InSecTT Summary (English)

In recent years, technological development in consumer electronics and industrial applications has developed rapidly. More and smaller, networked devices are able to collect and process data anywhere. The Internet of Things (IoT) is a revolutionary change for many sectors like healthcare, building, automotive, railway, etc.

IoT helps to complete complex tasks, but the other side of the coin is the vulnerability of these devices in terms of security. Recent hacks of millions of webcams, printers, children's toys and even vacuum cleaners as well as Distributed Denial-of-service (DDoS) attacks reduce confidence in this technology. In addition, users are challenged to understand and trust their increasingly complex and smart devices, sometimes resulting in mistrust, usage hesitation and even rejection.

The tasks described above mostly cover processing of data in centralized cloud locations and hence cannot be used for applications where milliseconds matter or for safety-critical applications. By moving AI to the edge, i.e. processing data locally on a hardware device, real-time applications for self-driving cars, robots and many other areas in industry can be enabled.

The ECSEL project InSecTT (Intelligent Secure Trustable Things) is a European research project with Austrian coordination. Virtual Vehicle Research Center from Graz coordinates over 50 partners from 12 European countries. This partner consortium enables comprehensive vertical integration in several areas, from semiconductor manufacturers to system integrators, from operators to end users.

The InSecTT partners believe that Artificial Intelligence of Things (AIoT) is the natural evolution for both AI and IoT because they are mutually beneficial. AI increases the value of the IoT through machine learning by transforming the data into useful information knowledge, while the IoT increases the value of AI through connectivity and data exchange.

Important in InSecTT are not only the technical solutions, but also the social aspect, establishing acceptance and trust in these systems. InSecTT enables the traditionally very strong European industry in the field of embedded systems to keep up against the increasing influence of digital companies from the USA and China and to establish its own independent industrial products based on Artificial Intelligence.

In the frame of the InSecTT project (2020-2023), CISC was working on secure wireless identification, including technologies like RFID, NFC (Near Field Communication), BLE (Bluetooth Low Energy) or UWB (Ultra Wide Band). CISC was involved in two technical building blocks for reliable, robust and secure wireless communication as well as validation and verification. These developments where applied to three industrial use-cases and led to 3 demonstrators integrated with partners.

The results have shown more reliable and trustworthy tracking of luggage in an airport environment; a mobile identification device capable of accessing the infrastructure via secure wireless communication; and a novel testbed for interoperability, performance and conformance measurements of mobile devices as qualified equipment.