

## PROJECT IMPACT

17004

The SunRISE project aims for the development of new security solutions that address the numerous, global challenges that arise from the rapid increase of IoT devices and corresponding cyberattacks, as well as novel techniques that allow exploitation of privacy-sensitive data in a privacy-preserving way.



July 2023

In several domains systems benefit from the use of machine learning. However, machine learning performs well only if lots of meaningful data is used to the machine learning algorithm. Unfortunately, in many scenarios the data of interest is privacy-sensitive, as lots of harmful information can be inferred from data. For example, the fine-grained electricity consumption of a single household can be exploited to infer information about the residents. Sensitive information can be derived such as the number of residents, their habits, when they are asleep or away. Project SunRISE targets the development of novel methods, which enable usage of privacy-sensitive data under privacy-preserving circumstances.

### Background, objectives of the project and challenges

In recent years, the IoT device revolution has transformed our world into one where everything is connected, everything is smart, and everything is (or should be) secure. Connected devices do deliver clear benefits, but they also increase the risk of data manipulation, data theft and cyberattack. In 2015, European enterprises had at least a 1 in 5 chance of losing data through a targeted cyberattack. The lack of trust by businesses and consumers in smart, connected devices is a barrier to growth and jobs. There is an essential need to provide interoperable and resilient secure solutions and systems.

To obtain a comprehensive security solution, SunRISE addresses several key aspects, critical in future IoT systems. First, design intrusion detection, by using the latest novel results in machine learning to address security anomaly detection aspects. Second, sharing security intelligence data from IoT nodes to cloud backends, by creating a community with reference structures. Based on the larger dataset, machine learning can be accelerated and overall system security increased. This would result in security turning into a shared responsibility, interest, and effort, and into improved efficiency, cost, and resource usage. Third,

the lack of trust by fearing the loss of confidential data will be addressed by using privacy-enhancing technologies (PET), like homomorphic encryption and secure multi-party computation (MPC). Last, the efficient, power- and cost-effective introduction of PET will be addressed by designing and manufacturing suitable hardware supporting AI (Artificial Intelligence) specific to IoT end-nodes and for acceleration.

The SunRISE project focused on several Key Application areas as defined in the ECS-SRA, as published in January 2018, specifically on Digital Industry, Digital Life and Energy. Further, SunRISE will enable the development of the identified essential capabilities: Systems and Components, Connectivity and Interoperability, and Safety, Security and Reliability.

### To achieve the SunRISE objectives, the consortium focused on the following key innovations:

1. Machine learning on the edge nodes, for IoT security analytics and anomaly detection
2. Cloud platform applying machine learning techniques for sharing relevant security data
3. Privacy enhancing technology
4. Technologies for uniquely secure low-footprint ASICs (Application Specific Integrated Circuits)

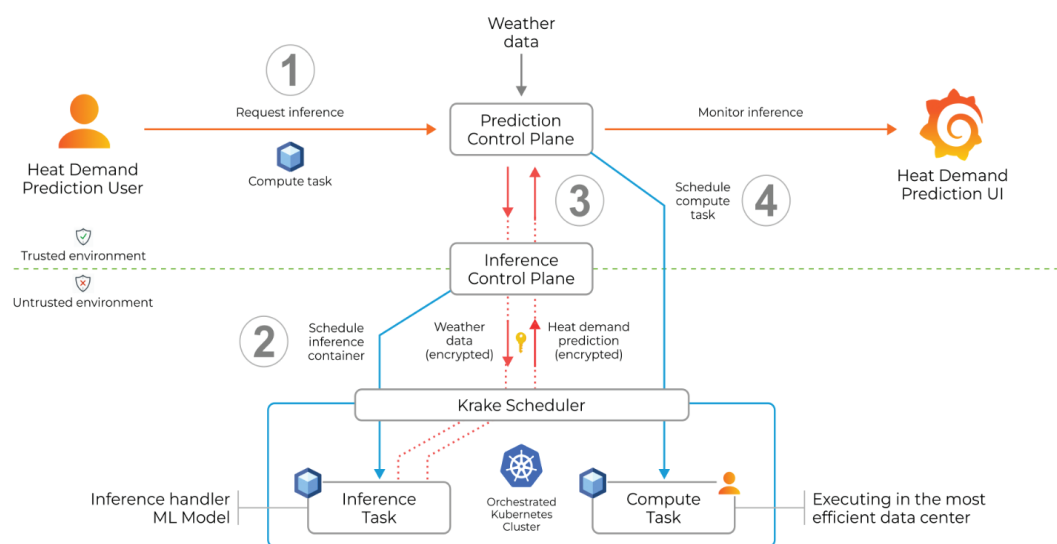


The diagram illustrates the SunRISE system architecture, categorized into three main sections: End nodes (out of scope), End nodes, and Edge nodes.

