**Détecter les Attaques par Inférences concernant les Données de Capteurs**

Le partage et le traitement des informations personnelles avec les organisations sont devenus de plus en plus essentiels pour les interactions sociales. En Europe, selon le RGPD (Règlement Général sur la Protection des Données), elles doivent protéger par conception et par défaut les données collectées. Les *Mécanismes de Contrôle d'Accès* (MCA) sont traditionnellement utilisés pour sécuriser les systèmes d'information contre l'accès non autorisé à des données sensibles. Cependant, la disponibilité croissante de données de capteurs motive de nouveaux services à fournir des informations sur les individus. Divers algorithmes d'exploration de données ont été proposés pour inférer de nouvelles données personnelles à partir de données de capteurs. Les données sensibles peuvent être accédées indirectement à l'aide de données non sensibles, telles que des informations inférées à partir de données de capteurs. Par conséquent, le risque de contourner les MCAs pour obtenir des informations à l'aide des données de capteur existe.

Nous proposons un système de détection d'inférence basé sur l'analyse des requêtes émises sur une base de données de capteurs. Les connaissances obtenu via ces requêtes, et les canaux d'inférence correspondant à l'utilisation des algorithmes d'exploration de données sur des données de capteur pour inférer les informations des individus, sont décrits grâce à "*Raw sensor data based Inference ChannEl Model*" (RICE-M). La détection est effectuée par "*RICE-M based inference detection System*" (RICE-Sy). RICE-Sy considère au moment de la requête, la connaissance qu'un utilisateur obtient via une nouvelle requête et a obtenues via son historique de requête, et détermine si cela suffit pour permettre à cet utilisateur d'exploiter un canal. Ainsi, les systèmes de protection de la vie privée peuvent tirer parti des inférences détectées par RICE-Sy, en prenant en compte les informations des individus obtenues par les attaquants via une base de données de capteurs, pour davantage protéger ces individus.