International Journal of Information Management 36 (2016) 618–625

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Towards performance evaluation of cloud service providers for cloud data security

Muthu Ramachandran*, Victor Chang

School of Computing, Creative Technologies and Engineering, Leeds Beckett University, Leeds, UK

ARTICLE INFO

Article history:
Received 13 March 2016
Received in revised form 14 March 2016
Accepted 14 March 2016
Available online 9 April 2016

Keywords:
Cloud service provider (CSP)
Business process management (BPM)
Business process modeling (BPMN)
Cloud computing
Data security

ABSTRACT

Today's data is sensitive that requires privacy and security both from the cloud service providers (CSP) as well as from users in its all the form of data states: data at rest, while transferring data, enquiring data, and processing the data. Cloud computing has been applied in the health sector, national security services, banking and other business and companies that store confidential data into the cloud as we have seen in recent years. Therefore, information and data security is a crucial issue that needs to be addressed thoroughly in the cloud computing business. This research deals with the performance analysis of recent cloud data security models. This paper proposes cloud data security models based on Business Process Modeling Notations (BPMN) and simulation results can reveal performances issues related to data security as part of any organizations initiative on Business process management (BPM).

1. Introduction

Cloud computing has become the influencing IT landscape and gained amplified attention in recent years as benefits of reduced IT costs and is management. The US spending on cloud computing for the last five years was estimated to grow at annual growth rate of 40% and was expected to reach $7 billion by the end of the year (Kaufman, 2009). It was reported that this speeding on cloud computing was expected to pass $95 billion in 2018 (Subashini & Kavitha, 2011). Moreover, it was estimated that 12% of the software market would shift towards the cloud (AlZain, Soh, & Pardede, 2013). However, based on the current growth rate of the cloud business and the trend of software market, it looks like that the software market in the cloud has already surpassed 12%. In addition, the use of cloud storage and social networks has revolutionized IT social interactions and communications of the people.

Among the variety of definitions of cloud computing, the most popular and commonly used definition that encapsulates the main constituents of cloud computing is the one by the National Institute of Standards and Technology (NIST) (Mell & Grance, 2011). Accordingly, cloud computing is an IT model for using on-demand, shared, measured and self adjustable computing resources, both software and hardware, conveniently via the Internet without the hassle of heavy management requirements and interaction between the client and the provider. There are five core components in the definition of cloud computing; network access, on-demand self-service, resource pooling, measured service and rapid elasticity (Rountree & Castrillo, 2014). NIST definition also includes generally three service models; IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service) and four deployment models (private, public, community and hybrid) of cloud computing.

With SaaS the user accesses software and applications through browsers or programming interfaces without direct control over the infrastructure. PaaS provides platform infrastructure such as operating system (OS) where the user can run and configure software and applications but the user does not have control over the hardware. In IaaS, the user is provided with a hardware and network infrastructure where the user does not have physical access but can use for running OS and applications independently.

According to NIST, in private cloud deployment model the cloud service provider (CSP) provides one of the service models for an organization managed by the organization itself or by the CSP or by a third party. While the community deployment model provides cloud service to a certain classified group of users, the public model provides service to the general public. The fourth service model, the hybrid, is a combination of two or more of the previous deployment models.

The three functional components that the cloud computing model, be it the service or delivery, rotates around are cloud service provider (CSP), client also called owner and user (Sood, 2012). The CSP manages the cloud playing a significant role in providing

* Corresponding author.
E-mail address: m.ramachandran@leedsbeckett.ac.uk (M. Ramachandran).

http://dx.doi.org/10.1016/j.ijinfomgt.2016.03.005
0268-4012/© 2016 Published by Elsevier Ltd.

storage space and computational resource. The client or the owner is individual or organization that rents or buys cloud-computing service for storing data and/or for computation. The user is the individual that utilizes the cloud service as a registered individual or registered through a customer organization.

However, cloud computing is not without a challenge. According to Armbrust et al. (2010) cloud computing has a number of challenges. Some of them are related to data such as lock-in, auditability, confidentiality and transfer problems. The rest include business continuity/availability, performance, unpredictability, storage scalability, bugs in big distributed systems and software licensing. Risks of adopting cloud computing as identified by Fogarty (2009) include compatibility, privacy and interoperability. Compatibility is related to the fact that data in one CSP may not be compatible in other CSP. The owner organization cannot control over the privacy of its data. Alzain, Pardede, Soh, and Thom (2011) also identified the issue of privacy and security related to the risks on data integrity, data intrusion and service availability.

