Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Vulnerabilities and mitigation techniques toning in the cloud
A cost and vulnerabilities coverage optimization approach using Cuckoo search algorithm with Lévy flights

Mhamed Zineddine

MIS Department, ALHOSN University, Abu Dhabi, United Arab Emirates

ARTICLE INFO

Article history:
Received 21 November 2013
Received in revised form
28 August 2014
Accepted 15 September 2014
Available online 28 September 2014

Keywords:
Cloud computing
ICT security
Vulnerabilities mapping
Cuckoo search algorithm
Lévy flights algorithm
Optimization

ABSTRACT

Information and Communication Technology (ICT) security issues have been a major concern for decades. Today's ICT infrastructure faces sophisticated attacks using combinations of multiple vulnerabilities to penetrate networks with devastating impact. With the recent rise of cloud computing as a new utility computing paradigm, organizations have been considering it as a viable option to outsource major IT services in order to cut costs. Some organizations have opted for a private or hybrid cloud to take advantage of the emerging technologies and services. However, ICT security issues have to be appropriately mitigated. This research proposes a cloud security framework and an approach for vulnerabilities coverage and cost optimization using Cuckoo search algorithm with Lévy flights as random walks. The objective is to mitigate an identified set of vulnerabilities using a selected set of techniques when minimizing cost and maximizing coverage. The results show that Cloud Computing providers and organizations implementing cloud technology within their premises can effectively balance IT security coverage and cost using the proposed approach.

1. Introduction

Frequently, large corporations announce and report on cost cutting. These announcements might be interpreted as an effort to reduce X-inefficiency.[1] Finding and trimming surpluses is an important, yet irregular activity (Borenstein and Farrell, 2000). Not all cost-cutting, however, is driven by X-inefficiency. Re-optimizing due to endogenous or exogenous factors might be the trigger. Whatever the cause, businesses all over the globe are continually striving to cut costs. Among the areas targeted is ICT. Cloud Computing has been a promising option to achieve this objective by allowing businesses to tap the best business applications and Information Technology (IT) infrastructure available at a fraction of the cost (Plummer et al., 2009). Cloud Computing has been of great interest to

E-mail addresses: m.zineddine@alhosnu.ae, z5868@yahoo.com.

[1] The difference between efficient behavior of businesses assumed or implied by economic theory and their observed behavior in practice (Leibenstein, 1966).

http://dx.doi.org/10.1016/j.cose.2014.09.002
0167-4048/

businesses due to it flexible options. Five main attributes characterizing Cloud Computing are: Service-Based; Scalable and Elastic; Shared; Metered by use; and Internet technologies dependent (Plummer et al., 2009). Adopting cloud computing has been very attractive due to many benefits such as:

> "*Fast deployment, pay-per-use, lower costs, scalability, rapid provisioning, rapid elasticity, ubiquitous network access, greater resiliency, hypervisor protection against network attacks, low-cost disaster recovery and data storage solutions, on-demand security controls, real time detection of system tampering and rapid re-constitution of services*" (Singh and Malhotra, 2012).

Despite these advantages, many organizations have been reluctant to join the Cloud Computing world, until the main risks are identified, well understood and managed effectively (Viega, 2009). Organizations form different industries reported that Cloud Computing's issues outweigh its benefits (Mullins, 2010). ICT Security concerns have been the primary issue related to Cloud Computing, followed by availability, performance and lack of interoperability standards (Mullins, 2010). Nevertheless, the growth of Cloud Computing has been beyond expectations. Small-to-medium-sized businesses have been shifting more of their IT infrastructure to the Cloud. Furthermore, significant funds had been reserved for Cloud Computing according to a survey conducted by the International Data Corporation (IDC) (Mullins, 2010). Estimates done by Merrill Lynch (MER) in 2008 predicted that Cloud Computing would surge by now to $95 billion and 12% of the global software market would migrate to the Cloud (King, 2008). Companies offering public IT services generated revenues of more than $21.5 billion in 2010 and their revenues will reach an estimated $72.9 billion in 2015 (International Data Corporation, 2013). U.S. Public IT Cloud Services' revenue is projected to reach $43.2 Billion in 2016 (Smith and Tiazkun, 2012). Merrill Lynch's projections were somewhat in line with a recently released report by Cisco. Cisco's report indicated that by 2011, 30% of data center workloads had shifted to the Cloud and 2014 will mark the tipping point when the majority of workload is handled by the Cloud (McKendrick, 2012). Moving to the Cloud has been an emerging economic concept supported by virtualizations, physical servers' capacity and performance increase and other technologies. Taking advantage of the business and technology opportunities offered by Cloud Computing has been the main driver behind its boom. New and traditional security vulnerabilities have been popping up at a speedy rate across cloud computing services and their underlying infrastructure. The problem is that applying security solutions subjectively have been mostly infective and cost prohibitive. The aim of this paper is to propose a systematic approach to identify an optimal set of solutions to mitigate a discovered set of vulnerabilities when minimizing cost if needed and maximizing coverage.

The remainder of this paper is structured as follows:

The background section introduces the different types of Cloud deployment models, Cloud Computing security challenges and benefits, some documented Cloud Computing hacking cases, and the main attacks that may target cloud computing and its possible mitigations. Section 3 deals with mapping vulnerabilities to security techniques and discusses the matching process between vulnerabilities and technologies. Cloud Computing security optimization using cuckoo search algorithm with Lévy flights algorithm as random walks is described in Section 4. Section 5 presents the empirical application of the algorithm to Cloud Computing security optimization. The discussion, limitations and future research are presented in Sections 7 and 8. The last section concludes the paper.

2. Background

Organizations of all sizes have been looking for opportunities to improve services or meet standards and regulations without major investments. Banks, for instance, are required to make heavy investments to meet financial services regulations. JPMorgan, Barclays, Goldman Sachs and Credit Suisse have agreed to build and share a data storage platform outsourced to the Depository Trust and Clearing Corporation in order to cut cost. The move was driven by 140 000 pages of financial services regulations published in the past two years that financial institutions must adhere to (Stafford, 2013). One of the most recent ICT emerging trends and solutions has been the migration of IT services to the Cloud. The ICT shift underlying the concept of considering IT as a Service has created new opportunities and challenges.

The Cloud or Cloud Computing originally emerged as a metaphor for the Internet. However, nowadays it "describes basically an abstraction of the underlying infrastructure it represents" (Rittinghouse and Ransome, 2010). Cloud Computing is defined as "a style of computing where massively scalable IT-enabled capabilities are delivered 'as a service' to external customers using Internet technologies" (Plummer et al., 2009). It is a pool of virtualized resources that can be allocated and dynamically reconfigured according to users' requirements and demands (Vaquero et al., 2009).

2.1. *Cloud computing delivery models*

In brief, Cloud Computing delivery models are Software as a Service (SaaS), where software applications are made available to users through the Cloud (Zhu et al., 2010); Platform as a Service (PaaS), which enables consumers to deploy acquired compatible applications or their own created applications using programming languages, libraries, services, and tools supported by the chosen provider (Mell and Grance, 2011); Infrastructure as a Service (IaaS) where consumers are able to acquire the necessary processing power, the storage, the bandwidth, and other vital computing resources to deploy and run their own software including operating systems and applications (Mell and Grance, 2011); and Data Storage as a Service (dSaaS) which consists of basic storage capability over the network (Fig. 1).

2.2. *Cloud deployment models*

Four deployment models are available for Cloud Computing:

Private cloud: the underlying infrastructure is under the control of the organization. However, the management and administration might be outsourced (Mell and Grance, 2011).