Tampere University

Factory Belt:

Secure and Trusted Industry 4.0 Architectures

Antonis Michalas

Network and Information Security Group,
Tampere University,
Tampere, Finland

Amjad Ullah, Hai-Van Dang, Tamas Kiss

Research Centre for Parallel Computing,
University of Westminster,
London, U.K.

Christian Gehrmann

Networks and Security,
Lund University,
Lund, Sweden

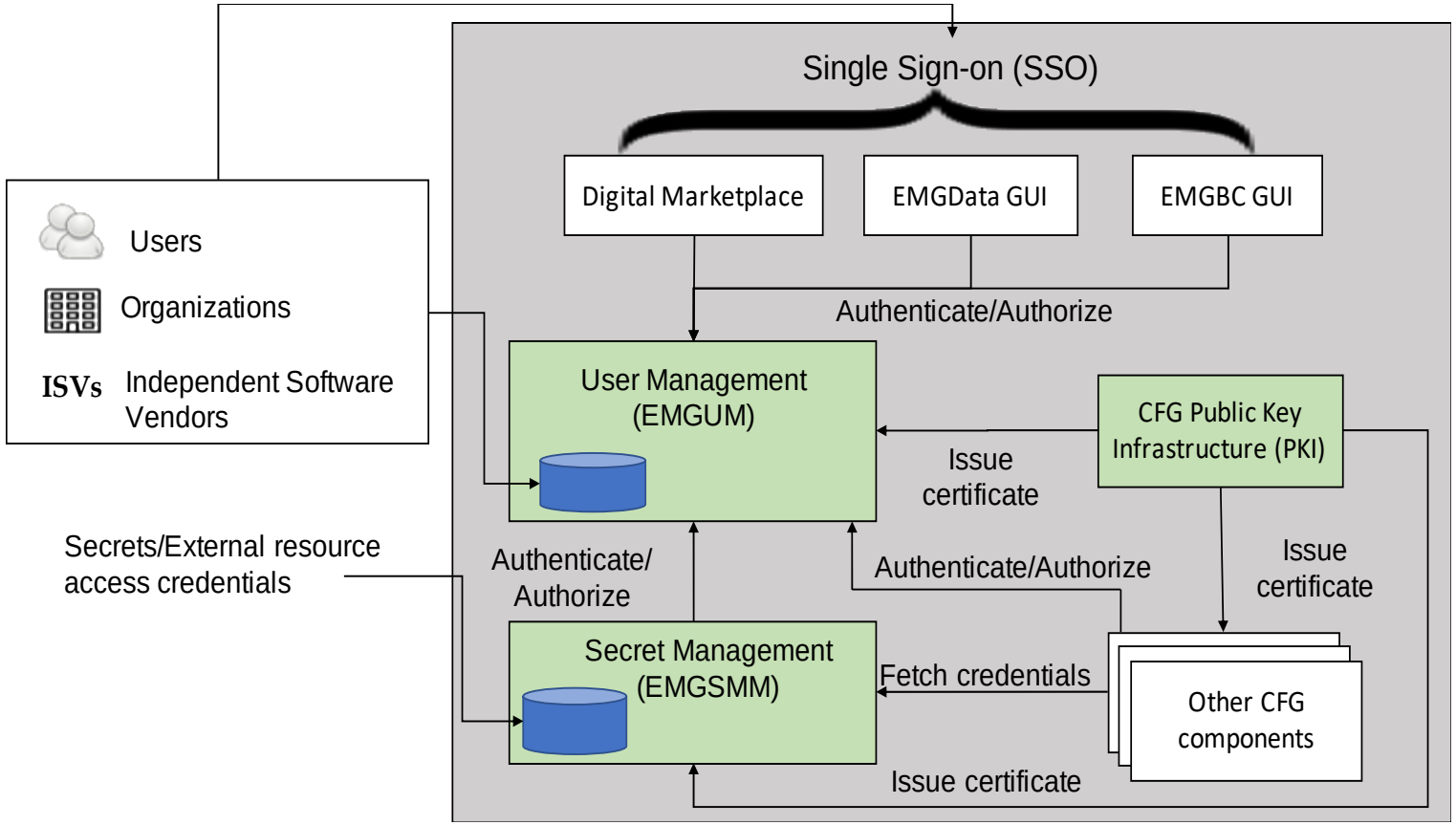
Contribution

- Security Requirements when building smart factories
- Security mechanisms in the CloudiFacturing Project
- Security in the DIGITBrain project
- Help protocol designers to build novel security protocols that can squarely fit the specific needs of Industry 4.0

Key security requirements of CloudiFacturing

- Confidentiality and integrity of manufacturing process and simulation data
- Single sign-on access to all services of CFG solution
- Authenticated and secure connections between the manufacturing process or simulation data owner and the cloud provider
- Authenticated and authorised access to services and processing of data
- Secure transfer of input and production data to/from end-user to compute and storage resources
- Secure storage and handling of external resources' credentials

CloudiFacturing Security Framework

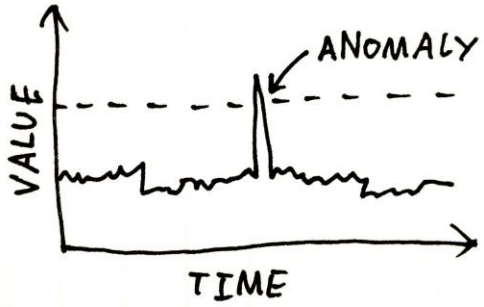


- EMGUM
  - Responsible for authentication, authorization and security policy management
  - Based on OpenID Connect (OIDC) standards
- CFG PKI
  - Secure mutual authentication between certified CFG components
- EMGSMM
  - Secure storage and retrieval of credentials for platform external resources

