Ubiquitous AI: Smart and Secure IoT as enabler contributors boosting servitization approach

Guido Bertoni
Security Pattern

Organizzato da

FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE

CONFINDUSTRIA

ANIE SERVIZI INTEGRATI

SECURITY PATTERN

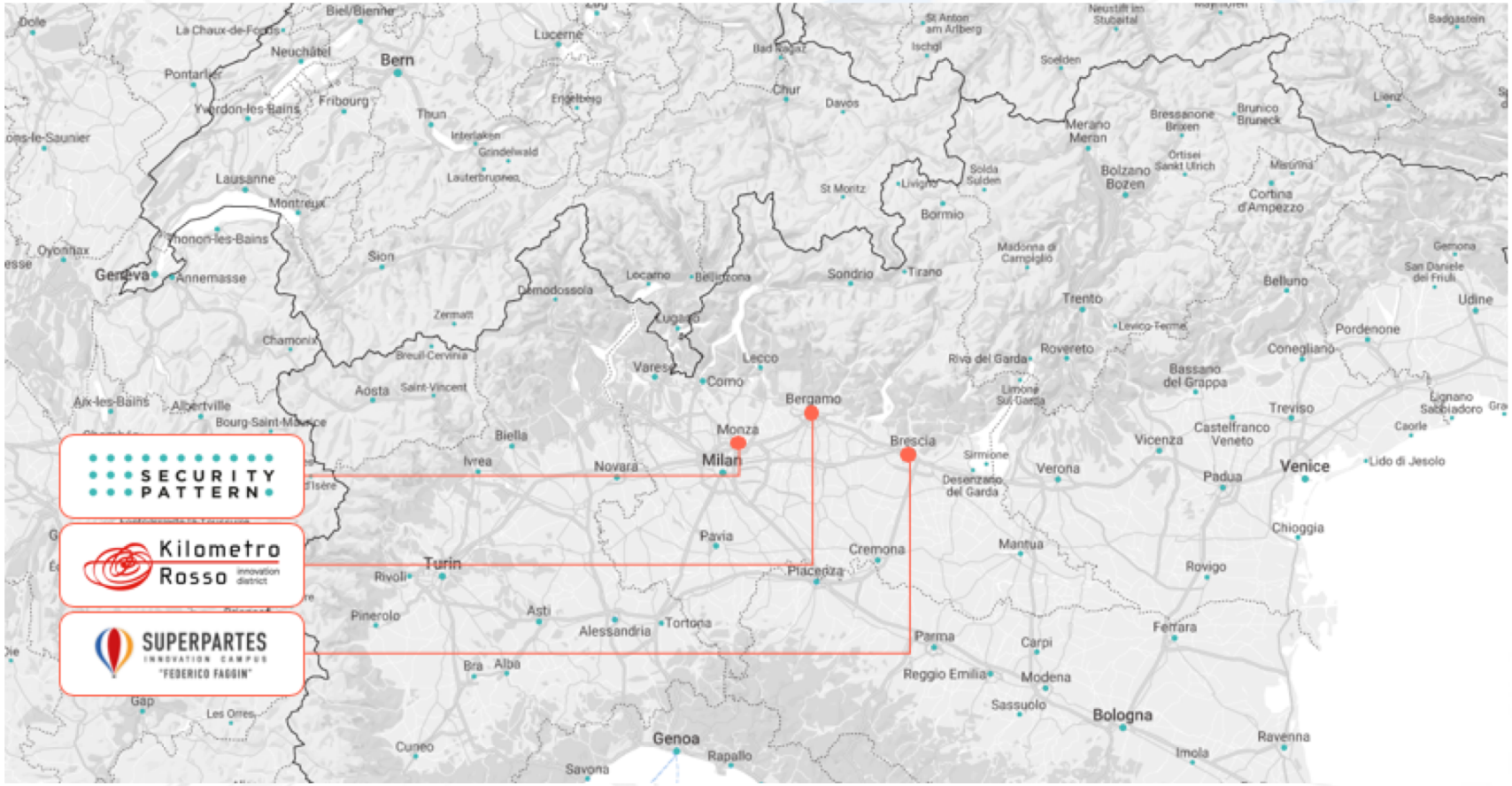
We help creators of intelligent connected devices to **design**, **implement** and **operate** their systems with a **sustainable security level**

FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE

CONFINDUSTRIA

ANIE SERVIZI INTEGRATI

Where we are



FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE

CONFINDUSTRIA

Data is the new Oil!

