grocery | SSI Schaeffer | Jacob Beer (SSI Schaeffer)  Jan Frick (UIS) | Chuyen van Do UIS  Kristian Omdahl UIS  Apena Ibrahim Adeboye RTU |
| Honeyjar | Talaia | Valentin Carela (Talaia)  Jens Myrup Pedersen (AAU) | Jacob Vejlin Jensen AAU  Peter Bolstad Møller AAU  Daniel Britze AAU  Magnus Stensli AAU  Robert Nedergaard Nielsen AAU  Ahmet Türkmen AGU  Anna Switala UTP |
| Industry 4.0 Security |  | Marite Kirikova | Jacob Kjersgaard AAU  Martin Eriksen AAU  Marina Harlamova RTU |
| Logistic 4.0 | SICK AG | Koojana Kuladinithi TUHH | Kaushik Hariharanagarajan TUHH  Thomas Stranden UIS |
| Research Funding App | AteneKOM | Anne Reichenbach (AteneKom)  Sukru Kuran (AGU) | Halil İbrahim Bilgin AGU  Adrian Jagodzinski UTP |

In the following sections, the details of projects will be presented.

1. Facility Management

**Facility Management Analytics within the Highly Scalable and Changing Business Environment**

**Company (profile)**

As a big representative of a huge corporation in its region, NOKIA modernize its work possibilities for its employees and we give the opportunity to work from home. As they are trying to plan the utilization of their resources in most efficient way, they had a vision to have an application that will be able to cover the functionality for planning the usage of different rooms in their facilities.

**Objective of the Project**

The project goal is to build a tool with the utilization & forecasting analysis modules, so the answers could be provided at any time: what is the capacity of the location taking into consideration different business models, teleworking policy as well as the hiring forecasts in the coming 3 years. The expected result is a creation of the online tool being able to provide the answers to questions as: what is the capacity of rooms, buildings, and location via graphical management reports.

It is challenge for a company to manage the resources efficiently and it is an optimization problem. The project aims to build an infrastructure to answer the question: What is the capacity of the location taking into consideration different business models, teleworking policy as well as the hiring forecasts in the coming 3 years?

**Case**

Depending on the business type the engineers’ office space is occupied in 8x5 or 24x7 mode. Assuming pretty often work from the home office of the employees it is challenging for the company to manage that effectively. The company would like to know at any time what is the remaining capacity of the rooms, buildings, and location in the short & long-term (i.e. including the hiring forecasts and changing telework policy.)

**Final Report**

The final report of the project can be found in [here](http://epic.agu.edu.tr/wp-content/uploads/2019/01/fr2018_Facility-management-analytics-within-the-highly-scalable-and-changing-business-environment.pdf).

2. e-Grocery

**Feasibility Model for Adopting Profitability Solution for E-Grocery Operators**

**Company (profile)**

SSI Schaefer is a German based multinational company, which has several branches around the world. The company specializes in consultancy, manufacturing, installation, automation and maintenance of warehousing and logistics solutions.

**Background**

Considering the way Information Technology is affecting almost every sector of life, SSI Shaefer is working towards expanding its solutions to grocery electronic commerce. The idea is to build solutions to support grocery retailers to expand their operations in a way that customers can order groceries online and received the ordered items at a specific place and agreed time.

Some research effort had been invested in this area by SSI Shaefer and researchers through Colibri project, some findings were already made but the major area of concern is that most electronic grocers are losing money while carrying out e-grocery activities with some existing Information Technology and automation solutions. Based on this, a research is required to investigate why it is difficult to make profit through e- grocery and to see the possibility of e-grocery as a profitable Industry to Invest. Some materials developed by previous researchers were provided for the actualization of this research, this were moderated by the SSI Schaefer Director of Business Development for Food Retail; Jakob Bear and the professor Jan Frick (University of Stavanger, Norway).

**Case**

Buying food online has been an emerging trend in the later years. There is a high demand from customers on this service. However, the e-grocers are losing money and goes out of business. The reason for that is low margins and customer's unwillingness to pay extra for this service.

