European Commission | Horizon 2020 European Union funding for Research & Innovation

SPEAR

SECURE AND PRIVATE SMART GRID

Short Project Overview

SPEAR

Project Identity, Challenges and Motivation

European Commission
Horizon 2020
European Union funding
for Research & Innovation

Project Identity

SPEAR: Secure and PrivatE smArt gRid

Call: *H2020-DS-2016-2017 submitted for H2020-DS-SC7-2017 / 24 Aug 2017*

Topic*: DS-07-2017-Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors*

Project Grant Agreement: *787011*

Budget: *2,965,569.14 €*

Project Start Date*: 01/05/2018 (M01)*

Project End Date: *30/04/2021 (M36)*

Project Challenges

"SPEAR comes to provide effective solutions in detecting, responding and taking countermeasures against advanced cyber threats and attacks targeted to modern smart grids"

- Detecting and responding to cyber-attacks using **new technologies** and capabilities.
- Developing all-in-one, robust and effective **security solutions for smart environments**.
- Leveraging advanced **forensics** subject to **privacy-preserving**.
- Confronting **APT** and targeted attacks in smart grids.
- Increasing the **resilience** of the smart grid innovation.
- Alleviating the **lack of trust** in smart grid operators.
- Empowering **EU-wide consensus**.

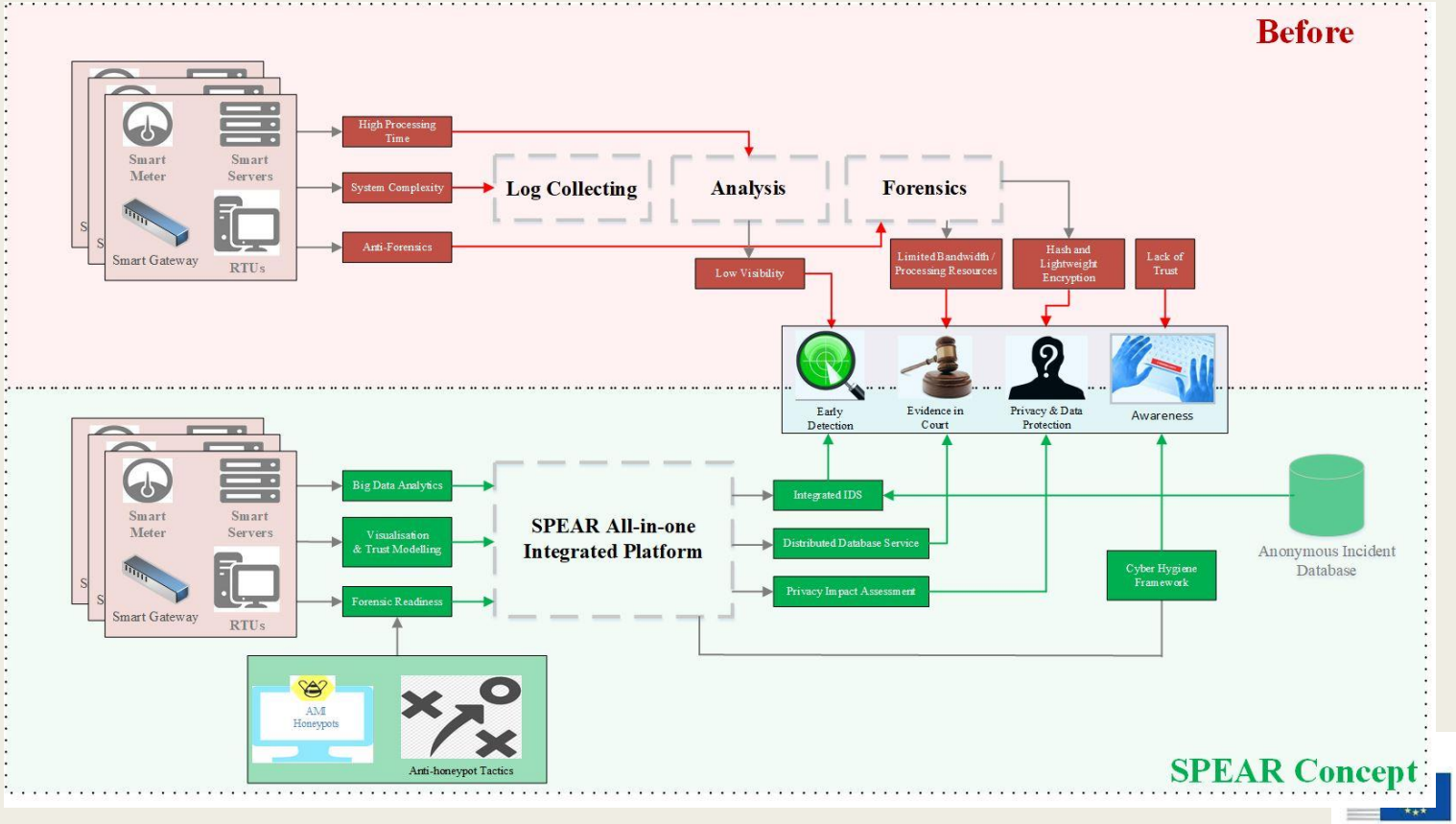
- *Advanced Persistent Threat – APT.*

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project Motivation & Vision

According to the European Network and Information Security Agency (ENISA):
"A cyber security incident to power grids could be defined as any adverse event that can impact the confidentiality, integrity or availability of the Information and Communication Technology systems supporting the different processes of the organisations involved in the well-functioning of the power system, including all its domains (e.g., markets, operation of the distribution or transmission grid, customers, etc.)".

