Risks in Adopting Cloud Computing: A Proposed Conceptual Framework

Ali Al-Badi[1], Ali Tarhini[1(✉)], and Nabeel Al-Qirim[2]

[1] Information Systems Department, Sultan Qaboos University, Muscat, Oman
{aalbadi,alitarhini}@squ.edu.om
[2] Department of Information Systems and Security,
UAE University, Al Ain, UAE
Nalqirim@uaeu.ac.ae

Abstract. Cloud computing has become highly strategic and necessary technology in the IT industry. Cloud computing provide many benefits to organizations but there are risks associated with it which hamper its adoption. Therefore, it is important in this research identify the risks which negatively affect cloud computing adoption decision in order to accelerate its adoption. The research has reviewed relevant literature and accordingly selected fifty research papers from leading information systems journals and conferences. Accordingly, several critical factors were identified. The most important critical factors are grouped into three different categories namely, legal (data privacy, compliance and regulations), technical (bandwidth, data integration, security, vendor lock-in) and operational (loss of control over the services, lack of equipment and knowledge, business continuity and disaster recovery) risks. Finally, a conceptual framework on cloud computing adoption risks is proposed based on those identified factors. This research is of great importance to researchers, cloud computing professionals and policymakers. It will also help in formulating strategies to encourage the adoption and acceptance of cloud computing services, where cloud computing is still considered a risky endeavor and outcomes are seen as uncertain.

Keywords: Cloud computing · Adoption · Risk management
Cloud computing inhibitors · Cloud computing barriers · Deployment models
Service models · Framework

1 Introduction

Cloud computing has gained popularity in recent years. The benefits of the cloud computing include scalability, availability, and cost saving. The cloud computing adoption enable organization to gain competitive advantage in the market (Bisong and Rahman 2011). Several statistics shows the important growth and future of cloud computing. Globally 80% of enterprises will be using cloud computing service (IaaS) and private clouds by 2016 (Illsley 2014). Spending in public cloud will double to $127.5 by 2018 (Leopold 2014). Cloud computing has reshaped the way of managing and acquiring IT resources in more efficient and profitable ways (Phaphoom et al. 2015).

M. H. Miraz et al. (Eds.): iCETiC 2018, LNICST 200, pp. 16–37, 2018.
https://doi.org/10.1007/978-3-319-95450-9_2

There is a transformation of delivering IT services. The new cloud-computing paradigm helps enterprises concentrate more on their core businesses and hence, increasing their productivity. Cloud computing is based on existing technologies like virtualization and grid computing (Oliveira et al. 2014). Virtualization refers to the creation of virtual version of the computing resources like storage device, operating system and hardware platform that hides the physical characteristics of such resources. Grid computing refers to the aggregation of distributed systems available in different geographical locations allowing users to use the system from almost anywhere.

However, there are some risks associated with this technology. Enterprise Management Associates (EMA) study covered 400 IT professionals around the world. The findings showed that the major risks included difficulties in management of the cloud service, services downtime, cloud provider support, performance and pricing model (EMA 2014). Security, cost, compliance, cloud service reliability, and limited configuration are considered global challenges in cloud computing (Internap 2014). KPMG's international Global cloud survey found several adoption challenges such as data loss, lack of visibility on future costs, legal and regularity compliance and interoperability (KPMG 2013). Other researchers pointed to other challenges that potential clouds computing users should avoid (Dave 2013). According to Research in Action CIO revealed that hidden costs relating to cloud computing adoption an important factor as well.

Cloud computing enables organizations adapt to changing business environments (Armbrust et al. 2010). Around 94% of the CIO have accepted importance of cloud computing (Dave 2013). Nowadays many cloud services are available for free and used by many users, e.g., Dropbox, Google Doc and Google app., and social networking sites like Facebook (Bernard 2011).

Cloud computing offers many benefits to enterprise (Al-Qirim 2011; Phaphoom et al. 2015). The important advantages of cloud computing include on-demand self-service, ubiquitous network access, location-independent resource pooling, rapid elasticity, and measured service (Takabi et al. 2010). The basic characteristics of cloud computing are accessibility, ease of scale-up and -down of resources, and charging for the service based on consumption. The pay as you use model is an attractive method pushing the organization to adopt cloud computing. The cost saved by using cloud computing could be three to five times less than existing infrastructure (Han 2010). Cloud computing helps to reduce the up-front cost needed to purchase the hardware and software (Armbrust et al. 2010). The other advantage of cloud computing is data integration across the networks (Ali et al. 2016). While the adoption of cloud computing keeps growing, there are still some skepticisms about its advantages. Existing research highlighted factor that are hindering cloud computing adoption such as data security, loose of control over the IT service, regulatory and compliance issues, lack of experience and knowledge about it from business and IT managers, compromised accounts' details and business continuity and disaster recovery challenges (Priyadarshinee et al. 2017). The same authors found perceived IT security risk (PITR), risk analysis (RA), technology innovation (TI), management style (MS) and trust (T) as main challenges in cloud computing adoption. Ackermann (2012) reported that IT security risks as important factors in cloud computing adoption. There is a relationship between perceived IT security risk and cloud computing adoption (Haile and Altmann 2016).

The risks associated with cloud computing from customers' point of view consisted of unavailability of data, unauthorized access to data (damage, modification, disclosure of data), non-provision of services (outages, defects, not ensuring continuity and restoration of services) (Fortinová 2013). In Saudi Arabia privacy, trust, and security are reported as important determinants of cloud computing adoption in private sector (Alkhater et al. 2018). Another kind of risk is the high amount of capital needed to invest in cloud computing (Ali et al. 2016). Cloud computing usage amongst government agencies is less than the private sector as they are more concerned about data security and risks of exposing their sensitive data to untrusted entities (Ali et al. 2016).

Given the gloom surrounding cloud computing research and its results, it is hoped here to focus on deterrents only as a proxy here to detect for cloud computing adoption. Therefore, by focusing on deterrents, the research will identify the factors that affects negatively cloud computing adoption decision. The problem that this research is attempting to resolve here is to shed more light on the relationship between such impediments and cloud computing adoption (Khajeh-Hosseini et al. 2010). The literature reported that IT managers fail to take decisions about adopting new technologies (Bisong and Rahman 2011). It is hypothesized here that by capitalizing on deterrents alone, this will provide sufficient help and guidelines for IT managers to mitigate risks and improve their adoption decisions.

