Cloud Computing Security: Opportunities and Pitfalls

Junaid Arshad, University of Leeds and University of West London, UK
Paul Townend, University of Leeds, UK
Jie Xu, University of Leeds, UK
Wei Jie, University of West London, UK

ABSTRACT

The evolution of modern computing systems has led to the emergence of Cloud computing. Cloud computing facilitates on-demand establishment of dynamic, large scale, flexible, and highly scalable computing infrastructures. However, as with any other emerging technology, security underpins widespread adoption of Cloud computing. This paper presents the state-of-the-art about Cloud computing along with its different deployment models. The authors also describe various security challenges that can affect an organization’s decision to adopt Cloud computing. Finally, the authors list recommendations to mitigate with these challenges. Such review of state-of-the-art about Cloud computing security can serve as a useful barometer for an organization to make an informed decision about Cloud computing adoption.

Keywords: Cloud Computing, Cloud Security, Computing Infrastructures, Opportunities, Pitfalls

INTRODUCTION

The evolution of internet technologies has directed the emergence of Cloud computing. It facilitates organizations to dynamically expand their infrastructures by outsourcing business components to third-party service providers whilst retaining the customization required by the enterprise and transparency to the end user. By providing the ability to expand at runtime, it facilitates development of highly scalable applications without having to worry about the physical limit to the available resources. It therefore, provides the illusion of availability of unlimited resources to fulfill dynamic and variable user requirements. The illusion of unlimited resource availability improves the ability of an organization to meet the requirement of a wider user-base. Furthermore, by dramatically reducing the time to establish infrastructures, it has substantial effects on the time to market for a product, thereby improving product promotion and delivery. Finally, Cloud computing introduces a pay-per-use model i.e., customers only have to pay for the resources they have used. This represents an attractive model as the organizations do not have to pay for establishment and maintenance of the resources thereby reducing the cost of providing services.

DOI: 10.4018/jghpc.2012010104
As with any other emerging paradigm, security underpins widespread adoption of Cloud computing. This has been highlighted by the surveys conducted by IDC Exchange where security features as the most challenging aspect towards the adoption of Cloud computing (Gens, 2008, 2009). Furthermore, the importance of security is increased as the users of the Cloud services have to pay for the resources they use. This represents a significant difference as compared to traditional high performance computing paradigms such as Grids where participating organizations are envisaged to voluntarily share resources without requiring any financial obligations from the users. As Cloud computing involves outsourcing of services, the authentication and security issues are pushed to the edge of an organization’s security perimeter. In other words, Cloud computing accelerates the externalization of security services such as identity management, authentication, security of application infrastructure and services (Dournaee, 2010). Furthermore, in order to achieve the flexibility and scalability of infrastructures described earlier, Cloud computing uses several novel methods and technologies which present novel security issues. These include technologies such as virtual machines (Goldberg, 1974) and web 2.0 along with contemporary technologies such as web services (Alonso et al., 2004) and, the Service Oriented Architectures (SOA) (Channabasavaiah et al., 2004).

In this paper, we emphasize on identifying the security challenges presented by Cloud computing and review existing approaches to address these challenges. We also, describe the limitations of existing approaches to address security issues surrounding Cloud computing. Furthermore, the paper is focused on security challenges due to both technological and non-technological aspects of Cloud computing from a consumer’s perspective. A brief outline of the paper follows. The evolution of modern computing systems to Cloud computing is described in the next section. We define Cloud computing and explain the three different models of Cloud computing i.e., Software as a Service, Infrastructure as a Service and Platform as a Service. We describe a number of security threats which are applicable to Cloud computing and need to be addressed and narrates our recommendations to address these challenges. We conclude this paper where we describe our conclusions.

MODERN SYSTEM ARCHITECTURE

An architecture can be defined as a formal description of a system, organized in a manner that supports reasoning about the structural properties of the system (Kazman et al., 1998). It defines the components of a system and facilitates robust system development by providing an overview of the intended system. Traditional system architectures for computer systems were constrained by physical boundaries and mostly included local components such as processor, memory and disk drives etc. (Maggs et al., 1995). This is mainly due to the fact that computer systems were usually established at a single geographical location. A featured example of such type of architectures can be the traditional parallel systems (Papadimitriou, 1994). With the advent of distributed systems and internet technologies, the physical boundaries have disappeared, leading to systems which can span across multiple geographical locations potentially involving multiple organizations (Andrews, 2000). A featured example of such computer systems are tiered computing systems (Alonso et al., 2004). Due to these advancements, a system architect now has the challenge to take into account both local and global resources including network structure thereby governing new strand of architectures.

A typical modern computing system is a modular system where each component represents a function that contributes to the overall objective of the system. Due to the advantages of SOAs, for instance; loose coupling (Gamma et al., 2007) and dynamic binding (Canfora & Penta, 2006), these components are usually realized as services (OASIS, 2005). Web services provide a popular implementation of the SOAs. Furthermore, services can be located at
On Construction of a Diskless Cluster Computing Environment in a Computer Classroom
[www.igi-global.com/article/construction-diskless-cluster-computing-environment/74169?camid=4v1a](www.igi-global.com/article/construction-diskless-cluster-computing-environment/74169?camid=4v1a)

Security Aspects in Utility Computing
[www.igi-global.com/chapter/security-aspects-in-utility-computing/139847?camid=4v1a](www.igi-global.com/chapter/security-aspects-in-utility-computing/139847?camid=4v1a)