Chapter 9
Security-as-a-Service: Enhancing Cloud Security Through Managed Security Solutions

Zainab Senan Attar Bashi
https://orcid.org/0000-0002-1452-8098
International Islamic University Malaysia, Malaysia

Azana Hafizah Mohd Aman
https://orcid.org/0000-0001-7337-6736
Universiti Kebangsaan Malaysia, Malaysia

Salem Sati
https://orcid.org/0000-0002-6062-497X
Misurata University, Libya

Nur-Adib Maspo
https://orcid.org/0000-0003-0031-1354
International Islamic University Malaysia, Malaysia

Aisha Hassan Abdalla Hashim
https://orcid.org/0000-0001-6331-1373
International Islamic University Malaysia, Malaysia

ABSTRACT

Cloud computing plays an important role in modern businesses by enabling flexible, efficient storage, analysis, and access to data and applications. However, this reliance also introduces new security challenges. Ensuring cloud security and resilience is now critical to prevent unauthorized access, data breaches, and service disruptions. This chapter examines the key principles, technologies, and policies that uphold the confidentiality, integrity, and availability of cloud systems.

DOI: 10.4018/979-8-3373-4455-3.ch009

It also highlights Security-as-a-Service (SECaaS) as a necessary part of the cloud ecosystem, offering specialized, scalable solutions to improve overall security. By delivering managed security services via the cloud, SECaaS allows organizations to outsource key functions such as threat intelligence, endpoint protection, access control, and compliance monitoring. It can enhance protection without heavy in-house investment

1. INTRODUCTION

In the era of digital transformation, cloud computing has become the backbone of modern business operations, offering unparalleled scalability, operational flexibility, and innovative capabilities (Kaluvuri et al., 2015). The migration to cloud environments allows enterprises to operate at a global scale, collaborate seamlessly, and use data-driven insights to remain competitive. However, this transition introduces a spectrum of security challenges that cannot be ignored, such as data breaches, unauthorized access, and compliance risks (Mostafa et al., 2023). These challenges arise due to the dynamic and interconnected nature of cloud networks, which demand robust and adaptive security mechanisms. Security-as-a-Service (SECaaS) has emerged as a vital solution, addressing these challenges by providing managed security services tailored to the unique demands of cloud-based infrastructures (Shen et al., 2013).

SECaaS revolutionizes the way organizations handle security by shifting the burden from internal IT teams to specialized service providers. This approach allows businesses to concentrate on their core operations while using advanced security tools and expertise from external providers. SECaaS embodies the principles of resilience, scalability, and real-time responsiveness, delivering comprehensive protection against an evolving threat landscape.

One of the core strengths of SECaaS lies in its ability to implement proactive security measures that safeguard cloud infrastructures (Talib et al., 2012). These measures include vulnerability scanning, penetration testing, and continuous monitoring (Casola et al., 2018), which are necessary for identifying and mitigating potential security weaknesses. Wang & Shen (2013) highlight the effectiveness of services like CloudProxy, which operate within network architectures to detect vulnerabilities in real time. Such tools act as intermediaries between clients and cloud services, scanning traffic flows and application layers for anomalies that may signal potential breaches.