1. Record Nr.   UNINA9910299347503321

   Autore   Lin Xiaodong

   Titolo   Privacy-Enhancing Fog Computing and Its Applications / / by Xiaodong Lin, Jianbing Ni, Xuemin (Sherman) Shen

   Pubbl/distr/stampa Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018

   ISBN   3-030-02113-0

   Edizione   [1st ed. 2018.]

   Descrizione fisica 1 online resource (98 pages)

   Collana   SpringerBriefs in Electrical and Computer Engineering, , 2191-8112

   Disciplina   005.8

   Soggetti   Data protection
                     Wireless communication systems
                     Mobile communication systems
                     Electrical engineering
                     Security
                     Wireless and Mobile Communication
                     Communications Engineering, Networks

   Lingua di pubblicazione Inglese

   Formato   Materiale a stampa

   Livello bibliografico Monografia

   Nota di contenuto 1 Introduction -- 2 Privacy-enhancing Technologies -- 3 Identity Privacy Protection in Smart Parking Navigation -- 4 Location Privacy Protection in Mobile Crowdsensing -- 5 Data Privacy Protection in Smart Grid -- 6 Conclusions and Future Directions.

   Sommario/riassunto This SpringerBrief covers the security and privacy challenges in fog computing, and proposes a new secure and privacy-preserving mechanisms to resolve these challenges for securing fog-assisted IoT applications. Chapter 1 introduces the architecture of fog-assisted IoT applications and the security and privacy challenges in fog computing. Chapter 2 reviews several promising privacy-enhancing techniques and illustrates examples on how to leverage these techniques to enhance the privacy of users in fog computing. Specifically, the authors divide the existing privacy-enhancing techniques into three categories: identity-hidden techniques, location privacy protection and data privacy enhancing techniques. The research is of great importance since security and privacy problems faced by fog computing impede the

healthy development of its enabled IoT applications. With the advanced privacy-enhancing techniques, the authors propose three secure and privacy-preserving protocols for fog computing applications, including smart parking navigation, mobile crowdsensing and smart grid. Chapter 3 introduces identity privacy leakage in smart parking navigation systems, and proposes a privacy-preserving smart parking navigation system to prevent identity privacy exposure and support efficient parking guidance retrieval through road-side units (fogs) with high retrieving probability and security guarantees. Chapter 4 presents the location privacy leakage, during task allocation in mobile crowdsensing, and propose a strong privacy-preserving task allocation scheme that enables location-based task allocation and reputation-based report selection without exposing knowledge about the location and reputation for participators in mobile crowdsensing. Chapter 5 introduces the data privacy leakage in smart grid, and proposes an efficient and privacy-preserving smart metering protocol to allow collectors (fogs) to achieve real-time measurement collection with privacy-enhanced data aggregation. Finally, conclusions and future research directions are given in Chapter 6. This brief validates the significant feature extension and efficiency improvement of IoT devices without sacrificing the security and privacy of users against dishonest fog nodes. It also provides valuable insights on the security and privacy protection for fog-enabled IoT applications. Researchers and professionals who carry out research on security and privacy in wireless communication will want to purchase this SpringerBrief. Also, advanced level students, whose main research area is mobile network security will also be interested in this SpringerBrief. .