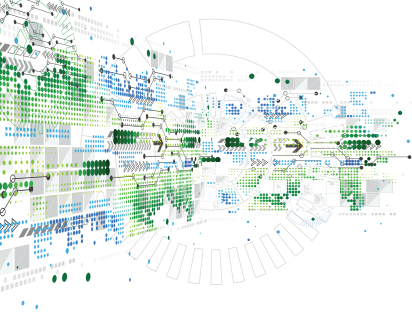
- End nodes (out of scope):** This section shows three types of end nodes:
  - Overall house devices:** Represented by a house icon, connected to a solar panel and a battery.
  - Electric vehicle charging point:** Represented by a green car icon, connected to a solar panel.
  - Old electric meter:** Represented by a house icon, connected to an old electric meter.
- End nodes:** This section shows three types of end nodes:
  - Electric meter:** Represented by a house icon, connected to a solar panel and a battery.
  - Electric meter:** Represented by a house icon, connected to a solar panel.
  - Old electric meter:** Represented by a house icon, connected to an old electric meter.
- Edge nodes:** This section shows three types of edge nodes:
  - Wired connection:** Represented by a house icon, connected to a solar panel and a battery.
  - Wired connection:** Represented by a house icon, connected to a solar panel.
  - Optical sensor:** Represented by a house icon, connected to an old electric meter.

Data from the end nodes is transmitted to the edge nodes via wired connections. The edge nodes then transmit data to the SunRISE cloud through a household internet network. The SunRISE cloud is represented by a cloud icon. The cloud then transmits data to a website for users to consult electrical consumption (out of scope), represented by a computer monitor icon.

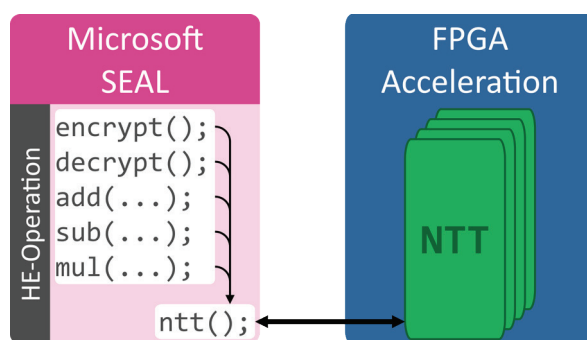
in a privacy-preserving manner. The data privacy was accomplished through technologies such as federated machine learning and multi-party computation. Malicious behavioural patterns can be detected on the edge device, e.g. the gateway in a household. The developed technologies are linked to the first key innovation.



so that an external observer could not exploit or misuse the information of the heat demand. This allows, without violation of data privacy regulations, the execution of the prediction model in an environment that is considered to be ‘honest but curious’, which could be a trusted third-party organisation. The developed methodologies are linked to the second key innovation.

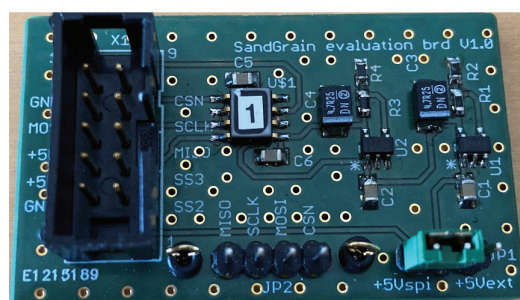
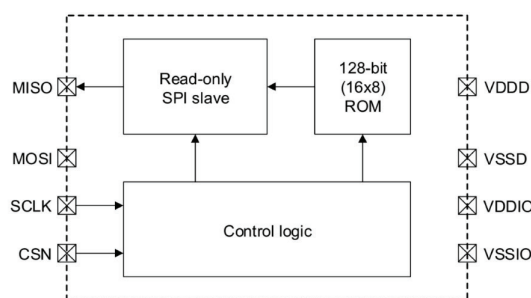


With regards to the third key innovation, there was extensive research on several approaches, such as federated machine learning, multi-party computation, differential privacy, and others. Especially worth mentioning is the development of an IP (Intellectual Property) block that accelerates the hardware of a computationally expensive component of HE (Homomorphic Encryption). This IP was also integrated into the Microsoft SEAL HE library and tested on an FPGA (Field Programmable Gate Array).



Furthermore, a robust and scalable authentication platform has been developed to address one of the main Internet-of-Things challenges: authentication of the many and widely dispersed end nodes.

The system uses a physical token, containing the unique ID generated by the central system, that can be read electronically, and is physically connected to the asset. These are the SandGrain tokens (ICs). The developed chip enhances the security of IoT devices and is linked to the fourth key innovation.



