Future Generation Computer Systems 28 (2012) 833–851

Contents lists available at SciVerse ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing

Md. Tanzim Khorshed, A.B.M. Shawkat Ali *, Saleh A. Wasimi

School of Information and Communication Technology, CQUniversity QLD 4702, Australia

ARTICLE INFO

Article history:
Received 15 August 2011
Received in revised form
11 January 2012
Accepted 18 January 2012
Available online 27 January 2012

Keywords:
Security
Threats
Machine learning
Trust
Cloud computing

ABSTRACT

The long-term potential benefits through reduction of cost of services and improvement of business outcomes make Cloud Computing an attractive proposition these days. To make it more marketable in the wider IT user community one needs to address a variety of information security risks. In this paper, we present an extensive review on cloud computing with the main focus on gaps and security concerns. We identify the top security threats and their existing solutions. We also investigate the challenges/obstacles in implementing threat remediation. To address these issues, we propose a proactive threat detection model by adopting three main goals: (i) detect an attack when it happens, (ii) alert related parties (system admin, data owner) about the attack type and take combating action, and (iii) generate information on the type of attack by analyzing the pattern (even if the cloud provider attempts subreption). To emphasize the importance of monitoring cyber attacks we provide a brief overview of existing literature on cloud computing security. Then we generate some real cyber attacks that can be detected from performance data in a hypervisor and its guest operating systems. We employ modern machine learning techniques as the core of our model and accumulate a large database by considering the top threats. A variety of model performance measurement tools are applied to verify the model attack prediction capability. We observed that the Support Vector Machine technique from statistical machine learning theory is able to identify the top attacks with an accuracy of 97.13%. We have detected the activities using performance data (CPU, disk, network and memory performance) from the hypervisor and its guest operating systems, which can be generated by any cloud customer using built-in or third party software. Thus, one does not have to depend on cloud providers' security logs and data. We believe our line of thoughts comprising a series of experiments will give researchers, cloud providers and their customers a useful guide to proactively protect themselves from known or even unknown security issues that follow the same patterns.

1. Introduction

Cloud computing can be viewed as the transformation into reality of a long held dream called "Computing as Utility", it emerged into the market with a huge potential to fulfill this dream. It promises on-demand services for a customer's software, platform and infrastructure needs. In its fold, companies do not even need to plan for their IT growth in advance with this new "pay as you go" system. Already, there has been upbeat assessment about its great potential for utility, scalability and instant access features; but on the flip side, some are also apprehensive of security gaps involving for instance, trust, threats and risks.

While cloud computing has received mixed reviews from its customers, some experts describe it as the reinvention of distributed main frame model [1]. It could be the most significant shift in IT infrastructure area in recent times as it appears promising but still a great deal of work is warranted in the domain of security to minimize the gaps. At the time of writing this paper, we discovered a propensity in many small or midsized organizations to adopt cloud computing mainly to reduce upfront investment costs, minimize maintenance work in IT infrastructure and to enhance on-demand capabilities. However, there is a risk of depredation for not doing an assessment on security and privacy. Before we explore the security and privacy issues in cloud computing, it is worthwhile to revisit the definition of cloud computing.

In our quest for the definition of cloud computing, we perused books and articles [2–7] and came up with our own definition that is easy to comprehend and yet broad in its scope, which can be visualized in graphical form as described in Fig. 1. Put in words:

Cloud computing is a system, where the resources of a data center is shared using virtualization technology, which also provide elastic, on demand and instant services to its customers and charges customer usage as utility bill.

* Corresponding author. Fax: +61 7 4930 9729.
E-mail addresses: t.khorshed@cqu.edu.au (Md.T. Khorshed), s.ali@cqu.edu.au (A.B.M.S. Ali), s.wasimi@cqu.edu.au (S.A. Wasimi).

0167-739X/$ – see front matter
doi:10.1016/j.future.2012.01.006

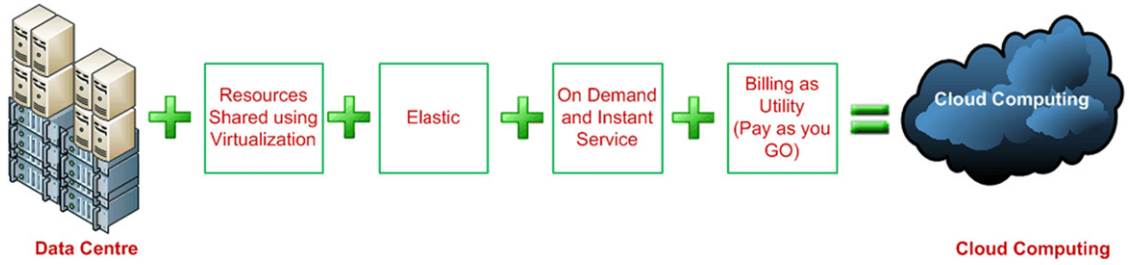

Fig. 1. Schematic definition of cloud computing.

