Journal of Information Security and Applications 38 (2018) 50–64

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Secure migration to compliant cloud services: A case study

Fahad F. Alruwaili[a,1,*], T. Aaron Gulliver[b]

[a] College of Computing and Information Technology, Shaqra University, P.O. Box 33, Shaqra 11961 Saudi Arabia
[b] Department of Electrical and Computer Engineering, University of Victoria, P.O. Box 1700, STN CSC, Victoria, BC V8W 2Y2 Canada

ARTICLE INFO

Article history:

Keywords:
Readiness assessment
Maturity level
Information security
Privacy
Compliance
Cloud computing
Service provider
Financial payment systems

ABSTRACT

Adoption of cloud computing technology in the financial sector is increasing to improve the efficiency of payment transactions, risk management, and business processes. This is occurring more rapidly in developed countries such as USA, Canada, and the UK while cloud implementation in less developed countries such as Saudi Arabia is still emerging. Implementation of cloud technologies in the financial sector requires diligent decisions such as selecting the most suitable secure cloud deployment model, service level agreement, and cloud vendor. In this paper, cloud migration using an information security, privacy, and compliance (ISPC) readiness model is presented. Several types of cloud services are available, therefore evaluating migration readiness and selecting an appropriate vendor is critical, as this will have an impact on the requirements of stakeholders such as local banks. Cloud migration decisions are obtained by analyzing ISPC requirements considering the strategic initiatives of the organization. A case study involving the Saudi Arabian central bank is presented to demonstrate the implementation of the ISPC readiness model.

1. Introduction

With the rapid evolution of the internet and data processing and storage capabilities, cloud computing has become a viable business model and computing paradigm. Cloud services enable powerful, scalable, cost-effective, on-demand, and efficient computing resources [1]. A variety of cloud computing service models such as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) form the core cloud computing technologies. These service models are supported by different deployment models, i.e. public, private, community, and hybrid [2]. 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 (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [3]. Further, cloud models are considered to have five essential characteristics, three service models, and four deployment models with different attributes compared to grid and distributed computing [4]. These attributes are described in Table 1. In addition, new service models are being developed such as storage as a service (STaaS), security and data protection as a service (SDPaaS), and security operations center as a service (SOCaaS) [5].

Many organizations are considering moving some or all of their information technology (IT) capabilities to the cloud due to the advantages of cloud systems. However, migration decisions are not easily made and can require significant time, resources, and personnel to assess the feasibility and readiness of an organization to make such a move [6]. This assessment considers decisions such as the selection of suitable cloud services and deployment models. If sensitive and business critical information are involved, a careful migration analysis must be conducted to identify the risks and benefits of cloud services [7].

The rapid growth in financial industry services and payment solutions require greater agility to adopt and implement changes [8]. Cloud computing services enable organizations to quickly respond to new business requirements and can be applied to financial applications and systems [8]. In this paper, information security, privacy, and compliance (ISPC) requirements are examined via a case study of the readiness and feasibility of the Saudi Arabian central bank migrating to cloud services. The organizational and operational challenges are analyzed using the four main components of the ISPC model, i.e. cubic model, control assessment, cloud feasibility analysis, and readiness for migration. The focus is on the ISPC requirements that personnel should consider in the migration of payment systems to the cloud. In addition, commercial cloud solutions are investigated and considered in

* Corresponding author.
E-mail addresses: alruwaili@su.edu.sa (F.F. Alruwaili), agullive@uvic.ca (T.A. Gulliver).

[1] The research of the first author was sponsored by Shaqra University, Shaqra, Saudi Arabia.

https://doi.org/10.1016/j.jisa.2017.11.004
2214-2126/

Table 1
Cloud deployment and service models.

Cloud Deployment Models	**Private**	The cloud services are exclusively provisioned to a single organization. These services are managed by the organization or delegated to a third party.
	Community	The cloud services are provided to and shared by multiple organizations who have agreed to share similar concerns, e.g. mission, policy, security requirements, and compliance.
	Public	The cloud services are provided for public use so that multiple organizations can share cloud resources using a multi-tenancy model.
	Hybrid	The cloud services are provided as a combination of two or more of the above deployment models. These models retain their unique attributes but are bound together by standardized or proprietary technology.
Cloud Service Models	**Infrastructure as a Service (IaaS)**	Cloud service provider provisioning of processing instances, storage, network, and other computing infrastructure resources.
	Platform as a Service (PaaS)	Cloud service provider provisioning of middleware, programming tools, operating systems, and other tools.
	Software as a Service (SaaS)	Cloud service provider provisioning of their deployed cloud applications.

the migration assessment. These solutions are (1) threat intelligence, i.e. evidence-based knowledge including threat indicators, implications, and actionable advice about existing and emerging cyber security threats, and (2) eLearning systems, i.e. a system that administrates, documents, distributes, tracks, monitors, and reports user awareness assessments.