Identified Security Requirements

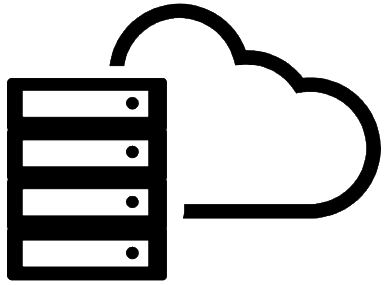
Secure Execution Layer

Crypto Layer



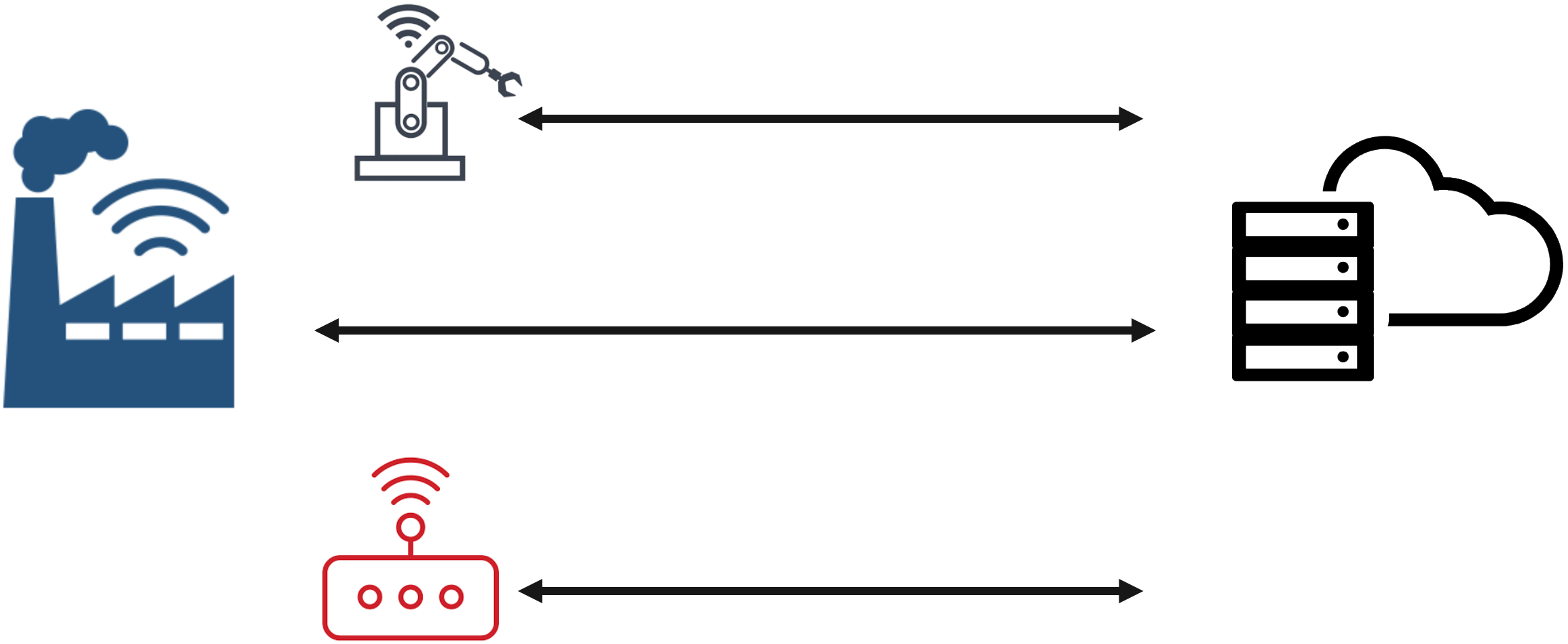
Anomaly Detection Layer

Analytics Layer

