Analyzing and Mitigating Security Risks in Cloud Computing

Part of the Advances in Information Security, Privacy, and Ethics Book Series

Pawan Kumar Goel (Raj Kumar Goel Institute of Technology, India), Hari Mohan Pandey (Bournemouth University, UK), Amit Singhal (Raj Kumar Goel Institute of Technology India) and Sanyam Agarwhal (Ace Group of Colleges, India)

Description:

In the dynamic field of modern business, where cloud computing has become the primary focus of operations, a pressing issue arises – the persistent concerns of security, privacy, and trust in cloud environments. Organizations find themselves at a crossroads, caught between the immense benefits of cloud adoption and the escalating challenges of safeguarding sensitive data and maintaining user trust. The need for a comprehensive and practical guide to navigate these intricate landscapes has never been more critical.

Despite the transformative potential of cloud computing, security breaches, privacy infringements, and a lack of trust continue to plague organizations. The evolving threat landscape, coupled with the complexity of regulatory frameworks, creates a difficult environment for IT professionals, security practitioners, researchers, and decision-makers. Without a strategic and informed approach, the adoption of cloud technologies risks becoming a double-edged sword, potentially exposing organizations to unprecedented risks, and preventing them from being compromised.

Analyzing and Mitigating Security Risks in Cloud Computing is a groundbreaking guidebook tailored to address the very challenges that organizations face in securing their cloud infrastructures. With a focus on real-world examples, case studies, and industry best practices, the book equips its readers with actionable insights and tools to fortify their cloud security posture. From understanding the fundamentals of cloud computing to addressing emerging trends and implementing robust security strategies, the book serves as a holistic solution to bridge the knowledge gap and empower professionals at every level.

The book is intended for IT professionals, security practitioners, researchers, decision-makers, and cloud service providers, aimed at democratizing knowledge and empowering a diverse audience. By providing comprehensive coverage of topics ranging from data encryption and privacy frameworks to incident response and emerging trends, the book contributes to a paradigm shift in how organizations approach cloud security. With **Analyzing and Mitigating Security Risks in Cloud Computing** in hand, professionals are not merely readers – they become architects of a more secure, private, and trustworthy cloud computing landscape.
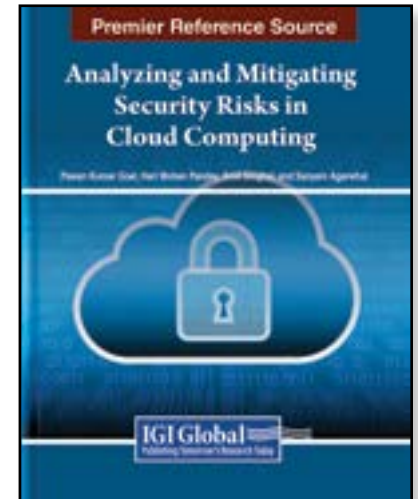
ISBN: 9798369332498   **Pages:** 320   **Copyright:** 2024   **Release Date:** January, 2024

Hardcover: **$290.00**   **E-Book:** **$350.00**   **Hardcover + E-Book:** **$350.00**

Topics Covered:

- Authentication and Authorization Mechanisms
- Benefits and Challenges of Cloud Adoption
- Building a Secure Cloud Strategy
- Case Studies and Practical Examples
- Cloud Governance Frameworks
- Cloud-Native Security Solutions
- Compliance and Governance in the Cloud
- Data Encryption and Access Controls
- Detecting and Responding to Security Incidents
- Digital Forensics in Cloud Environments
- Emerging Trends in Cloud Computing
- Ensuring Data Security in the Cloud
- Evaluating Cloud Service Providers
- Fundamentals of Cloud Computing
- Identity and Access Management in the Cloud

Subject: Security and Forensics

Classification: Edited Reference

Readership Level: Advanced-Academic Level (Research Recommended)

Research Suitable for: Advanced Undergraduate Students; Graduate Students; Researchers; Academicians; Professionals; Practitioners