The research aims to answer the following two questions:

1. What are the major risk-factors that influence the decision to adopt cloud computing?
2. What precautions are required to mitigate such risks associated with cloud computing adoption?

Cloud computing has been investigated from different perspectives: organizational level, individual level and technical level relating to cloud services specifics (IaaS, PaaS, SaaS). This study is limited to the adoption of cloud computing at the organization level only. The objective of this research is to identify the different cloud computing risks that influence cloud computing adoption decisions in organizations. The research will examine the influencers of cloud computing adoption (independent variables) from four different aspects technical, security, financial and legal and organization.

2 Literature Review

This section describes the cloud computing concepts, cloud-computing trends, cloud computing risks and, proposed conceptual framework.

2.1 Cloud Computing Concepts

Cloud computing has attained greater popularity in recent years. Cloud computing is defined by NIST 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. This cloud model is composed of five essential characteristics, three service models, and four deployment models" (Mell and Grance 2011). There are four deployment methods:

1. *Public Cloud*: The ownership of the infrastructure is dedicated to the cloud provider. Amazon, Microsoft Azure and Rackspace are example of public cloud providers.
2. *Private Cloud*: The services are offered to specific client through private network. The offered e.g., hardware service is dedicated to one client in a single-tenant environment. Normally this method is used with the application that contain sensitive data especially for government and legal organizations. Therefore, it ensures the full control in the hand of the organization. The infrastructure is owned by the organization itself.
3. *Hybrid Cloud*: It is a combination of two or more private, public or community clouds. Normally, the organization will keep the critical application as private. Here the organization can control the cost and keep the security at an acceptable level based on the organization requirements.
4. *Community Cloud*: The cloud infrastructure is shared by many organizations, which have similar requirements like policy and compliance standards. The ownership of the infrastructure can be on one or more inside the community.

There are three main service models of cloud: Software as Service (SaaS), Platform as Service (PaaS), and Infrastructure as Service (IaaS).

1. *Software as Service (SaaS)*: Applications or software's are hosted somewhere and delivered via web browser like Google Doc, Salesforce CRM and Microsoft Exchange. Usually the cloud provider offer the software based on the user demand through license model. It eliminates the upfront investment by charging the user per usage and demand. Also, clients don't spend effort and time in the software support, maintenance and patch since it is provider's responsibility. Normally, the user cannot change the basic configuration of the software since it is provider's accountability. For example, web content management, social networking and video conferencing.
2. *Platform as Service (PaaS)*: It provides a platform that allows developing, running and deploying the application without maintaining the low-level infrastructure. The PaaS consists of a set of a development environment (servers used by programmers to continuously develop applications), testing and/or Q&A environment (set of servers is used by testers) (Fortinová 2013). Google app Engine and Microsoft Azure are example of the PaaS. These allow the developers or customers to manage database, application server and other middleware remotely. Therefore, the cloud client can develop the application without installing the software or purchasing any hardware. The cloud providers provide all required development toolkits, which help to eliminate any upfront cost for buying hardware or software and saves time. The potential risk of this service model is that each provider has its own platform and development language and this creates difficulties to move to another vendor.
3. *Infrastructure as Service (IaaS)*: It provides full infrastructure services such as server, storage, virtualized resources over the internet like virtual machine and

operating system instead of buying the physical hardware and software in the house. These allow organizations to respond quickly to the change through scaling up and scaling down easily. Amazon Elastic Compute Cloud (EC2) and Rackspace are example of IaaS. The implementation of IaaS depends on virtualization technologies, as well as grids or clusters (Fortinová 2013).

The importance of the cloud is derived from its essential characteristics. The basic characteristics of the cloud computing according to NIST definition (Mell and Grance 2011) are as follows:

- *Self-Service* (Client can provision and de-provision cloud services without human interaction. Client can order and manage cloud services through web page).
- *Broad Network Access* (Cloud services can be accessed through network through internet) *Resource Pooling* (Cloud computing resources like storage, virtual machine, memory and processing are shared among different clients)
- *Elasticity* (Client can scale up and down computing resources)
- *Measured Service* (Client can control and optimize the usage of the cloud services. Pay as you use model used to calculate the client service usage)

2.2 Cloud Computing Trends

Several statistic data shows positive trend towards cloud computing adoption around the world. More than 60% of the organizations will have half of the infrastructure on the cloud-based platform by 2018 (McNee 2014). Software as a service (SaaS) is expected to continue at 20% rise each year throughout 2018 (Comella-Dorda et al. 2015).

Cloud computing is highly beneficial to clients, reduced investment cost in infrastructure, offer increased scalability, improve accessibility from anywhere and anytime, and reduced the number of needed skilled employees (Erl et al. 2013, Siefker and Lucas 2013). Cost reduction is considered as the most important benefit (KPMG 2013). Pay as you use in cloud computing allows charging the clients as resources used on hourly basis. Thus saving costs as compared to the high cost of owning the hardware or software (Armbrust et al. 2010). The other type of benefits include time saving to implement new solutions and avoid over provisioning of the resources (Archer 2015). Cloud computing adoption is influenced by flexibility, accessibility, and low investments at the beginning of the project (Wease et al. 2018, Nayar and Kumar 2018). But moving from traditional to cloud computing system is still seen as a challenge (Al-Shamsi and Al-Qirim 2016; Fahmideh and Beydoun 2018). Security and privacy are the main issues (Ahmad and Jolly 2018, Garrison et al. 2018) such as security challenges in the integration of Internet of Things (IoT) and cloud computing (Stergiou et al. 2018).

Cloud based services can eliminate the up-front cost of the hardware and software. It enables the organizations focus more on their business. Moreover, cloud providers help focus on applying the security procedures in more effective and efficient manner, since it is a centralized environment. System availability in multiple locations is ensured in the cloud.

2.3 Cloud Computing Risk

This section provides an overview of previously published research in cloud computing risks. Those are slit into two parts. Firstly, the articles published by IT companies on the inhibitors and risks of adopting cloud computing. Secondly, this part discusses the research that explored the risks associated with cloud computing adopting decisions. In addition, cloud computing adoption risks are presented in a frequency table (below) to understand the common risks.

