


Chapter 1

Securing the Cloud for Big Data

Michael Robinson

 <https://orcid.org/0000-0002-4276-2359>

Airbus, UK

Kevin Jones

Airbus, UK

ABSTRACT

This chapter explores how organizations can seek to secure a public cloud environment for use in big data operations. It begins by describing the challenges that cloud customers face when moving to the cloud, and proposes that these challenges can be summarized as a loss of control and visibility into the systems and controls around data. The chapter identifies thirteen areas where visibility and control can be lost, before progressing to highlight ten solutions to help regain these losses. It is proposed that planning is the most significant step a customer can take in ensuring a secure cloud for big data. Good planning will enable customers to know their data and pursue a risk-based approach to cloud security. The chapter provides insight into future research directions, highlighting research areas which hold the potential to further empower cloud customers in the medium to long term.

INTRODUCTION

Cloud has become the ideal platform for big data (Hashem, Yaqoob, Anuar, Mokhtar, Gani, & Khan, 2015): a seemingly limitless pool of computing resources which can be rapidly provisioned and scaled up or down as needed on a pay per use basis. Whilst being ideal for big data activities, the use of cloud presents new security challenges that do not exist when using an on-premise solution or private data centre (Singh, Jeong, & Park, 2016).

Many of these new challenges emerge from the fact that the customer relinquishes control over the infrastructure, processes and handling of data when moving to cloud (Behl, 2011). They instead place trust into the cloud provider that their data will be secure and that the service will be available for use when required. We propose that this trust is often given based upon the assurances from the cloud provider, contractual agreements and upon their reputation.

DOI: 10.4018/978-1-5225-9742-1.ch001

The aim of the chapter is to provide practical managerial guidance in deploying big data operations securely. The chapter begins by providing a review of areas where big data customers face security risks when moving to a public cloud environment. Following this, a survey of solutions which can address these risks is provided. Where appropriate, we provide links to ongoing research efforts which seek to improve and enhance big data security in the cloud and finish with a discussion on future research directions.

Background

The National Institute of Standards and Technology (NIST) defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources” (Mell & Grance, 2011). It is a technology which fits many big data use cases well, removing upfront investment in hardware whilst providing agility, scalability and reliability in a pay-as-you-go context. As individuals and organisations continue to see the benefits of cloud for big data and other computing activities, it is an industry which continues to grow year on year. Evidencing the popularity of cloud, Gartner has predicted that the worldwide public cloud services market will grow 17.3 percent to total \$206.2 billion in 2019 (Gartner Research, 2018).

Despite the benefits of cloud, organisations can be hesitant in their adoption for a number of reasons. Firstly, cyberspace is becoming an increasingly hostile environment. In 2015 Symantec reported that data breaches led to over half a billion personal records being lost or stolen globally (Symantec, 2016). A year later, this figure had doubled to just over one billion (Symantec, 2017). These cyber threats are not just coming from cyber criminals, but also from states and intelligence services which seek to conduct espionage (Hoboken & Rubinstein, 2014). In this hostile cyber environment, organisations are understandably cautious about sending data out of their perimeter, across the public internet to be received, stored and processed at a remote location by a third party.

These concerns are amplified due to the fact that national governments and regulators are strengthening legislation in regard to the protection of personal data. The European General Data Protection Regulation (GDPR) came into force in May 2018, with heavy fines for data controllers found to have failed in their duty to protect personal data. These penalties alone can be significant enough to threaten the financial health of an organisation, before reputational damage is even considered.

Cloud can also fundamentally change the architecture of systems and requires an understanding of new risks and controls to mitigate them (Gou, Yamaguchi, & Gupta, 2016; Singh, Jeong, & park, 2016). Without cloud expertise, the security of a deployment can be hard to assess and many customers accept that a level of control and transparency over their data will be lost in exchange for the benefits it brings (Flittner, Balaban, & Bless, 2016). This loss of control and increase in risk has been visualised by Saxena and Choudrey (2014) in Figure 1:

APPROACH

The focus of this chapter is to provide practical security guidance to those operating cloud based big data operation so that risks are lowered whilst control is raised. To achieve this goal, the flow of the chapter is as follows. We first describe thirteen areas where big data cloud customers face increased risks and

21 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/securing-the-cloud-for-big-data/234804

Related Content

Secure Data Hiding Using Eight Queens Solutions

Sunil Kumar Muttou, Vinay Kumar and Abhishek Bansal (2012). *International Journal of Information Security and Privacy* (pp. 55-70).

www.irma-international.org/article/secure-data-hiding-using-eight/75322

Critical Evaluation of Hazards Operability Versus Safety Integrity Risk Analysis Techniques

Mohammed Malik (2018). *International Journal of Risk and Contingency Management* (pp. 37-45).

www.irma-international.org/article/critical-evaluation-of-hazards-operability-versus-safety-integrity-risk-analysis-techniques/191218

A Full Review of Attacks and Countermeasures in Wireless Sensor Networks

Pejman Niksaz and Mohammad Javad Kargar (2012). *International Journal of Information Security and Privacy* (pp. 1-39).

www.irma-international.org/article/full-review-attacks-countermeasures-wireless/75320

Securing the Internet in New Zealand: Threats and Solutions

Jairo A. Gutierrez (2000). *Internet and Intranet Security Management: Risks and Solutions* (pp. 24-37).

www.irma-international.org/chapter/securing-internet-new-zealand/24596

Cybersecurity in Europe: Digital Identification, Authentication, and Trust Services

Joni A. Amorim, Jose-Macario de Siqueira Rocha and Teresa Magal-Royo (2021). *Handbook of Research on Advancing Cybersecurity for Digital Transformation* (pp. 18-36).

www.irma-international.org/chapter/cybersecurity-in-europe/284144