One of the most vulnerable and high-impact CIN is the smart grid since the collapse of an energy production utility may cause **human lives**, **millions of euros**, **denial** of a very important and common good such as **energy** and days or even months of **recovering**.



Horizon 2020
European Union funding
for Research & Innovation

SPEAR Consortium

European Commission
Horizon 2020
European Union funding
for Research & Innovation

SPEAR Consortium

Industry	University	Research Center	SME
• EUROPEAN DYNAMICS LUXEMBOURG SA (**ED**) • SCHNEIDER ELECTRIC FRANCE SAS (**SCHN**) • ENEL IBERIA SRL (**ENI**) • PUBLIC POWER CORPORATION S.A. (**PPC**)	• PANEPISTIMIO DYTIKIS MAKEDONIAS (**UOWM**) • UNIVERSITY OF SURREY (**SURREY**) • GOTTFRIED WILHELM LEIBNIZ UNIVERSITAET HANNOVER (**LUH**) • TECHNICAL UNIVERSITY OF SOFIA (**TUS**)	• FUNDACION TECNALIA RESEARCH & INNOVATION (**TEC**) • ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS (**CERTH**) • G.E. PUKHOV INSTITUTE FOR MODELINGIN ENERGY ENGINEERING OF THE NATIONAL ACADEMY OF SCIENCES OF UKRAINE (**PIMEE**)	• EIGHT BELLS LTD (**8BL**) • INCITES CONSULTING SARL (**INC**) • SIDROCO HOLDINGS LIMITED (**SH**) • 0 INFINITY LIMITED (**0INF**) • MVETS LENISHTA OOD (**VETS**)

European Commission | Horizon 2020 European Union funding for Research & Innovation

SPEAR Objectives

European Commission
Horizon 2020
European Union funding
for Research & Innovation

SPEAR Objectives

Objective 1: To define the **SPEAR system architecture**, the security components and the privacy frameworks for situational awareness provisioning in relation to cyber security threats.

WP2, WP6

Objective 2: To build attack **detection** mechanisms and promote **resilience** operations in smart grids.

WP3, WP6

Objective 3: To increase situational **awareness** in smart grid networks.

