Premier Reference Source

Security Management in Mobile Cloud Computing

Kashif Munir

IGI GLOBAL
DISSEMINATOR OF KNOWLEDGE

Security Management in Mobile Cloud Computing

Kashif Munir
University of Hafr Al-Batin, Saudi Arabia

A volume in the Advances in Information Security, Privacy, and Ethics (AISPE) Book Series

www.igi-global.com

Published in the United States of America by
IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Munir, Kashif, 1976- editor.
Title: Security management in mobile cloud computing / Kashif Munir, editor.
Description: Hershey, PA : Information Science Reference, [2017] | Includes bibliographical references and index.
Identifiers: LCCN 2016017812| ISBN 9781522506027 (hardcover) | ISBN 9781522506034 (ebook)
Subjects: LCSH: Cloud computing--Security measures. | Mobile computing--Security measures. | Computer networks--Security measures.
Classification: LCC QA76.585 .S444 2017 | DDC 005.8--dc23 LC record available at https://lccn.loc.gov/2016017812

This book is published in the IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) (ISSN: 1948-9730; eISSN: 1948-9749)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Advances in Information Security, Privacy, and Ethics (AISPE) Book Series

ISSN: 1948-9730
EISSN: 1948-9749

Mission

As digital technologies become more pervasive in everyday life and the Internet is utilized in ever increasing ways by both private and public entities, concern over digital threats becomes more prevalent.

The **Advances in Information Security, Privacy, & Ethics (AISPE) Book Series** provides cutting-edge research on the protection and misuse of information and technology across various industries and settings. Comprised of scholarly research on topics such as identity management, cryptography, system security, authentication, and data protection, this book series is ideal for reference by IT professionals, academicians, and upper-level students.

Coverage

- CIA Triad of Information Security
- Privacy Issues of Social Networking
- Global Privacy Concerns
- Tracking Cookies
- Internet Governance
- Device Fingerprinting
- Cyberethics
- Telecommunications Regulations
- Access Control
- Security Classifications

IGI Global is currently accepting manuscripts for publication within this series. To submit a proposal for a volume in this series, please contact our Acquisition Editors at Acquisitions@igi-global.com or visit: http://www.igi-global.com/publish/.

The Advances in Information Security, Privacy, and Ethics (AISPE) Book Series (ISSN 1948-9730) is published by IGI Global, 701 E. Chocolate Avenue, Hershey, PA 17033-1240, USA, www.igi-global.com. This series is composed of titles available for purchase individually; each title is edited to be contextually exclusive from any other title within the series. For pricing and ordering information please visit http://www.igi-global.com/book-series/advances-information-security-privacy-ethics/37157. Postmaster: Send all address changes to above address.

Titles in this Series

For a list of additional titles in this series, please visit: www.igi-global.com

Cryptographic Solutions for Secure Online Banking and Commerce
Kannan Balasubramanian (Mepco Schlenk Engineering College, India) K. Mala (Mepco Schlenk Engineering College, India) and M. Rajakani (Mepco Schlenk Engineering College, India)
Information Science Reference • copyright 2016 • 375pp • H/C (ISBN: 9781522502739) • US $200.00 (our price)

Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security
Brij Gupta (National Institute of Technology Kurukshetra, India) Dharma P. Agrawal (University of Cincinnati, USA) and Shingo Yamaguchi (Yamaguchi University, Japan)
Information Science Reference • copyright 2016 • 589pp • H/C (ISBN: 9781522501053) • US $305.00 (our price)

Innovative Solutions for Access Control Management
Ahmad Kamran Malik (COMSATS Institute of Information Technology, Pakistan) Adeel Anjum (COMSATS Institute of Information Technology, Pakistan) and Basit Raza (COMSATS Institute of Information Technology, Pakistan)
Information Science Reference • copyright 2016 • 330pp • H/C (ISBN: 9781522504481) • US $195.00 (our price)

Network Security Attacks and Countermeasures
Dileep Kumar G. (Adama Science and Technology University, Ethiopia) Manoj Kumar Singh (Adama Science and Technology University, Ethiopia) and M.K. Jayanthi (King Khalid University, Saudi Arabia)
Information Science Reference • copyright 2016 • 357pp • H/C (ISBN: 9781466687615) • US $205.00 (our price)

