Company: Bright Cape B.V.

Supervisor(s) at company (name + e-mail addresses):
Mart Althuizen (m.althuizen@brightcape.nl)………………………………………………………..
William Lekatompessy (w.lekatompessy@brightcape.nl)………………………………………………………..

University
Supervisor(s) at university (name + e-mail addresses; TU/e will look for suitable supervisors if left blank):
………………………………………………………..
………………………………………………………..

Project title (or topic):
Security infrastructure for a quality prediction tool
Researching security challenges for an industrial data analysis tool in an enterprise setting

Description
Understanding the behavior of manufacturing systems is important for providing high product quality, while keeping the production latency short, and production and maintenance costs low. In manufacturing processes quality is often sample wise checked to avoid that products with defects hit the market. With the internet of things (IoT) in which objects (products, machines, factories, warehouses, customers) are all connected, there is increased availability of massive amounts of sensor and manufacturing data.

As part of an Industry 4.0 initiative Bright Cape has developed a machine learning tool that predicts product quality through machine learning. This tool enables manufactures to have a shorter control loop (faster detection of defects and root causes) and thereby resulting in cost savings and increased quality. In the current state-of-art there is the need for a reliable and secure system environment.

Challenges
Finding the right balance between security, flexibility and usability in an industrial setting faces several challenges:

- How to keep the tool maintainable whilst making it both secure and scalable for deployment in a variety of enterprise environments / architectures (cloud, on premise, etc.).
- How to ensure GDPR compliancy for big data handling in both on- and off-site implementations.
- How to optimize licensing and version control for both on- and off-site implementations.

Objective
Research the architecture and functionalities for security of the PQP tool