WP3, WP5

Objective 4: To create and maintain an **anonymous repository** of smart grid incidents.

WP5

Objective 5: To provide smart **network forensics** subject to data protection and privacy.

WP4, WP6

Objective 6: To empower **EU-wide consensus** of cyber security in smart grid systems.

WP5

Objective 7: To validate the SPEAR architecture capabilities in **proof-of-concept Use Cases**.

WP7

Objective 8: To design an innovative **business model and conduct a techno-economic analysis** to strengthen the role of European smart grid and cyber-security industry in the global market.

WP8

European Commission | Horizon 2020 European Union funding for Research & Innovation

SPEAR

SPEAR Use Cases

European Commission
Horizon 2020
European Union funding
for Research & Innovation

SPEAR Use Cases

The Hydro Power Plant Scenario

- VETS plant, **Bulgaria**.
- Validating the SPEAR architecture towards securing renewable energy smart grid utilities.

The Substation Scenario

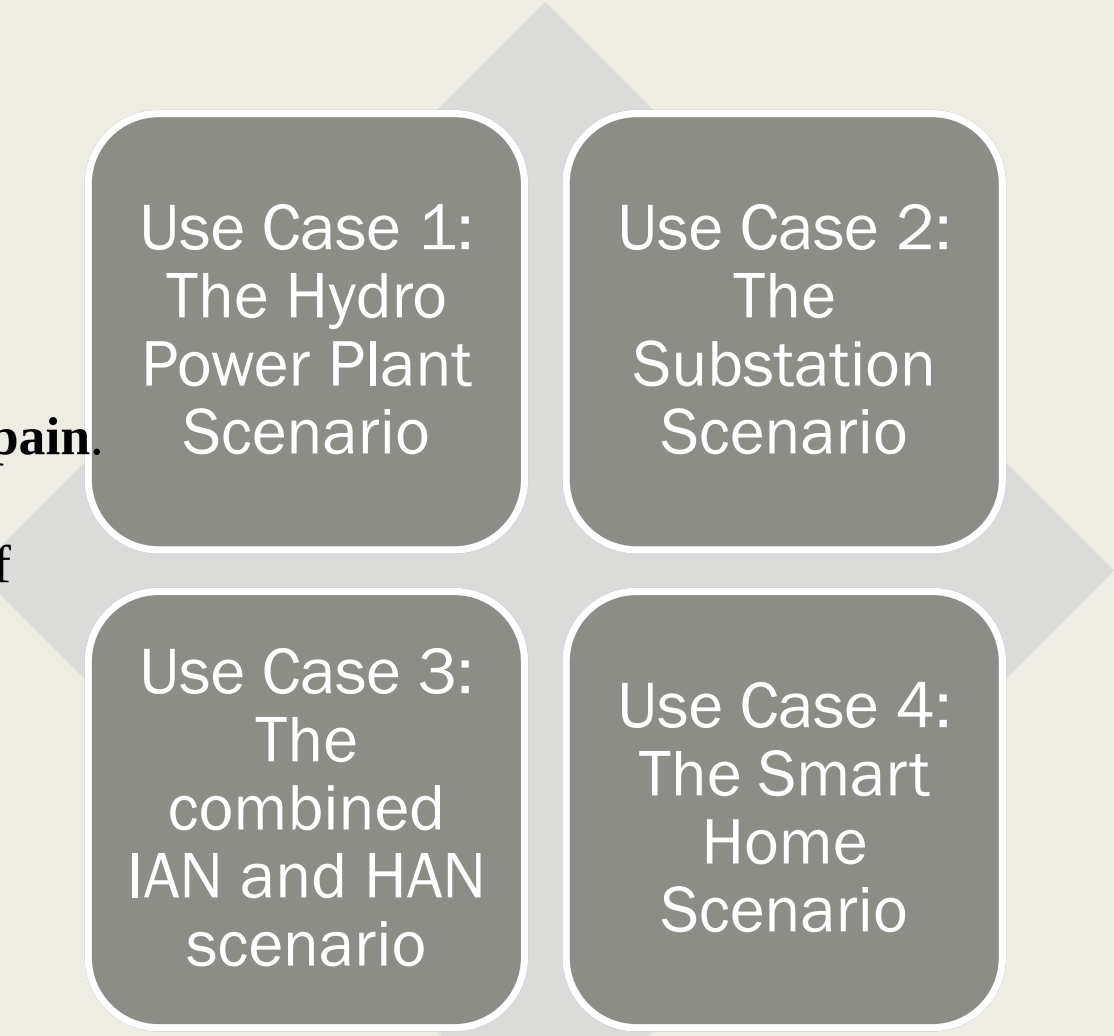
- SCHN ES premises & INGRID lab TEC, **Spain**.
- Analysis of how resistant the SPEAR defense system can be against different types of cyber-attacks in the heart of the substation automation systems.

