JOURNAL OF INFORMATION SECURITY AND APPLICATIONS 27-28 (2016) 19–34

Available online at www.sciencedirect.com

ScienceDirect

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

An investigation of the challenges and issues influencing the adoption of cloud computing in Australian regional municipal governments

Omar Ali *, *Jeffrey Soar*, *Jianming Yong*

School of Management and Enterprise, University of Southern Queensland, Toowoomba, Australia

ARTICLE INFO

Article history:
Available online 11 December 2015

Keywords:
Challenges
Issues
Adoption
Cloud computing
Regional councils

ABSTRACT

New developments in information technology (IT) provide opportunities for a better quality of life through benefits such as increased comfort and convenience. Compared to dedicated infrastructures such as cluster and grid computing, cloud computing can better cater to users' needs by increasing effectiveness, efficiency and functionality at a potentially lower cost. This research aims to provide insights into the challenges and issues faced by implementers and users of cloud computing by comparing the extant literature about this issue with current insights provided by IT managers. A systematic literature review and in-depth interviews with IT managers in local government councils were conducted for this research. The research indicated that the factors in the extant literature were supported; additional challenges and issues emerged which are related to effective network, data storage location, availability of different service providers, policy makers, a limited understanding of the cloud and business transformation. The findings of this research are expected to assist managers to evaluate possible adoption and increase their awareness about challenges and issues that influence the cloud adoption when planning to adopt it.

1. Introduction

Cloud computing, a recent development in information and communication technology (ICT), has superseded some older technologies such as virtualisation, utility computing, elasticity, distributed computing, and grid computing (Wang et al., 2011). It offers simplicity and potential for scalability, reliability and high performance service delivery at a relatively low cost (Ali et al., 2015a; Mell and Grance, 2009; NIST, 2009). Cloud computing is changing the way industries and enterprises do their businesses in that dynamically scalable and virtualised resources are provided as a service over the Internet; it offers new opportunities for enterprises (Xu, 2012).

Growth in the adoption of cloud computing is expected (Opitz et al., 2012); predictions for growth range from $46.3 billion reported in 2008 to $148.8 billion and $150 billion by 2014 and $222.5 billion market by 2015 (Opitz et al., 2012). Cloud computing spending is predicted to grow from $16 billion in 2008 to around $55 billion in 2014 (Gens, 2010; Leavitt, 2009). The expectations of the business with cloud computing are high and it is important for organisations to consider the potential benefits for their operations (Opitz et al., 2012). There is an expectation that 7.1 percent of total ICT spending in Australia in 2015 will be directly cloud related, up from 2.8 percent in 2011; this will be a net increase in value of around $4.3 billion (IT Industry Innovation Council, 2011).

Research about cloud computing in the public sector in general is limited (Janssen and John, 2011). There is research

* *Corresponding author.* School of Management and Enterprise, University of Southern Queensland, Toowoomba, Australia. Tel.: +61411593870.
E-mail address: Omar.Ali@usq.edu.au (O. Ali).

http://dx.doi.org/10.1016/j.jisa.2015.11.006

on the challenges and issues of cloud computing in relation to security, privacy, trust issues (Ali and Soar, 2014; Buyya et al., 2011; Ghanam et al., 2012; Kim, 2009; Takabi et al., 2010), and policies (Ali et al., 2015a, 2015b; Jaeger et al., 2008; Tweneboah-Koduah, 2012). There is a lack of exploratory studies that provide an in-depth and holistic investigation of all the actual challenges and issues in a relation to cloud computing adoption (Low et al., 2011; Misra and Mondal, 2011). That is, we could not find any studies that listed all challenges and issues and explained why and how they are influencing the adoption of cloud computing.

Despite its potential benefits, the adoption rate of cloud computing in regional municipal government sectors in Australia has been lower compared to urban areas (IT Industry Innovation Council, 2011). The paucity of empirical studies about challenges and issues to cloud computing adoption in Australian regional municipal governments has hindered understanding and thus strategy development to improve its adoption (IT Industry Innovation Council, 2011). This situation has prompted regional municipal governments to request further research related to challenges and issues that influence the adoption of cloud computing with the purpose to guide their cloud adoption and implementation decisions (Department of Innovation Industry Science and Research, 2011). The current gap in the literature has led us to the following research problem: What are the actual challenges and issues that influence the adoption of cloud computing in Australian regional municipal governments.

This research identifies and provides an overview of the challenges and issues affecting the adoption of cloud computing in Australian regional municipal governments. The paper provides an overview of cloud computing, a report on a systematic literature review and a report on interviews with IT managers in Australian local government councils about their opinions on the challenges and issues that influence the adoption of cloud computing. Then, we conclude this paper with contributions, research limitations, future research, and conclusions.

2. The basic concept of cloud computing

Cloud computing has been a paradigm shift in the IT domain (Kantarcioglu et al., 2011). It is the result of significant innovations in virtualisation, utility computing, distributed computing, grid computing, storage, content outsourcing, security, Web 2.0, and networking (Catteddu and Hogben, 2009). The most widely used definition of the cloud computing model is introduced by the U.S. National Institute of Standards and Technology (NIST, 2009) as:

> *"A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of services (for example, networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".*

The NIST definition recognises the availability of cloud computing and describes its five essential characteristics: on-demand self-service; broad network access; resource pooling; rapid elasticity; and measured service (NIST, 2009).

Cloud services can be categorised on the basis of the following three service/delivery models: Software as a Service; Platform as a Service; and Infrastructure as a Service (Ali et al., 2014; Buyya et al., 2011; Cloud Security Alliance, 2009; Mell and Grance, 2009). Software as a Service (SaaS) enables consumers to use the service provider's applications running on a cloud infrastructure. Consumers can access the applications using various client devices through a client interface such as a Web browser. Consumers have access to limited user-specific application configuration settings and cannot manage or control the underlying cloud infrastructure such as its network, servers, operating systems or storage (Clemons and Chen, 2011; Cloud Security Alliance, 2010; Mell and Grance, 2009; Velte et al., 2010; Wang et al., 2008).

The Platform as a Service (PaaS) model of cloud computing is somewhat similar to the SaaS model. This model enables the consumer to deploy consumer-created or -acquired applications onto the cloud infrastructure with the help of programming languages and tools the provider supports. Just like the SaaS model, the consumer does not manage or control the underlying cloud infrastructure, but can control the deployed applications and possibly the application-hosting environment configurations (Cloud Security Alliance, 2010; Dillon et al., 2010; Velte et al., 2010).

The third platform, Infrastructure as a Service (IaaS), provides the consumers with processing, storage, network and other fundamental computing resources (Bhardwaj et al., 2010). The consumer can deploy and run arbitrary software, including operating systems and applications. Like the other two models, the consumer cannot manage or control the underlying cloud infrastructure but has control of the operating systems, storage and deployed applications and possibly has limited control over select networking components, such as host firewalls (Bhardwaj et al., 2010; Cloud Security Alliance, 2010; Mell and Grance, 2009; Sohan and Zeng, 2010).

There are believed to be four cloud deployment models: public; private; community; and hybrid (Ali et al., 2014; Catteddu and Hogben, 2009; Cloud Security Alliance, 2009; Dustin-Amrhein et al., 2010; Mell and Grance, 2009). Public cloud enables the cloud infrastructure to be made available to the general public. The infrastructure is owned by an organisation that provides cloud services (Dustin-Amrhein et al., 2010). In the private cloud model, the cloud infrastructure is deployed solely for a single organisation. The organisation may itself manage the infrastructure or outsource it to a third party, and the cloud infrastructure may exist in the organisation's premises or be based off-premise (Armbrust and Fox, 2009; Dustin-Amrhein et al., 2010). Community cloud deploys the cloud infrastructure to several organisations at the same time and supports a specific community that shares similar concerns. The cloud infrastructure may be managed by the organisations or by a third party and may exist in the organisations' premise or be based off-premise (Dustin-Amrhein et al., 2010). In the hybrid cloud model the cloud infrastructure is composed of two or more clouds (private, community or public) that remain unique entities but are bound together by standardised or proprietary technology that enables data and application portability (Cloud Security Alliance, 2009).