Next Generation Wireless Network Security and Privacy
Kamaljit I. Lakhtaria (Gujarat University, India)
Information Science Reference • copyright 2015 • 372pp • H/C (ISBN: 9781466686878) • US $205.00 (our price)

Improving Information Security Practices through Computational Intelligence
Wasan Shaker Awad (Ahlia University, Bahrain) El Sayed M. El-Alfy (King Fahd University of Petroleum and Minerals, Saudi Arabia) and Yousif Al-Bastaki (University of Bahrain, Bahrain)
Information Science Reference • copyright 2016 • 327pp • H/C (ISBN: 9781466694262) • US $210.00 (our price)

IGI GLOBAL
DISSEMINATOR OF KNOWLEDGE
www.igi-global.com

701 E. Chocolate Ave., Hershey, PA 17033
Order online at www.igi-global.com or call 717-533-8845 x100
To place a standing order for titles released in this series,
contact: cust@igi-global.com
Mon-Fri 8:00 am - 5:00 pm (est) or fax 24 hours a day 717-533-8661

Editorial Advisory Board

Foreword

The number of mobile device users and mobile apps available for these users are increasing dramatically. According to the International Telecommunication Union (ITU, 2016), by the end of 2015, there were more than 7 billion mobile cellular subscriptions, corresponding to a penetration rate of 97%, up from 738 million in 2000. Cisco (2016), reports that global mobile data traffic grew 74 percent in 2015 and has grown 4,000-fold over the past 10 years and almost 400-million-fold over the past 15 years. Most of these mobile device users and their mobile network operators are connected to cloud computing service providers to offer rich computational and Internet resources, which is Mobile Cloud Computing (MCC).

As we move from traditional desktop/laptop computing to mobile cloud computing, we also need to take into consideration the security management in mobile cloud computing. Mobile cloud computing uses wireless network technology for connectivity to the servers and cloud service providers, which is more vulnerable than wired networks. Almost all of the mobile device users data is stored with the cloud service providers server so that there is "always on" 24/7 access. Storage of an individual's data or a company's data with a third party always poses a security risk. Therefore, this book on Security Management in Mobile Cloud Computing is a timely publication for readers, academics, researchers and professionals to gain first-hand knowledge about the issues and challenges faced in managing security in Mobile Cloud Computing systems.

The number of variants of malicious software aimed at mobile devices has reportedly risen from about 14,000 to 40,000 or about 185% in less than a year, the United States Government Accountability Office stated (GAO, 2012). With the consumerisation of Information Technology, employees now bring their own devices (BYOD) and connect it to the corporate network. According to the Cloud Security Alliance (CSA, 2012), 69% of companies do not have a BYOD security policy and 64% of companies do not mandate or enforce mobile device security. Such ignorance might be due to lack of information about the risks and loss associated with such vulnerability. This book is aimed at informing the policy makers and practitioners on the different aspects of Security Management in Mobile Cloud Computing. It

investigates the different protocols and architectures that can be used to design, create, and develop security mechanisms. It proposes innovative approaches and solutions to Mobile Cloud Computing security challenges.

Readers of this book will be enlightened on the following in regards to security management in mobile cloud computing: Chapter 2 presents an intrusion detection system to enhance security. Chapter 3 provides specific guidelines to reduce risks resulting from utilizing middle circle providers. Chapter 4 explores proper recovery planning in the event of disasters resulting from cyber-attacks. Chapter 6 proposes a framework that provides security with minimum processing overheads. Chapter 7 looks at security issues and vulnerabilities and the possible solutions to such issues. Chapter 8 discusses a security model for Mobile Cloud Database as a Service (DBaaS). In addition to the above, Chapter 1 presents a new routing protocol based on smart energy management and Chapter 5 looks at the Game Theory in modelling Peer-to-Peer network systems.