The combined IAN and HAN Scenario.

- PPC, **Greece**.
- Validating the SPEAR platform in a big scale electric power plant

The Smart Home Scenario.

- Smart House at CERTH premises, **Greece**
  - ***Digital Innovation Hub***
  - Extensive trials on the SPEAR technologies to smart home and micro-generation scenarios



Industrial Area Network – IAN.
Home Area Network – HAN.

European Commission | Horizon 2020 European Union funding for Research & Innovation

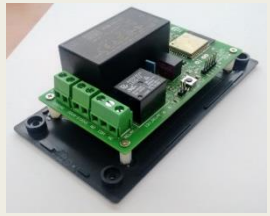
Smart Home Use Case – Digital Innovation Hub

European Commission
Horizon 2020
European Union funding
for Research & Innovation

SPEAR

Smart Devices in Smart Home



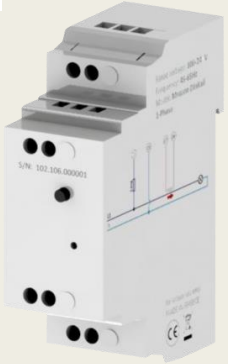




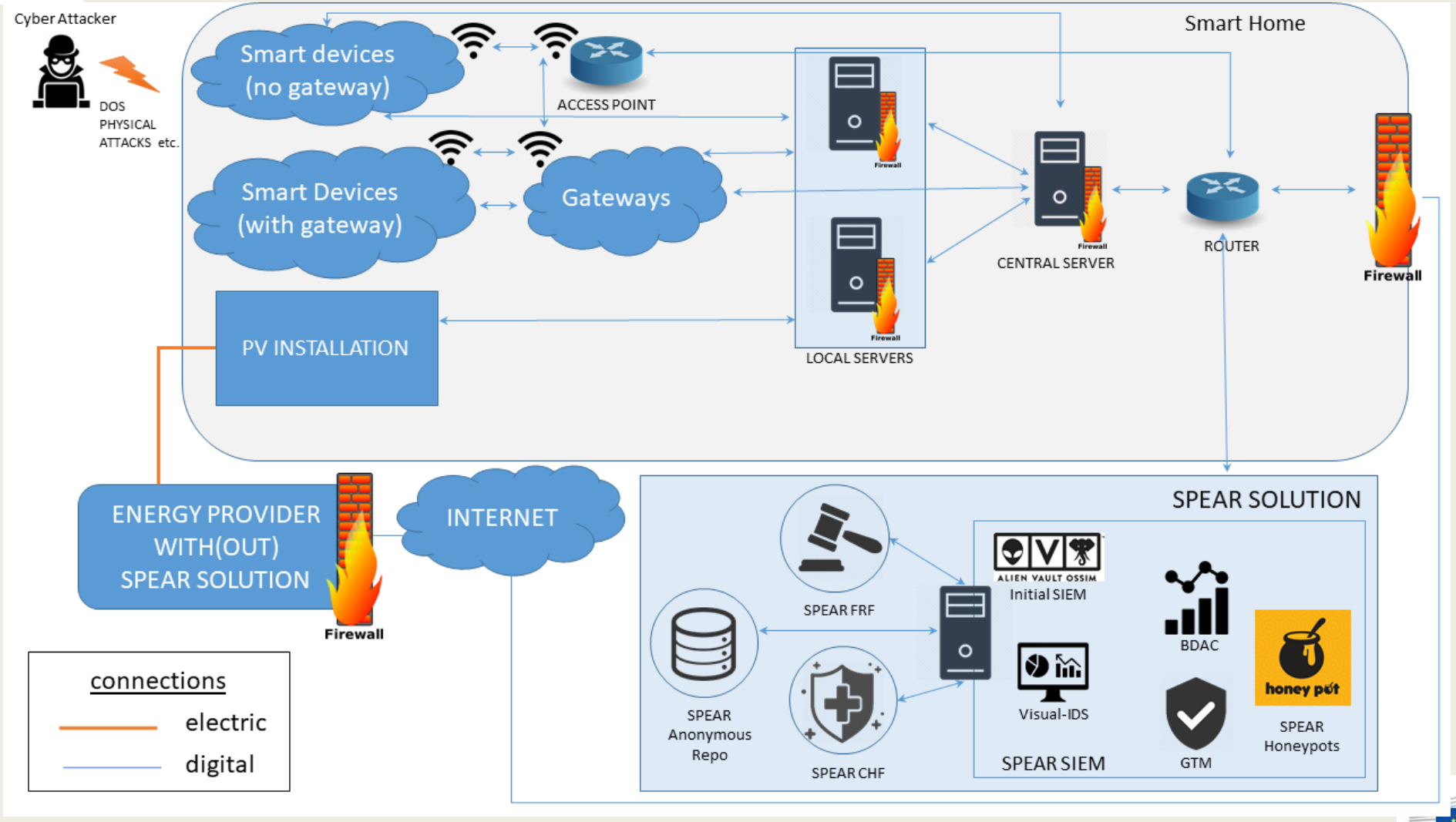