2. Related Work

Computing security is a major concern of organizations and government agencies considering migrating IT resources, e.g. email services, business process management, threat intelligence, security operations, training and awareness, and applications, to the cloud [9]. Migrating to the cloud can provide benefits such as flexibility and scalable on-demand IT services [10]. Further, the cost of IT operations and maintenance can be significantly reduced. However, there are few case studies that investigate the migration of IT capabilities to the cloud [11]. Moreover, the implications of cloud services from an enterprise and business perspective have not been well understood [12].

In [13], several potential benefits in moving to the cloud were identified. These benefits were viewed from a managerial perspective such as improved employee and customer satisfaction, opportunities to develop new applications, and reduced operational costs. Understanding these benefits and their associated risks are far from straightforward, so a conceptual framework was introduced to assist organizations in determining the cost, suitability, and impact of adopting cloud services. However, the challenges of cloud security and privacy were not addressed, and these have a significant influence on cloud migration [14]. Many security experts believe that organizations hosting their data and applications on the internet and/or public cloud are vulnerable to threats and cybercrime [15]. Therefore, examining the potential benefits and drawbacks of cloud services and assessing organizational readiness is a goal of this paper.

In [16], a forensic readiness model based on cloud capabilities was presented. This model allows cloud service providers to manage and deliver the data needed for digital forensic investigations. These investigations are important components of information security programs and incident response activities. A number of techniques have been designed for readiness assessment, such as the tools and models described in the WEF 2009–2010 global information technology report [17] and the Waseda University world e-government ranking [18]. However, these approaches are limited to evaluating the readiness of data for forensic analysis. A comprehensive approach is needed to address security and privacy concerns and the compliance status of cloud services.

In [33], the critical security factors that affect Saudi Arabia government agencies deciding to adopt cloud technology were examined. A framework was constructed to investigate cloud security risks and features and analyze their influence on cloud adoption. However, this framework can only identify and confirm, via expert review, the factors that are significant to the implementation of cloud services. In [34], a similar framework was presented to identify and analyze the influence of a set of key critical success factors (CSFs) to the migration of Saudi Arabia universities to the cloud. Nevertheless, readiness assessment for migration was not considered and security and success factors were only investigated for the educational services sector which differs significantly from the financial industry. Hence the focus of this paper is on the financial sector.

A survey was conducted with 147 members of healthcare organizations from Malaysia, Saudi Arabia, and Pakistan to assess their confidence in secure cloud healthcare services as an emergent technology [35]. The results indicated that there is a direct relationship with the years of experience of the respondents to cloud security and privacy. This influences user decision to implement cloud-based healthcare systems. The results of a survey of four Saudi organizations was presented in [36] to determine the critical factors affecting cloud services adoption. It was found that 95% of the 169 respondents indicated that security is a critical factor impacting their cloud use decisions.

The study in [37] explored the impact and security significance of 70 public domains and cloud platforms in Saudi Arabia. The focus was on the application layer to ensure security safeguards throughout the entire software development life cycle (SDLC). While such work is effective in addressing application layer security issues, it cannot provide a holistic approach to assess the adoption of cloud services for payment systems, which is the subject of this work.

In [19], an ISPC readiness model was proposed to facilitate making decisions related to ISPC requirements. This model allows organizations to assess cloud risks based on the probability of threats occurring and their potential impact prior to and after migration. Both technical and non-technical issues were considered, i.e. payment technology, processes and procedures, and personnel awareness and readiness for cloud migration. In the case study presented here, an implementation of the ISPC readiness model and ISPC cubic controls [20] is used to evaluate migration readiness and the decision-making process.

3. Case Study

A case study was conducted to examine the feasibility of cloud service implementation in the financial industry. The Saudi Arabia central bank governs all electronic bill payment transactions in the region. It is dedicated to streamlining electronic billing and payment systems operations while employing the highest information security standards and risk management principles. The agency currently employs a system developed in-house for