Despite the potential advantages provided by cloud computing, there are still several challenges and issues for its

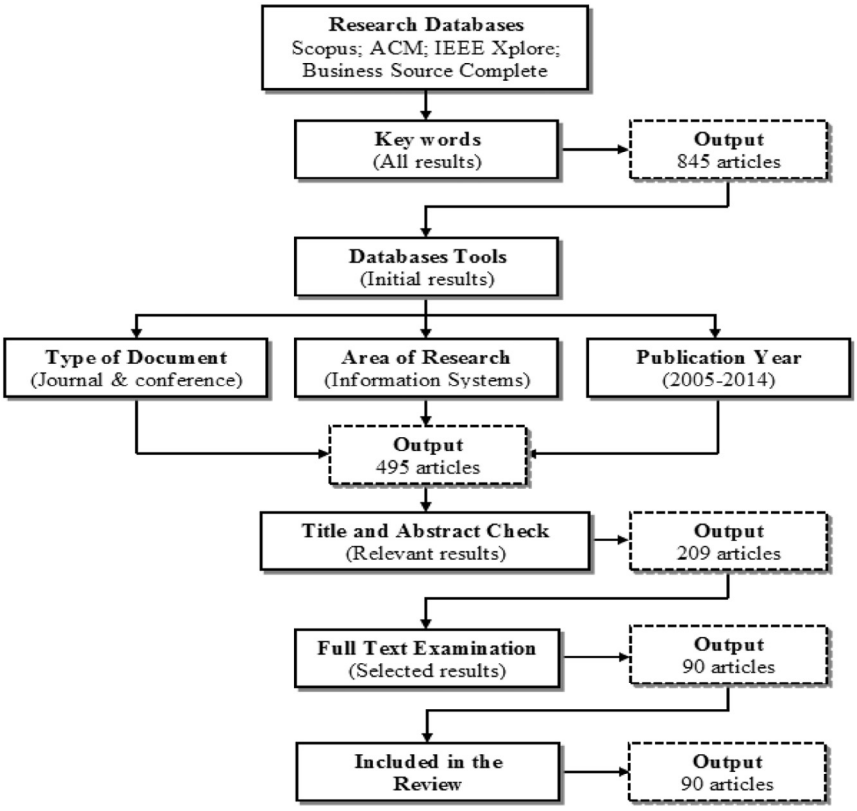

Fig. 1 – Research strategy steps (Pucher et al., 2013).

adoption in the public sector (Catteddu and Hogben, 2009; Martucci et al., 2012; Reed et al., 2011). Cloud computing is still considered to be in the early adoption stage (Lyer and Henderson, 2010; Vaquero et al., 2008). Concerns about cloud computing relate to security, privacy and trust issues (Paquette et al., 2010; Subashini and Kavitha, 2011). Security is about protecting data from unauthorised access, and privacy refers to who is allowed to access data, while trust refers to the security and privacy of the data. All of these are critical concerns for organisations (Paquette et al., 2010; Subashini and Kavitha, 2011). The challenges and issues that emerge while implementing cloud computing in the public sector include security issues such as access; availability and backup; control over data lifecycle; and audit (Ali and Soar, 2014; Chen and Zhao, 2012; Harauz et al., 2009; Joint et al., 2009; Pearson, 2009). There are privacy issues such as lack of user control; unauthorised secondary usage; and trans-border data flow and data proliferation (Ali and Soar, 2014; Chen and Zhao, 2012; Harauz et al., 2009; Joint et al., 2009; Pearson, 2009; Verma and Kaushal, 2011); and trust is a significant issue (Ali and Soar, 2014; Karaoglanoglou and Karatza, 2011; Mathur and Nishchal, 2010; Tian et al., 2010).

3. Data collection and analysis method

3.1. *Systematic literature search process*

The systematic literature review began with the computer-based sources including Scopus, ACM Digital Library, IEEE Xplore, and Business source complete. These databases were selected because they provided accessible volumes of research papers relating to challenges and issues that influence the adoption of cloud computing. Researchers believe that these databases include a representative sample of the literature produced in the subject matter as pertinent to this research.

The electronic literature search was conducted on August 27, 2013 until April 11, 2014 and followed the approach of Pucher et al. (2013). This search process had five strategies (see Fig. 1). The *first strategy* was the selection of the exact key words that covered the research topic. The researchers must use the AND; OR; NOT; and the truncation symbol * all work in Web of Science (Golder et al., 2014; Higgins and Green, 2011). The search terms that were used to mine data from these databases included the following key words: “cloud computing” AND “challenges and issues” AND “adoption” OR “factors affecting” AND “government” OR “public sector” AND “Australia”. These key words were researched on their own or in combination with others.

The *second strategy* was to select more than two databases to increase sensitivity (Lopes, 2002; Pucher et al., 2013; Shea et al., 2007). The main databases that the researchers employed for the systematic literature section are the four above mentioned databases. The *third strategy* was to use all available tools of each database to limit the research results by selected published year (2005–2014), area of research (Information Systems) and type of document (Aleixandre-Benavent et al., 2011; Golder et al., 2014; Higgins and Green, 2011). The *fourth strategy* was to check the title and abstract of articles (Golder et al., 2014; Higgins and Green, 2011; Pucher et al., 2013)

Table 1 – Results on databases.

Database	Key Words	All results	Initial results	Relevant results	Selected results
Scopus	"cloud computing" AND	177	116	52	28
ACM Digital Library	"challenges and issues" AND	258	76	44	16
IEEE Xplore	"adoption" OR "factors affecting"	316	241	89	37
Business Source Complete	AND "government" OR "public sector" AND "Australia"	94	62	24	9
Total		**845**	**495**	**209**	**90**

to ensure that they match the goals of the research. The *fifth strategy* was to examine full texts of selected articles. In the final strategy the researcher must check methods, participant's details and the outcome of the selected articles for methodological rigour (Pucher et al., 2013). Fig. 1 illustrates the research strategy steps with the findings of each step.

3.2. *Systematic literature search criteria*

In order to evidence the database searches conducted, the research fields were narrowed to the main topic. Table 1 shows how many entries and results appeared on different databases and how the results were narrowed and selected. Table 1 is merely an example of the most common key words that mentioned above when searching the relevant topics. This table shows the major databases used in the research while indicating the initial results of the research, relevant results and the selected results for the research. Several changes in keywords gave various sources which have all been filtered through search options.

The approach produced a large number of articles (all results **845** articles). Database tools were used to limit the research results by selected published year, area of research, and type of document needed (initial results **494** articles). The next step was to check the title and abstract of articles to ensure that they match the goals of the research. These lists in Table 1 were then shortened by selecting only the articles relevant to the research question based on the review of their titles and their abstracts (relevant results **209** articles). The final step was to examine full texts of selected articles. In this step the researcher must check methods, participant's details and the outcome of the selected articles for methodological rigour. These selections shown in Table 1 were then scrutinised by doing an in-depth study and by analysing their contents, and the articles which contained the information considered suitable for citing in this research were selected (selected results **90** articles).

3.3. *In-depth interview process*

This research is exploratory, seeking to provide a qualitative overview of the concepts with the highest salience relating to challenges and issues that influence cloud computing adoption in Australian regional municipal governments. A series of in-depth interviews were conducted between May 13, 2014 and August 12, 2014. These obtained inputs from 24 top management levels: IT Manager (10); IT Coordinator (4); Technical Director (2); Information Service Manager (2); IT Officer (1); IT Consultant (1); IT Network Manager (1); Chief Information Officer (1); Enterprise Architecture Manager (1); and Team Leader ICT Operation (1). These occupational groups were selected based on the assumption that they represent key stakeholder groups likely to be responsible for planning and adoption of cloud computing for regional municipal governments.

Participating regional government councils were selected from all 77 local government councils that are dispersed around Queensland. According to the classification provided by LGAQ (2013), the 77 local government councils were separated into five different segments: Coastal, Resource, Indigenous, Rural/Remote and South East Queensland as shown in Table 2.

The principal motivation behind using these established segments is to investigate which of them has an effective communication infrastructure base to move to cloud computing and which do not and why. These segments are all further classified by size of the councils. The size of the councils is determined based on the number of employees in each local council. For example, extra small (less than 50); small (50–100); medium (100–250); large (250–750); and very large (750–1500). Based on the classification of the local councils, the researcher selected one local council from every classification and size to ensure inclusion of all segments to obtain a comprehensive overview of issues. Also, the sample reflects the geographical spread and size classifications of regional municipal governments throughout Queensland (Coastal with 29

Table 2 – Size classification.

Segments	Size classification					Total	%
	Extra small	Small	Medium	Large	Very large		
Coastal	0	1	2	2	1	6	25%
Resource	0	1	0	2	0	3	12%
Indigenous	0	2	2	0	0	4	17%
Rural/Remote	2	1	2	1	1	7	29%
South East Queensland	0	0	1	1	2	4	17%
Total						**24**	**100%**

percent; Resource with 14 percent; Indigenous with 10 percent; Rural/Remote with 29 percent; South East Queensland with 18 percent) as shown in Table 2.

To improve the reliability of this research, the process explained by Kirsch (2004) was followed; this defines a set of procedures: identify and select the research issues, determine who to interview and determine how the interviews will be conducted. An interview protocol was developed and used to guide the interview process. The interviewer followed a sequence of steps: Planning the interview, introductions at the commencement of the interview and establishing rapport with the respondent through small chat (Gaskell, 2000). Ethical clearance was obtained through the University Southern Queensland (USQ). Each interview was structured around four questions, with the interviewers asking probing questions based on responses. The questions required the participants to first describe their IT/IS role. Then, they were asked to describe their background, experience and knowledge in relation to cloud computing. The third section comprised a question about the length of time that they have been involved with cloud computing projects and in what capacity. Finally, they were asked to describe the actual challenges and issues that influence the adoption of cloud computing in Australian regional municipal governments.

The interviews lasted between 30 and 50 minutes. The interview questions were designed as largely open questions to encourage the interviewees to provide answers that revealed their attitudes and perceptions relating to the research topic (Carson et al., 2001). A total of 24 interviews were carried out with IT managers of the chosen local councils. The research reached the saturation level within the interview number 18, when the researcher notice that there is no more new information or patterns in the data emerging from the interview. Another six interviews were conducted to ensure inclusion of all segments and size classification of the local councils to obtain a comprehensive overview of issues (refer to Table 2). There were 21 interviews which took part in the analysis process. The other 3 interviews were excluded from the analysis process because it was discovered during the interview that these 3 IT managers did not come from an IT background and did not have any experience or knowledge related to cloud computing.

