

Wireless Networks

Series Editor

Xuemin Sherman Shen, University of Waterloo, Waterloo, ON, Canada

The purpose of Springer's Wireless Networks book series is to establish the state of the art and set the course for future research and development in wireless communication networks. The scope of this series includes not only all aspects of wireless networks (including cellular networks, WiFi, sensor networks, and vehicular networks), but related areas such as cloud computing and big data. The series serves as a central source of references for wireless networks research and development. It aims to publish thorough and cohesive overviews on specific topics in wireless networks, as well as works that are larger in scope than survey articles and that contain more detailed background information. The series also provides coverage of advanced and timely topics worthy of monographs, contributed volumes, textbooks and handbooks.


** Indexing: Wireless Networks is indexed in EBSCO databases and DPLB **

More information about this series at <http://www.springer.com/series/14180>


Longxiang Gao • Tom H. Luan • Bruce Gu •
Youyang Qu • Yong Xiang


Privacy-Preserving in Edge Computing

Longxiang Gao 
School of Information Technology
Deakin University
Burwood, VIC, Australia

Tom H. Luan 
School of Cyber Engineering
Xi'an Dianzi University
Xi'an, Shaanxi, China

Bruce Gu 
College of Engineering and Science
Victoria University
Melbourne, VIC, Australia

Youyang Qu 
School of Information Technology
Deakin University
Melbourne, VIC, Australia

Yong Xiang 
School of Information Technology
Deakin University
Melbourne, VIC, Australia

ISSN 2366-1186

Wireless Networks

ISBN 978-981-16-2198-7

<https://doi.org/10.1007/978-981-16-2199-4>

ISSN 2366-1445 (electronic)

ISBN 978-981-16-2199-4 (eBook)

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2021

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

With the rapid development of big data, it is necessary to transfer the massive data generated by end devices to the cloud under the traditional cloud computing model. However, the delays caused by massive data transmission no longer meet the requirements of various real-time mobile services. Therefore, the emergence of edge computing has been recently developed as a new computing paradigm that can collect and process data at the edge of the network, which brings significant convenience to solving problems such as delay, bandwidth, and off-loading in the traditional cloud computing paradigm. By extending the functions of the cloud to the edge of the network, edge computing provides effective data access control, computation, processing, and storage for end devices. Furthermore, edge computing optimizes the seamless connection from the cloud to devices, which is considered the foundation for realizing the interconnection of everything. However, due to the open features of edge computing, such as content awareness, real-time computing, and parallel processing, the existing problems of privacy in the edge computing environment have become more prominent. The access to multiple categories and large numbers of devices in edge computing also creates new privacy issues.

In this book, we discuss on the research background and current research process of privacy protection in edge computing. In the first chapter, the state-of-the-art research of edge computing are reviewed. The second chapter discusses the data privacy issue and attack models in edge computing. Three categories of privacy-preserving schemes will be further introduced in the following chapters. Chapter 3 introduces the context-aware privacy-preserving scheme. Chapter 4 further introduces a location-aware differential privacy-preserving scheme. Chapter 5 presents a new blockchain-based decentralized privacy preserving in edge computing. Chapter 6 summarizes this monograph and proposes future research directions.

In summary, this book introduces the following techniques in edge computing: (1) describes an MDP-based privacy-preserving model to solve context-aware data privacy in the hierarchical edge computing paradigm; (2) describes an SDN-based

clustering method to solve the location-aware privacy problems in edge computing; and (3) describes a novel blockchain-based decentralized privacy-preserving scheme in edge computing. These techniques enable the rapid development of privacy preserving in edge computing.

Melbourne, VIC, Australia
Xi'an, China
Melbourne, VIC, Australia
Melbourne, VIC, Australia
Melbourne, VIC, Australia
March 2021

