Book: Security in the Private Cloud

Edited by John R. Vacca

Publisher: CRC Press

Chapter 5: Software and Data Segregation Security

5.1 Introduction

Cloud Computing has been perceived as striking technology and management system since the turn of twenty-first century. It changes the business operation landscape, which is dominated in physical building. Cloud Computing offers a scalable and global ecosystem of computing resources, storage arrays, and instant provision (Figure 5.1). It is worthwhile to revisit the definition and architecture in cloud computing. Architecture and weakness of the cloud computing environment is walked through and leading to the issue of security, access control, audit measurement, authentication, and authority. Aggregately, the segregation of duties applies in software and data conventionally. The innate characteristic of multitenancy in the cloud system relies extensively on the subscriber identity as the master framework of data segregation. This applies to cloud computing resources, cloud storage, access control, change control, software development, backup and restore, global data replication, and business continuity.

5.2 Origins of Cloud Computing

Cloud computing carries a main goal of maximizing the value of distributed resources (figure 5.2) through combining disparate components to achieve a higher transaction rate. This enable a high capability oto solve bigger scale of computational issues. Under the hood of cloud computing spanning private, public, and hybrid deployment, key ingredients are quality of services, virtualization, interoperability, and scalability. John McCarthy was the first one to quote the concept of cloud computing in 1960s (Foster et al., 2008) According to this seminal opinion, computation was organized as a public utility similar to water, gas, and electricity. The associated characteristics were depicted in the book of Douglas Parkhill, *The Challenge of the Computer Utility*, in 1966 (Zhang et al., 2010).

Historically, the paradigm of cloud emerges from the telecommunications industry. This is where operators commonly offer virtual private network (CPN) services, which bear similar services quality in term of engineering (see Figure 5.3), but charge a very low cost of execution. This averts the former situation in telecommunication in which dedicated point-to-point telecommunication circuits show a high degree of resources redundancy. Cloud computing provokes a more balanced utilization of network and computing resources plainly through a computer browser. This is independent of the devices used and available at any location where users stay. Cloud infrastructure is supported through the latest state of art of internet infrastructure offering high resiliency in throughput and reliability such that more intensive computing jobs can be handled.

Sophisticated technology skills are demanded in cloud computing installation. High-level reliable services (Figure 5.4) in cloud computing are obtained through sharing over multiple work sites (Popa et al., 2012). This is good for better action in business continuity and a good provision for disaster recovery in case of infrastructure outage. Metropolitan sharing of computing resources and infrastructure drives a higher efficient utilization of the infrastructure. This facilitates a simpler maintenance for cloud-based applications since the actual installation happens in shared cloud data center. Nothing is installed in the front-end system. This increases the business agility in cloud computing.

“Pay as you go” is a core characteristic of cloud computing (Sotola, 2011). This is a two-sided sword (Figure 5.5). Cloud computing subscribers can minimize huge amount of prepayment and capital expenses as ain a conventional internal technology platform, and this can measure the usage of cloud computing through a granular control of metering. This, performance is carefully monitored because the meter payment is scalable in cloud computing investment.

The centralization nature (Mather et al., 2009) in cloud computing renders a high position of information security in enterprise subscribers. Providers can devote more time and effort to mitigate technology security issues, which is not possible in an individual enterprise user.