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.