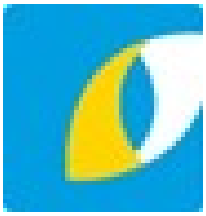

Detecting Inference Attacks Involving Sensor Data

The collection of personal information by organizations has become increasingly essential for social interactions. Nevertheless, according to the GDPR (General Data Protection Regulation), the organizations have to protect collected data. *Access Control* (AC) mechanisms are traditionally used to secure information systems against unauthorized access to sensitive data. The increased availability of personal sensor data, thanks to IoT-oriented applications, motivates new services to offer insights about individuals. Consequently, data mining algorithms have been proposed to infer personal insights from collected sensor data. Although they can be used for genuine purposes, attackers can leverage those outcomes, combining them with other type of data, and further breaching individuals' privacy. Thus, bypassing AC mechanisms thanks to such insights is a concrete problem.

We propose an inference detection system based on the analysis of queries issued on a sensor database. The knowledge obtained through these queries, and the inference channels corresponding to the use of data mining algorithms on sensor data to infer individual information, are described using *Raw sensor data based Inference ChannEl Model* (RICE-M). The detection is carried out by *RICE-M based inference detection System* (RICE-Sy). RICE-Sy considers at the time of the query, the knowledge that a user obtains via a new query and has obtained via his query history, and determines whether this is sufficient to allow that user to operate a channel. Thus, privacy protection systems can take advantage of the inferences detected by RICE-Sy, taking into account individuals' information obtained by the attackers via a database of sensors, to further protect these individuals.