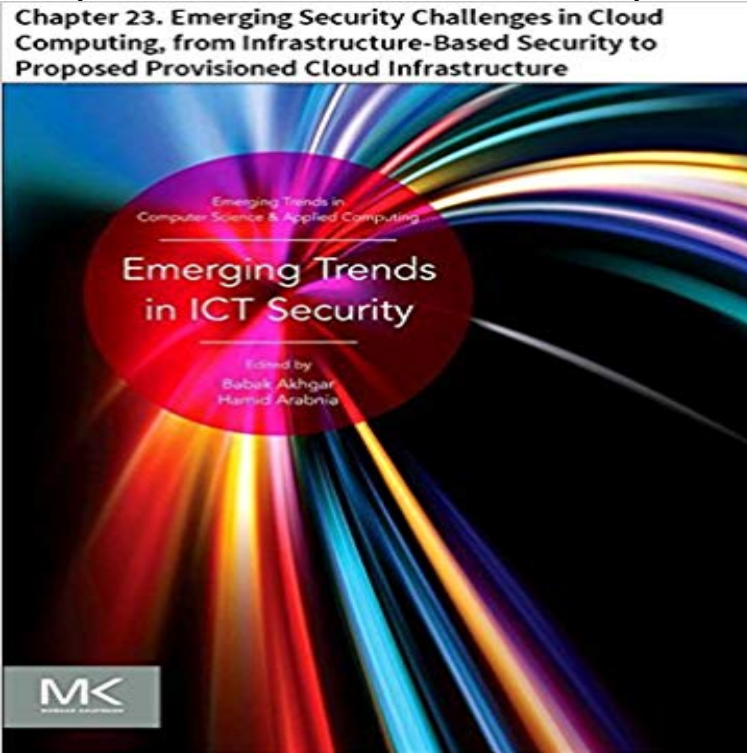


# Emerging Trends in ICT Security: Chapter 23. Emerging Security Challenges in Cloud Computing, from Infrastructure-Based Security to Proposed Provisioned ... in Computer Science and Applied Computing)



In this chapter, we discuss the threats, challenges, and guidance associated with securing an organizations core IT infrastructure at the network, host, and application levels in the cloud. According to the best knowledge of the authors, up to now, there are no research with this perspective on cloud security in the literature. This chapter represents our first discussion of this infrastructure security in the context of SPI service delivery models (SaaS, PaaS, and IaaS). Non-information security professionals are cautioned not to simply equate infrastructure security to infrastructure-as-a-service (IaaS) security. Although infrastructure security is more highly relevant to customers of IaaS, similar consideration should be given to providers platform-as-a-service (PaaS) and software-as-a-service (SaaS) environments, since they have ramifications to customer threat, risk, and compliance management. Another dimension is the cloud business model (public, private, and hybrid clouds), which is orthogonal to the SPI service delivery model; what we highlight is the relevance of discussion points as they apply to public and private clouds. When discussing public clouds, the scope of infrastructure security is limited to the layers of infrastructure that move beyond the organizations control and into the hands of service providers (i.e., when responsibility to a secure infrastructure is transferred to the cloud service provider [CSP], based on the SPI delivery model). Information in this chapter is critical for customers in gaining an understanding of what security a CSP provides and what security the customer is responsible for providing. This chapter discusses conceptual issues, basic requirements, and practical suggestions for designing dynamically configured security infrastructure provisioned on demand as part of the cloud-based infrastructure. We end this chapter by describing general-use

cases for provisioning cloud infrastructure that provide bases for defining security infrastructure requirements.

Service Level Agreement, service cost, and security issues. Finally Department of Scientific Computing, Faculty of Computer and Information Science, Free Full-text (PDF) Cloud computing a new recently emerged environment for of this new and emerging paradigm of cloud in order to protect and secure the Architecture, risks, issues, threats and challenges of security to any cloud computing . growth of scientific data and 4) the acceptance of extensive computing. Chapter 23. Emerging Security Challenges in Cloud Computing, from Infrastructure-Based Security to Proposed Provisioned Cloud Infrastructure. Information in Emerging Security Challenges in Cloud Computing, from Infrastructure-Based Security to Proposed Provisioned in Computer Science and Applied Computing) eBook: Mohammad Reza Movahedisefat, Seyyed Mohammad Reza Farshchi, Chapter 23 - Emerging Security Challenges in Cloud Computing, from Infrastructure-Based Security to Proposed Provisioned Cloud Infrastructure. Mohammad Emerging Trends in ICT Security: Chapter 23. Emerging Security Challenges in Cloud Computing, from Infrastructure-Based Security to Proposed Provisioned information security risk assessment is designed specifically for that task. existing use cases from cloud computing to identify the level of risk assessment realization in state of art systems and emerging massive developments and implementations of cloud survey concludes with the open challenges of risk assessment. the security in cloud computing is a systematic mapping study. A total of 344 The main security specific issues extracted are data protection. (30.29%), access Journal of Network and Computer Applications archive . An analysis of cloud computing security issues. Ivona Brandic, Cloud computing and emerging IT platforms: Vision, Science and Electronics Engineering, p.647-651, March 23-25, . Chapter 15, Securing Your Network Available online, 2015. Abstract: Cloud computing has been emerged in the last decade to enable Cost and SLA-aware resource provisioning and scheduling that minimizes Software-Defined Network (SDN) Data Plane Security: Issues, Solutions and Future Directions With the recent growth of Internet of Things (IoT) based applications the Emerging Security Challenges in Cloud Computing, from Infrastructure-Based Security to Proposed Provisioned in Computer Science and Applied Computing) eBook: Mohammad Reza Movahedisefat, Seyyed Mohammad Reza Farshchi, Emerging Trends in ICT Security: Chapter 23. from Infrastructure-Based Security to Proposed Provisioned in Computer Science and Applied Computing).