Chapter 4
The Convergence of Cybersecurity and Cloud Computing

Adline Freeda
https://orcid.org/0009-0002-3335-0907
KCG College of Technology, India

R. Kanthavel
https://orcid.org/0000-0001-5537-2571
PNG University of Technology, Papua New Guinea

R. Dhaya
https://orcid.org/0000-0002-3599-7272
PNG University of Technology, Papua New Guinea

ABSTRACT

The quick development of cloud computing, which offers scalability, flexibility, and cost-efficiency, has completely changed how businesses store, manage, and access data. But this change has also brought up serious cybersecurity issues, calling for the establishment of a strong framework to safeguard private data and guarantee the integrity of cloud environments. We start by giving a thorough introduction to cloud computing, including its salient features, deployment patterns. Subsequently, we explore the foundations of cybersecurity, highlighting the essential concepts of confidentiality, integrity, and availability In addition to addressing the shared responsibility model, legal and compliance concerns, and the crucial function of identity and access management (IAM) in the cloud, the chapter emphasizes the convergence of cloud computing and cyber security. We demonstrate real-world implementations of cloud security solutions through a series of case studies, high-

DOI: 10.4018/979-8-3693-6859-6.ch004

lighting industry best practices and insights gained from protecting public and hybrid cloud deployments.

INTRODUCTION

Cloud computing has emerged as a revolutionising impact in the digital era as it drastically changed business operations and delivery across the spectrum. Organisations are able to gain access to a variety of computing resources over the internet through cloud computing, which makes flexibility, productivity, and creativity significantly easier. As more and more organisations turn to cloud services, this translates into the creation of a wide array of cyber security issues to protect sensitive data and guarantee integrity in cloud settings (Caviggioli., 2016).

With cyber threats increasingly sophisticated and frequent, cyber security—the practice of protecting systems, networks, and information from digital attacks—has emerged as a matter of prime importance. It has been indispensable due to the growing dependency on cloud computing. (Dhaya et al., 2022). Because of this confluence, a deep understanding of the two domains is needed, but so is the development of robust defences against possible threats to infrastructures in the cloud. This chapter discusses the confluence of cloud computing and cyber security, looking into the ways in which those two fields interact and influence each other. It is important to understand these basic concepts to be able to identify the specific security risks associated with working on cloud systems.

We then explore the basics of cyber security, focusing on the three key ideas that form its foundation: availability, confidentiality, and integrity (Dhaya & Kanthavel.,2020). We discuss common threats and vulnerabilities that organisations face in cyberspace, stressing how imperative it is to establish robust cyber security defences.

We discuss such important subjects as the shared responsibility model, legal and compliance concerns, and the role of identity and access management (IAM) in the cloud as we explore the relationship between cloud computing and security. We also explore important security technologies and approaches put into play, with an emphasis on their role in securing cloud infrastructures. We offer several case studies showing how cloud security controls are really used in the field for helpful insights (Dhaya & Kanthavel.,2021a). Those case studies offer insightful advice for organisations charting their way through the complexity of cloud security by showing industry best practices and lessons learnt from secure public and hybrid cloud deployments.