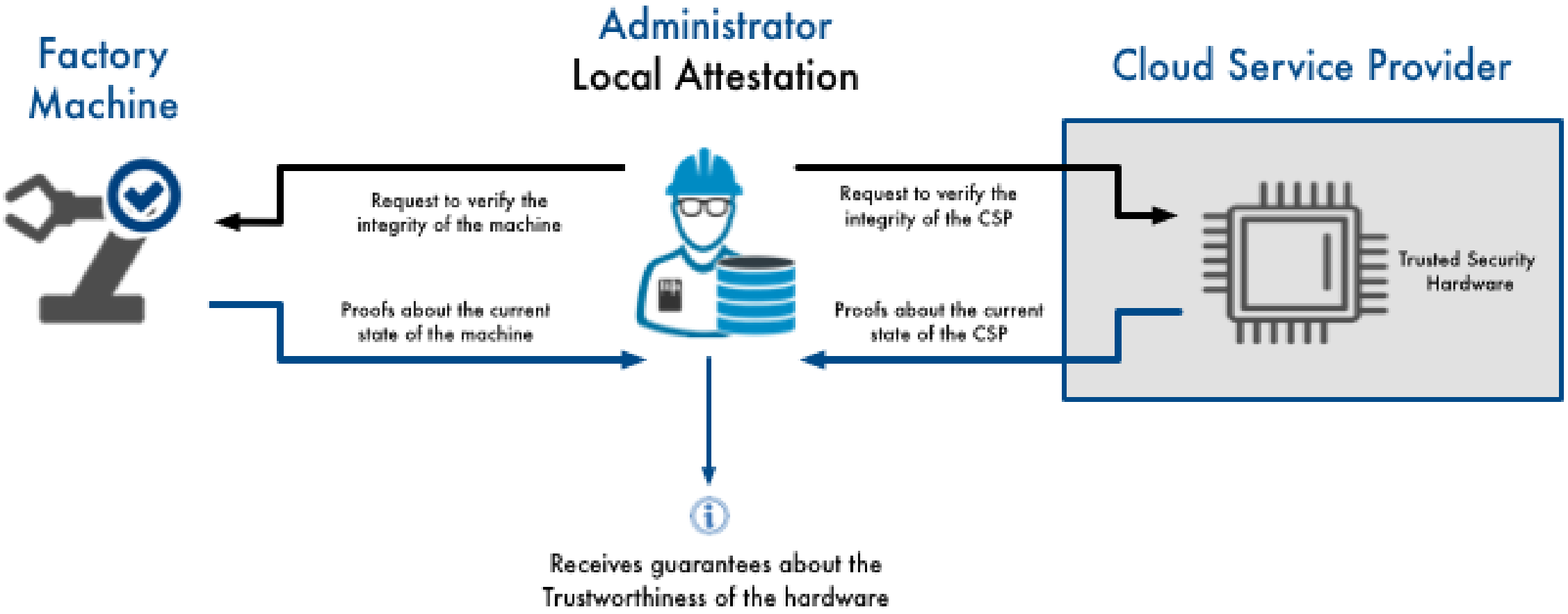


Edge Multicloud Layer

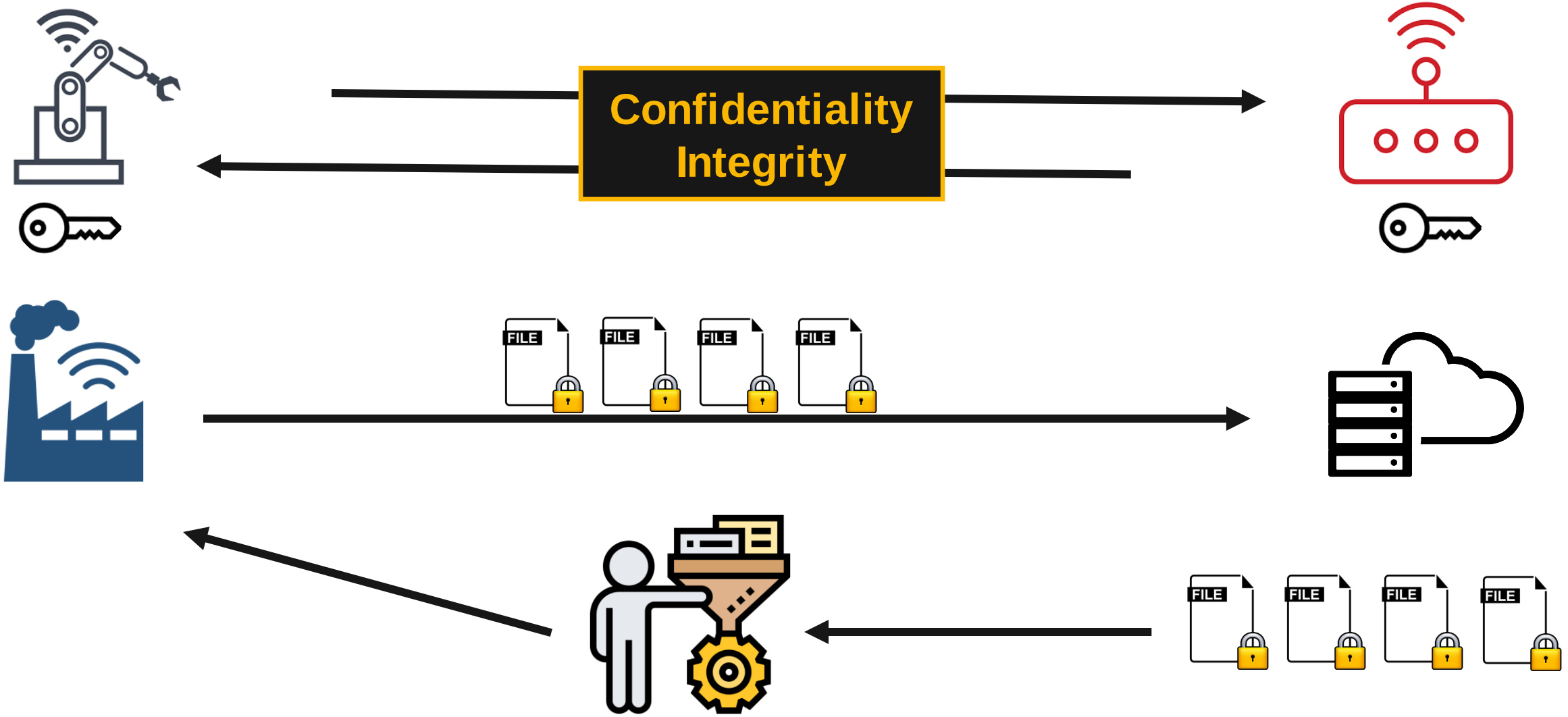
Edge Multicloud Layer