SPEAR – Smart Home



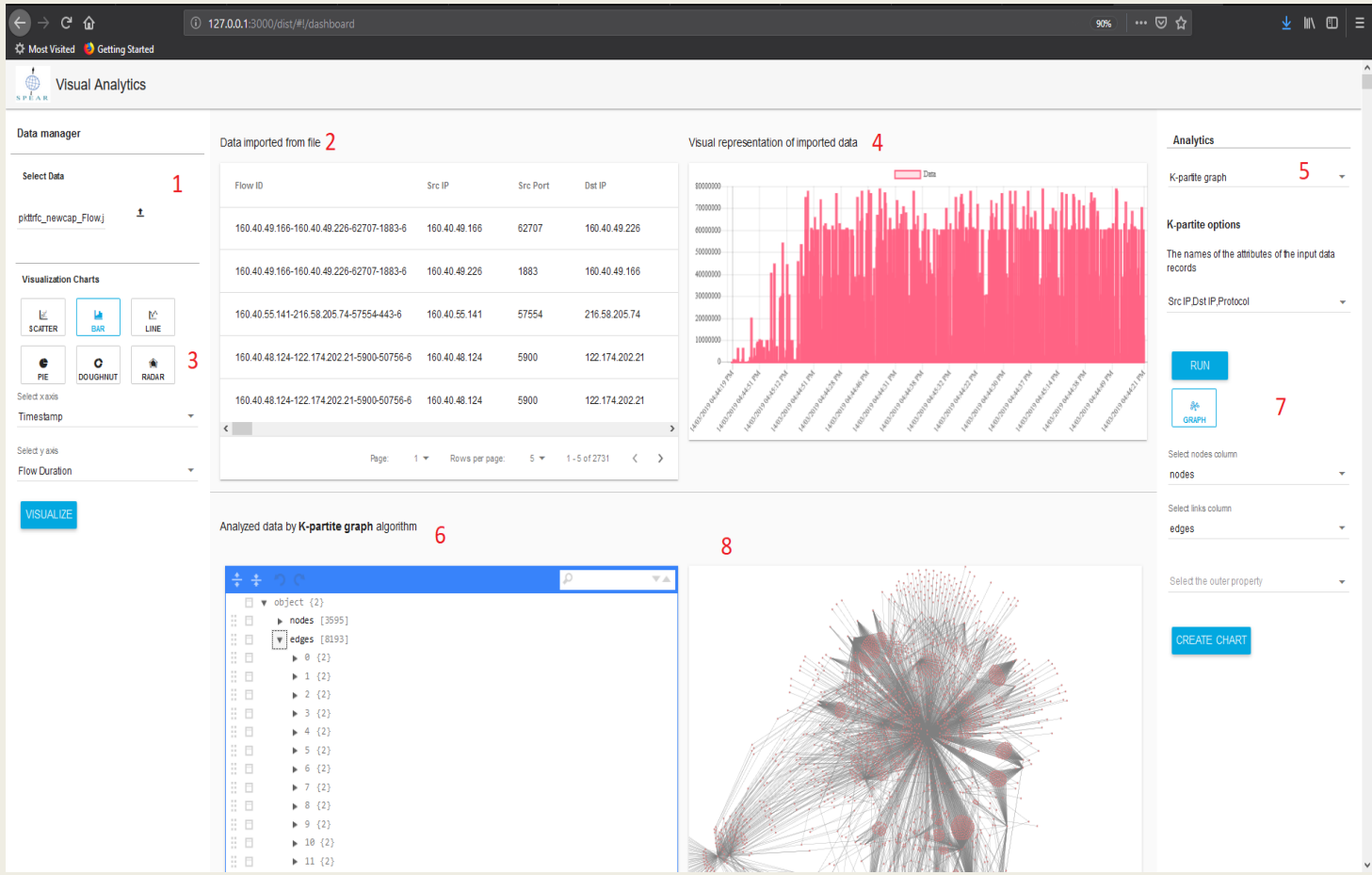
SPEAR solution:

1. Enhance Cyber-security.
2. Real-time monitoring and anomaly detection.
3. Smart device reputation.
4. Report incidents anonymously.

European Commission | Horizon 2020 European Union funding for Research & Innovation

VIDS – Visual Analytics Dashboard

- Visual Analytics Dashboard
  1. *Simple Workflow*
  2. *Intuitive UI Design*
- Visualization Methods
  1. *Scatter Plot – Correlation between variables*
  2. *Bar chart – Data among Categories.*
  3. *Line chart – Continuous variables.*
- Analytics Methods
  1. *Local Outlier Factor – Anomaly Score*
  2. *K-partite – Graph representation*
  3. *New methods: 2x LSTM NN Anomaly Score visualization methods*



European Commission
Horizon 2020
European Union funding for Research & Innovation

VIDS – LSTM Analytics Methods

- LSTM - NN
  - Smart-Home network traffic capture (2 GB)
  - Extraction of **MQTT** features/attributes from .pcap files (t-shark)
  - **7 different message types** of MQTT (connect, connect acknowledgement, publish, publish acknowledgement, ping request, ping response, disconnect)
- Anomaly Visualization Methodology
  - **Spike observation** in the loss function that indicates an anomaly in the **smart home MQTT traffic**.
  - Use of **graph visualization methods of the VIDS** (e.g k-partite) to further investigate the MQTT network flows features/protocol attributes in order to specify problematic network nodes