Most of the past research studies have not illustrated risks as a challenge to cloud computing adoption (Priyadarshinee et al. 2017). According to a research conducted by "Research in Action", 79% of the CIOs were suspecting hidden costs as hindering cloud computing adoption. The CIOs were also concerned about the performance that would negatively affects user experience (Siefker and Lucas 2013). Low performance is one of the reported obstacles in cloud computing adoption (Armbrust et al. 2009). A survey conducted by Symantec concluded that potential users should avoid risks before adopting cloud computing (Dave 2013).

It is difficult to restore the backup data from the cloud and confidential information are often exposed (Dave 2013). Vendor lock or interoperability is another concern for the client (Ghanam et al. 2012, Marinescu 2013). Lack of standards among the different vendors force the client to tie with one vendor (Marinescu 2013). Enterprise Management Associates surveyed 400 IT professionals around the world and concluded that the major risks faced by clients were difficulties in management of the cloud service, services downtime, cloud provider's support, performance and pricing models (EMA 2014).

Internap Network Services Corporation released findings of its global survey showing challenges and risks faced by cloud clients which included security, compliance, cost increase, compliance, cloud service reliability and limited configuration (Internap 2014). KPMG international Global cloud survey addressed the adoption challenges, including data loss, lack of visibility of the future cost, legal and regularity compliance and interoperability (KPMG 2013). In 2014, there was a downtime and service outage in the cloud services e.g., Microsoft Azure service storage went down for 10.89 h, Google cloud computing platform went down for 4 h and Amazon storage services went down for fewer than 5 h (Coldewey 2014). Table 1 highlights important cloud computing risks as discussed by articles published by the IT industry.

Risks in Moving to Cloud Computing from an Industrial Viewpoint

Evaluating the business perspective in the cloud is another study where the report listed cloud trends, factors deriving transformation, workforce mobility, cloud and data analytical, cloud challenges and tips to raise the success of cloud transformation (KPMG 2014). The cloud security alliance noted that data security as the top barrier to cloud adoption (Coles et al. 2015). Enterprise Cloud Computing conducted a study in 2014 on cloud trends and challenges faced by decision-makers in planning and adoption phase, adoption drivers from business perspective and effects of cloud adoption on business strategy (IDGEnterprise 2014). The study of the future of cloud computing conducted by North Bridge and partners explored the key drivers, inhibitors and trends of cloud computing (NorthBridge 2014). Cloud Connect and Everest Group conducted a survey

Table 1. Industrial papers

S. no	Organization	Year	Method	Num	Geography	Cloud Computing Risks and their percentage
1	Cloud Security Alliance (CSA)	2015	Online questionnaire	212	Americas, Asia-Pacific (APAC), Europe-Middle-East-Africa (EMEA)	• Data Security (73%) • Loose of control over the IT services (38%) • Regulatory and compliance (38%) • Lack of experience and knowledge of business managers and IT (34%) • Compromised accounts (30%) • Business continuity and disaster recovery (28%)
2	KPMG	2014	Online questionnaire	539	United states, Asia-Pacific (APAC), Europe-Middle-East-Africa (EMEA), Latin and south America, Canada and Mexico	• Privacy and data loss (53%) • Risk of intellectual property theft (50%) • Impact on IT organization (49%) • Measuring the ROI (48%) • High cost of implementation (48%) • Legal and regulatory compliance (46%) • Integrity with existing architecture (46%) • Lack of clarity of total cost ownership (46%)

(*continued*)

Table 1. (*continued*)

S. no	Organization	Year	Method	Num	Geography	Cloud Computing Risks and their percentage
3	IDG	2014	Online questionnaire	1,600	Global	• Security (61%) • Integration challenge (46%) • Information governance (35%) • Measuring ROI (30%) • Meeting industry standard (27%) • Lack of vendor strategy on implementing the solution (20%) • Business leader not receptive the cloud solution (11%) • Employees are not receptive to the cloud (10%)
4	North bridge Venture Partners	2014	n-a	1358	Global	• Security (49%) • Regulatory and compliance (34%) • Vendor lock-in interoperability (29%) • Interoperability (17%) • Privacy (31%) • Reliability (22%) • Network bandwidth (25%) • Complexity (15%) • Expense (12%)

(*continued*)

Table 1. (*continued*)

S. no	Organization	Year	Method	Num	Geography	Cloud Computing Risks and their percentage
5	Cloud Connect and Everest Group	2013	Online questionnaire	302	EU	• Security (30%) • Integration of the cloud solution (27%) • Lack of budget for new initiatives • Fear of vendor lock (27%) • Lack of suitable cloud solution (25%) • Lack of management buy-in (24%) • Lack in house capability to evaluate cloud solution (24%) • Lack of attractive business cases for cloud adoption (22%)

on 2013. The objective of the survey was to identify the cloud adoption patterns, cloud adopting barriers and making decision patterns for cloud adoption (EversetGroup 2013). International Data Corporation (IDC) explored the status of cloud adoption and barriers such as security, loose of control over IT asset, and regulatory in the financial services and government entities (IDC 2015). Table 2 consolidates the cloud computing adoption risks as reported by different journal publications.

Risks in Moving to Cloud Computing from an Academic Viewpoint

Phaphoom et al. (2015) explored the major technical and security-related inhibitors to organizational adoption decisions of the cloud. The study consisted of 352 participants from different organizations. The study compared non-adopters' and adopters' perceptions. The study concluded that the major inhibitors were security, data privacy and portability. Another study identified the critical factors affecting cloud computing adoption decision by CIOs in hospitals in Taiwan (Lian et al. 2014). The study revealed data security, cost, top manager support, complexity and perceived technical competence as critical factors. Therefore, technology dimension is the most influential amongst the other dimensions (organization, environment and human) pertaining to cloud computing adoption (Liana et al. 2014). Oliveira et al. (2014) explored the factors that influenced cloud computing adoption in service and manufacturing sectors in Portugal using a questionnaire distributed to 369 firms. The theories of TOE