Sam Goundar
Victoria University of Wellington, New Zealand & KYS Business School, Malaysia

REFERENCES

Cisco. (2016). *Cisco visual networking index: Global mobile data traffic forecast update, 2015-2020*. Retrieved from: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html

CSA. (2012). *CSA identifies 17 key components for effective mobile device management of BYOD and company-owned devices*. Retrieved from: https://cloudsecurityalliance.org/media/news/csa-publishes-mobile-device-management/

GAO U.S. Government Accountability Office. (2012). *Information security: Better implementation of controls for mobile devices should be encouraged*. Retrieved from: http://www.gao.gov/products/GAO-12-757

ITU Telecommunication Development Bureau. (2015). *ICT facts and figures*. Retrieved from: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFacts-Figures2015.pdf

Preface

Mobile Cloud Computing (MCC) is gaining stream. According to the latest study from Juniper Research, the number of mobile cloud computing subscribers is expected to grow rapidly in the next five years. Considered as one of today's hottest new technology markets. MCC integrate different major technologies such as smart phones, tablets, services, big data and cloud computing in one platform provided to the end users. Many issues such as networking, cloud services, security, quality and the availability of services, user data management are still challenging to the rapid growth of MCC.

This book is essential for researchers, engineers, and professionals interested in exploring recent advances in Mobile Cloud Computing security. This book looks to discuss and address the difficulties and challenges faced in managing security in Mobile Cloud Computing Systems. This book chapters address different aspects of Security Management in MCC and investigates different protocols and architectures that can be used to design, create, and develop security mechanism by highlighting recent advances, trends, and contributions to the building blocks for solving security issues in MCC.

OBJECTIVES

The main objective of this book to provide opportunity to scientists, researchers, students, and practitioners to share their latest research results, ideas, and developments in the area of Mobile Cloud Computing. It provides an overview of the state of the art, latest techniques, studies, and approaches as well as future directions in this field.

TARGET AUDIENCE

Policy makers, academicians, researchers, advanced-level students, technology developers, and government officials will find this text useful in furthering their research exposure to pertinent topics in Mobile Cloud Computing and assisting in furthering their own research efforts in this field.

APPROACH

This book incorporates the concepts of security management in mobile cloud computing as well as design techniques, architecture and application areas. It also addresses advanced security issues such as digital forensic, big data, access control and fault tolerance etc. The chapters are organized as follows:

Chapter 1: (SET) Smart Energy Management and Throughput Maximization – A New Routing Protocol for WSNs

This chapter present a new routing protocol based on smart energy management and throughput maximization for clustered WSNs. The main objective of this protocol is to solve the constraint of closest sensors to the base station which consume relatively more energy in sensed information traffics, and also decrease workload on CHs.

Chapter 2: A Cloud Intrusion Detection Based on Classification of Activities and Mobile Agent

This paper presents an intrusion detection system that is based on mobile agent to collect and analysis gathered data from several virtual machines, in order to benefit from the advantages of mobile agents. This chapter propose to use C4.5 algorithm which is one of tree decision algorithms that classify data into normal and malicious one.

Chapter 3: Considering Middle Circles in Mobile Cloud

This chapter provides specific guidelines to provide governance directions to align MCC into enterprise strategy and reduce risks resulted from utilizing middle circle providers; In this context, this chapter also promote and discuss some ethics that help client enterprises and MCC providers understand roles and obligations in an ever changing environment.

Chapter 4: Managing Risk in Cloud Computing

This chapter explore proper recovery planning in the event of disaster resulting from cyber-attacks. In this chapter, several means of limiting vulnerabilities and minimizing damages to information systems are discussed.

Chapter 5: On the Role of Game Theory in Modelling Incentives and Interactions in Mobile Distributed Systems

This chapter explore the game theory which provides a mathematical framework for understanding the complexity of interdependent decision makers with similar or conflicting objectives. Chapter investigate different classes of game theory, review and analyse their use in the modelling of P2P system.

Chapter 6: Security and Privacy Issues, Solutions, and Tools for MCC

This chapter proposes lightweight secure framework that provides security with minimum communication and processing overhead on mobile devices. This chapter also discusses secure mobile-cloud application services.

Chapter 7: Security and Privacy Issues and Solutions in Mobile Cloud Computing

This chapter presents a review on the mobile cloud computing concepts as well as security issues and vulnerabilities affecting Cloud Systems and the possible solutions available to such issues within the context of cloud computing. It also describes the pros and cons of the existing security strategy and also introduces the existing issues in cloud computing such as data integrity, data segregation, and security.

Chapter 8: Security Model for Mobile Cloud Database as a Service (DBaaS)

This n chapter discusses a security model for Mobile Cloud Database as a Service (DBaaS). A user can change his/her password, whenever demanded. This chapter also presents security analysis to realize the feasibility of the proposed model for DBaaS.

Table of Contents

Detailed Table of Contents