

# Preface

## Introduction

Cloud computing is revolutionizing all aspects of technologies to provide scalability, flexibility and cost-effectiveness. It has become a challenge to ensure the security of cloud computing that supports cross-domain services on a federation of multilevel secure servers. To secure cloud services and resources, cloud auditing and rapid response tasks are very important to meet the Service Level Agreement (SLA) requirements that may specify the levels of availability, serviceability, performance, security, or other attributes of the service. This book mainly focuses on cloud security and high performance computing for cloud auditing. Big cloud audit data sets may consist of client and server audit logs, router logs, etc. Since cloud computing may deploy services in federated cloud environments, audit data are collected and stored in distributed environments. It is necessary to feasibly capture, store, and analyze logs in order to identify threats and prevent attacks. Capturing security relevant information and auditing the results to determine the existence of security threats in the clouds are still challenging problems.

There is a growing demand for cloud computing standards. Establishing cloud computing standards is challenging because it is very complicated to integrate existing standards and new cloud computing related standards to provide reliable cloud services in federated cloud computing environments. Standards organizations (see Table 1) and working groups are documenting the guidelines and specifications to prepare cloud computing standardizations (see Table 2). The National Institute of Standards and Technology (NIST), the Cloud Security Alliance (CSA) and the Distributed Management Task Force (DMTF) Cloud Auditing Data Federation (CADF) Working Group have released essential cloud computing related publications. The NIST cloud computing publications provide comprehensive cloud computing, cloud security and cloud auditing guidelines. The CSA has released cloud security guidelines to establish a stable and secure baseline for cloud operations. The DMTF CADF cloud auditing specifications contain useful information for cloud auditing.

**Table 1** Cloud-related standards organizations

| Standards organization                                                       |               |
|------------------------------------------------------------------------------|---------------|
| National Institute of Standards and Technology (NIST)                        | United States |
| Distributed Management Task Force (DMTF)                                     | International |
| IEEE Standards Association (IEEE-SA)                                         | International |
| International Telecommunications Union (ITU)                                 | International |
| European Telecommunications Standards Institute (ETSI)                       | European      |
| Organization for the Advancement of Structured Information Standards (OASIS) | International |
| International Organization for Standardization (ISO)/IEC                     | International |

**Table 2** Cloud security and auditing publications

|       | Publication title                                                            |
|-------|------------------------------------------------------------------------------|
| NIST  | Challenging Security Requirements for US Government Cloud Computing Adoption |
| NIST  | Cloud Computing Security Reference Architecture                              |
| NIST  | Guide to Security for Full Virtualization Technologies                       |
| CSA   | Security Guidance for Critical Areas of Cloud Computing                      |
| CSA   | Trusted Cloud Initiative (TCI) Reference Guidelines                          |
| DMTF  | The CADF Data Format and Interface Definitions Specification                 |
| CSC   | Digital Trust in the Clouds                                                  |
| OACIS | Security, Access and Identity Policy Standards                               |
| ITU   | Focus Group on Cloud Computing Technical Report (Parts 1–6)                  |

The NIST has collaborated on cloud computing to define and advance standards with United States Government (USG) agencies, federal Chief Information Officers (CIOs), private sector experts, and international bodies to identify and reach consensus on cloud computing technology and standardization priorities. The NIST released a two-volume “USG Cloud Computing Technology Roadmap” document (see NIST Special Publication 500-293) to support secure and effective cloud computing for the purpose of reducing costs and improving federated cloud computing services. These volumes put forth ten NIST strategic and tactical objectives related to cloud computing. The NIST has also established public working groups to achieve the ten requirements by leveraging the expertise of the broad cloud computing stakeholder community. The NIST Cloud Computing Security Working Group (NCC-SWG) is working on six of these requirements which facilitate secure adoption of cloud services.

The goal of the CSA Trusted Computing Initiative (TCI) is to support cloud providers in developing industry-recommended secure and interoperable identity, access and compliance management configurations, and practices. The TCI-Reference Architecture (TCI-RA) has been developed to provide a methodology and a set of tools that enable security architects, enterprise architects and risk management professionals to leverage a common set of solutions to meet the security requirements for a secure and trusted cloud. The NCC-SWG has developed the NIST Cloud Computing Security Reference Architecture

(NCC-SRA) that was derived from the NIST Cloud Computing Reference Architecture (NCC-RA). The NIST leveraged the CSA TCI-RA to identify the set of security components in the NCC-SRA. The set of security components for a particular cloud model is introduced in detail in NCC-SRA. The NCC-SRA security components are carried on the three root-domains (Business Operation Support Service (BOSS), Information Technology Operation Support (ITOS) and Security and Risk Management (S&RM)) and the four service layers. Eighteen security control families are identified in the NIST SP 800-53.