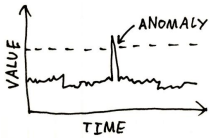


Secure Execution Layer

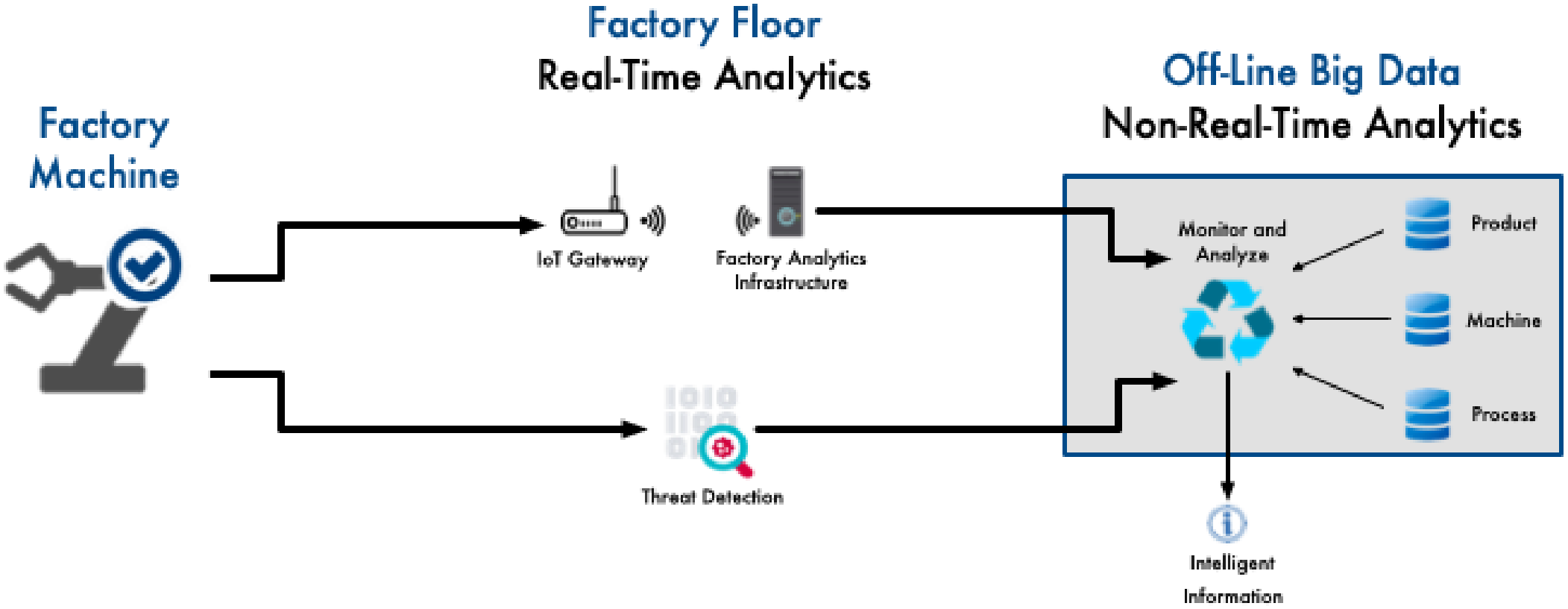
