

Risk Assessment for Cloud-Based IT Systems

Yuyu Chou, Berlin Institute of Technology, Germany

Jan Oetting, Consileon Business Consultancy GmbH, Germany

ABSTRACT

The use of Cloud Computing services is an attractive option to improve IT systems to achieve rapidly and elastically provisioned capability, and also to offer economic benefits. However, companies see security as a major concern in migrating to the Cloud. To bring clarity in Cloud security, this paper presents a systematic approach to manage the risks and analyzes the full range of risk in Cloud Computing solutions. Furthermore, as a study case, Google App Engine Platform is assessed based on ISO/IEC 27002 and OWASP Top 10 Risk List in this paper. Knowing the risks of Cloud solutions, companies can execute well-informed decisions on going into the Cloud and build their Cloud solutions in a secure way, relying on a robust e-trust relationship.

Keywords: Cloud Computing, Google App Engine, ISO/IEC 2700x, OWASP, Risk Management

INTRODUCTION

Many companies have problems with existing systems. They need greater business agility, cost effective, stable IT infrastructures and the operation can keep pace with fast growing technology and the changing environment. However, maintenance of the current environment accounts for over 70% of the IT budget, leaving less than 30% available for new projects (Bain, Read, Thomas, & Merchant, 2009). Cloud Computing is the model that can fit their requirements, for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interac-

tion (Mell & Granc, 2009). A Cloud is the type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based upon the service level agreements established through negotiation between service provider and service user (Buyya, Yeo, Venugopal, Broberg, & Brandic, 2009). However, the security standards for Cloud Computing forms slowly, if without cautious understanding the know-how and the risk evaluation when we adapt the systems based on Cloud structures, it will become a disaster.

Not all risks of Cloud Computing can be addressed on a global level. Individual risks arise at different Cloud solutions. Before going into Clouds, a company needs to know the specific of the individual Cloud providers. Therefore,

DOI: 10.4018/jghpc.2011040101

it will be very helpful if research institutes will analyze and publish individual risk profiles after intensive analysis. This paper performed such an analysis for the Google Cloud Platform (called "Google App Engine") for industry as a reference first. This analysis is based on the security domains of ISO/IEC 27002 Standard (International Organization for Standardization, 2007) and OWASP Top 10 (OWASP, 2010) risks in web application to check if using the Google Platform can alleviate these risks.

RISK MANAGEMENT

Though an IT system can be evaluated in terms of functionality, completeness, consistency, accuracy, performance, reliability, usability, fit with the organization, and other relevant quality attributes (Hevner, March, Park, & Ram, 2004), if the system is not secure enough, the whole enterprise will be exposed to the high risk of getting into vulnerable situations. Despite the promising business model, security is a major concern that could limit the Cloud Computing paradigm's impact (Jaeger & Schiffman, 2010). Owing to the fact that customers must perform their applications, or store their data on the Internet, moving application servers to Clouds means a considerable risk for enterprises. How to build up the trust in the remote execution becomes the biggest challenge. Identifying threats and vulnerabilities plays a crucial role in securing the system. Consequently, we need a systematic approach to identify the appropriated security requirements on Clouds which can fulfill the Business Strategy and reduce risks to create an effective and efficient IT system.

Security Risk management analyses what can happen and what the possible consequences can be, before deciding what should be done and when, to reduce the risk to an acceptable level (International Organization for Standardization, 2008). Risk should be identified, assessed, and monitored regularly.

The level of risk should be estimated by the likelihood of incident scenario, mapped against the estimated negative impact (Catteddu

& Hogben, 2009). After assessing the risks, priority order for the risks and treatments should be also established before hosting the system on the Cloud. The risk executive function does not make authorization decision; rather, the intent is to provide visibility into the decisions of authorizing officials and a holistic view of risk to the organization beyond that risk associated with the operation and use of individual information systems (The National Institute of Standards and Technology, 2008). Companies can follow the process that suggest by ISO/IEC 27005, as Figure 1 shows.

RISK ANALYSIS IN CLOUD COMPUTING SOLUTIONS

The massive concentrations of resources and data present a more attractive target to attackers, but Cloud-based defenses can be more robust, scalable and cost-effective (Catteddu & Hogben, 2009) if well-organized. Outsourcing IT services has been a highly controversial topic for many years. Not only costs should be considered but also other relevant aspects. To evaluate the risks before hosting a solution on the Cloud, customers can reference the items, which shows the main considerations and the detail analysis are as below:

- *Investment cost.* Typical *aaS offerings are over a public network, and without purchasing hardware and serve via the Internet. The service is rented, not purchased, the cost is controlled, paid by use and the capital investment can be zero (Sun, 2009). Software is easier to install, maintain, and update than client-based computing, which requires installing and configuring software and updating it with each new release, as well as revising other programs with every update (Parikh, 2009). However, carefully balance all costs and benefits associated with Cloud Computing and the conventional system in both the short and long terms is necessary. Underestimating or overestimating the provision of resources

11 more pages are available in the full version of this document, which may be purchased using the "Purchase" button on the product's webpage:

www.irma-international.org/article/risk-assessment-cloud-based-systems/54192/

Related Content

Programming Interfaces for Realtime and Cloud-Based Computing

Gregory Katsaros, and Tommaso Cucinotta (2012). *Achieving Real-Time in Distributed Computing: From Grids to Clouds* (pp. 41-58).

www.irma-international.org/chapter/programming-interfaces-realtime-cloud-based/55241/

Health and Health Care Grid Services and Delivery Integrating eHealth and Telemedicine

Thomas Clark (2011). *Grid Technologies for E-Health: Applications for Telemedicine Services and Delivery* (pp. 36-64).

www.irma-international.org/chapter/health-health-care-grid-services/45558/

Efficient Communication Interfaces for Distributed Energy Resources

Heinz Frank, and Sidonia Mesentean (2010). *International Journal of Grid and High Performance Computing* (pp. 23-36).

www.irma-international.org/article/efficient-communication-interfaces-distributed-energy/43882/

A Decentralized Directory Service for Peer-to-Peer-Based Telephony

Fabian Stäber, Gerald Kunzmann, and Jörg P. Müller (2011). *Cloud, Grid and High Performance Computing: Emerging Applications* (pp. 330-344).

www.irma-international.org/chapter/decentralized-directory-service-peer-peer/54938/

Fednets: P2P Cooperation of Personal Networks Access Control and Management Framework

Malohat Ibrohimovna, and Sonia Heemstra de Groot (2010). *Handbook of Research on P2P and Grid Systems for Service-Oriented Computing: Models, Methodologies and Applications* (pp. 956-980).

www.irma-international.org/chapter/fednets-p2p-cooperation-personal-networks/40835/