Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 110 (2017) 465–472

Procedia Computer Science

www.elsevier.com/locate/procedia

The 3rd International Workshop on Cyber Security and Digital Investigation (CSDI 2017)

A Comprehensive Survey on Security in Cloud Computing

Gururaj Ramachandra[†,‡], Mohsin Iftikhar[†,*], Farrukh Aslam Khan[§]

[†]*School of Computing and Mathematics, Charles Sturt University, Wagga Wagga, NSW, Australia.*
[‡]*Dimension Data Australia, 15 Lancaster place, Majura Park, Canberra ACT 2611, Australia*
[§]*Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia*

E-mail: gururaj.ramachandra@dimensiondata.com, miftikhar@csu.edu.au, fakhan@ksu.edu.sa

Abstract

According to a Forbes' report published in 2015, cloud-based security spending is expected to increase by 42%. According to another research, the IT security expenditure had increased to 79.1% by 2015, showing an increase of more than 10% each year. International Data Corporation (IDC) in 2011 showed that 74.6% of enterprise customers ranked security as a major challenge. This paper summarizes a number of peer-reviewed articles on security threats in cloud computing and the preventive methods. The objective of our research is to understand the cloud components, security issues, and risks, along with emerging solutions that may potentially mitigate the vulnerabilities in the cloud. It is a commonly accepted fact that since 2008, cloud is a viable hosting platform; however, the perception with respect to security in the cloud is that it needs significant improvements to realise higher rates of adaption in the enterprise scale. As identified by another research, many of the issues confronting the cloud computing need to be resolved urgently. The industry has made significant advances in combatting threats to cloud computing, but there is more to be done to achieve a level of maturity that currently exists with traditional/on-premise hosting.

Peer-review under responsibility of the Conference Program Chairs.

Keywords: Cloud computing; Security in cloud; Security Threats

* Corresponding author. Tel.: +61-2-6933-2048; fax: +61-2-6933-4766.
E-mail address: miftikhar@csu.edu.au

1877-0509
Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.06.124

1. Introduction

Cloud computing is increasingly being adapted by a wide range of users starting from commercial entities to consumers. A survey by Right Scale[1] found that an average user runs at least four cloud-based applications and at any point in time is evaluating another four. The survey also found that 41% of commercial entities run significant workload on public clouds. With so much of our workload moving to cloud, security in cloud computing is under increased scrutiny. This assessment is also supported by the 2017 report by Forbes[2], which says that in 15 months, while 80% of all IT budgets will be committed to cloud solution, 49% of the businesses are delaying cloud deployment due to security skills gap and concerns. The problem appears to be multi-dimensional, with lack of skilled resources, lack of maturity, conflicting best practices, and complex commercial structures to name a few. Adaption of cloud has reached a tipping point and it is expected that more workloads will move from traditional local storage to cloud from not just average Internet users, but also from most if not all commercial entities. While there are many problems that need identifying, analyzing, and addressing, this document attempts to survey the security in cloud computing and reports on various aspects of security vulnerabilities and solutions. Some questions that need urgent answers are: (a) Privileged User Access Management, (b) Regulatory Compliance, (c) Data Location, (d) Data Segregation, (e) Data Protection and Recovery Support, (f) Investigative Support, and (g) Long-term Viability.

It is highly recommended that these questions, along with other risks, are assessed and addressed. Some of the assessments could be as follows:

a. *Organization capability and maturity*
b. *Technology & data risks*
c. *Application migration and performance risk*
d. *People risks*
e. *Process risks*
f. *Policy risks*
g. *Extended supply chain risks*

This article consolidates various works that address the risks, vulnerabilities, and potential controls in cloud computing. It also provides information on leading cloud architectures and frameworks. Moreover, the article identifies potential future research areas related to security in cloud computing.

The remainder of the paper is organized as follows: The cloud architecture is discussed in section 2. Section 3 discusses the security implications based on deployment and delivery models. General vulnerabilities, attacks, and threats are explained in section 4, whereas section 5 gives insights into countermeasures and controls. Finally, section 6 concludes the paper with potential future directions.

2. Cloud Architecture

Before we dive into the security issues, it is important to understand the cloud definition and architecture. According to Sharma and Trivedi[3], cloud computing is a set of resources that can scale up and down on-demand. It is available over the Internet in a self-service model with little to no interaction required with the service provider. Cloud enables new ways of offering products and services with innovative, technical, and pricing opportunities.

As per NIST's Cloud Computing Reference Architecture[4], there are five major actors that influence and are impacted by cloud computing, along with its security implications. This document focuses on cloud consumer and cloud provider's threat and risk perceptions.