Most of the drawbacks of cloud computing as mentioned by most of the authors as discussed above and others are related to privacy and security of data. Today's data is sensitive that requires privacy and security both from the CSP side and from the user side at its state of rest, transfer and processing. Cloud computing is applied in the health sector, national security services, banking and other business and companies that store confidential data into the cloud (e.g. Flinders, 2014; Gill, 2013; Toxen, 2014). Therefore, information and data security is a crucial issue that needs to be addressed thoroughly in the cloud computing business. This research deals with the performance analysis of recent cloud data security models. This paper outlined structure consists of Section 1 provides introduction to this article, Section 2 provides background and related literature on cloud security & cloud data security, Section 3 discusses approaches on cloud security, Section 4 provides critical evaluation of cloud data security approaches and models, Section 5 provides BPMN modesl for Cloud Service providers (CSP-1 & CSP-3), and finally Section 6 provides BPMN simulation process steps on setting performance parameters for cloud data security simulation of the business processes.

2. Background

To date cloud computing can be defined based on resource sharing (multi-tenancy), elasticity, scalability, self-provisioning and pay when you use (e.g. Mell & Grance, 2011; Winkler, 2011). One of the modern cloud computing features is its business model where same resource is shared between multiple users at network, host and application level. Elasticity refers to the fact that cloud users can change their computing needs and provide resources to others when they do not need them any more. The current technology in cloud computing provides the customers to scale systems, bandwidth and storage size due to the scalability feature of cloud computing. Another important attribute in cloud computing is self-provisioned by the user for computing capacity, software and disc space and network. Most cloud computing service providers charge the users only for the time and resource used, this is referred as pay as use.

The most common cloud computing services have three delivery models (SaaS, PaaS and IaaS), four deployment models (private, public, community and hybrid), and several application domains (computing, storage, finance, web and many others).

According to IDC forecast in 2009, cloud computing services were estimated to grow annually at a rate of 27% with investment of 42 billion by 2012 compared to the traditional IT services estimated to grow at a rate of 5% annually (Mather, Kumaraswamy, & Latif, 2009). The fast growth of cloud computing is attributed to technological advancements in software such as browsers, processors, storage devices, virtualization technology, broadband Internet technology, servers, application programing interface (API) and others (Winkler, 2011). Currently, cloud computing services are on the tip of our finger accessed using PCs, smart phones, tablets, devices in refrigerators, cares and even smart watches.

Some of the main features that are driving the adoption of cloud computing are small initial investment and low running cost, reliability and sustainability, repeated pattern, resource elasticity, location independence, resources sharing at enormous scale, better automation, on-demand access, computational efficiency, and technology transparency (e.g. Mather et al., 2009; Winkler, 2011; Modi, Patel, Borisaniya, Patel, & Rajarajan, 2013). To ensure better automation, reliability and efficiency, a cloud is designed based on repeating pattern. When a computing service is delivered by abstracting the technology through an interface, it makes the technology transparent. Transparency lowers the cost of the cloud provider that makes it beneficiary in terms of operation and competitiveness. On demand access and self-service enables the providers to deliver the cloud service to the customers with cost effectiveness and agility. All these features to be true, they need more abstraction, which brings more complexity. That is the trade-off of all the good features in cloud computing. Since complexity makes the attack surface wider, it makes security in cloud computing challenging.

Thus the growth of cloud computing is with barriers that include security, privacy, connectivity and open access, reliability, interoperability, independence from CSPs, economic value, IT governance and changes in IT organization. The cloud will not be efficient, reliable and cost-effective without reliable and fast network connectivity. A few minutes disruption of connection and lagging network may mean costly to the customer. Availability and reliability are interconnected in terms of security. The most useful features of cloud computing to be cost-effective and agile are connectivity and security. Security issue in the cloud mainly data security will be addressed in the next section.

Cloud computing particularly refers to transferring, manipulating, computing and storage of data via a network to an offsite computing infrastructure managed and maintained by a third party. The computing resources are configured to run applications simultaneously to multiple users or multiple tenants. Under such computing environment, CSP should be able to ensure the security of the client data through the security principles such as firewall, virtual private network (VPN) and user authentication, private and public keys, encryption and other security policies. Due to the concept of resource pooling with other clouds, the clients' data is available both to third party cloud and the cloud in use (Julisch & Hall, 2010). Thus, security is a critical component in cloud computing business to ensure data is available and access is permitted only to authorized users (Overby, Bharadwa, & Sambamurthy, 2006).

Some of the advantages of adapting cloud computing include, but are not limited to, reducing initial capital expenditure (Creeger, 2009), minimal management (Pröhl, Repschläger, Erek, & Zarnekow, 2012), optimized resource utilization (elasticity) (Armbrust et al., 2010; Cusumano, 2010) and energy efficiency (Katz, 2009). Iyer and Henderson (2010) summarize a number of potentials of cloud computing: virtual business environment, controlled interfaces, ubiquitous access, location independence, rapid elasticity, sourcing independence, addressability and traceability. Hoberg, Wollersheim, and Krcmar (2012) identified other aspects of cloud computing: increased scalability, increased agility, reduction of IT infrastructure complexity, cost reduction and improved alignment of business and IT.