3.4. *Analysis methods*

The interview data were analysed using manual content analysis method (Miles and Huberman, 1984) and the visual text analytical software tool Leximancer (Smith, 2003; Smith and Humphreys, 2006). Manual content analysis was undertaken as a first step in the analysis which included three concurrent flows of activities: data reduction, data display and conclusion drawing/verification (Faust, 1982; Hsieh and Shannon, 2005; Miles and Huberman, 1984).

Data reduction refers to the process of focusing, transforming, selecting, abstracting, and simplifying the raw data collected through interviews (Miles and Huberman, 1984; Miles et al., 2014). After the completion of each interview session, the recorded interviews were immediately transcribed. The interview transcripts were reviewed to create summary sheets for every interview (Carson et al., 2001; Rao and Perry, 2007). A summary sheet is a single sheet consisting of a series of focusing or summarising questions about a particular field contact. These summary sheets included main themes, issues, problems and brief answers to each question, resulting in an overall summary of the main points in the research data (Patton, 2002; Schilling, 2006). Then the summary sheets were reviewed to develop a pattern code for the research data. Pattern codes are explanatory codes that identify an emergent theme, pattern or explanation suggested to the analyst. These codes convert various materials to meaningful and parsimonious units of analysis that is into a smaller number of overarching themes or constructs (Miles et al., 2014; Weber, 1990).

The next step of the analysis was to develop data display. Data display involves the organised assembly of information to permit the researcher to draw conclusions and take actions (Faust, 1982; Miles and Huberman, 1984; Miles et al., 2014). During this step, the researcher designs rows and columns of a matrix for qualitative data, after reviewing the previously created summary sheets and pattern codes.

The final step of the manual content analysis process is conclusion drawing and verification. During the process of data collection, the qualitative analyst decides on the 'meaning' of the different collected notes, patterns, explanations, possible configurations, causal flows and propositions (Bradley, 1993; Glaser and Strauss, 1967; Miles et al., 2014) so as to draw conclusions and to verify them. The summarising and coding of data in data reduction phase leads to new ideas on what should be entered into the matrix for data display. Entering data into the matrix requires further data reduction and as the matrix fills up, preliminary conclusion is drawn (Miles and Huberman, 1984; Miles et al., 2014). Qualitative content analysis is a challenge to adapt for the research; therefore, usually common quotations are used to draw conclusions (Schilling, 2006).

After the completion of manual coding, the data were re-evaluated using Leximancer for improving the results validity (Middleton et al., 2011; Smith and Humphreys, 2006). Leximancer is an instrument of conceptual analysis of collection contents which includes text documents and representation of drawn information visually (Smith, 2003; Smith and Humphreys, 2006). Occurrence and co-occurrence of statistics of word is utilised for the determination of important concepts in a text corpus (Cummings and Daellenbach, 2009). Thematic analysis by collecting similar concepts and semantic analysis to recognise the connections between the concepts were conducted. Concept map provides the text data ideas by examination of connections through visual summaries of the interviews and their co-occurrences to get the mind-gap (Cummings and Daellenbach, 2009). In order to profoundly give details of concepts, gathered dimensions and themes, both manual and software analytical approaches are consumed (Middleton et al., 2011; Smith and Humphreys, 2006).

4. Findings and discussion

4.1. *Systematic literature findings*

The extant literature revealed five major categories of challenges and issues related to adopting cloud computing: security and privacy, trust, data management, cost, and infrastructure.

A brief discussion of the literature about these challenges and issues is provided next.

4.1.1. *Security and privacy*

Security issues are a central concern for private institutions, such banks, medical research centres, and more recently, public institutions (Behl, 2011; Jensen et al., 2009; Julisch and Hall, 2010; Pearson, 2009; Ramgovind et al., 2010; Wyld, 2010). Security and privacy relate to administrative and technical concerns in order to ensure that all cloud based services have the appropriate amount of protection and confidentiality of data (Paquette et al., 2010; Subashini and Kavitha, 2011). Issues of security include software security (verification and management of identity and access control), platform security (security relevant to framework, elements and interface) and infrastructure security (security related to the online habitat and any combined storage) (Krumm, 2009; Pearson, 2009; Pearson and Benameur, 2010). For example, concerns, both internal and external to an enterprise (Behl, 2011), relating to security include verification (Verma and Kaushal, 2011), encryption (Hay et al., 2011), detection of malware, and side channel attacks (Ren et al., 2012). In turn, privacy issues in cloud computing relate to data privacy protection in situations of data transfer, usage, apportionment, archiving and elimination (Chen and Zhao, 2012; Krumm, 2009; Mahmood, 2011; Pearson, 2009; Pearson and Benameur, 2010). Security and privacy concerns have been noted as challenges and issues to cloud computing adoption because few rules and regulations exist for its adoption (Wang and Mu, 2011). Only Service Level Agreements (SLA) have been deemed necessary between Cloud Services Provider (CSP) and the end users to ensure privacy and security (Ramgovind et al., 2010; Verma and Kaushal, 2011; Weinhardt et al., 2009).

As cloud computing becomes prevalent in more industries, new security and privacy concerns arise and potential solutions suggested (Atanassov et al., 2012; Lagesse, 2011; Poolsappasit et al., 2011; Tan and Ai, 2011). For example, concerns about security and privacy when the cloud computing is integrated with universal systems (Lagesse, 2011), sensor networks (Poolsappasit et al., 2011) and grid computing (Atanassov et al., 2012) have been raised. In order for the cloud to be used for larger systems such as cloud networks (Schoo et al., 2011), the necessity for an efficient and fool-proof protection solution is paramount to conquer any security-related concerns which have already been emphasised immensely. According to Harauz et al. (2009), the CSP should apply encryption schema, rigid access control, and continuous and periodic data backups in order to prevent unverified access as well as ensure data integrity, concealment and availability.

4.1.2. *Trust*

The next category of concern identified in the literature is trust. It appears to be an essential factor in encouraging the acceptance of and dependence on cloud based services (Karaoglanoglou and Karatza, 2011; Mathur and Nishchal, 2010). Distrust between client and service providers (Abbadi, 2011) does arise during deployment of cloud based services (Tian et al., 2010). For example, clients are concerned that their data would be lost in the event that the cloud storage provider either goes bankrupt or is bought out (Yang and Chen, 2010). These types of concerns have shown that trust issues have prevented efficient solutions being provided for cyber-attacks in the cloud, even though control is provided over essential tasks (Dillon et al., 2010). Some researchers indicate that there was a lack of trust between the CSPs and the client (Khorshed et al., 2011). Others believe that a trusted cloud can be achieved only through a properly protected system and environment (Zou and Zhang, 2011). Shen et al. (2010) speculated that a trustable cloud along with security components included availability, incorruptibility, protection and dependability.

4.1.3. *Data management*

The demand for cloud computing is increasing due to its efficiency and effectiveness, and its ability to run data-intensive applications on a wide forum (Agrawal et al., 2010). However, this capability is accompanied by data management concerns. Data management concerns relate to data storage (Chang and Choi, 2010; Jaeger et al., 2009) from a single storage provider to data federation (various providers giving storage) (Forell et al., 2011); data segmentation and recovery (Mathur and Nishchal, 2010); data resiliency (Jadeja and Modi, 2012); data fragmentation and duplication (Goyal, 2012); and data backup (Hemant et al., 2011). Other issues include data processing (Khalid and Mujtaba, 2009), data provenance (Sakka et al., 2010), and data anonymisation (Qureshi et al., 2011).

4.1.4. *Cost*

The next category of the challenges and issues was financial issues. Hardware and associated administrative costs need to be accurately estimated by businesses to determine how they can remain economically viable, feasible and imperishable (Forell et al., 2011; Li et al., 2009). Such economic feasibility can be achieved through applying costing models (Dillon et al., 2010; Ramgovind et al., 2010) and/or by producing profitable pricing and licensing strategies, and optimisation of resources (Suleiman et al., 2012) that ensures a high service turnover (Rafique et al., 2011).

An organisation that wants to adopt cloud computing needs to compare the cost of transferring to the cloud as opposed to staying on local hardware systems (Cardoso and Simões, 2012; Greenberg et al., 2009). These costings should include cost items related to transferring the remote business aspects to the cloud, increasing bandwidth to increase efficiency and ensuring feasibility (Assuncao et al., 2009; Kim, 2009; Kondo et al., 2009). Costs are usually higher for data-intensive applications (Dey, 2012; Kondo et al., 2009).

4.1.5. *Infrastructure*

The final category of challenges and issues involve concerns about the hardware and software infrastructure for cloud based services (Mathur, 2010). Complications occur either in networking areas, including traffic management (Savu, 2011), network agility and cost (Zheng, 2011), or in resource planning, for example dynamic resource supplying (Goyal, 2012), scaling (Forell et al., 2011) and allocation (Endo et al., 2011). The most critical issues are related to server allocation optimisation (Kusaka et al., 2011) and load balancing (Radojevic and Zagar, 2011), both of which are elements of the broad dilemma of effectiveness.