The DMTF CADF Working Group proposed the open standards to meet the cloud customer expectations that cloud providers must provide standard mechanisms for their tenant customers to self-manage and self-audit application security. A cloud providers ability to provide specific audit event, log and report information on a per-tenant and application basis is essential. Therefore, the DMTF CADF Working Group has released the CADF Data Format and Interface Specification to enable information sharing by supporting the federation of normative audit event data in the form of customized reports and logs. This documentation also defines domain specific identifiers, event classification values and tags that can be used to dynamically generate customized logs and reports for cloud subscribers or customers.

Cloud federation is still a new and emerging research area. Federated cloud computing faces challenges relating to policy, technology, guidance, security, and standards. Cloud computing related specifications, standards and implementation technologies are required to establish security, interoperability, and portability to support federated cloud computing. Comprehensive federated computing technologies are critical to ensure cost-effective and secure cloud computing, and to assure mission-critical requirements. Therefore, standards organizations have worked with numerous cloud security and auditing working groups to develop cloud computing standards. In summer 2011, the United States Air Force Research Laboratory (AFRL) CyberBAT Cloud Security and Auditing Team initiated the exploration of the cloud security challenges and future cloud auditing research directions that are covered in this book.

## Expected Audience

This book provides cloud security and auditing implementation strategies and research directions to diverse audiences:

- **Academics and students:** This book contains a comprehensive review of cloud security and auditing technologies, secure cloud architectures, programming languages, software and/or hardware based implementation and evaluation strategies for high performance cloud auditing and applications. It also provides introductory course materials for students.

- **Researchers:** This book puts forth future research directions and provides important references to a variety of research areas. Researchers can find this material useful in developing their concepts and strategies.
- **Standard developers and policy makers:** The standard developers need to use the high performance cloud auditing technology to adapt cloud security into the NCC-SRA or other cloud security reference models. Cloud access control and assured information sharing are useful to the policy makers.
- **Cloud vendors and auditors:** This book presents a comprehensive treatment of cloud security and auditing technologies. This book provides useful knowledge for building secure clouds to process and analyze massive audit data sets and to meet the SLA requirements.

## Book Overview

The objectives of this book are to present surveys, concepts, algorithms, techniques and components of high performance cloud auditing systems in order to reduce cloud security risks, and to increase availability and performance of cloud computing for surviving in a contested network environment. The book consists of 13 chapters contributed by 40 authors. The book chapters are split into three parts.

## Part I: Cloud Architectures and Security Issues

Part I contains surveys of cyber threats and security issues in cloud computing and presents secure cloud architectures. This part is designed to provide introductory materials for cloud auditing technologies.

Chapter “An Overview of Issues and Recent Developments in Cloud Computing and Storage Security” presents an overview of issues and recent developments in cloud computing and storage security. This chapter addresses security and privacy concerns due to lack of data protection transparency and accountability in the cloud. The survey topics include recent security threats, authentication, virtualization, availability, accountability, and privacy and integrity of remote storage and outsourced computation.

Chapter “Moving Target Defense for Cloud Infrastructures: Lessons from Botnets” proposes the novel moving target defense (MTD) for cloud infrastructures. Botnets are fast-moving targets that are difficult to detect with conventional security tools. Therefore, MTD has become a major theme in cyber security researches. The authors comprehensively survey the botnet literature, describe the evolution in botnet technologies, draw lessons from botnets in identifying cloud security challenges, and propose solutions to MTD for cloud infrastructures in order to make the network more resilient against novel and persistent attacks.

Chapter “Secure Mobile Cloud Computing and Security Issues” discusses secure mobile cloud computing and security issues. This chapter provides an overview of the latest mobile computing models and architectures focusing on security properties. A wide range of threats against the availability, privacy and integrity of mobile cloud computing architectures is investigated in order to develop defense mechanisms for secure mobile cloud computing and applications.

Chapter “Information Fusion in a Cloud-Enabled Environment” presents information fusion in a cloud-enabled environment. This chapter describes three aspects of current developments to low/high-level information fusion (LLIF/HLIF) and cloud computing such as agent-based service architectures, ontologies, and metrics for timeliness, confidence and security, and introduces the Cloud-Enabled Bayes Network (CEBN) for wide area motion imagery target tracking and identification.

## **Part II: Cloud Auditing and Assured Information Sharing**

Part II aims to provide in-depth cloud auditing techniques, federated cloud security architectures, cloud access control models, and access assured information sharing technologies. The cloud access control and assured information sharing technologies are in this part because cloud data contain sensitive information which needs to be shared in order to aggregate, analyze and query the data in federated cloud computing environments.