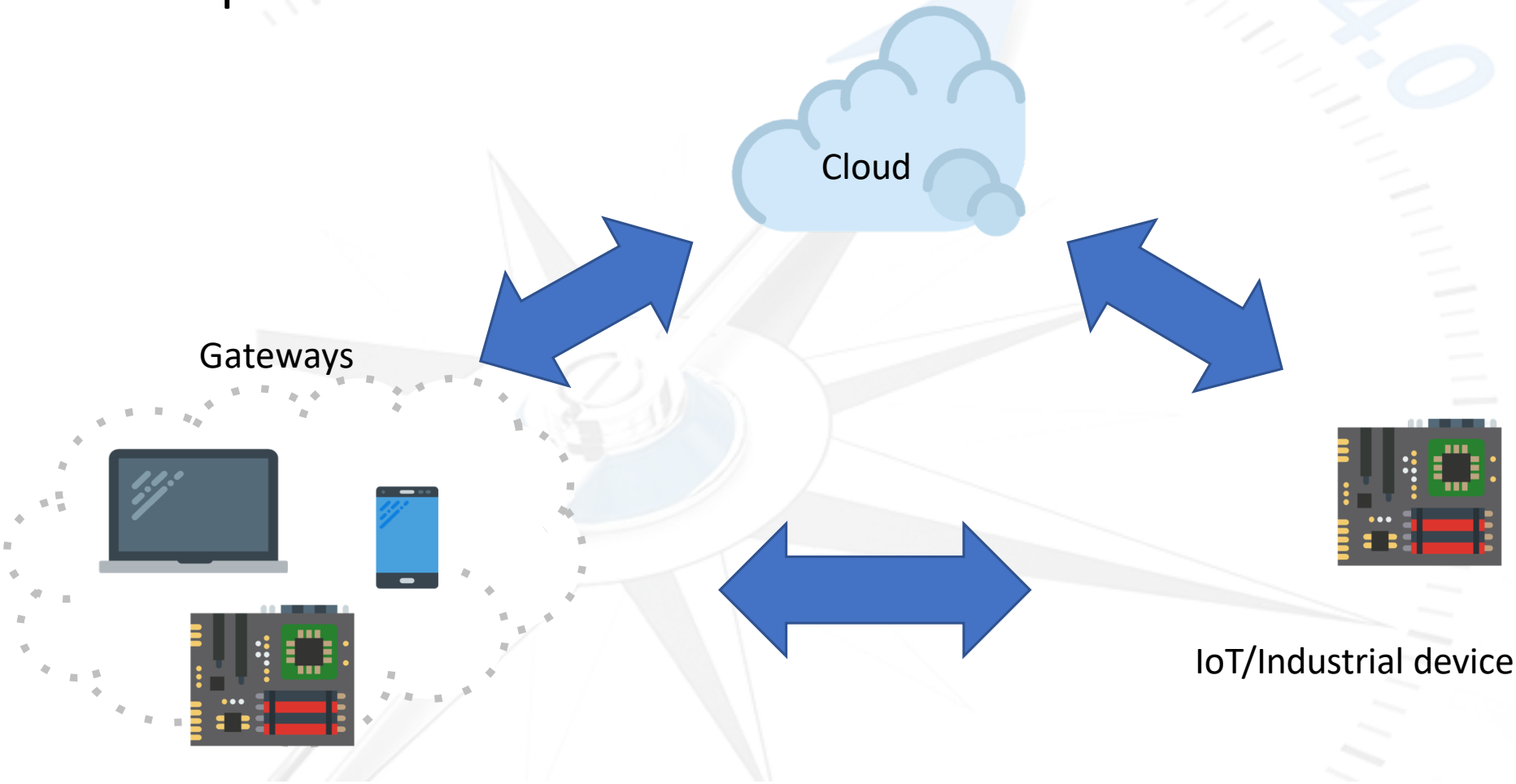
If Data is the new oil AI is the new....

