Chapter 4
Cloud Computing Security Issues of Sensitive Data:

Manpreet Kaur Walia
Charles Sturt University, Australia

Malka Halgamuge
University of Melbourne, Australia

Nadeesha D. Hettikankanamage
Charles Sturt University, Australia

Craig Bellamy
Charles Sturt University, Australia

ABSTRACT

Numerous organizations are using aspects of the cloud to store data, but as sensitive data is placed on the cloud, privacy and security become difficult to maintain. When users upload data to the cloud, they may become increasingly vulnerable to account hijacking, unauthorized access, and the data may become unavailable because of various technical reasons. Questions remain about the security of sensitive data in the cloud, and in this chapter, the authors perform an analysis of 36 peer reviewed publications describing 30 observations of cloud computing technology (2010-2017). In the articles, applications of cloud computing include, for instance, business (26%) and the internet of things (IoT; 2%), and the result suggests that some issues are unique to a particular domain (such as business, education, health) and some issues cross all domains. The results suggest that data integrity issues have the highest number of solutions whereas data breaches have the lowest number of solutions.

BACKGROUND

Cloud computing is a rapidly developing technology, partly because of its ability to lessen the cost of computing through distributing data and computational resources along with the scalability and adaptiveness of its architecture. Consequently numerous organisations are now using 'the cloud' to store data but as more data is placed on the cloud privacy and security issues increase. Within this review we perform

DOI: 10.4018/978-1-5225-7335-7.ch004

an analysis of 36 peer-reviewed publications describing 30 observations of cloud computing technology relating to security (2010-2017). In the articles applications of cloud computing to the Internet of Things and broader business uses are examined and our result suggests that some security issues are unique to a particular domain but some issues cross all domains. The results also suggest that 'data integrity' issues have the highest number of solutions (20%) whereas data breaches have the lowest number of solutions (8%). This study should be useful as a reference for researchers interested in cloud computing security and privacy and their current and emergent solutions.

1. **Graphical Abstract:** Pictorial representation of the abstract of this research is shown in Figure 1.

INTRODUCTION

Internet use in all domains is growing rapidly with increasing requests for the processing and storage of complex data (Weihua & Shibing, 2013). Cloud computing evolved from the convergence of Grid Computing, Effectiveness Computing and SaaS and the move to third-party vendors for large-scale computing solutions. The name 'cloud computing' originated from a cloud symbol often used in presentations and flowcharts to denote the Internet (Zissis & Lekkas, 2012). Cloud Computing provides a system where patrons can operate and install IT services and is not a precise technology, but an architecture built upon virtual machines and various software as service technology (Zhang, Yang, Zhang, Liu, & Chen, 2012). The features of cloud computing are defined in Table 1(Ghobadi, Karimi, Heidari, & Samadi, 2014).

There are various models for cloud computing including hybrid cloud, private cloud, community cloud and public cloud, described in Table 2.

Figure 1. Graphical abstraction of the study: this chapter examined the recent scientific works; data for this examination is gathered from 30 scientific works (2010-201)