An immense amount of energy is required for operating a large-scale infrastructure (Forell et al., 2011); concerns including

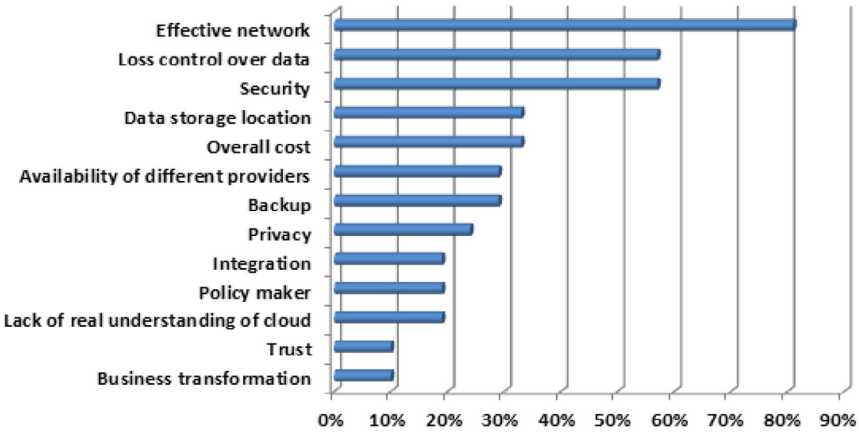

Fig. 2 – Challenges and issues that influence the adoption of cloud computing.

infrastructure design (Goyal, 2012; Kim et al., 2009) and virtualisation (Elmroth et al., 2011; Min et al., 2011) have been emphasised. Infrastructure characteristics, including accessibility (Pham et al., 2012; Wei and Blake, 2012), dependability (Jadeja and Modi, 2012) and expandability (Patibandla et al., 2012), have been speculated.

Due to these factors, government agencies often do not want to store their data in the cloud due to a lack of trust and the risk of exposing their data in an un-trusted environment. Government agencies are often bound by data sovereignty concerns to host their application or data within specific geographic boundaries. A key challenge is the provisioning of secure and trusted data storage that can be operated in such a cloud environment. Existing software systems typically consist of different parts and subsystems such as Web frontend, client application, business services, workflows, database layer or message queuing. Such systems often have rigid quality of service requirements in terms of performance, dependability, security and trust. Monitoring and enforcing those quality of service requirements is a key challenge to fulfil SLA between the cloud application owner and the customer (IT Industry Innovation Council, 2011; Department of Innovation Industry Science and Research, 2011).

4.2. *In-depth interview findings*

The researchers used in-depth interviews as a data collection method in order to investigate the most important challenges and issues that influence the adoption of cloud computing in Australian regional and municipal governments. Even though the adoption of cloud computing offers various benefits to performance, adoption is seen to have certain challenges and issues. The main important challenges and issues as identified by the participants based on their knowledge and experience as IT managers are presented in Fig. 2. Each of these challenges and issues will be discussed next.

4.2.1. *Effective network*

This research strongly confirmed the findings in the literature review that effective network is one of the significant issues that affect cloud computing adoption. Approximately 81 percent (17/21) of the sample population affirmed this issue. Not having a good Internet connection, which can result to latency, is a crucial obstruction for the adoption of cloud computing: *"essentially, one of the top challenges that influence the adoption of cloud computing is the Internet connection. Without good Internet connection cloud computing is useless"* (C7-RTS). Some participants noted that given their location, Internet connection was not readily available: *"the first challenge would be the reliability and availability of Internet connection. Because we are in remote area, we have not got the physical NBN connections"* (C11-RAV). Other participants noted that having an effective network goes hand-in-hand with higher costs and expenditures to obtain it: *"the most important issue in rural and regional areas is the internet connectivity. The connectivity is the stable and the cost effective, that what we found when looking to the existing internet connection and what we need to deliver some of our core systems through the cloud. The cost of getting sufficient Internet connection is quit high cost at this stage. I think this will be one of the big issues, the cost of the Internet connection"* (C61-URM).

An efficient government cloud service system should be highly responsive, economical and user-friendly (Liu and Wassell, 2011). Any organisation planning to adopt cloud must ensure reliable and stable Internet connectivity (Myoung and Crespi, 2010; Tweneboah-Koduah, 2012).

4.2.2. *Security and loss control over data*

This research confirms that security and loss control over data is a crucial issue that emerged upon the adoption of cloud computing. Approximately 57 percent (12/21) of the sample population reported this as an issue. Participants explained that security could be considered a concern during the adoption as the loss of control over data can significantly bring greater problems to the organization: *"security is a big thing it comes back to the control. If you are in control you know what security you have got, and who to trust. To push that at someone else as a service then you need to make sure you have a good relationship with the supplier so they can establish the level of trust. The security, that is just a technical sort of things that would come back to uses anyway that the lowest point of security"* (C39-URM). Others described how data security is the biggest issue or concern for cloud computing especially in the regional area. Participants had apprehensions given how security can become immense issues once data control is lost and not properly managed by the providers and

organisations: *"in relation to the security of cloud computing, do we trust the cloud provider to store that data? Yeah. Now, I suppose challenges, I suppose making sure that your provider is reputable"* (C45-RAV).

A challenge is concerns over security and loss of control over data with processing or relocating potential databases into the cloud (Duffany, 2012; Gharehchopogh and Hashemi, 2012). A survey by IDC in 2008 rated security and loss of control over data as the top challenge of the adoption of cloud model (Kuyoro et al., 2011). The security challenges exist at the network, host and application levels (Pearson and Benameur, 2010). The main issues relate to defining which parties are responsible for which aspects of security. Such division of responsibility is hampered by the lack of standardisation of cloud APIs, loss control over data, unauthorised collection and usage of data, and the CSP not adequately protecting data (Chandrareddy et al., 2012; Hamlen et al., 2010).

4.2.3. *Data storage location*

Approximately 33 percent (7/21) of the sample population stated that the data storage location could potentially be an issue. This is because of the lack of clarity between the providers and vendors with the placement of data: "*pointed to the data storage location, some of the users are concerned about that; they want to know where it is located and who has access to it*" (C55-URS), also "*looking at the location of the servers, where that information going to be holds under specific policy, we need to inform people if we are going to store information off-shore in servers outside the country*" (C61-URM).

There is a wide range of policy issues related to data storage locations related to cloud computing (Ali et al., 2015b; Jaeger et al., 2008). There has been a lack of policy-making related to the storage data in cloud computing (Ali et al., 2015b; Jaeger et al., 2008). Cloud computing raises a range of important policy issues, which include issues of privacy, security, communications capacity, and government surveillance (Delaney and Vara, 2007; Ma, 2007). There are significant uncertainties about and tensions between public policy and technological capacity in the development and provision of cloud computing (Ali et al., 2015b; Jaeger et al., 2008).

4.2.4. *Cost*

This research found that while cost–benefits might ultimately flow from the adoption of cloud computing, the start-up cost hindered organisations from fully adopting it. This finding was especially related to the smaller and less exposed organisations. Approximately 33 percent (7/21) of the sample population indicated the total expense that organisations may need to disburse in order to afford the transition to the cloud model. Participants noted the risk of the high amount of capital funds needed for cloud computing which then brings higher pressure and demands for the organisations: *"as large amounts of capital funds become harder to get as this done with pressure on resourcing or particularly in regional areas that might have difficulty attracting IT staff to their employment. IT is a service particularly soft gross of service and number forms of outsourcing become attractive. You get to spread your cost over a multiple years and you get to move the risks and problem of staffing and resourcing out to your provider so they are the main benefits for small and regional organizations"* (C68-URL). Some participants pointed that there were no figures that justify cloud computing as a cost effective: *"the cost is one of the significant challenges and needs to be justified. Because we have not seen any figures that proved or justified cloud computing as cost effective"* (C11-RAV).

According to the literature review, the best profits that cloud computing have in contrast with different innovations is that it offers low start-up expenses (Saeed et al., 2011; Saini et al., 2011); one of the major benefits that organisations are expecting from using cloud services is cost saving (Miller, 2008). For start-up organisations, using cloud services can help them to decrease their capital expenses and hurdles to entry into business (Grossman and Gu, 2009). Cloud computing provides almost direct access to shared computing resources, and small and start-up businesses can launch new operations quickly with little to no upfront capital investment; this will assist with a faster time to market in many businesses (Marston et al., 2011).

4.2.5. *Availability of different providers*

One new finding that was not covered in the literature was the issue of availability of different providers. This research found that availability of different providers is a new important issue that emerged upon the adoption of cloud computing. Approximately 29 percent (6/21) of the sample population described this issue as a hindrance into fully adopting the cloud model. There would be one provider that would be providing or coming out with their business grade data solutions and data network solutions.

The availability of different providers will give chance to the organisations to select the provider who will provide the high quality of services: *"we have only got one vendor we can go to. We cannot — I know Noosa, for instance, being in South East Queensland there is a lot more resources available to them and they have got two different networking vendors they use to… they have got the redundancy built into their network. We cannot do that here, we need to be convinced that the network is solid"* (C16-RAL). The IT managers discussed the difficulty of choosing the right provider for an organisation as trust is needed for quality service to be achieved. The availability of more than one provider will make more competitive, and hopefully these providers will provide high quality of services and reduce the cost of these services: *"because there would be one vendor that would be providing the services. I think the service cost at the moment is fairly high"* (C15-RAL).

