SENSIBLE-KI

SENSIBLE-KI

Secure and trustworthy mobile AI

Motivation: Artificial Intelligence (AI) methods are already used in a variety of ever-growing heterogeneous mobile and embedded platforms. Due to their heterogeneity, it is difficult to protect such platforms against cyber-attacks and to prevent the manipulation of machine learning / deep learning models. In particular, there are no uniform approaches to securing AI systems in mobile and embedded contexts, which leads to security vulnerabilities.

Goal: The aim of the project is to integrate AI-supported systems into mobile and embedded devices (e.g. smartphones, IoT surveillance cameras, edge servers) in a secure and easy-to-use manner. In the SENSIBLE-KI project, concepts, methods and demonstrators are to be developed that significantly impede or prevent attacks on AI systems through the use of proven mechanisms of trusted computing.

Intended outcomes: Existing mobile and embedded AI systems on the market, as well as state-of-the-art trusted computing and software-based security mechanisms will be examined and classified. Based on the protection needs, suitable trusted computing mechanisms and software-based security methods will be assigned to the functional application classes. Reference architectures will be conceptualised and used for the implementation of concrete prototypes. The collected experiences and insights will additionally be collected and shared in best practice documents and publicly available code libraries.

Expected impact: In addition to the expert knowledge from cybersecurity research and industry, the project also relies on a broad developer community from various industries and domains. This ensures that the approaches and methods developed also deliver the protection that is needed in practice. In general, the project will contribute to the increased security and privacy for users and it will provide support for developers.

Tags: AI, security, trusted computing, smart living, digital identities and biometric access systems

Contact of the German consortium
Fraunhofer AISEC
Kinga Wróblewska-Augustin
kinga.wroblewska-augustin@aisec.fraunhofer.de

3 YEARS DURATION

March 2021 – February 2024

4 PARTNERS

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC; Hochschule Darmstadt h_da; Bundesdruckerei GmbH; neXenio GmbH

€ 1.5 MILLION FUNDING

The total project costs are € 2.2 million, of which € 1.5 million will be funded.

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Icons: Freepik, Kiranshastry / flaticon.com