Table 2. Research papers

Dependent variable	Independent variables	Theory	Methods	Num	Geography	Key findings	Author
Adoption decision of cloud computing	Availability, portability, integration with current enterprise system, migration complexity, data privacy and security	–	Logistic regression	352	Europe, North America, Asia, Africa, Australia and south America	Security, data privacy and portability are the inhibitors factors for cloud adoption	(Phaphoom et al. 2015)
Adoption decision of cloud computing	Technological factor (Security, compatibility, complexity & cost) Human factor (CIO innovativeness, technical competence) organizational factor (management support, relative advantage, resources & benefits) environmental factors (government policy & industry pressure)	TOE and HOT-FIT	ANOVA and Mean Value	60	Taiwan	Most critical factors data security, cost, top manager support, complexity and perceived technical competence	(Jiunn-Woei Liana et al. 2014)
Cloud computing adoption	Technology (Technology readiness), organization (Top management support & firm size), environmental (competitive pressure and regulatory support), innovation (relative advantage, complexity & compatibility), security concern & cost saving	Diffusion of innovation (DOI) and TOE	Structural model	369	Portugal	Cost saving, relative advantage, complexity, technology readiness, top management support and firm size are significant factors to cloud adoption	(Oliveira et al. 2014)

(*continued*)

Table 2. (*continued*)

Dependent variable	Independent variables	Theory	Methods	Num	Geography	Key findings	Author
Cloud computing adoption	Technology (complexity, compatibility & relative advantage), Organization (technology readiness, top management support & firm size) and Environment (trading partner pressure, competitive pressure)	TOE	Logistic regression and principal component analysis	257	UK	Competitive pressure, complexity, technology readiness and trading partner pressure	(Anabel Gutierrez et al. 2015)

(Technology-organization-environment) and DOI (diffusion of innovation) are used to organize the different factors. The factors used in the TOE theory were technology readiness (Technology context), top management support and firm size (organizational context) and competitive pressure and regulatory support (environmental context). The factors used in the DOI were relative advantage, complexity and compatibility. Security concern and cost saving used as the factors affect relative advantage. The study revealed cost saving, relative advantage, complexity, technology readiness, top management support and firm size as significant determinants of cloud adoption (Oliveira et al. 2014). Gutierrez et al. (2015) investigated the factors that influence decision makers adopt cloud computing in UK by using TOE framework. The data collected through questionnaire from 257 decision makers and IT professional in UK. The factors used for analysis were complexity, compatibility, technology readiness, trading partner pressure, competitive pressure, relative advantage, top management support and firm size. Among the eight factors, competitive pressure, complexity, technology readiness and trading partner pressure were found to be significant. Table 3 shows the frequency of each risks reported by industrial and research papers

Conceptual Framework and Hypotheses Construction

Adoption of new technology is one of the complex issues in information systems research. It plays a significant role in the organization's ability to gain a competitive advantage. The decision to adopt new technology require clear understanding of its impact on the organization either positively or negatively. The adoption decision criteria need to be as much comprehensive as possible. Adoption of new technology such as cloud computing is complicated due to the numerous uncertainties in terms of captured value and risk-susceptibilities.

There are different theories used as a framework to determine the factors influencing the adoption decision. Many researches have used theories like diffusion of innovations theory (DOI) and the technological, organizational and environmental

Table 3. Frequency table

Risk name	Data security	Loose of control over IT service	Lack of experience and knowledge	Regulatory compliance	Compromised account	Privacy	Lack of clarity of total cost ownership in terms of ROI	High cost of implementation	Integrating with existing architecture	Meeting industry standards	Bandwidth	Vendor lock	Measuring the ROI	Reliability	Business continuity and recovery
Cloud security Alliance (CSA)	*	*	*	*	*									*	*
IDC	*	*		*											
KMPG	*			*		*	*	*					*		
IDG	*						*		*				*		
North bridge venture partner	*			*		*				*	*	*			
Cloud connect and event group	*		*						*			*			
Phapoom et al. (2015)	*					*						*			
Lian et al. (2014)	*								*						
Total	7	2	2	4	1	3	2	1	3	1	1	3	2	1	1

theory (TOE) as a comprehensive framework to identify the factors that affecting adoption decision. The DOI theory measures adoption by five factors: relative advantage, complexity, compatibility, observability and trial ability while the TOE framework is classified into three main categories: technical, organizational and environmental context. Both theories aid IT managers and decision makers understand the business values and risks of implementing new technologies. However, as this research focuses on the risks side of adopting cloud computing, none of these theories have been used in this research.

There are many studies on cloud computing risks and corresponding categories. There are 39 cloud computing risks and they are classified into four categories i.e., organizational, technical, legal and operational risks (Dutta et al. 2013). The studies conducted by (Alzadjali et al. 2015, Sharma et al. 2016, AlKharusi and Al-Badi 2016, Al-Harthy and Al-Badi 2014, Al-Musawi et al. 2015) highlight the challenges faced by decision makers in accepting cloud computing in Oman. The success of cloud computing depends upon providing effective and efficient solutions to risks associated with cloud computing security and privacy (Takabi et al. 2010). There are organizational, legal, security, technical, and financial risk. In this research, as per the risks identified in Table 3, the research framework in this research comprises of the following three components:

Organizational Risks: It assesses the impact of cloud adoption from an organizational aspect including IT employees and non-IT employees, IT planning, business and IT operations and IT governance and management.

Technical Risks: The complicated cloud infrastructure and inherent IT deficiencies that exists inside the organization can raise a set of technical risks during cloud computing adoption.

Legal Risk: The features of the cloud computing may lead to different legal issues relating to regulations and compliance policies, contracts, data privacy and intellectual property (Fig. 1).

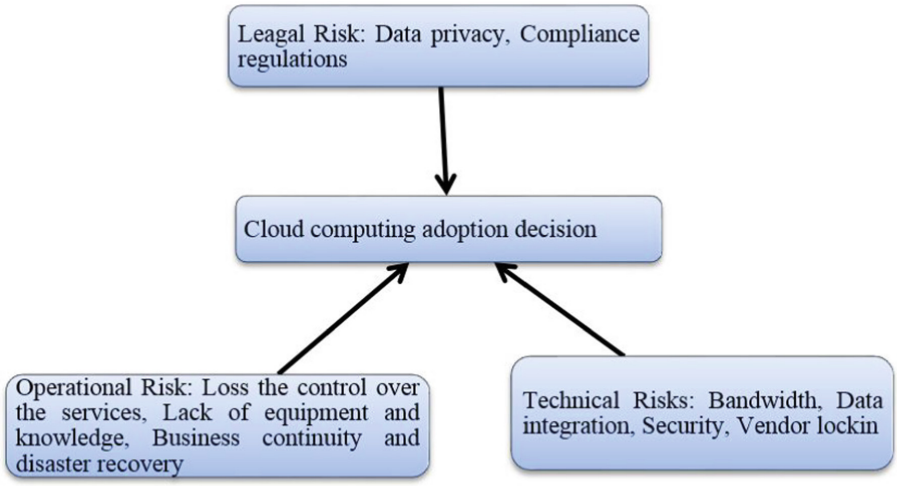

Fig. 1. Conceptual framework

The identified risks in the conceptual framework is presented as hypothesis such as H1, H2, H3, H4, H5, H6, H7, H8, H9, and H10:

Security: Cloud Security Alliance (CSA) in a survey distributed across 17 countries found that security of data was the greatest challenge for cloud adaptors (Coles et al. 2015). In general, there is unwillingness to allow confidential data be hosted outside the organization's firewall (Gnanasambandam. et al. 2014). One of the major adoption barriers in European countries is security (Porter 2015). In Tunisia, risk plays a mediating factor in cloud computing adoption (Hachicha and Mezghani 2018). Usually it is cited as the number one concern and resistance for cloud computing adoption (Armbrust et al. 2010, Akande et al. 2013). Accordingly, the following hypothesis is posited:

H1: Security risk negatively influences the cloud computing adoption decision.

Data Privacy: Data privacy was cited as one of the cloud computing adoption risks (Phaphoom et al. 2015, KPMG 2014, Donnelly 2015, Dutta et al. 2013). Privacy is directly related to security (Ali et al. 2016). Security was raised as the most important roadblock in the way of cloud computing adoption (Grobauer et al. 2011). Security and hence, trust needs to be shared between the different clients and service providers (Yeager and Morin 2018). Cloud providers should be responsible for the data once it is moved to the cloud (Phaphoom et al. 2015). The laws of protecting data vary from one country to another country which represents a challenge here. It creates inconsistencies in data protection between countries that generate the data and the country which store the data (Dutta et al. 2013). O'Donohue speaking at the Data Cloud Europe event claimed that the diversity of data protection laws is one of the legislative challenges that may prevent some EU members from accessing cloud services (Donnelly 2015). The cloud client should read the terms and conditions before moving to the cloud to avoid any legal issue. Accordingly, the following hypothesis is posited:

H2: Data privacy risk negatively influences the cloud computing adoption decision.

Vendor Lock-In or Portability: It refers to the difficulty of the cloud client to move from one vendor to another. It is considered as one of the risks that affect cloud computing adoption (Phaphoom et al. 2015, NorthBridge 2014, EverestGroup 2013). The decision of switching between cloud providers could be expensive and time taking (Siefker and Lucas 2013). The effort spent in customizing the solution with one cloud provider may requires redoing it again with another (Erl et al. 2013). Bringing back the service inhouse including data and applications is not an easy mission (Leavitt 2009). For example, there is no standard API (application programming interface) between the different vendors. The closed and different architecture and unique applications of the cloud services of the different vendors make switching between them a very difficult task for adopters (Gordon 2010, Phaphoom et al. 2015). Accordingly, the following hypothesis is posited:

H3: Vendor lock-in risks negatively influence the cloud computing adoption decision.

Bandwidth is defined as the amount of data transferred in a given time from one point to another. Basically, cloud computing is an internet based services and having

adequate bandwidth is therefore very essential. Adopting cloud is cost effective for hardware, software, maintenance and other services but could increase as the bandwidth increases (Leavitt 2009). Applications are becoming data-intensive which means that data going back and forth from a client to a cloud provider will require more bandwidth and hence, the cost will increase (Armbrust et al. 2010). Bandwidth remains an issue especially in developing countries (NorthBridge 2014). Accordingly, the following hypothesis is posited:

H4: Bandwidth risk negatively influences the cloud computing adoption decision.

Data Integration: Moving some systems to the cloud and keeping others in house creates data integration issues (Neske 2015). Integration with existing systems is considered one of the cloud computing risks (KPMG 2014, Phaphoom et al. 2015, EverestGroup 2013). Some organizations tend to adopt hybrid clouds, integrating private and public cloud that might address integration complexities (Kim et al. 2009, Phaphooma et al. 2015). Integration between partners require constant connectivity and standardization of data (Phaphooma et al. 2015). Accordingly, the following hypothesis is posited:

H5: Data integration risk negatively influences the cloud computing adoption decision.

Compliance and Regulations: Compliance is considered one of the major obstacles in adopting the cloud in North America and Asia Pacific (Gordon 2010). Compliance and regulations remain an inhibitor to moving to the cloud (Coles et al. 2015, KPMG 2014, NorthBridge 2014, IDC 2015). Organizations are subject to some regulations and compliance issues that must be met. The compliance is concerned with privacy, secure storage and disclosure of data. According to the cloud security alliance, clients face many cloud computing adoption risks including compliance. Once data moves to the cloud, organization needs to ensure that cloud providers apply the same compliance standards (Coles et al. 2015). Compliance and regulations are considered major barrier, especially for some organizations that have sensitive data like the financial sector and the government that need to keep data safe (IDC 2015). Accordingly, the following hypothesis is posited:

H7: Compliance and regulations risk negatively influence the cloud computing adoption decision.

Loose Control over IT Service: The on-premise allows the organization to have full control over the IT assets including the hardware and software. Moreover, the organization has the accountability for data security and access control as well. Moving to the cloud transfer these privileges to cloud providers (Morgan and Conboy 2013). The cloud provider is responsible for physical hardware, location, security, accessibility and other services (Sheppard 2014). Therefore, many organizations still deem this issue as an inhibitor to adoption (Coles et al. 2015, KPMG 2014). Accordingly, the following hypothesis is posited:

H8: Loose control over IT service risk negatively influence the cloud computing adoption decision.

Business Continuity and Disaster Recovery: According to the cloud security alliance, 28% of the respondents highlighted business continuity and disaster recovery as a barrier to cloud adoption (Coles et al. 2015). Business continuity refers to the procedure and polices that are put in place to ensures the essential functioning and processing of the organization's operations before and after a disaster. This includes disaster recovery processes that help the organization recover and restore their operations (Techopedia 2017). Accordingly, the following hypothesis is posited:

H9: Business continuity and disaster recovery risk negatively influence the cloud computing adoption decision.