4.2.6. *Back-up of data*

This research confirms that back-up has emerged as an important issue facing the adoption of cloud computing. Approximately 29 percent (6/21) of the sample population indicated back-up to be a problem when considering the adoption of cloud computing. The presence of a back-up is a concern for participants as back-ups ensure the organisations of protection and defence once unexpected events or incidents take place: "*if they can guarantee that they have a back-up solution, they have got policies and procedures in place, so if there is a catastrophic failure, we will be back-up and running within a decent time frame and none of the data get lost. Because we would be losing hundred thousand dollars a year*" (C74-RTM).

There is not any surety of back-up of data in cloud computing (Hemant et al., 2011). Recovery of data from cloud is critical for businesses in the case of failure. The CSPs in turn might rely on seamless back-ups to enforce resilience of their

infrastructure. Since these back-ups might be done without the customer's active informed consent, it could lead to serious security issues and threats. One of the top threats identified by Cloud Security Alliance (2010) is 'data loss or leakage' where records may be deleted without a back-up of the original content. From a larger context, a record might be unlinked, or the data stored on an unreliable media could be effectively destroyed in the event of a key management failure.

4.2.7. *Privacy*

This research confirms that privacy of the data being uploaded and stored on the cloud model was an important issue that faced the adoption of cloud computing. Approximately 24 percent (5/21) of the sample population described how privacy can affect the adoption of cloud computing. Privacy is connected to the security issues. The danger of uploading all important and guarded data on the cloud can cause discomfort for organisations: *"another challenges related to the privacy concern where the data will be stored and if have privacy role in those particular organization where the data been housed, some people worry about the security where the data housed and this comes as a risk"* (C61-URM).

The risk to privacy is perceived in services that deal with different aspects of data (collecting, transferring, processing, sharing or storing) relating to personal information. It warrants adequate measurement for protecting privacy with regard to those services dealing with highly sensitive information, especially information relating to location, preferences, social networks of individuals and personal health data (Alshomrani and Qamar, 2013; Alvi et al., 2011; Yadav and Singh, 2012). Although public cloud is the most preferred economically viable architecture, it poses a threat to privacy because customers' data are handled and managed by the CSP (Pearson and Benameur, 2010). According to previous studies, there are a number of aspects that illustrate the best privacy issues in public cloud such as lack of user control; unauthorised secondary usage; and trans-border data flow and data proliferation (Ali and Soar, 2014; Alshomrani and Qamar, 2013; Alvi et al., 2011; Pearson and Benameur, 2010; Yadav and Singh, 2012).

4.2.8. *Integration*

This research finds integration of data and software as one of the major issues that faced the adoption of cloud computing, as seen by 19 percent (4/21) of the sample population. The risk of the data programs and software not being able to work properly and match, as the cloud model requires, is a potential cause of failure of the adoption: *"one of the major challenges is integration. Integration is to some extent easier when you are hosting all of your main systems within your own data centre but if you move to a software service model and they are being host to 4 different continents then some of your application integration and application performance complexities might change"* (C68-URL).

Lack of integration between networks makes it difficult for organisations to combine their IT systems with the cloud computing and realise the gains from the technology (Tripathi and Parihar, 2011; Tweneboah-Koduah, 2012). Organisations need to automatically provision services, manage virtual machine instances, and work with both cloud-based and enterprise-based applications using a single tool set that can function across existing programs and multiple cloud service providers (Brohi and Bamiah, 2011).

4.2.9. *Policy makers*

Another new finding that was not covered in the literature was the influence of policy makers. This research found that policy makers is a new important issue that emerged upon the adoption of cloud computing. Approximately 19 percent (4/21) of the sample population described this issue as a barrier to the adoption of the cloud model. A participant explained how the policy makers could become hindrances in the adoption of cloud computing especially by having wrong perceptions and lack of proper understanding of the new technology: *"policy makers are going to get caught up in the hype of cloud computing rather than being analytical about cloud computing and yeah, determining what is best and what is not best, so the policy makers will dictate to the ICT infrastructure caretakers about direction I think that is a risk because you know every other council is doing it so it must be good so we should do it too rather than analysing our maybe unique and particular circumstances and making a proper assessment"* (C42-URL).

4.2.10. *Lack of real understanding of the cloud*

Another new finding that was not covered in the literature was the lack of real understanding of the cloud. This research found that lack of real understanding of the cloud is a new important issue that emerged upon the adoption of cloud computing. Approximately 19 percent (4/21) of the sample population highlighted how the lack of proper orientation and awareness of the new technology could lead to the failure of the adoption: *"the biggest risk is understanding and clarity of what the actual concepts are in cloud computing"* (C53-RTL). Other participants indicate that the top management who made the decision to adopt cloud had a limited knowledge: *"senior management get a lot of information from external sources which I do not think they understand"* (C15-RAL) and *"they suggest that the cloud is a great thing and there should not be any fears of moving there and it is very cost effective. But they do not really have an understanding of the factors. They do not understand what it is"* (C15-RAL). Many in top management did not come from an IT background and did have not any experience or knowledge in relation to cloud computing: *"top management do not know what to do and so they do not do anything to improve the adoption of any new technology"* (C15-RAL).

4.2.11. *Trust*

This research confirmed that the concept of trust emerged as an important issue for the adoption of cloud computing. This concept has continually and constantly appeared throughout the analysis of the whole data. Approximately 10 percent (2/21) of the sample population explained that trust is needed given the amount of crucial and significant information uploaded on the cloud by organisations: *"related to the trust issue, I think in regard to if you are going to be adopting a cloud provider and you are going to put all of your capsule data in there. I am sure that cloud provider is going to be utilizing their data centres for other organizations and storing data for not just local or state governments. They probably storing it for commercial companies as well so there is definitely a risk there in regard to security of that data or whether or not that cloud provider is secure enough from possible attacks and hacks and that sort of thing so I guess by keeping*

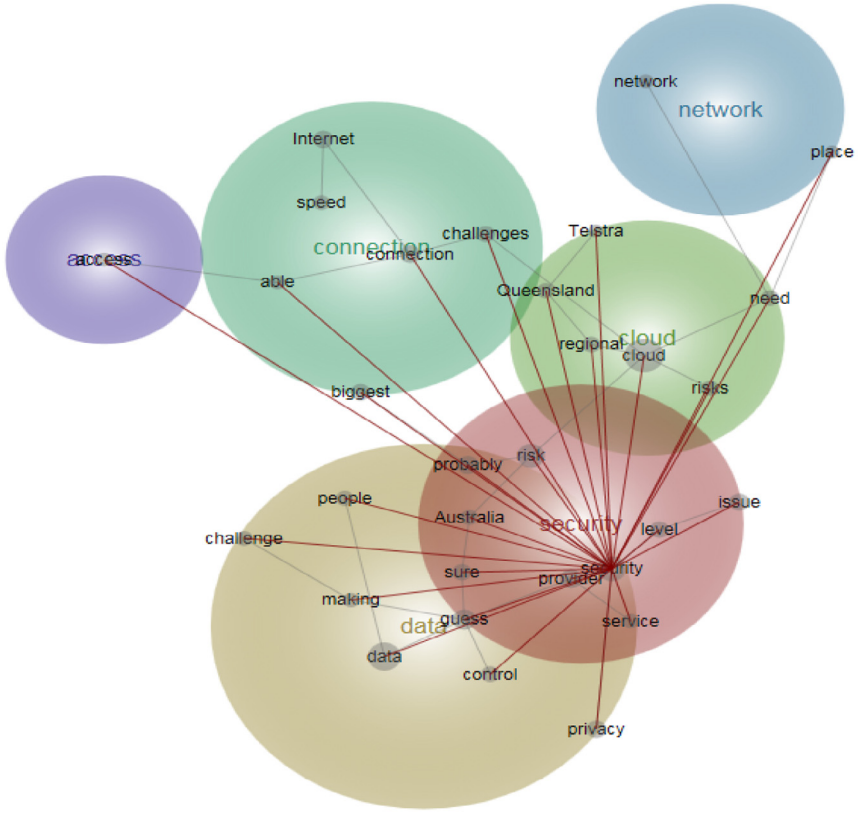

Fig. 3 – Challenges and issues key concepts map.

our data in house then we take that responsibility and we take our own issue for our data" (C28-URS). Organisation's data being under the control of CSP created a risk of data leakage that posed a barrier against trusting of this type of technology.

One of the major key concerns, particularly with regard to financial and health data, is the higher risk for data privacy and security attached to the vendor offerings which actually aim to assist business and encourage them to use cloud computing (Pearson and Benameur, 2010). Both the financial and health sectors deal with confidential and sensitive information. The associated vulnerability of the cloud computing system is the key business inhibitor in such sectors. These domains need control against unauthorised or secondary access or any kind of misuse, and cloud computing systems do not allow such customer control. Some sectors such as finance and health rely on mechanisms, such as insurance, court action, or penalties, which provide compensation in case of breach of SLAs.

4.2.12. *Business transformation*

Based on the literature review, there appears to be a lack of studies that have been conducted to assess business transformation with the challenges and issues that faced the adoption of cloud computing. This research found that business transformation was one of the important issues that faced the adoption of cloud computing. Business transformation as a risk pertains to the willingness of the stakeholders to accept the new way of doing things. This challenge was posted as business transformation is not always readily and easily accepted by the government and society especially the traditional ones: *"Business transformation is another one that I would see a bigger issue if how do you actually change the business to accept this new way of doing business"* (C40-UDV).

