SPRINGER BRIEFS IN
ELECTRICAL AND COMPUTER ENGINEERING

Xiaodong Lin
Jianbing Ni
Xuemin (Sherman) Shen

Privacy-Enhancing Fog Computing and Its Applications

Springer

SpringerBriefs in Electrical and Computer Engineering

SpringerBriefs present concise summaries of cutting-edge research and practical applications across a wide spectrum of fields. Featuring compact volumes of 50 to 125 pages, the series covers a range of content from professional to academic. Typical topics might include: timely report of state-of-the art analytical techniques, a bridge between new research results, as published in journal articles, and a contextual literature review, a snapshot of a hot or emerging topic, an in-depth case study or clinical example and a presentation of core concepts that students must understand in order to make independent contributions.

More information about this series at http://www.springer.com/series/10059

Xiaodong Lin • Jianbing Ni
Xuemin (Sherman) Shen

Privacy-Enhancing Fog Computing and Its Applications

Springer

Xiaodong Lin
Department of Physics and Computer Science
Wilfrid Laurier University
Waterloo, ON, Canada

Jianbing Ni
Electrical and Computer Engineering Department
University of Waterloo
Waterloo, ON, Canada

Xuemin (Sherman) Shen
Electrical and Computer Engineering Department
University of Waterloo
Waterloo, ON, Canada

ISSN 2191-8112 ISSN 2191-8120 (electronic)
SpringerBriefs in Electrical and Computer Engineering
ISBN 978-3-030-02112-2 ISBN 978-3-030-02113-9 (eBook)
https://doi.org/10.1007/978-3-030-02113-9

Library of Congress Control Number: 2018959867

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Fog computing has been considered as a key enabler to reach the increasing demands on local data analysis and numerous device connections for Internet-of-Things (IoT), by extending computing, storage, and networking resources to the network edge. Deployed between user devices and cloud centers, fog nodes monitor or analyze real-time data from network-connected "things," supporting a variety of IoT services, such as smart traffic lights, home energy management, and augmented reality. As a promising extension of cloud computing, fog computing can offer on-demand and ubiquitous applications on nearby devices that can result in superior user experience and increase redundancy in case of failures. Despite the appealing advantages, fog computing is confronted with various security and privacy threats due to ubiquitous connections and limited resources, which have not been systemically discussed in the literature.

In this monograph, we address the security and privacy challenges in fog computing and propose secure and privacy-preserving schemes to deal with these challenges for securing fog-assisted IoT applications. The research is of great importance since security and privacy problems faced by fog computing impede the healthy development of its enabled IoT applications. In Chap. 1, we introduce the architecture of fog-assisted IoT applications and the security and privacy challenges in fog computing. In Chap. 2, we review several promising privacy-enhancing techniques and show examples on how to leverage these techniques to enhance the privacy of users in fog computing. Specifically, we divide the existing privacy-enhancing techniques into three categories: identity privacy-enhancing techniques, location privacy-enhancing techniques, and data privacy-enhancing techniques. With the advanced privacy-enhancing techniques, we propose three secure and privacy-preserving schemes for fog computing applications, including smart parking navigation, mobile crowdsensing, and smart grid, which will be detailed in the next three chapters. In Chap. 3, we introduce the identity privacy leakage in smart parking navigation systems and propose a privacy-preserving smart parking navigation scheme to prevent identity privacy exposure and support efficient parking guidance retrieval through road-side units (fogs) with high retrieving

probability and security guarantees. In Chap. 4, we introduce 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 based on fog computing without exposing knowledge about the location of participators in mobile crowdsensing. In Chap. 5, we introduce the data privacy leakage in smart grid and propose an efficient and privacy-preserving smart metering scheme to allow collectors (fogs) to achieve real-time measurement collection with privacy-enhanced data aggregation, even if the collectors are compromised or curious about collected data. Finally, remarks and future research directions are given in Chap. 6. This monograph 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.

We would like to thank Prof. Kuan Zhang at the University of Nebraska-Lincoln and Prof. Yong Yu at Shaanxi Normal University for their contributions in the presented research works. We would also like to thank Dongxiao Liu, Cheng Huang, Meng Li, and Liang Xue for reviewing parts of this monograph, and all the members of broadband communication research group for the valuable discussions and their insightful suggestions and comments. Special thanks are also due to the staff at Springer Science+Business Media, especially Susan Lagerstrom-Fife for her help throughout the publication preparation process.

Waterloo, Canada

Xiaodong Lin
Jianbing Ni
Xuemin (Sherman) Shen

Contents