Lack of Experience and Knowledge: Cloud based services require some training before acceptance. The lack of understanding of cloud, its benefits, and how to deal with it play a role in adopting cloud computing (Coles et al. 2015, IDC 2015). Many studies found that prior experience as important factor in technology adoption decisions. The IT staff's familiarity with cloud computing technologies like clustering and virtualization can influence the adoption decision (Alshamaila et al. 2013). Introducing cloud services in the organization may result in mustering employee's resistance if there is a lack of knowledge (Morgan and Conboy 2013). Accordingly, the following hypothesis is posited:

H10: Lack of experience and knowledge risk negatively influences the cloud computing adoption decision.

3 Research Methodology

The objective of this research is to identify as to what extent the different types of risks influences cloud computing adoption decisions and accordingly, proposes a conceptual adoption framework. Online databases such as Science direct, Scopus, Google scholar, Springer, and IEEE explore were searched to get relevant studies for this research. This study reviewed 50 research papers from leading information systems journals and conferences. The articles were searched and ordered based on the categories of risks in adopting cloud-computing services such as technical (data integration, security, vendor lock-in and bandwidth), legal (data privacy and compliance and regulation) and operational risks (lack of knowledge and experience, loose of control over IT service, and business continuity and disaster recovery).

4 Discussion

It has already been established that cloud computing numerous advantages. On the other hand, there are many researchers that raise alarming concerns about security and privacy issues. Therefore, providing effective and efficient solutions to risks related to cloud computing adoption could contribute to its success. The risks associated with cloud computing can be reduced by the following guidelines.

4.1 Avoiding Cost and Vendor Locks

The project and corresponding processes need to be studied thoroughly before implementing a cloud computing project. Clients often develop negative attitude towards cloud computing adoption due to recurring costs and costs related to moving to another cloud. Most of the recurring costs are related to the services and corresponding infrastructure. Therefore, top management must select the right cloud-service providers.

4.2 Clear and Defined Technical Contract and Service Level Agreement (SLAs)

The contracts between the cloud provider and clients must be detailed specifying exact roles and responsibilities. Legal consultations could be sought to craft a legally binding agreement. It should serve as a legally binding technical document for both parties to avoid litigations in the future.

4.3 Outsourcing and Authorization of Data

What part of the data belongs to the provider and what parts belong to the client must be documented to avoid conflicting data ownership and privacy issues. Only authorized persons are expected to access the data stored in the cloud. It is important to develop both technical and non-technical frameworks regarding data specifications, relationships and interrelationships. In case of data theft and leakage, proper legal frameworks must be available to protect the interests of clients.

4.4 Trust Building, Security, and Usage of Software and Programs

Trust is required between the different stakeholders of cloud computing. Cloud computing has a large amount of data uploaded every day and hence, cloud computing providers must ensure that the data does not go in the wrong hand e.g., a third party, without the owner's consent. The specific program and software running on the cloud that is used by a client cannot be transferred to another without the consent of that client. The security and privacy relating to the usage of software and hardware need to be shared between client and service providers only. For example, public clouds service providers are more responsible as compared to private ones in the case of SaaS. In PaaS, clients are more responsible for running and usage of programs on the platforms (Aleem and Al-Qirim 2012). In IaaS, the client is expected to ensure secure operating systems, applications, and content.

4.5 Management Decisions and Lack of Knowledge

Drafting proposer policies by policymakers influence cloud computing adoption decisions. The limited knowledge and the lack of understanding of cloud computing technology could lead to taking wrong adoption decisions. Such decision makers like top management are often have no IT background and hence, have limited awareness of

the new technology. This further aggravate the risks involved in cloud computing adoption decisions.

4.6 Data Integration, Bandwidth, and Disaster Recovery

Both clients and service providers share data integration and limited bandwidth risks. The client must ensure that the data is regularly updated from their sides while the service providers should ensure the consistency and visibility of the data irrespective of networks failure through e.g., backup plans. Also, it is the responsibility of client to have enough bandwidth for uninterrupted access to the cloud.

4.7 Compliance of Agreement and Regulations

It must be ensured that both clients and cloud service providers comply with the "legally" signed contracts and agreements relating to cloud computing services. The top management must study carefully review the past records of the service provider with respect to fulfillment and compliance with the agreement's roles and responsibilities. The security-risks must be covered in the SLAs between the client and the service provider (Rojas et al. 2018). Also, proper channels need to be established to guide pursuing and reporting violations (Hussain et al. 2018).

5 Conclusion

There is no doubt that cloud computing has gained significant attention from IT industries. Cloud computing provides more flexibility in the usage of IT services, help in cost reduction, and increase accessibility. Nevertheless, there are challenges which still hinders the adoption of cloud computing. This study suggests a conceptual framework for the smooth adoption of cloud computing. The framework provides different guidelines relating to cost-reduction, avoiding vendor's locking, having clear and defined contracts and agreements, outsourcing and authorization of data, trust building, security, and usage of software and programs, management decisions and lack of IT knowledge, data integration, bandwidth, and disaster recovery, compliance of agreement and regulations. The present study is theoretical in nature and hence, future empirical study will be conducted to assess the significance of the proposed model in detecting cloud computing adoption barriers.

References

Ackermann, T.: IT Security Risk Management: Perceived IT Security Risks in the Context of Cloud Computing. Springer, Wiesbaden (2012). https://doi.org/10.1007/978-3-658-01115-4

Ahmad, S.J., Jolly, R.K.: Immense implementation of Cloud Computing on distinct pilot projects as a specimen of the delineation of cost effectiveness to manifest as Cloud Computing democracy to be or not to be. GSJ **6**, 191 (2018)

Akande, A.O., April, N.A., Belle, J.-P.V.: Management issues with Cloud Computing. In: Proceedings of the Second International Conference on Innovative Computing and Cloud Computing. ACM (2013)

Aleem, S., Al-Qirim, N.: Cloud applications: a perspective on PaaS. In: The Proceedings of the 2012 International Conference on Business and Information (BAI2012), 3–5 July 2012, Sapporo, Japan (2012)

Al-Qirim, N.: A roadmap for success in the clouds. In: IEEE Explore and in the Proceedings of the 7th International Research Conference on Innovations in Information Technology (Innovations 2011), 25–27 April, Abu Dhabi, UAE (2011)

Al-Harthy, L.Y., Al-Badi, A.H.: To cloudify or not to cloudify. World Acad. Sci. Eng. Technol. Int. J. Soc. Behav. Educ. Econ. Bus. Ind. Eng. **8**, 2453–2464 (2014)

Al-Musawi, F., Al-Badi, A.H., Ali, S.: A road map to risk management framework for successful implementation of Cloud Computing in Oman. In: 2015 International Conference on Intelligent Networking and Collaborative Systems (INCOS), pp. 417–422. IEEE (2015)