4.3. *Comparative analysis of challenges and issues of cloud adoption*

As stated in the methodology, the interview data were reanalysed using Leximancer to enhance the reliability of the findings from the manual content analysis (Middleton et al., 2011; Smith and Humphreys, 2006). The first step of this process focused on the wide range of business-related words used by the respondents and identified from the exploratory Leximancer analysis. The second step for analysing the data was to examine the thematic groupings. Leximancer uses a natural language processing algorithm, so the theme is titled by the concept with highest prominence in the thematic aggregation. In this analysis, Leximancer clustered the concepts into six themes (security, cloud, data, connection, network, access), each theme aggregating two or more concepts and represented by labelled circles. Fig. 3 illustrates the IT managers' views about challenges and issues that influence the adoption of cloud computing in Australian regional municipal governments. This figure depicts that the central theme within the map was 'security', and being strongly linked to the themes cloud, and data. The dominate theme security has strong associations with most other concepts on the map. Security is multifaceted in its use: relating to provider, service, level, issue, and risk. The concepts privacy, level, people, provider, issue, and risk are shown to be

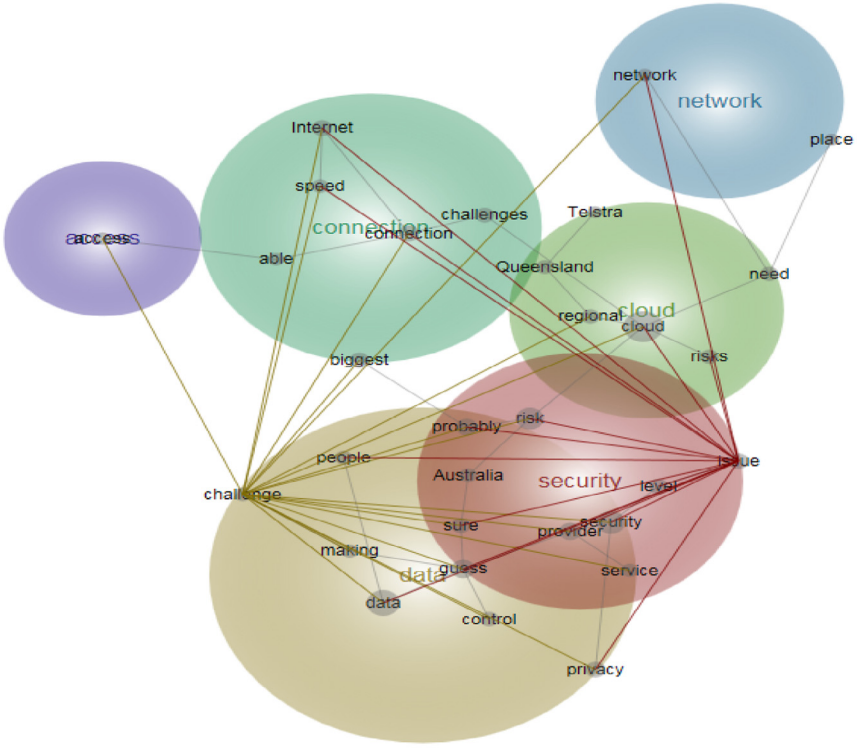

Fig. 4 – Challenges and issues related linkages.

frequently occurring and strongly connected to the theme security. Other themes illustrated but not connected to the theme 'security' include 'network', 'connection' and 'access'. The centrality of this theme provides a starting point for the research analysis.

Because this research concentrated to find out the challenges and issues that influence the adoption of cloud computing in Australian regional municipal governments, the theme 'data' which contains the concept 'challenge' and the theme 'security' which contains the concept 'issue' link strongly to the findings of the manual content analysis that suggested that IT managers saw as challenges and issues of cloud computing technology on their organisational unit, as shown in Fig. 4.

The concepts 'challenge' and 'issue' and their linkages on the concept map, through the analysis, have been illustrated through Fig. 4. These concepts are linked to the most concepts on the map. These linkages are to be expected, with 'challenge' and 'issue' being the top ranking concepts. The strongest linkages shown in Fig. 4 are: (a) between *challenge* and *service*, (b) between *challenge* and *control*, (c) between *challenge* and *speed*, (d) between *challenge* and *access*. Also, the strongest linkages shown in Fig. 4 are: (a) between *issue* and *provider*, (b) between *issue* and *security*, (c) between *issue* and *network*, (d) between *issue* and *privacy*.

All these strengths are expected due to the focus of the research and the qualitative questions asked, which were related to the challenges and issues that influence the adoption of cloud computing.

When discussing the concepts 'challenge' and 'issue', the IT managers were referring to the impact of security, provider, network, speed, data, connection, cloud, control, and regional. In relation to the mentioned concepts, Table 3 illustrates the representative quotes of each concept.

Through the analysis of the data, it is clear that in the discussion of challenges and issues a number of aspects are addressed by IT managers. These aspects include challenge and issue of provider, security, network, privacy, service, control, speed, and access. After having a comparison between the results from Leximancer and the manual analysis, it was found that both the methods gave the same result in a relation to challenges and issues that influence the adoption of cloud computing in Australian regional municipal governments.

5. Contributions

In this research, Table 4 represents the local council's cloud adoption stages. The table indicates that 13 of the participating local councils (62 percent) did not adopt cloud computing at their local councils, 5 of the participant local councils (24 percent) have some cloud adoption, 3 of the participating local councils (14 percent) have full adoption to some of the cloud services. This indicated that most of the participating local councils were affected by the challenges and issues presented in the previous section.

As a result, this research contributes to the ICT technology adoption literature by studying challenges and issues that influence the adoption of cloud computing in local councils. Looking at local council's adoption of new IS innovations can help to enrich knowledge and understanding of the innovation

Table 3 – Challenges and issues concepts and themes.

Leximancer-derived concepts	Representative quotes	Themes
Security	'The other big issue of course is the risk of a security exposure. By having your information up in a third party provider'.	Security
Provider	'We have only got one vendor we can go to. We cannot — I know Noosa, for instance, being in South east Queensland there is a lot more resources available to them and they have got two different networking vendors they use to… they have got the redundancy built into their network. We cannot do that here. We need to be convinced that the network is solid'.	Security
Network	'The other big issue is the latency. So with the network you have bandwidth and latency'.	Network
Speed	'You got to qualify or assess which applications are best suited for the cloud. And in doing that assessment, you got to take in consideration the speed of the Internet because the Internet speed is one issue because you are using the Internet to get to the cloud; you are not using your own private network anymore'.	Connection
Data	'It depends on the type and the importance of data we are talking about and the level of privacy requirement for it'	Data
Connection	'The first challenge would be the reliability and availability of speed and Internet connection. Because we are in remote area, we have not got the physical NBN connections here yet'.	Connection
Cloud	'Specifically for local government I think integration of cloud solution can be a challenge'.	Cloud
Control	'The top challenge is that, the change in how we do business. It is an in control of certain data and never format that private to someone else as a service provider so losing control of your data is a risk and it is a challenge to accept that in some regard'.	Data
Regional	Major challenge is the provision of competitive network data access in rural and regional areas. Cost of network access and data is prohibitive	Cloud

adoption process in this era of rapid development of new technologies. This research also leads to important practical implications for technology consultants. Local councils represent as organisations that provide services to the local citizen and the businesses in most economies, and consequently represent an important market segment for software vendors or service providers. Cloud computing providers may need to improve their interaction with local councils who are involved in the cloud computing experience, in an effort to create a healthy environment for cloud computing adoption, and to remove any vagueness surrounding this technology. A rapidly developing and uncertain environment represents a key challenge within which business leaders make decisions. Recent studies can be used by managers to improve their decision making process in such an environment. The findings of this research may help managers to evaluate possible adoption and increase their awareness about challenges and issues that influence the adoption of cloud when planning to adopt cloud computing. Taking all the above into account, this research presents some useful information for organisations, technology consultants, and vendors. This research is viewed as being relevant to the current era of rapid developments of cloud computing technologies.

Table 4 – Councils cloud adoption stages.

Segments	Councils cloud adoption stages		
	Not adopted	Some adoption	Full adoption of some services
Coastal	3	1	1
Resource	1	1	0
Indigenous	4	0	0
Rural/Remote	5	1	0
South East Queensland	0	2	2
Total	**13**	**5**	**3**
Percent	**62%**	**24%**	**14%**

6. Limitations and future research

This research expands our knowledge about the challenges and issues that influence the adoption of cloud computing in regional municipal governments. There has not been much research done on cloud computing in reference to Australia and much more can be discovered. Future research could build on this research by examining challenges and issues that influence the cloud computing adoption in different sectors and industries. On a geographical dimension, this research was primarily limited to the Queensland State. For this reason, empirical investigations in different regional municipal governments might be needed.

7. Conclusion

Recent developments have ensured the increasing fame of cloud computing as it is an online shared computing resource. Based on the above arguments, it can be deduced that even though it is economical and ensures an increase in performance, productivity and competency, there are a lot of challenges and issues relating to the acceptance of cloud computing. In this research, the analysis has proved that some of the challenges and issues such as security, privacy, trust, management of data, cost, and infrastructure were part of the systematic literature, and there were concerns regarding effective network, data storage location, availability of different providers, policy makers, lack of real understanding of the cloud, and business transformation with the incorporation of cloud computing,

which were raised by the IT managers. Despite the significant overlap between the challenges and issues being discussed in the systematic literature and the challenges and issues raised by the IT managers, there clearly is a gap between the two camps. The findings of this research were expected to assist managers to evaluate possible adoption and increase their awareness about challenges and issues that influence the cloud adoption when planning to adopt it.

