Enhancing Data Integrity: A Solution to Predict Data Disturbance in IoT Systems

Meriem Smati*[1,2], Vincent Cheutet[1], Jannik Laval[1], and Christophe Danjou[2]

[1]Décision et Information pour les Systèmes de Production – Université Lumière - Lyon 2, Université Claude Bernard Lyon 1, Institut National des Sciences Appliquées de Lyon – France
[2]Laboratoire Poly-Industrie 4.0, Département de Mathématiques et Génie Industriel, Polytechnique Montréal – Canada

Résumé

The concept of Digital Twin (DT) has evolved to encompass cognitive capabilities, leading to the emergence of Cognitive Digital Twin (CDT). This new ability has enabled them to exhibit greater intelligence and comprehension concerning prediction. This research paper delves into the potential of CDTs to enhance an Internet of Things (IoT) system's resilience and facilitate its maintenance. The integration of CDTs into IoT systems holds potential for improving maintenance and avoidance strategies. This is achieved by introducing a Cognitive Super Digital Twin (CSDT) that not only replicates the actions of the system but also generates data to simulate normal and abnormal scenarios, thereby enhancing the system's security and ensuring its continuity. The CSDT can identify data vulnerabilities and devise appropriate countermeasures, aiding the user in decision-making. This proactive approach enables the system to adapt and fortify its security measures in real-time or in advance, mitigating potential risks and ensuring uninterrupted operation. The findings of this research underscore the transformative impact of CDTs in strengthening IoT system security, realized by harnessing the capabilities of cognitive technologies and the additional layer of data generation.

*Intervenant