Al-Shamsi, A., Al-Qirim, N.: Cloud healthcare-records manager. In: The Proceedings of the WorldCist 2016 - 4th World Conference on Information Systems and Technologies, 22–24 March 2016, Recife, PE, Brazil (2016)

Ali, O., Soar, J., Yong, J.: An investigation of the challenges and issues influencing the adoption of cloud computing in Australian regional municipal governments. J. Inf. Secur. Appl. **27**, 19–34 (2016)

Alkharusi, M.H., Al-Badi, A.H.: IT personnel perspective of the slow adoption of cloud computing in public sector: case study in Oman. In: 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), pp. 1–8. IEEE (2016)

Alkhater, N., Walters, R., Wills, G.: An empirical study of factors influencing cloud adoption among private sector organisations. Telematics Inform. **35**, 38–54 (2018)

Alshamaila, Y., Papagiannidis, S., Li, F.: Cloud computing adoption by SMEs in the northeast of England: a multi-perspective framework. J. Enterp. Inf. Manage. **26**, 250–275 (2013)

Alzadjali, A.M., Al-Badi, A.H., Ali, S.: An analysis of the security threats and vulnerabilities of Cloud Computing in Oman. In: 2015 International Conference on Intelligent Networking and Collaborative Systems (INCOS), pp. 423–428. IEEE (2015)

Gutierrez, A., Boukrami, E., Lumsden, R.: Technological, organisational and environmental factors influencing managers' decision to adopt cloud computing in the UK. J. Enterprise Inf. Manage. **28**, 788–807 (2015)

Archer, G.: Government CIOs see expected cloud cost savings evaporate (2015). https://www.cio.com.au/article/572878/government-cios-see-expected-cloud-cost-savings-evaporate/. Accessed 30 June 2017

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I.: A view of Cloud Computing. Commun. ACM **53**, 50–58 (2010)

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M.: Above the clouds: a berkeley view of Cloud Computing (2009)

Dutta, A., Peng, G.C.A., Choudhary, A.: Risks in enterprise cloud computing: the perspective of IT experts. J. Comput. Inf. Syst. **53**(4), 39–48 (2013)

Bernard, L.: A risk assessment framework for evaluating Software-as-a-Service (SaaS) cloud services before adoption, University of Maryland University College (2011)

Bisong, A., Rahman, M.: An overview of the security concerns in enterprise cloud computing (2011). arXiv preprint arXiv:1101.5613

Coldewey, D.: Google services suffer outage (2014). http://www.nbcnews.com/tech/internet/google-services-suffer-outage-n34986. Accessed 12 Apr 2015

Coles, C., Yeoh, J., Guanco, F., Mishra, E.: Cloud adoption practices & priorities survey report. Cloud Security Alliance, 9 (2015)
Comella-Dorda, S., Gnanasambandam, C., Shah, B., Strålin, T.: From box to cloud: An approach for software development executives. McKinsey & Company (2015). http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/from-box-to-cloud. Accessed 30 June 2017
Dave, D.: Avoiding the hidden costs of the cloud (2013). http://www.symantec.com/connect/blogs/avoiding-hidden-costs-cloud. Accessed 30 June 2017
Donnelly, C.: European Commission calls for cloud data protection law reforms (2015). http://www.computerweekly.com/news/4500247442/European-Commission-calls-for-cloud-data-protection-law-reforms. Accessed 30 June 2017
Dutta, A., Peng, G.C.A., Choudhary, A.: Risks in enterprise cloud computing: the perspective of IT experts. J. Comput. Inf. Syst. **53**, 39–48 (2013)
EMA. Casualties of Cloud Wars: customers are paying the price (2014). http://www.iland.com/wp-content/uploads/2014/06/EMA-iland_VMware_CloudWars-0614-WP.pdf. Accessed 12 Apr 2015
Erl, T., Puttini, R., Mahmood, Z.: Cloud Computing: Concepts, Technology & Architecture. Prentice Hall, Upper Saddle River (2013)
Everestgroup. Enterprise Cloud Adoption Survey 2013: Summary of Results (2013). http://www.everestgrp.com/wp-content/uploads/2013/03/2013-Enterprise-Cloud-Adoption-Survey.pdf. Accessed 30 June 2017
Eversetgroup Enterprise Cloud Adoption Survey 2013: Summary of Result (2013)
Fahmideh, M., Beydoun, G.: Reusing empirical knowledge during cloud computing adoption. J. Syst. Softw. **138**, 124–157 (2018)
Fortinová, J.: Risks of cloud computing. Systémová Integrace, 20 (2013)
Garrison, G., Rebman Jr., C.M., Kim, S.H.: An identification of factors motivating individuals' use of cloud-based services. J. Comput. Inf. Syst. **58**, 19–29 (2018)
Ghanam, Y., Ferreira, J., Maurer, F.: Emerging issues & challenges in cloud computing-a hybrid approach. J. Softw. Eng. Appl. **5**, 923 (2012)
Gnanasambandam, C., Sprague, K., Huskins, M.: Next-Generation IT Infrastructure. McKinsey & Company (2014)
Gordon, J.: Exploring the future of cloud computing: riding the next wave of technology-driven transformation. In: World Economic Forum, White Paper (2010)
Grobauer, B., Walloschek, T., Stocker, E.: Understanding cloud computing vulnerabilities. IEEE Secur. Priv. **9**, 50–57 (2011)
Gutierrez, A., Boukrami, E., Lumsden, R.: Technological, organisational and environmental factors influencing managers' decision to adopt cloud computing in the UK. J. Enterp. Inf. Manage. **28**, 788–807 (2015)
Hachicha, Z.S., Mezghani, K.: Understanding intentions to switch toward cloud computing at firms' level: a multiple case study in Tunisia. J. Global Inf. Manage. (JGIM) **26**, 136–165 (2018)
Haile, N., Altmann, J.: Structural analysis of value creation in software service platforms. Electron. Mark. **26**, 129–142 (2016)
Han, Y.: On the clouds: a new way of Computing. Inf. Technol. Libraries **29**, 87 (2010)
Hussain, W., Hussain, F.K., Hussain, O., Bagia, R., Chang, E.: Risk-based framework for SLA violation abatement from the cloud service provider's perspective. Comput. J. (2018)
IDC. Public Cloud Spending to Reach Nearly $70 Billion Worldwide in 2015 (2015). According to IDC. http://www.businesswire.com/news/home/20150721005355/en/Public-Cloud-Spending-Reach-70-Billion-Worldwide. Accessed 30 June 2017
IDG Enterprise 2014. IDG Enterprise Cloud Computing Study (2014)