Virtualization, elasticity, on-demand, instant service and pay as you go are the main characteristics that convert a data center into cloud computing. In a typical depiction, the word 'data center' may be restrictive because it could be any IT resource that can be shared using virtualization technology. But if we walk through any of today's cloud provider's office we will witness a large data center full of computer systems in the racks which are used to share resources. So, we may as well include the word "data center" to make our definition more relevant to the real world. We have noticed that some existing data center providers are already rebranding themselves as cloud providers taking advantage of their existing infrastructure as they do not wish to miss out on the "next big thing" in IT industry.

In some definitions, we found that experts have added the phrase "using internet technology" [8,9] as a must for cloud computing. But our interpretation does not make that feature imperative because on-premise single organization's private cloud would not need internet to access cloud services. Thus, we exclude internet from our definition. Furthermore, in cloud computing, virtualization is used to create multi-tenant architecture, but we did not use the word 'multi-tenant' in our definition to keep it simple as the encompassing word 'virtualization' is already there.

As with any change in IT infrastructure where there are accompanying novel risks and opportunities, cloud computing is no exception. Shared, on-demand nature of cloud computing expose it to some unique risks that have not been experienced before. In this paper, a survey of cloud computing with the main focus on gaps and their proposed solutions are presented. The presentation of the paper is in two discourses. The first discourse is on the survey for an easy but comprehensive definition of cloud computing and understanding its main aspects and gaps. The second discourse is on thoughts for some novel approaches to identify cyber attack types using modern machine learning techniques including rule-based learning and statistical learning theory. We believe our thoughts encapsulated through a series of experiments will give researchers, cloud providers and their customers the initiative to proactively protect themselves from known or even unknown security risks.

2. Review of cloud computing standards

Cloud computing standards are currently the topic of research of several groups and organizations. 'Cloud Standard Coordination' was formed in July 2009, their main "goal is to create a landscape of cloud standards work, including common terminology" [10]. In that vein they created a Wiki page where different cloud oriented Standard Developing Organizations (SDOs) can update their part of research [11]. We have visited each of these SDOs websites and attempt here to capture the essence of their areas of research. The intent is to give aspiring researchers a lead as to where to start in the sky of clouds.

Cloud Security Alliance (CSA) is a non-profit organization promoting the use of best practices, common level of understanding, awareness and guidelines for cloud related security threats [12–14]. The goal of CloudAudit working group, which has been working under the guidance of CSA from October 2010, is to provide a common interface and namespace for cloud providers to automate the audit, assertion, assessment, and assurance of their service environments so that their authorized clients can access the services using a similar secured interface [15].

Distributed Management Taskforce's (DMTF's) cloud efforts are focused on standardizing management protocols for interactions and development of cloud environments. To reach this goal, they have formed two working groups—Cloud Management Work Group (CMWG) and Cloud Audit Data Federation (CADF) work group [16]. To address convergence issues between cloud computing and telecommunications the European Telecommunications Standards Institute (ETSI) established the cloud project. Their particular interest is on the Infrastructure as a Service (IaaS) delivery model [17]. The National Institute of Standards and Technology (NIST) is a United States government agency; their long term goal is to provide specific guidance to the industry and government, they aim to shorten adoption cycle and identify gaps in cloud standards [18].

Open Grid Forum's (OGF) Open Cloud Computing Interface (OCCI) working group was originally formed to create remote management API for Infrastructure as a Service (IaaS), but their current release of open computing interface is even suitable for other service delivery models such as Platform as a Service (PaaS) and Software as a Service (SaaS) [19]. Open Cloud Consortium (OCC) works with development of standards for interoperability, benchmarks and open source reference implementations. They have several working groups working at the moment, such as The Open Science Data Cloud (OSDC) working group, The Open Cloud Testbed working group and Intercloud Testbed working group [20].

The Storage Networking Industry Association (SNIA) has created the Cloud Storage Technical work group with the aim of developing SNIA architecture related to cloud storage technology [21]. In May 2010 "the open group" merged "SOA and Security" and "Security in cloud" projects to form "Security for Clouds and SOA". Their main objective is to develop best practices and to describe and understand security and cloud security architecture [22]. The Open Cloud Manifesto group is working on a set of principles for the cloud community "in the belief that cloud computing should be as open as all other IT technologies". In their document, they pointed out choice, flexibility, skills and speed, and agility as goals for open cloud with six principles [23].

Before we discuss the gaps and unique security concerns of cloud computing, it is imperative that we portray the main aspects of cloud computing as many of those are actually generated because of its unique features.

3. Main aspects of cloud computing

'Cloud Computing' can be viewed as the evolution of 'Grid Computing'. Foster et al. [24] argue that "Cloud Computing is not a completely new concept; it has intricate connection to the thirteen-year established Grid computing paradigm, and other