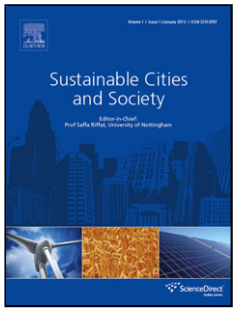

Title: Privacy-enhancing Aggregation of Internet of Things Data via Sensors Grouping

Author: Stefano Bennati Evangelos Pournaras

PII: S2210-6707(17)31077-6
DOI: https://doi.org/doi:10.1016/j.scs.2018.02.013
Reference: SCS 980

To appear in:

Received date: 15-8-2017
Revised date: 8-2-2018
Accepted date: 12-2-2018

Please cite this article as: Stefano Bennati, Evangelos Pournaras, Privacy-enhancing Aggregation of Internet of Things Data via Sensors Grouping, *<![CDATA[Sustainable Cities and Society]]>* (2018), https://doi.org/10.1016/j.scs.2018.02.013

Privacy-enhancing Aggregation of Internet of Things Data via Sensors Grouping

Stefano Bennati[a,*], Evangelos Pournaras[a]

[a]*Professorship of Computational Social Science*
ETH Zurich, Zurich, Switzerland

Abstract

Big data collection practices using Internet of Things (IoT) pervasive technologies are often privacy-intrusive and result in surveillance, profiling, and discriminatory actions over citizens that in turn undermine the participation of citizens to the development of sustainable smart cities. Nevertheless, real-time data analytics and aggregate information from IoT devices open up tremendous opportunities for managing and regulating smart city infrastructures in a more efficient and sustainable way. The privacy-enhancing aggregation of distributed sensor data, such as residential energy consumption or traffic information, is the research focus and challenge tackled in this paper. Citizens have the option to choose their privacy level by reducing the quality of the shared data at a cost of a lower accuracy in data analytics services. A baseline scenario is considered in which IoT sensor data are shared directly with an untrustworthy central aggregator. A grouping mechanism is introduced that improves privacy by sharing data aggregated first at a group level compared to a baseline scenario in which each individual shares data directly to the central aggregator. Group-level aggregation obfuscates sensor data of individuals, in a similar fashion as differential privacy and homomorphic encryption schemes, thus inference of privacy-sensitive information from single sensors becomes computationally harder compared to the baseline scenario. The proposed system and its generic applicability are evaluated using real-world data from two smart city pilot projects. Privacy under grouping increases, while preserving the accuracy of the baseline scenario. Intra-group influences of privacy by one group member on the other ones are measured and fairness on privacy is found to be maximized between group members with similar privacy choices. Several grouping strategies are compared. Grouping by proximity of privacy choices provides the highest privacy gains. The implications of the strategy on the design of incentives mechanisms are discussed.

Keywords: privacy, Internet of Things, Smart City, network, sensor, grouping, agent, aggregation

*Corresponding author
Email addresses: sbennati@ethz.ch (Stefano Bennati), epournaras@ethz.ch (Evangelos