## Market Potential

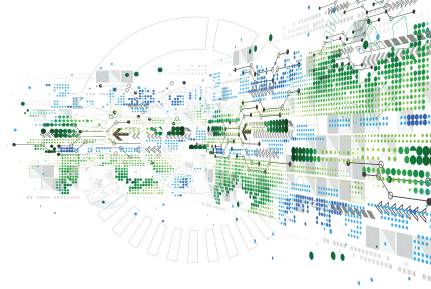
The technologies and methodologies developed in SunRISE are already being incorporated into Integrated Circuits (ICs) such as hardware encryption accelerators and IoT end-nodes, as well as in distributed AI solutions and ML for privacy preservation for businesses using cloud and IoT technologies. Overall, SunRISE will allow European companies and research institutes to reinforce and expand their leading market position in cybersecurity solutions. These are applicable in numerous use cases including anomaly detection, predictive maintenance, heat / energy prediction, denial of service attacks or the identification of malfunctioning devices.

The markets analysis of the use cases, for which the technologies have been developed, show a quickly growing market potential, in which the SunRISE technologies will help the actors to distinguish themselves from their competitors. In the healthcare domain, in particular the MRI (Magnetic Resonance Imaging) domain, a CAGR (Compound Annual Growth Rate) of 6.2 % is expected from 2022-2030. The global smart home domain is expected to grow with a CAGR of 21.1% from 2021 to 2028. In the cloud infrastructure domain, a CAGR of 19.2 % is expected from 2020 to 2028. The, from Technolution, newly explored space domain is expected to grow with a CAGR of 7.5% from 2020 to 2028.




## Societal & Economic Impact

SunRISE addresses many of the privacy and security concerns of AI/ML and IoT devices. With the technologies researched in SunRISE, both businesses and consumers can increase their trust in smart, connected devices that use ML. This enables the usage of smart devices and ML in fields where they provide a benefit but could not be deployed previously due to security and privacy risks. An example of such a field is the medical domain, which was also highlighted in SunRISE. In addition, the SunRISE technologies could also be deployed in domains where IoT and ML are already widespread, reducing the impact of security and privacy threats.

Furthermore, the SunRISE technologies enable European manufactures to distinguish themselves from others, with a focus on aspects such as privacy and security, which are important in European markets, for both, businesses, and end users. The SunRISE project was essential for the project partners to finance their research in the fields of edge computing, IoT security, data privacy and AI/ML. Several engineers in companies and PhD students at universities could be hired in Europe to work on the project. Especially noteworthy is the funding of the semiconductor start-up company SandGrain that aims for increased manufactury of semiconductors in Europe. Funding for European semiconductor companies such as NXP and SandGrain as part of the SunRISe project has made a significant contribution to the European chips act.



## KEY APPLICATION AREAS

-  Energy
-  Digital Industry
-  Digital Life



## ESSENTIAL CAPABILITIES

-  Systems and Components
-  Connectivity & Interoperability
-  Safety, Security & Reliability

## PARTNERS

Ancud IT,  
AnyWi,  
Cloud & Heat Technologies,  
Eindhoven University of Technology,  
Engie Laborelec,  
Fraunhofer IIS,  
imec,  
Philips,  
Sandgrain,  
Sirris,  
Technical University of Munich,  
TU Delft,  
Technolution,  
Ulm University  
Vattenfall

## COUNTRIES INVOLVED

-  Belgium
-  Germany
-  The Netherlands

## PROJECT LEADER

Leonard Püttjer  
NXP Semiconductors

## KEY PROJECT DATES

01 September 2019- 31 August 2022

While not being the main objective of SunRISE, the project results showed some clear benefits for sustainable use of resources in the computing world. In the Energy Community use case, computations were performed locally on the edge with low-power hardware, instead in energy-exhaustive cloud infrastructure. In the Cloud Infrastructure use case, an algorithm was implemented in a privacy-preserving way, that uses a combination of forecasting green-energy production and prediction of warm-water usage to shift computing loads to distributed cloud containers, so that the amount of green energy used can be maximized, while the warm-water provision to the households is guaranteed.

## Patents/Standardisation/ Publications

Within the SunRISE project, 26 scientific publications have been reported by all project partners combined as part of the Sunrise Project. In addition, 19 university theses were completed.

The SunRISE project was also presented at 10 different events, such as at EF ECS2022 and EluciDATA 2020.

Throughout the project, the project partners reported that 4 patent applications were submitted.

## Future Developments

This is not a complete list, but a summary of some noteworthy future developments:

Engie will start to test the developed privacy-preserving techniques in their production environment and will conduct a performance analysis to benchmark pre-selected approaches.

Philips will focus increasingly on IoT environment instead of cloud services in development, as well as moving toward security-related services in the Healthcare domain.

Cloud & Heat is aiming for deployment of the developed algorithms to enhance security and energy efficiency of their cloud infrastructure.

The SandGrain chip is expected to be ready for production in 2023-2024.

NXP is ramping up development of edge AI accelerators that support federated learning and neuromorphic computing, as well as gauging market interest for a HE accelerator in edge devices.

Technolution is entering the airspace market in which high security standards need to be applied, using the technologies and expertise from the SunRISE project.

The universities will continue their research in the fields of side-channel attacks (TU Delft), data privacy (Uni Ulm), Time-sensitive networking (TU Munich) and artificial intelligence / data privacy (TU Eindhoven).