Illsley, R.: The role of cloud in IT modernisation: the DevOps challenge. http://docplayer.net/10458737-The-role-of-cloud-in-it-modernisation-the-devops-challenge-ovum.html. Accessed 30 June 2017

Internap. Intrernap public cloud survey reveals performance as top challenge (2014). http://cloudtweaks.com/2014/01/internap-public-cloud-survey-reveals-performance-as-top-challenge/. Accessed 12 Apr 2015

Liana, J.W., Yenb, D.C., Wang, Y.-T.: An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. Int. J. Inf. Manage. **34**, 28–36 (2014)

Khajeh-Hosseini, A., Sommerville, I., Sriram, I.: Research challenges for enterprise cloud computing (2010). arXiv preprint arXiv:1001.3257

Kim, W., Kim, S.D., Lee, E., Lee, S.: Adoption issues for cloud computing. In: Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia, pp. 2–5. ACM (2009)

KPMG. The cloud take shapes (2013). http://www.kpmg-institutes.com/institutes/advisory-institute/articles/2013/02/cloud-takes-shape.html. Accessed 30 June 2017

KPMG. Elevating business in the cloud (2014). http://www.kpmginfo.com/EnablingBusinessInTheCloud/downloads/2014%20KPMG%20Cloud%20Survey%20Report%20-%20Final%2012-10-14.pdf. Accessed 30 June 2017

Leavitt, N.: Is cloud computing really ready for prime time? Computer **42**, 15–20 (2009)

Leopold, G.: Forecasts call for cloud burst through 2018 (2014). http://www.enterprisetech.com/2014/11/03/forecasts-call-cloud-burst-2018/. Accessed 19 Sept 2015

Lian, J.-W., Yen, D.C., Wang, Y.-T.: An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. Int. J. Inf. Manage. **34**, 28–36 (2014)

Marinescu, D.C.: Cloud Computing: Theory and Practice. Morgan Kaufmann, Boston (2013)

Mcnee, B.: Digital Business Rethinking Fundamentals. NYC: Saugatuck Technology (2014)

Mell, P., Grance, T.: The NIST definition of cloud computing. U.S. Department of Commerce (2011)

Morgan, L., Conboy, K.: Factors affecting the adoption of cloud computing: an exploratory study. In: 21st European Conference on Information Systems 2013 (ECIS), 5–8 June 2013. Utrecht University (2013)

Phaphooma, N., Wanga, X., Samuelb, S., Helmera, S., Abrahamssona, P.: A survey study on major technical barriers affecting the decision to adopt cloud services. J. Syst. Softw. **103**, 167–181 (2015)

Nayar, K.B., Kumar, V.: Cost benefit analysis of cloud computing in education. Int. J. Bus. Inf. Syst. **27**, 205–221 (2018)

Neske, D.: Hidden costs of the cloud: here is your umbrella (2015). http://services.ricoh.com/knowledge-center/blog/2015-02-25-hidden-costs-of-the-cloud-here-is-your-umbrella. Accessed 30 June 2017

Northbridge. The Future of the Cloud Computing (2014). https://www.slideshare.net/mjskok/2014-future-of-cloud-computing-4th-annual-survey-results. Accessed 30 June 2017

Oliveira, T., Thomas, M., Espadanal, M.: Assessing the determinants of cloud computing adoption: an analysis of the manufacturing and services sectors. Inf. Manage. **51**, 497–510 (2014)

Phaphoom, N., Wang, X., Samuel, S., Helmer, S., Abrahamsson, P.: A survey study on major technical barriers affecting the decision to adopt cloud services. J. Syst. Softw. **103**, 167–181 (2015)

Porter, S.: The state of cloud computing in Europe (2015). http://www.thoughtsoncloud.com/. Accessed 19 Sept 2015

Priyadarshinee, P., Raut, R.D., Jha, M.K., Gardas, B.B.: Understanding and predicting the determinants of cloud computing adoption: a two staged hybrid SEM - Neural Networks Approach. Comput. Hum. Behav. **76**, 341–362 (2017)

Rojas, M.A.T., et al.: Managing the lifecycle of security SLA requirements in cloud computing. In: Rocha, Á., Reis, L.P. (eds.) Developments and Advances in Intelligent Systems and Applications. SCI, vol. 718, pp. 119–140. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-58965-7_9

Sharma, S.K., Al-Badi, A.H., Govindaluri, S.M., Al-Kharusi, M.H.: Predicting motivators of cloud computing adoption: A developing country perspective. Comput. Hum. Behav. **62**, 61–69 (2016)

Sheppard, D.: Is loss of control the biggest hurdle to cloud computing? (2014). http://www.itworldcanada.com/blog/is-loss-of-control-the-biggest-hurdle-to-cloud-computing/95131. Accessed 30 June 2017

Siefker, K., Lucas, J.: Hidden cost of cloud computing (2013). http://investor.compuware.com/releasedetail.cfm?ReleaseID=777461. Accessed 12 Apr 2015

Stergiou, C., Psannis, K.E., Kim, B.-G., Gupta, B.: Secure integration of IoT and cloud computing. Future Gener. Comput. Syst. **78**, 964–975 (2018)

Takabi, H., Joshi, J.B., Ahn, G.-J.: Security and privacy challenges in cloud computing environments. IEEE Secur. Priv. **8**, 24–31 (2010)

Techopedia. Business continuity and disaster recovery (BCDR) (2017). https://www.techopedia.com/definition/13767/business-continuity-and-disaster-recovery-bcdr. Accessed 30 June 2017

Wease, G., Boateng, K., Yu, C.-J., Chan, L., Barham, H.: Technology assessment: cloud service adoption decision. In: Daim, T.U., Chan, L., Estep, J. (eds.) Infrastructure and Technology Management. ITKM, pp. 447–471. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-68987-6_16

Yeager, W.J., Morin, J.-H.: Introduction to the minitrack on security and critical infrastructure for Cloud, IOT and Decentralized trust. In: Proceedings of the 51st Hawaii International Conference on System Sciences (2018)