Chapter “Diagnosing Vulnerability Patterns in Cloud Audit Logs” analyzes the diagnosis of vulnerability patterns in cloud audit logs. Existing security standards, protocols and auditing mechanisms can provide audit logs but auditable events of web service compositions in service cloud architectures are not well defined. This chapter specifies the audit log and defines the Vulnerability Diagnostic Trees (VDTs) to determine security vulnerability patterns emerging from Service Orientation Architecture (SOA) communications in conjunction with service composition allocation and cross-cloud communication.

Chapter “Exploiting Timing Side Channel in Secure Cloud Scheduling” exploits a timing side channel in secure cloud scheduling. In multi-tenancy cloud environments, a malicious user can learn about the service usage pattern of an innocent user by a timing based side channel attack. This chapter demonstrates the information leakage of a timing side channel in shared schedulers, discusses timing side channel threats and countermeasures, and introduces the design of secure scheduling policies.

Chapter “Federated Cloud Security Architecture for Secure and Agile Clouds” introduces the federated cloud security architecture for secure and agile clouds. This chapter describes cloud security threats and proposes a novel federated security architecture that consists of a set of seamlessly integrated systematic security mechanisms at the application layer, the network layer and the system layer in federated cloud computing environments.

Chapter “Trust-Based Access Control for Secure Cloud Computing” presents trust-based access control for secure cloud computing. Multi-tenancy, elasticity and dynamicity pose several novel challenges for access control in a cloud environment. This chapter summarizes traditional and modern access control models, explores challenges of cloud access control, identifies various authorization and enforcement requirements and desirable properties of access control models, and introduces graph-theoretic semantics of an access control model.

Chapter “Assured Information Sharing (AIS) Using Private Clouds” introduces the concept of assured information sharing in private clouds. The authors provide basic characteristics of an AIS framework, discuss the state of the art in the realm of AIS, and provide contemporary cloud-based AIS implementation methodologies for Cloud-centric Assured Information Sharing System (CAISS) and CAISS XACML policies (CAISS-X). The CAISS uses a cloud-based framework for both data storage and retrieval as well as policy enforcement and CAISS-X employs a cloud-centric framework to store and query large amounts of data via a non-cloud policy engine that enforces XACML-based policies.

## **Part III: High Performance Cloud Computing**

Part III outlines a wide range of challenges and provides solutions to manage and control very large and complex data sets. It is impractical to process a huge audit data set using existing on-hand database management tools or data processing applications in real-time. CPU-GPU computing, MapReduce and router-based filtering technologies are employed to face the challenges of big data processing.

Chapter “GPGPU Computing for Cloud Auditing” presents GPGPU computing for cloud auditing. There is a growing need for computing platforms that are able to rapidly analyze data-intensive cloud audit data. GPGPU computing can perform data analysis with a high level of parallelism employing tools like Hadoop MapReduce. The chapter contains a broad background on GPGPU computing, architectures, and programming options, illustrated by helpful programming examples.

Chapter “CPU-GPU System Designs for High Performance Cloud Computing” discusses CPU-GPU system designs for high performance cloud computing. This chapter focuses on the improvement of cloud computing performance by combining the powerful scalar processing on CPU with the efficient parallel processing on GPU. The authors also introduce the mainstream and emerging memory hierarchy designs in CPU-GPU systems and optimization techniques of the data allocation and migration between CPU and GPU for performance improvement.

Chapter “MapReduce Performance in Federated Cloud Computing Environments” introduces MapReduce optimization in federated cloud computing environments. The demand for federation among multiple distributed clusters is growing, in order to process data-intensive and compute-intensive applications. The MapReduce framework coupled with cloud computing is emerging as a viable

solution for distributed big data processing. The authors describe various cloud based applications over distributed clouds and provide a network aware MapReduce optimization technique.

Chapter “Improving Cloud Performance with Router-Based Filtering” presents improving cloud performance with router-based filtering. The router-based filtering technology has been developed to enhance the availability of cloud computing and performance of cloud auditing. An overview of the specification and generation of filtering rules used by routers, and a theoretical model to find the best locations for hardware routers in a network to block malicious traffic, and experimental results are provided in this chapter.

Rome, NY, USA  
Kansas City, MO, USA  
College Station, TX, USA

Keesook J. Han  
Baek-Young Choi  
Sejun Song

High Performance Cloud Auditing and Applications

Han, K.J.; Choi, B.-Y.; Song, S. (Eds.)

2014, XXIV, 360 p. 89 illus., 62 illus. in color., Hardcover

ISBN: 978-1-4614-3295-1