On the other side; phases of e-grocery was modeled In As-Is and To-Be. The work identified four major phases with e-grocery, which are supply, order administration, order picking and delivery of order to customer. A lot of the time and cost is spent in picking, more so, an automated picking system would support the digitization of the picking process to get and increase the accuracy of time it would take to pick order.

**Final Report:**

The final report of the project can be found in [here](http://epic.agu.edu.tr/wp-content/uploads/2019/01/fr2018_Feasibility-Model-for-Adopting-Profitability-Solution-for-E-grocery-Operators.pdf).

3. Honeyjar

**Company (profile)**

Talaia, being a company that is already successful within the cypher security industry, had a lot to bring to the table no matter what they were asked. It was through their input that the final business model was created and also the final version of our networks analysis system.

The business model is made by SAX University. The business perspective is what is going to make the system possible, as no matter how good something is it is useless if no one uses it. By making sure the product is marketed correctly it will allow it to sustain it as its own product.

**Background**

AAU Honeyjar was established around 5 years ago as a platform for running malware in a controlled environment. The platform is currently being rebuild on brand new hardware – two powerful servers with plenty of CPU cores, memory and disk space – and a dedicated Fiber connection to the Danish research network.

The platform has three main components: (1) The Test Environment, where large numbers of virtual machines can be installed, run, infected, and reset/wiped. This is also where emulated infrastructure exists, to make the environment as realistic as possible. (2) The containment, which filters out any harmful traffic, but allows for some Internet connectivity necessary for the malware to run. It is also used for monitoring traffic. (3) The analysis part, which receives traffic and other information that is monitored, and can be used for analysis of everything observed.

The platform can accessed through a VPN channel, so no physical presence in Aalborg is necessary (in fact it is just two powerful servers).

**Future challenges**

The HoneyJar project proposal was very optimistic and ultimately did not produce the initially expected results. However, we understand the difficulties that have arisen during the project. Even so, the project produced interesting knowledge and ideas about a topic currently being studied by the research community.

**Question**

How would it be possible to recognize Malware, and present intelligence on the nature of the Malware that is captured and contained in the quarantine?

**Case**

Companies as well as regular consumers have a lot of sensitive data stored on their smartphones, for example (but not limited to):

* Credit card data
* Compromising photos
* Passwords
* E-mails
* Customer data

This in itself is worrisome, however the popularity of smartphones is rising as well. At this point in time smartphones outsell PC’s. Computers have been susceptible to malware since they were first introduced to the market, however it seems that Android phones, while vastly gaining popularity over PC’s, are still relatively under protected to Malware attacks.

To exploit the fact that the market hasn’t really focused on security on Android phones yet, the project members from AAU created a basic Honeypot system.

A Honeypot, as to be derived from its name, is a virtual machine that emulates a system, in our case an Android Phone, presenting it in such a way that it becomes interesting for malware to attack. This Honeypot system in its current state is still very basic and needs improving.

The three computers in the example will be running an emulated version of Android, making the emulation seem as realistic as possible, i.e. emulating human behavior. Once these systems are infected through the Internet, the malware will be contained, and analyzed to determine what the category of the Malware is.

**Final Report:**

The final report of the project can be found in [here](http://epic.agu.edu.tr/wp-content/uploads/2019/01/fr2018_Honeyjar.pdf).

4. Industry 4.0 Security

**Industry 4.0 Security**

**Trust and Access Control in Industry 4.0**

**Background**

Industry 4.0 is the new buzzword within manufacturing. The term is closely related to industrial Internet of Things and data analytics. Industry 4.0 enables existence of “smart” production lines. Within this environment physical processes are monitored, sensor and production data are collected. Common intelligence is distributed in the network. Production lines are becoming more self-aware by means of self-optimization and self- configuration. These abilities give the manufacturer new insight there can be used for production optimization and the ability to get more dynamic production lines that can be reconfigured as the demand on products shift.

