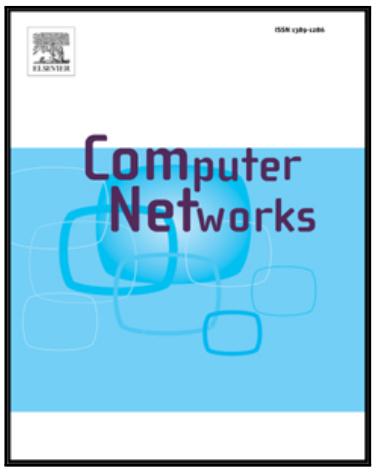


Security and Privacy in Cloud-Assisted Cyber-Physical Systems

Cristina Alcaraz , Xinyi Huang , Erich Rome

PII: S1389-1286(18)30146-4
DOI: 10.1016/j.comnet.2018.03.026
Reference: COMPNW 6453

To appear in: *Computer Networks*

Please cite this article as: Cristina Alcaraz , Xinyi Huang , Erich Rome , Security and Privacy in Cloud-Assisted Cyber-Physical Systems , *Computer Networks* (2018), doi: 10.1016/j.comnet.2018.03.026

Security and Privacy in Cloud-Assisted Cyber-Physical Systems

Increasingly, we are witnessing technological advances in the areas of Cyber-Physical Systems (CPS) and cloud-computing, and the coupling of their technologies within a critical environment, so as to optimize operations and essential services. Particularly, Cloud-assisted Cyber-Physical Systems (Cloud-CPS) can be viewed as the bridge between physical components, processes and the cyber space. CPSes provide computing (e.g., sensing, analyzing, and predicting), communications (e.g., interaction, intervene, and interface management), and controlling (e.g., inter-operation and evolving) to reach intelligent systems with autonomous capacity that satisfy specific services of the applications' context, such as health care, smart electricity grid, smart factories, and smart buildings.

This autonomy level also brings about numerous technical problems, mainly associated with technical capacities of most of the embedded systems together, combined with the processing of a large fast-growing data volume. Most of the present CPSes are not able to support ultra-fast computing (e.g., including the use of sensors, actuators, and remote terminal units) to guarantee real-time and reliable services. That is, they fail to meet the minimal requirements such as performance and productivity in respective times determined by dedicated thresholds, which are generally demanded by mission-critical systems. Fortunately, this lack can be remedied by cloud infrastructures and platforms, since they can provide flexible and on-demand processing power and high-capacity storage for data streams as well as provisioning of a variety of services using telecommunication and networking technologies.

However, although the large-scale nature of CPSes can be effectively and efficiently supported and assisted by cloud systems—which is referred to as a Cloud-CPS—, the coupling of these two technologies is subject to multiple kinds of risk. CPSes often collect sensitive and private information about the physical environment, especially in critical systems. Therefore, a loss of security for a CPS can have significant negative impacts including the loss of data protection, privacy, potential physical harm, discrimination, and abuse. Though numerous security primitives have been developed in the cyber domain to address the very same problems, their applicability to the Cloud-CPS domain is still questionable due to the reason that they are usually complex to implement and oblivious to cyber-physical interactions.

This special issue of *Computer Networks*, devoted to "*Security and Privacy in Cloud-Assisted Cyber-Physical Systems*", presents a collection of articles that investigate and address the aforementioned challenges, while providing new insights and proposing solutions for some of the issues raised. The first article, entitled "*Lightweight Attribute Based Encryption Scheme for Mobile Cloud assisted Cyber-Physical Systems*" presents a new approach, called the Lightweight Attribute Based Encryption Scheme (LABE), for mobile Cloud-assisted CPSes based on a proxy service architecture and a cipher-text policy related to Attribute Based Encryption. The authors show the feasibility of the approach and guarantee fine grained-through access control and revocation capacity.

The following paper, entitled "*An Efficient and Expressive Ciphertext-Policy Attribute-Based Encryption Scheme with Partially Hidden Access Structures, Revisited*", also explores the problem of Ciphertext-Policy Attribute-based Encryption (CP-ABE) and