Longxiang Gao
Tom H. Luan
Bruce Gu
Youyang Qu
Yong Xiang

Contents

- 1 An Introduction to Edge Computing** 1
 - 1.1 Definition of Edge Computing 2
 - 1.2 Architecture of Edge Computing 3
 - 1.2.1 Storage 4
 - 1.2.2 Computing 5
 - 1.2.3 Communication 6
 - 1.3 Advantages of Edge Computing 9
 - 1.4 Exemplary Applications 12
 - References 13
- 2 Privacy Issues in Edge Computing** 15
 - 2.1 Context-Aware Privacy Issue 16
 - 2.2 Location-Aware Privacy Issue 17
 - 2.3 Decentralized Privacy Issue 19
 - 2.4 Common Privacy Attacks and Potential Attacking Windows 21
 - References 28
- 3 Context-Aware Privacy Preserving in Edge Computing** 35
 - 3.1 System Modeling 36
 - 3.1.1 Actions of Adversary 36
 - 3.1.2 Problem Formulation 39
 - 3.1.3 Markov Decision Process (MDP) 39
 - 3.1.4 System State 39
 - 3.1.5 State Transition 40
 - 3.1.6 MDP-Based Nash Equilibrium 41
 - 3.2 System Analysis 42
 - 3.2.1 QoS Data Utility Measurement 42
 - 3.2.2 Privacy Loss Analysis 43

3.3	Reinforcement Learning in Optimal Defense Strategy	44
3.3.1	Fast Convergence Reinforcement Learning	44
3.3.2	The Best Strategy with Unlimited Computing Capabilities.....	46
3.3.3	The Best Strategy with Limited Computing Capabilities	46
3.4	Performance Evaluation	47
3.4.1	Iteration Times Evaluation	48
3.4.2	Payoff Changes Evaluation.....	52
3.4.3	Privacy Loss Changes	56
3.4.4	Convergence Speed Evaluation	60
3.5	Summary	60
	References	62
4	Location-Aware Privacy Preserving in Edge Computing	65
4.1	System Modeling	67
4.1.1	Adversaries Attack Formulation	67
4.1.2	Edge Nodes Clustering Scheme.....	69
4.2	System Analysis.....	72
4.3	Differential Privacy Protection Scheme	73
4.4	Performance Evaluation	75
4.4.1	Clustering Analysis	76
4.4.2	Data Utilities Performance	77
4.4.3	Performances Against Attacking Models.....	78
4.5	Summary	81
	References	81
5	Blockchain Based Decentralized Privacy Preserving in Edge Computing	83
5.1	System Modeling	84
5.1.1	Federated Learning in FL-Block	84
5.1.2	Blockchain in FL-Block	86
5.2	System Analysis.....	89
5.2.1	Poisoning Attacks and Defense	89
5.2.2	Single-Epoch FL-Block Latency Model.....	90
5.2.3	Optimal Generation Rate of Blocks.....	92
5.3	Decentralized Privacy-Preserving Protocols	94
5.3.1	Hybrid identity	94
5.3.2	Accessional Functions	96
5.3.3	Access Control and Data Load	97
5.3.4	Discussion	97
5.4	Performance Evaluation	98
5.4.1	Simulation Environment Description	99
5.4.2	Global Models and Corresponding Updates.....	100
5.4.3	Evaluation on Convergence and Efficiency.....	101

- 5.4.4 Evaluation on Blockchain 104
 - 5.4.5 Evaluation on Poisoning Attack Resistance 107
 - 5.5 Summary 108
 - References 108
- 6 Conclusion and Future Research Issues 111**
 - 6.1 Conclusion 111
 - 6.2 Future Work 112

Acronyms

AP	Affinity propagation
AWGN	Additive white Gaussian noise
CCDF	Complementary cumulative distribution function
CCDP	Classic customizable differential privacy
CDN	Information centric network
CDP	Classic ϵ -differential privacy
CNN	Condensed nearest neighbor
CP-ABE	Ciphertext policy-attribute based encryption
DDoS	Distributed denial-of-service attack
DDSDP	Dynamic dual-scheme ϵ -customized differential privacy
DHT	Distributed hash table
DP	Differential privacy
DSL	Dynamic solution layer
EWM	Entropy weight method
FDMA	Frequency division multiple access
FL	Federated learning
FL-Block	Blockchain-enabled federated learning
GCA	Grid-based clustering algorithm
ICN	Information centric network
IIoTs	Industrial Internet of Things
IoTs	Internet of Things
LTE	Long-term evolution
MDP	Markov decision process
MDP-PPFC	Markov decision process based privacy preserving
NE	Nash equilibrium
PCP	Privacy-preserving content-based publish
PoW	Proof of work
PPFA	Privacy preserving fog-enabled aggregation
QoS	Quality of service

ReLU	Rectified linear unit
SARSA	State action reward state action
SDN	Software defined network
SVRG	Stochastic variance reduced gradient