8. Compliance with ethical standards

The authors have no known potential conflicts of interest (financial or non-financial) with the research. Informed consent was obtained from participants and a Participant Information Sheet was provided. Participation was voluntary, there were no consequences for non-participation, no personally-identifying data were captured and data were anonymised. This research was funded through an Australian Post-graduate awarded at the USQ. The research was approved by the USQ Ethics Committee and was performed in accordance with the ethical standards as laid down in the 1964 Declaration of Helsinki and its later amendments or comparable ethical standards.

REFERENCES

Abbadi IM. Toward trustworthy clouds' internet scale critical infrastructure. In: Proceedings of the 7th information security practice and experience conference, vol. 6672. Berlin: Springer; 2011. p. 73–84.

Agrawal D, El-Abbadi A, Antony S, Das S. Data management challenges in cloud computing infrastructures. In: Proceedings of the 6th international conference on databases in networked information systems; 2010. p. 1–10.

Aleixandre-Benavent R, González Alcaide G, González De Dios G, Alonso-Arroyo A. Sources of bibliographic information rationale for conducting a literature search. ACTA Paediatric 2011;69(3):131–6.

Ali O, Soar J. Challenges and issues within cloud computing technology. In: The fifth international conference on cloud computing, GRIDs, and virtualization; 2014. p. 55–63.

Ali O, Soar J, Yong J. Impact of cloud computing technology on e-government. In: Information and software technologies, 456. Springer International Publisher; 2014. p. 272–90.

Ali O, Soar J, McClymont H, Yong J, Biswas J. Anticipated benefits of cloud computing adoption in Australian regional municipal government: an exploratory study. In: Pacific Asia conference on information systems (PACIS); 2015a. p. 1–17.

Ali O, Soar J, Yong J, McClymont H. Level of policy for cloud computing adoption in Australian regional municipal government: an exploratory study. In: The 11th international conference on grid & cloud computing and applications; 2015b. p. 30–5.

Alshomrani S, Qamar S. Cloud based e-government: benefits and challenges. Int J Multidiscip Sci Eng 2013;4(6):15–19.

Alvi FA, Choudary BS, Jaffery N, Pathan EA. Review on cloud computing security issues and challenges. Pakistan: Department of Electronic Engineering, QUEST Nawabshah; 2011.

Armbrust M, Fox A. Above the clouds: Berkeley view of cloud computing. Technical Report, University of California, Berkeley; 2009.

Assuncao M, Costanzo A, Buyya R. Evaluating the cost-benefit of using cloud computing to extend the capacity of clusters. In: Proceedings of the 18th ACM international symposium on high performance distributed computing, Munich, Germany; 2009. p. 141–50.

Atanassov E, Gurov T, Karaivanova A. Security issues of the combined usage of grid and cloud resources. In: Proceedings of the 35th international convention of information communication technology, electronics and microelectronics (MIPRO); 2012. p. 417–20.

Behl A. Emerging security challenges in cloud computing: an insight to cloud security challenges and their mitigation. In: World congress on information and communication technologies (WICT), Mumbai; 2011. p. 217–22.

Bhardwaj S, Jain L, Jain S. Cloud computing: a study of infrastructure as a service (IaaS). Int J Eng Inf Technol 2010;2(1):60–3.

Bradley J. Methodological issues and practices in qualitative research. Libr Q 1993;63(4):431–49.

Brohi SN, Bamiah MA. Challenges and benefits for adopting the paradigm of cloud computing. International Journal of Advanced Engineering, Science and Technology 2011;2:286–90.

Buyya R, Broberg J, Gościński A. Cloud computing: principles and paradigms. USA: John Wiley & Sons; 2011.

Cardoso A, Simões P. Cloud computing: concepts, technologies and challenges, virtual and networked organizations, emergent technologies and tools. In: Computer and information science, 248. Berlin: Springer; 2012. p. 127–36.

Carson D, Gilmore A, Perry C, Gronhaug K. Qualitative marketing research. London: Sage Publications; 2001.

Catteddu D, Hogben G. Cloud computing: benefits, risks and recommendations for information security. European Network and Information Security Agency (ENISA); 2009.

Chandrareddy J, Mahesh GU, Bandi S. Cloud zones: security and privacy issues in cloud computing. Asian J Int Technol 2012;11(3):83–93.

Chang H, Choi E. Challenges and security in cloud computing. Commun Netw Commun Comput Inf Sci 2010;120:214–17.

Chen D, Zhao H. Data security and privacy protection issues in cloud computing. In: Proceedings of the IEEE international conference on computer science and electronics engineering; 2012. p. 156–9.

Clemons E, Chen Y. Making the decision to contract for cloud services: managing the risk of an extreme form of it outsourcing. In: Proceedings of 44th Hawaii international conference on system sciences, Hawaii; 2011. p. 1–10.

Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing. CSA; 2009.

Cloud Security Alliance. Top threats to cloud computing. CSA; 2010.

Cummings S, Daellenbach U. A guide to the future of strategy? The history of long range planning. Long Range Plann 2009;42(2):234–63.

Delaney KJ, Vara V. Google plans services to store users' data. Wall Str J <http://online.wsj.com/article/SB119612660573504716.html?mod=hps_us_whats_news>; 2007 [accessed 16.03.14].

Department of Innovation Industry Science and Research. Cloud computing — opportunities and challenges. IT Industry Innovation Council; 2011. p. 1–31.

Dey S. Cloud mobile media: opportunities, challenges, and directions. In: International conference on computing, networking and communications; 2012. p. 929–33.

Dillon T, Wu C, Chang E. Cloud computing: issues and challenges. In: Proceedings of the 24th IEEE international conference on advanced information networking and applications (AINA), Perth, WA; 2010. p. 27–33.