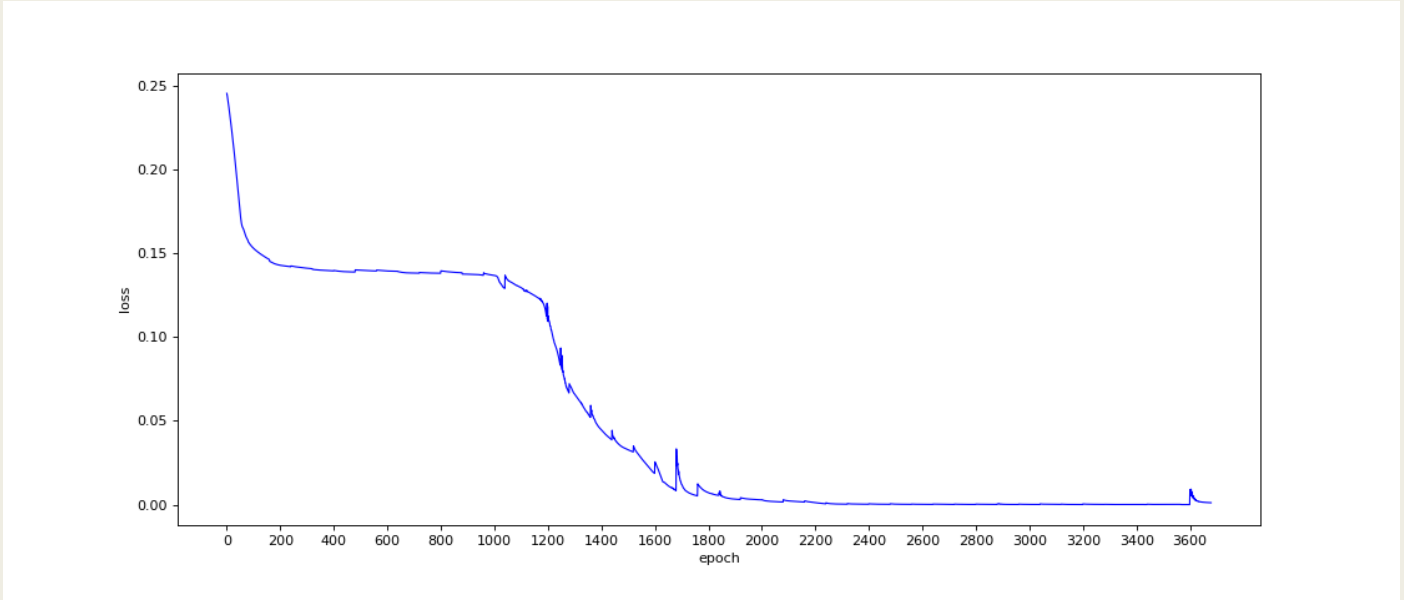
- Seq2Seq LSTM
  - **Electricity measurements** from Smart-Home devices.
  - Time-series (historical data from at least 2 years)
- Anomaly Visualization Methodology
  - **Use of threshold**. Threshold value is a hyper-parameter.
  - MSE between input data and predicted sequence samples of a day.
  - **Bigger** than threshold is marked as anomaly.

European Commission | Horizon 2020 European Union funding for Research & Innovation

VIDS – Proof of Concept on LSTM Analytics

- LSTM NN - Proof-of-concept Results
  - Model tested by feeding and training with normal data intercepted with abnormal synthetic data.
  - Each observation has a sequence with 500 messages.
  - Test data: [21N 1A 23N 1A]
  - Abnormal: Sequence with 500 messages shuffled (partially (10%) or all shuffled).

Loss diagram - LSTM NN



Apparent Power Total (VA)

European Commission
Horizon 2020
European Union funding
for Research & Innovation

SPEAR

Thank you!

Questions?

Dr. Dimosthenis Ioannidis
djoannid@iti.gr

European Commission
Horizon 2020
European Union funding
for Research & Innovation