Cloud Computing Security

S. Srinivasan
Professor of Information Systems
JHJ School of Business
srinis@tsu.edu

Abstract

Cloud Computing has emerged as an important technology implementation alternative to many businesses, both large and small. It is essential for the workforce of today and in the future to know how they should interact with this new option and to see how security aspects could be suitably adjusted when using the cloud. In this presentation we will talk about the most commonly accepted definitions of this new technological alternative and how it is a major paradigm shift in computing. First we will introduce the three main types of cloud service - SaaS, PaaS, IaaS and the four major deployment models - public cloud, private cloud, hybrid cloud and community cloud. Use of cloud service offers numerous benefits but also brings with it several disadvantages. We will look at these and how new alliances are evolving to make the cloud service more useful. One of the main challenges for a business planning to adopt cloud service is to know how they should evaluate various providers in the market place. In this connection we will point out the role of Cloud Security Alliance, a global enterprise that is developing new best practices and tools to evaluate various providers on the same features. One of the important challenges in the cloud concerns security of data stored in the cloud. We will address the security challenges that businesses face when using the cloud and how to over come them. When businesses choose to adopt a cloud service provider for their computing needs they should have the ability to provide necessary documentation to their own accrediting agencies on their compliance with both security and privacy. Such requirements are commonplace in industries such as heath care and finance. We will discuss these aspects in this presentation. We will conclude the discussion with the role of emerging cloud service brokers.