- A neural network is the result of:
  - Data collection
  - Data classification
  - NN selection and training
- The synthesis of the data you collect goes in the neural network training
- This is an important asset!

Why IoT is so important

- In some contexts, like social media, raw data are provided directly by the source (users)
- In other cases raw data should be extracted from physical systems
  - with a cost for deployment of sensors, data collection, data aggregation…
- The acquisition of data from the field enables new business models and new opportunities
  - Predictive maintenance
  - Just in time manufacturing
  - Energy efficiency
  - …

Simplified IoT



Edge, fog computing..

- The scenario where “everything goes in the cloud” is not always feasible or scalable
- If the end node is not powerful enough, or for security reason the network is segregated, or there is not enough bandwidth... there might be some local computation:
  - Fog computing
  - Edge computing
  - Intelligent gateway
  - …
- The architecture can be quite complex and fragmented

What should be protected?

- Two main aspects
  - The data streams
  - The platform security

The Data Streams

- These are the “classical” IoT security requirements
- First, authenticate the counterparty:
  - Cloud authenticates IoT devices
  - IoT device authenticates cloud, gateway and other devices
- Set up a secure communication channel
  - Encrypt data, and use standard protocols, if possible, such as TLS for TCP/IP
- Use of blockchain
- Even if these requirements are now pretty understood, we are still an initial deployment phase

Platform security

- Device under attack!

- The focus is on the robustness and capabilities of being protected against attacks
- The higher the value of the data inside the device, the higher the incentive to apply attacks
- The case of pay tv....

ANSA.it › Cronaca › **Blitz anti tv pirata, stop a 5 milioni di utenti. Multe fino 25mila euro**

Blitz anti tv pirata, stop a 5 milioni di utenti. Multe fino 25mila euro

Indagini in tutta Europa, nel mirino le Iptv illegali

L'operazione interessa numerosi Paesi europei: in Italia sono coinvolti 5 milioni di utenti, che saranno ora oscurati. Si tratta di un volume d'affari di 2 milioni di euro al mese….

con un abbonamento da 12 euro al mese riuscivano a guardare i programmi trasmessi dalle principali pay tv…

Standards IoT and Industrial security

- **ETSI** TS 103 645: Cyber Security for Consumer Internet of Things
- **NIST** IR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
- **NIST** IR 8259 (DRAFT) Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers

- **ISA/IEC** 62443 Security for industrial automation and control system
- **NIST** SP 800-82: Guide to Industrial Control Systems (ICS) Security

Security starts in the device

- Standards are a very good start and references but do not provide the implementations...
- The security journey starts with a threat analysis
  - Identify assets and possible threats
- During the design of a device it is important to select the right components with the fundamental security primitives
  - Secure boot
  - Random number generator
  - Secure storage
  - ....

Where Neural Networks are?

- NN can be in the end node (or edge, fog..)! Not only in the cloud!
- NN can be the result of a very big effort of:
  - Data set acquisition campaign
  - Classify data with the support of experts
  - Train different neural networks for finding the best one
- Finally the network is ready to go
  - It is the result of an investment and non negligible effort
- This investment deserves protection!

Conclusions

- Artificial intelligence is becoming more and more pervasive, with the possibility of being deployed even in end nodes
- The training and the parameters of the neural network is an asset that is a result of an investment
- The asset and the corresponding investment should be protected since it is a competitive advantage
- There are suitable security solutions for protecting AI deployment

FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE

CONFINDUSTRIA

ANIE SERVIZI INTEGRATI

SECURITY PATTERN

Thank you!

hello@securitypattern.com