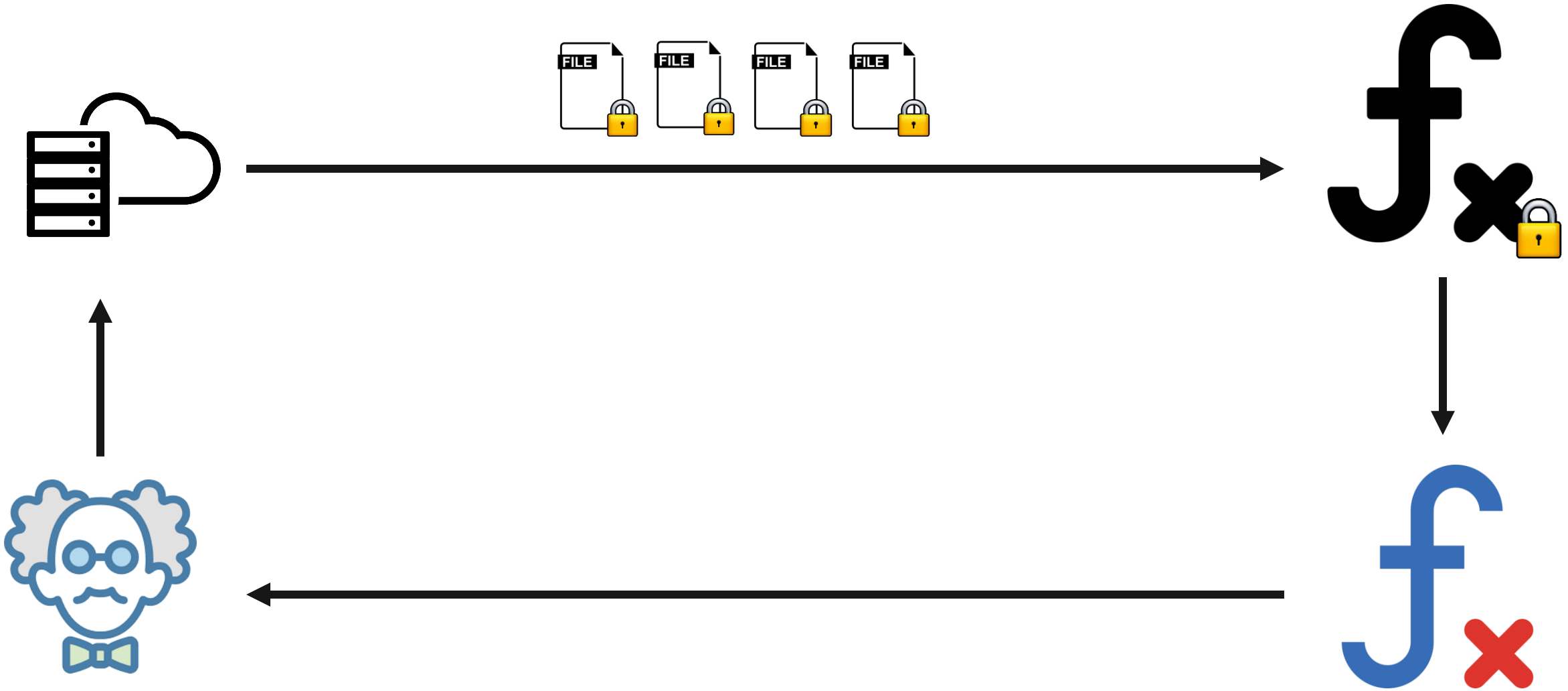


Crypto Layer





Anomaly Detection Layer



Analytcis Layer