Chapter 7.7
Security Issues in Cloud Computing:
A Survey of Risks, Threats and Vulnerabilities

Kamal Dahbur
New York Institute of Technology, Jordan

Bassil Mohammad
New York Institute of Technology, Jordan

Ahmad Bisher Tarakji
New York Institute of Technology, Jordan

ABSTRACT

Cloud Computing (CC) is revolutionizing the methodology by which IT services are being utilized. It is being introduced and marketed with many attractive promises that are enticing to many companies and managers, such as reduced capital costs and relief from managing complex information technology infrastructure. However, along with desirable benefits come risks and security concerns that must be considered and addressed correctly. Thus, security issues must be considered as a major issue when considering Cloud Computing. This paper discusses Cloud Computing and its related concepts; highlights and categorizes many of the security issues introduced by the "cloud"; surveys the risks, threats, and vulnerabilities; and makes the necessary recommendations that can help promote the benefits and mitigate the risks associated with Cloud Computing.

INTRODUCTION

Cloud computing is arguably one of the most significant technological shifts of our time. The mere idea of being able to use computing in a similar manner to using a utility, such as electricity, is revolutionizing the IT services world and holds great potential. Customers, whether large enterprises or small businesses, are drawn toward the cloud's promises of agility, reduced capital costs, and enhanced IT resources. IT companies are

DOI: 10.4018/978-1-4666-0879-5.ch7.7

shifting from providing their own IT infrastructure to utilizing the computation services provided by the cloud for their information technology needs (Carr, 2008).

Cloud computing introduces a level of abstraction between the physical infrastructure and the owner of the information being stored and processed. Such indirect control of the physical environment introduces vulnerabilities unknown in previous settings. Such a radical change is of course not risk free. As IT services are contracted outside of the enterprise, the dependency on third party providers compels companies to rethink their risk management techniques and adapt accordingly.

After this brief introduction, the remainder of this paper is organized as follows: First, we provide an overview of cloud computing, its services, and core technologies; we provide a survey of known general risks, vulnerabilities and threats, and then explore the additional risks introduced by (or relevant to) cloud computing; some real world examples of vulnerabilities of cloud computing that have been reported in the literature are discussed; and we provide our conclusion and recommendations.

OVERVIEW OF CLOUD COMPUTING

As with any new technology, the definition of cloud computing is changing with the evolution of technology and its services. No standard definition for cloud computing has yet been agreed upon, especially since it encompasses so many different models and potential markets, depending on venders and services. In the simplest of terms, cloud computing is basically internet- based computing. The term "cloud" is used as a metaphor for the Internet, and came from the well known cloud drawing that was used in network diagrams to depict the Internet's underlying networking infrastructure. The computation in the internet is done by groups of shared servers that provide on demand hardware resources, data and software to devices connected to the net.

The National Institute of Standards and Technology NIST, gives a more formal definition: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (NIST, 2010) also notes that this definition will probably change over time.

In this sense, users of cloud computing are raised to a level of abstraction where they are hidden and relived from the details of the hardware or software infrastructures that supports their computations. This greatly simplifies the costs involved in establishing and managing the IT that is needed to meet the requirements of any business. And since businesses will pay only for the required IT resources when and as they are needed, more and much more powerful resources can be provided at a fraction of the price of the real value for such resources.

Core Technologies

To better understand the security issues that are associated with CC, it is important to discuss the core concepts and technologies in cloud computing. CC is based on the general principle of utility computing – providing metered services of computing resources in a similar manner to the other utilities such as electricity. The measured service-oriented perspective for computing resources can be easily understood for the hardware resources. But this perspective can also be extended to software systems because they are designed and built in the form of autonomous interoperable services (Wei & Blake, 2010).

The large variety of devices that can connect to the internet, such as PDAs, mobile phones and handheld and static devices, all expanded the number of ways the cloud can be accessed.