

Local Differential Privacy-Based Data-Sharing Scheme for Smart Utilities

Authors : Veniamin Boiarkin, Bruno Bogaz Zarpelão, Muttukrishnan Rajarajan

Abstract : The manufacturing sector is a vital component of most economies, which leads to a large number of cyberattacks on organisations, whereas disruption in operation may lead to significant economic consequences. Adversaries aim to disrupt the production processes of manufacturing companies, gain financial advantages, and steal intellectual property by getting unauthorised access to sensitive data. Access to sensitive data helps organisations to enhance the production and management processes. However, the majority of the existing data-sharing mechanisms are either susceptible to different cyber attacks or heavy in terms of computation overhead. In this paper, a privacy-preserving data-sharing scheme for smart utilities is proposed. First, a customer's privacy adjustment mechanism is proposed to make sure that end-users have control over their privacy, which is required by the latest government regulations, such as the General Data Protection Regulation. Secondly, a local differential privacy-based mechanism is proposed to ensure the privacy of the end-users by hiding real data based on the end-user preferences. The proposed scheme may be applied to different industrial control systems, whereas in this study, it is validated for energy utility use cases consisting of smart, intelligent devices. The results show that the proposed scheme may guarantee the required level of privacy with an expected relative error in utility.

Keywords : data-sharing, local differential privacy, manufacturing, privacy-preserving mechanism, smart utility

Conference Title : ICCMS 2023 : International Conference on Cyber Manufacturing Systems

Conference Location : Rome, Italy

Conference Dates : September 11-12, 2023