Chapter 16

Cloud Security Threats and Techniques to Strengthen Cloud Computing Adoption Framework

Nabeel Khan
University of Salford, UK

Adil Al-Yasiri
University of Salford, UK

ABSTRACT

Cloud Computing allows firms to outsource their entire information technology (IT) process, allowing them to concentrate more on their core business to enhance their productivity and innovation in offering services to customers. It allows businesses to cut down heavy cost incurred over IT infrastructure without losing focus on customer needs. However, to a certain limit adopting Cloud computing has struggled to grow among many established and growing organizations due to several security and privacy related issues. Throughout the course of this study several interviews were conducted, with cloud developers and security experts, and the literature was reviewed. This study enabled us to understand, current and future, security and privacy challenges with cloud computing by providing suitable solutions to identified challenges. The outcome of this study led to identification of total 18, current and future, security issues affecting several attributes of cloud computing. In this process of identification, the author also found mitigation techniques to avert these security issues. A security guide is formulated which enables organizations to be aware of security challenges, vulnerabilities and techniques to evade them.

1. INTRODUCTION

The scalability and extensibility of distributed software architectures have led to the concept called Cloud Computing. Cloud computing is a technology used to deliver the hosted services over the Internet. Through this technology, users don't have to manage their own IT resources; instead they purchase their IT needs as services over the internet (Mell and Grance, 2011).

Cloud computing main objective is to provide secure, quick and convenient data storage with all services delivered over the internet. Cloud computing has a distributed architecture and contains a computational paradigm which enables it to enhance availability, scalability, agility, collaboration and adaptability of the system. Cloud computing technology allows in reducing the rates spent on computing infrastructure, boosting performance and increasing efficiency of an organization (Zhao et al. 2009; Zhang et al. 2010; Clous security alliance, 2011; Marinos and Briscoe, 2009; center for protection of national infrastructure, 2010; Khalid, 2010).

With more and more explorations of cloud technology, it has faced challenges that need to be resolved to improve the pace of cloud adoption among SMEs. One of the most significant barriers to adoption is security and privacy of the data in the cloud. There is a huge uncertainty of the security of data in clouds at all times as cloud computing represents relatively new idea of computing and that's the reason for security experts to be more concerned about data security in clouds.

Cloud has many specific attributes compared to many traditional technologies such as huge pool of resources and mostly belonging to cloud providers are heterogeneous, distributed and completely virtualized. It's because of this reason traditional security measures like identification, authentication and authorization is not enough in case of cloud computing (Li and ping, 2009). Security controls and mechanisms in traditional IT is more or less very similar and useful to that of current form of cloud for most of its delivery models. But, cloud computing presents different organizational risks than traditional IT due to its ways of service deployment, operations and enabling technologies. Unfortunately, security integration into these services often makes it more difficult to provide more substantial solution to the problem (Rittinghouse and Ransome, 2009).

Moving organization's critical applications and legacy database full of sensitive information to cloud service provider (CSP) with no control of their own data is a concern of many organizations. To diminish this concern, CSP must ensure that they continue to provide customers with same security and control to their applications and sensitive data as onshore system. In order to achieve this CSP must provide evidence to a customer that all service level agreements are met and compliance can be proved to auditors (GiljeJaatun, 2009).

We have tried to present security issues related to cloud computing based on service delivery models i.e. security issues with software as a service, platform as a service and infrastructure as a service. Also, we have identified vulnerabilities and threats in cloud computing which leads to these security issues, where vulnerabilities refer to gaps in a system which allows attack to be successful and threats refers to an attack which is attempted on gaps in a system to exploit resources or information. Based on these identified threats and challenges we have provided possible remedy to avoid incidents leading to a security breach or system failure.

Several studies have been conducted on cloud issues and what is really affecting cloud industry. There are around more than cloud frameworks in the market at present to deal with IT services or architecture but none of them is designed for cloud adoption for any size of an organization (this proposed cloud framework is only for SMEs in particular) (Weinhardt et al, 2009). Some of these frameworks are Cloud Business Model Framework (CBMF), IBM Framework for Cloud Adoption, Cloud Computing Business Framework, framework for ranking and comparing cloud services, cloud genius, Decision making in cloud computing environments based on cost and risk associated with cloud, Cloud advisor etc. (IBM, 2010; Chang et al. 2013; Garg et al. 2011; Menzel and Ranjan, 2012; Martens and Teutberg, 2012; Jung et al. 2013).

16 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/cloud-security-threats-and-techniques-to-strengthen-cloud-computing-adoption-framework/203510

Related Content

Combining Data Preprocessing Methods With Imputation Techniques for Software Defect Prediction
Misha Kakkar, Sarika Jain, Abhay Bansaland P.S. Grover (2021). *Research Anthology on Recent Trends, Tools, and Implications of Computer Programming (pp. 1792-1811).*
www.irma-international.org/chapter/combining-data-preprocessing-methods-with-imputation-techniques-for-software-defect-prediction/261102

Recent Developments in Cryptography: A Survey
Kannan Balasubramanian (2018). *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications (pp. 1272-1293).*
www.irma-international.org/chapter/recent-developments-in-cryptography/203560

True Color Image Segmentation by MUSIG Activation Function Using Self-Supervised QMLSONN Architecture With Context-Sensitive Thresholding
Pankaj Paland Siddhartha Bhattacharyya (2018). *Quantum-Inspired Intelligent Systems for Multimedia Data Analysis (pp. 213-261).*
www.irma-international.org/chapter/true-color-image-segmentation-by-musig-activation-function-using-self-supervised-qmlsonn-architecture-with-context-sensitive-thresholding/202549

Virtualizing Network Functions in Software-Defined Networks
Vishal Kaushik, Ajay Sharmaand Ravi Tomar (2018). *Innovations in Software-Defined Networking and Network Functions Virtualization (pp. 26-51).*
www.irma-international.org/chapter/virtualizing-network-functions-in-software-defined-networks/198192

Solutions of Fuzzy System of Linear Equations
Laxminarayan Sahoo (2020). *Handbook of Research on Emerging Applications of Fuzzy Algebraic Structures (pp. 26-33).*
www.irma-international.org/chapter/solutions-of-fuzzy-system-of-linear-equations/247645