When the production equipment gets features of self-awareness it transforms into a cyber-physical system (CPS). Before CPS can be widely deployed some technological challenges need to be solved. Many of the CPS use cases require dynamicity; therefore wireless networks with low latency and high reliability are to be achieved. Security of such network is crucial, as CPS implies interaction with the physical world, and a security breach could result in machines doing damage to humans and industrial property.

This project aims to enhance the network security in Industry 4.0. As an attempt to cover the network security requirements a conceptual trust handling model for Industry 4.0 is designed. The trust framework proposes six dimensions of trust in an Industry 4.0 CPS. Access control is identified as a crucial trust dimension in the framework that defines the level of initial trust of a CPS element. It is then analyzed in more detail by investigation of current access control mechanisms of Industry 4.0, leading to a proposal of an enhanced access control protocol.

**Network Challenges in Future Systems**

To achieve an industrial breakthrough; users, applications and work processes must be integrated with the network. The network changes from a wire-static to a highly dynamic wireless network. It is out of the scope of this report to make a thorough investigation of which wireless technologies to use, but some of the candidates are Wi-Fi and 5G.

Wireless networks are expected to ensure transmission reliability for the needs of the production environment. Features that are specific for industrial wireless network nodes, if compared to wired networks, are as follows:

1. Latency. Sensor devices are configured to monitor module, tool and environment status, deliver and receive real-time instructions and information. Therefore, low latency is required for these functions [5].
2. Energy consumption. Battery driven devices should consume as little energy as possible to postpone the moment of battery or device replacement.
3. Capacity. Elements in Industry 4.0 CPS need to be able to execute tasks autonomously, as well as be able to communicate and collaborate. Problems such as signal interference, moving paths and data processing arise [5].
4. Mobility and flexibility. The reconfiguration of the production lines enforces mobility in the network that should be handled automatically. Large number of devices will join or leave the network as modules are moved around. In addition, the network is to be connected to the Internet. These changes will increase the attack surface for potential network intruder.

Increased attack surface implies stronger security mechanisms are required in industrial wireless networks to ensure operational environment. Securing such an unconventional communication environment is a top-priority challenge. Further work addresses the security issues of Industry 4.0 CPS.

**Case**

Industry 4.0 is the next industrial revolution; the revolution transforms production lines, digitalized during the third industrial revolution, into self-aware and interconnected CPS. The network of Industry 4.0 is of high density and mobility. Devices of low computational power are connected to devices with high computational power and are dynamically added and removed from the network. In previous sections various challenges of Industry 4.0 were identified. It was concluded that network in Industry 4.0 is exposed to many security risks, leaving room for development of secure and reliable networks. In scope of this work we accentuate the network security issues and argue that security issues are a top-priority challenge that needs to be solved before adapting concepts of Industry 4.0 in industrial manufacturing.

The first step of ensuring confidentiality and integrity in the network is to ensure only trusted devices could communicate with each other. In scope of this work is to propose a conceptual trust framework to determine the trustworthiness of each node. A critical module of the framework is access control, as it defines the initial trust level of the element. The access control process must be adjusted to specifics of Industry 4.0, i.e. should be automated due to the limited or non-existent user interface of devices. Access control covers authentication, authorization and accounting. There is within the time frame of this project not time to investigate all three parts, and therefor the focus is put on the first part authentication.

**Final Report:**

The final report of the project can be found in [here](http://epic.agu.edu.tr/wp-content/uploads/2019/01/fr2018_Industry-4.0-Security.pdf).

5. Logistic 4.0

**SMART LOGISTIC 4.0**

**Company (profile)**

SICK AG is a company with more emphasis on robotics and the usage of sensors in robotics. The problem the group works on is a localization solution for indoor logistics of a factory floor.

**Future challenges**

The distance between todays manufacturing and the Industry 4.0 manufacturing is very big. Probably the biggest problem is to ID where I4.0 has an impact. Many people say that they have a lot of opportunities and endless of data and they don’t know what to do with it. Companies buy sensors and attached them in the production and are wondering what they will do with the data.

Many people thing that, with data analytics, they only need to throw in data and then there will be great results automatically. It might be the case in the future but with todays system this isn´t a reality. The main issue targeted to be solved in the project is following:How to optimize the flow of data from localization sensors to a cloud service which updates and creates a dynamic map. What are the different market segments regarding opportunities for sensors.

**Case**

Microsoft and Google platforms for subscriptions services of different data handling solutions, work as generic data handling services that could fit into every business. Having the full service of the data handling where one could subscript to this service, can use any data that make sense of it and in that the costumer decides the inputs that are important for their business/activity, ex. Brewery yeast, sugar, PH level, alcohol level. The sensors and analytics can make predictions and control the process so that the company can make corrective measures to adjust the process. The system need to be built up a knowledge base where actions are fed into the system where it knows what and why some actions are made, so the system can suggest an action or do some decisions on its own. In that way, it can increase the productivity, so the employees can do more productive things for controlling when the production is independent and automated.

**Final Report:**

The final report of the project can be found in [here](http://epic.agu.edu.tr/wp-content/uploads/2019/01/fr2018_Industry-4.0-Security.pdf).

6. Research Funding App

**Mobile App for Funding Research**

**Company (profile)**

The ateneKOM GmbH is a pan-European operating company based in Berlin with further representations throughout Germany and Brussels. atene KOM provides consultancy in the areas of regional development and the roll-out of digital infrastructure as well as mobility, energy and education.

**Background**

ateneKOM seeks for help in creating a professional mobile application, which supports actors throughout the EU in finding the right funding for their purposes. The project team worked on a mobile application, its web admin panel and its RESTful API, which allows communication between the admin panel and the mobile application.

**Future challenges**

The ateneKOM offers a broad variety of consultancy services to its customers, including strategic planning, project and network management, and application development with a broad focus on regional development. Due to their expertise on funding advisory ateneKOM wants to offer a tool to easily get an overview about current funding options. ateneKOM has a current app for funding research available, which shall be improved.

In this project, the main issue to be solved is;how can ateneKom get a quick overview about the funding options?

**Case**

ateneKOM has a current app for funding research available, which shall be improved. The project aimed to develop a mobile application for funding advice, where the clients can overview funding opportunities on a national and international scale

**Final Report:**

The final report of the project can be found in [here](http://epic.agu.edu.tr/wp-content/uploads/2019/01/fr2018_Mobile-app-for-research-funding.pdf).

7. Energy Dashboard

**Company (profile)**

Saxion plays an important role within the energy transition of the Eastern part of the Netherlands. There are a number of projects aiming at decreasing energy consumption, smart control and integration of renewable energy in which Saxion research chairs are taking part. The project Clean Tech Energy Crossing is a large project sponsored by the Kiem Smart Industry program. Saxion is a partner in this project and works on the analysis of energy production and usage in the building area “Leesten-Oost in Zutphen, where residents live in energy neutral homes.

**Background:**

The Dutch government has committed itself to the global climate change limitation targets. Besides implementation schemes for increasing the share of renewable energy, the “energy agreement” that the government signed with industry and other organizations contains targets for improving energy efficiency of buildings (houses, offices) and industrial processes.

The built environment will make steps the coming years to decrease building energy consumption, e.g. electric consumption and thermal consumption for heating and cooling. Partly by building or renovating towards more efficient buildings, partly by smarter control methods which avoid unnecessary energy consumption but maintain sufficient levels of comfort for people. Such control methods can also be coupled to other optimization targets such as demand response and self-consumption of renewable energy generated by the building through solar PV panels and energy storage facilities.

The challenges of the project are:

- Design and implementation of an “Energy Dashboard” including a web interface, database, mobile app

- Integration of thermal sensors and heat-pump energy meter into existing Zipato environment

- Discussion with researchers and residents into what the requirements of the Energy Dashboard are

- Analysis into behaviour of residents and system (including energy usage, PV production, functioning of Smart Home).

**Final Report:**

The final report of the project can be found in [here](http://epic.agu.edu.tr/wp-content/uploads/2019/01/fr2018_Energy-Dashboard.pdf).