Duffany JL. Cloud computing security and privacy. In: Proceedings of the 10th Latin American and Caribbean conference for engineering and technology; 2012. p. 1–9.
Dustin-Amrhein PA, De Andrade A, Armstrong EAB, Bartlett J, Bruklis R, Cameron K. Cloud computing use cases. White Paper, version 3.0 ed.; 2010. p. 1–7.
Elmroth E, Tordsson J, Hernández F, Ali-Eldin A, Svärd P, Sedaghat M, et al. Self-management challenges for multi-cloud architectures. In: Proceedings of the 4th European conference on towards a service-based internet; 2011. p. 8–49.
Endo PT, De AV, Palhares A, Pereira NN, Goncalves GE, Sadok D, et al. Resource allocation for distributed cloud: concepts and research challenges. Proc IEEE Netw 2011;25(4):42–6.
Faust D. Needed component in prescription of science: empirical knowledge of human cognitive limitations. Sci Commun 1982;3:555–70.
Forell T, Milojicic D, Talwar V. Cloud management: challenges and opportunities. In: Proceedings in the IEEE international symposium on parallel and distributed processing workshops and PhD forum; 2011. p. 881–9.
Gaskell G. Individual and group interviewing. In: Bauer M, Gaskell G, editors. Qualitative researching with text, image and sound. London: Sage; 2000.
Gens F. IDC's public IT cloud service forecast: new numbers, same disruptive story, <http://blogs.idc.com/ie/?p=922>; 2010 [accessed 20.12.14].
Ghanam Y, Ferreira J, Maurer F. Emerging issues and challenges in cloud computing — a hybrid approach. J Softw Eng Appl 2012;923–37.
Gharehchopogh FS, Hashemi S. Security challenges in cloud computing with more emphasis on trust and privacy. Int J Sci Technol Res 2012;1(6):49–54.
Glaser B, Strauss AL. Discovery of grounded theory: strategies for qualitative research. Chicago: Aldine; 1967.
Golder S, Loke YK, Zorzela L. Comparison of search strategies in systematic reviews of adverse effects to other systematic reviews. Health Info Libr J 2014;31:92–105.
Goyal P. Enterprise usability of cloud computing environments: issues and challenges. In: Proceedings of the 19th IEEE international workshops on enabling technologies: infrastructures for collaborative enterprises; 2012. p. 54–9.
Greenberg A, Hamilton J, Maltz D, Patel P. Cost of a cloud: research problems in data centre networks. ACM SIGCOMM Comput Commun Rev 2009;39(1):68–73.
Grossman RL, Gu Y. On the varieties of clouds for data intensive computing. Data Eng 2009;44.
Hamlen K, Kantarcioglu M, Khan L, Thuraisingham B. Security issues for cloud computing. Int J Inf Secur Priv 2010; 4(2):39–51.
Harauz J, Kauifman LM, Potter B. Data security in the world of cloud computing. Proc IEEE Secur Priv 2009;7(4):61–4.
Hay B, Nance K, Bishop M. Storm clouds rising: security challenges for IaaS cloud computing. In: Proceedings of the 44th Hawaii international conference on system sciences; 2011. p. 1–7.
Hemant P, Chawande NP, Sonule A, Wani H. Development of servers in cloud computing to solve issues related to security and backup. In: Proceedings of the IEEE international conference on cloud computing and intelligence systems; 2011. p. 158–63.
Higgins JPT, Green S. Cochrane handbook for systematic reviews of interventions 5.1.0. The Cochrane Collaboration. <http://www.cochrane-handbook.org>; 2011 [accessed 12.09.13].
Hsieh HF, Shannon SE. Three approaches to qualitative content analyses. Qual Health Res 2005;15(9):1277–88.
IT Industry Innovation Council. Cloud computing — opportunities and challenges; 2011. p. 1–31.
Jadeja Y, Modi K. Cloud computing concepts, architecture and challenges. In: International conference on computing, electronics and electrical technologies; 2012. p. 877–80.
Jaeger P, Lin J, Grimes J, Simmons S. Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing. First Monday 2009;14(5):1–9.
Jaeger PT, Lin J, Grimes JM. Cloud computing and information policy: computing in a policy cloud. J Inf Technol Polit 2008;5(3):269–83.
Janssen M, John A. Challenges for adopting cloud-based software as a service in the public sector. European Conference on Information Systems 2011;1–13.
Jensen M, Schwenk JO, Gruschka N, Iacono LL. Technical security issues in cloud computing. In: Proceedings of the IEEE international conference on cloud computing (CLOUD-II 2009), India; 2009. p. 109–16.
Joint A, Baker E, Eccles E. Hey, you, get off of that cloud. Comput Law Secur Rev 2009;25(3):270–4.
Julisch K, Hall M. Security and control in the cloud. Inf Secur J 2010;19(6):299–309.
Kantarcioglu M, Bensoussan A, Hoe SR. Impact of security risks on cloud computing adoption. In: Forty-ninth annual Allerton conference. Illinois, USA: Allerton House, UIUC; 2011. p. 670–4.
Karaoglanoglou K, Karatza H. Resource discovery in a grid system: directing requests to trustworthy virtual organizations based on global trust values. J Syst Softw 2011;84(3):465–78.
Khalid A, Mujtaba H. Data processing issues in cloud computing. In: Proceedings of the 2nd international conference on machine vision; 2009. p. 301–4.
Khorshed M, Ali A, Wasimi S. Trust issues that create threats for cyber-attacks in cloud computing. In: Proceedings of the 17th IEEE international conference on parallel and distributed systems (ICPADS), Tainan; 2011. p. 900–5.
Kim W. Cloud computing: today and tomorrow. J Object Technol 2009;8(1):65–72.
Kim W, Kim SD, Lee E, Lee SY. Adoption issues for cloud computing. In: Proceedings of the 11th international conference on information integration and web-based applications and services; 2009. p. 3–6.
Kirsch LJ. Deploying common systems globally: the dynamics of control. Inf Syst Res 2004;15(4):374–95.
Kondo D, Javadi B, Malecot P, Cappello F, Anderson DP. Cost benefit analysis of cloud computing versus desktop grids. In: Proceedings of the IEEE international symposium on parallel and distributed processing; 2009. p. 1–12.
Krumm J. A survey of computational location privacy. Pers Ubiquitous Comput 2009;13(6):291–399.
Kusaka T, Okuda T, Ideguchi T, Tian X. Queuing theoretic approach to server allocation problem in time-delay cloud computing systems. In: Proceedings of the 23rd international tele-traffic congress; 2011. p. 310–11.
Kuyoro SO, Ibikunle F, Awodele O. Cloud computing security issues and challenges. Int J Comput Netw 2011;3(5):247–55.
Lagesse B. Challenges in securing the interface between the cloud and pervasive systems. In: Proceedings of the IEEE international conference on pervasive computing and communications workshops (PERCOM); 2011. p. 106–10.
Leavitt N. Is cloud computing really ready for prime time. Computing Now; 2009. p. 15–20.
Li X, Li Y, Liu T, Qiu J, Wang F. The method and tool of cost analysis for cloud computing. In: Proceedings in the IEEE international conference on cloud computing; 2009. p. 93–100.
Liu R, Wassell I. Opportunities and challenges of wireless sensor networks using cloud services. In: Proceedings of the workshop on internet of things and service platforms, Tokyo; 2011. p. 1–7.

Lopes IL. Estratégia de busca na recuperação da informação: revisão da literature. Clin Inform 2002;31(2):60–71.
Low C, Chen Y, Wu M. Understanding the determinants of cloud computing adoption. Ind Manage Data Syst 2011;11:1006–23.
Lyer B, Henderson J. Preparing for the future: understanding the seven capabilities of cloud computing. Manage Inf Syst Q Exec 2010;9(2):117–31.
Ma W. Google's G drives raise privacy concerns. Popular Mechanics, <http://www.popularmechanics.com/technology/industry/4234444.html>; 2007 [accessed 16.03.14].
Mahmood Z. Data location and security issues in cloud computing. In: Proceedings in the IEEE international conference on emerging intelligent data and web technologies; 2011. p. 49–54.
Marston S, Li Z, Bandyopadhyay S, Zhang J, Ghalsasi A. Cloud computing — the business perspective. Decis Support Syst 2011;51(1):176–89.
Martucci LA, Zuccato A, Smeets B, Habib SM, Johansson T, Shahmehri N. Privacy, security and trust in cloud computing the perspective of the telecommunication industry. In: The 9th international conference on ubiquitous intelligence and computing and 9th international conference on autonomic and trusted computing; 2012. p. 627–32.
Mathur M. Elucidation of upcoming traffic problems in cloud computing. Recent Trends Netw Commun Commun Comput Inf Sci 2010;90:68–79.
Mathur P, Nishchal N. Cloud computing: new challenge to the entire computer industry. In: The first international conference on parallel distributed and grid computing (PDGC); 2010. p. 223–8.
Mell P, Grance T. Draft NIST working definition of cloud computing, 15. 2009. p. 1–7.
Middleton S, Liesch PW, Steen J. Organizing time: internationalization narratives of executive managers. Int Bus Rev 2011;20(2):136–50.
Miles MB, Huberman M. Qualitative data analysis. Newbury Park: Sage Publication; 1984.
Miles MB, Huberman M, Saldana J. Qualitative data analysis. London: Sage Publication; 2014.
Miller M. Cloud computing: web-based applications that change the way you work and collaborate online. Indiana, IN: Que; 2008.
Min O, Park C, Lee J, Cho J, Kim H. Issues on supporting public cloud virtual machine provisioning and orchestration. In: Proceedings of the 13th international conference on advanced communication technology; 2011. p. 270–3.
Misra SC, Mondal A. Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding return of investment. J Math Comput Model 2011;53:504–21.
Myoung GL, Crespi N. Shaping future service environments with the cloud and internet of things: networking challenges and service evolution. In: Proceedings of the 4th international conference on leveraging applications of formal methods, verification, and validation; 2010. p. 399–410.
NIST. Cloud computing. Computer Security Resource Centre, <http://csrc.nist.gov/groups/SNS/cloudcomputing/>; 2009 [accessed 27.10.13].
Opitz N, Langkau TF, Schmidt NH, Kolbe LM. Technology acceptance of cloud computing: empirical evidence from German IT departments. In: The 45th Hawaii international conference on system sciences; 2012. p. 1–10.
Paquette S, Jaeger PT, Wilson SC. Identifying the security risks associated with governmental use of cloud computing. Gov Inf Q 2010;27(3):245–53.
Patibandla R, Kurra S, Mundukur N. A study on scalability of services and privacy issues in cloud computing. In: Proceedings of the 8th international conference on distributed computing and internet technology; 2012. p. 212–30.
Patton MQ. Qualitative research and evaluation methods. Thousand Oaks, CA: Sage Publications; 2002.
Pearson S. Taking account of privacy when designing cloud computing services. In: ICSE workshop on software engineering challenges of cloud computing. Washington, DC, USA: IEEE Computer Society; 2009. p. 44–52.
Pearson S, Benameur A. Privacy, security and trust issues arising from cloud computing. In: Proceedings of the 2nd IEEE international conference on cloud computing technology and science. IEEE Press; 2010. p. 693–702.
Pham C, Cao P, Kalbarczyk Z, Iyer R. Toward a high availability cloud: techniques and challenges. In: Proceedings of the IEEE/IFIP 42nd international conference on dependable systems and networks workshops, Boston; 2012. p. 1–6.
Poolsappasit N, Kumar V, Madria S, Chellappan S. Challenges in secure sensor-cloud computing. In: Proceedings of the 8th VLDB international conference on secure data management (SDM); 2011. p. 70–84.
Pucher KK, Boot NMWM, De Vries NK. Systematic review: school health promotion interventions targeting physical activity and nutrition can improve academic performance in primary and middle school children. Health Educ 2013;113(5):372–91.
Qureshi SS, Ahmad T, Rafique K, Shuja-ul-islam. Mobile cloud computing as future for mobile applications: implementation methods and challenging issues. In: Proceedings of the IEEE international conference on cloud computing and intelligence systems; 2011. p. 467–71.
Radojevic B, Zagar M. Analysis of issues with load balancing algorithms in hosted (cloud) environments. In: Proceedings of the 34th international convention; 2011. p. 416–20.
Rafique K, Tareen AW, Saeed M, Wu JZ, Qureshi SS. Cloud computing economics opportunities and challenges. In: Proceedings of the 4th IEEE international conference on broadband network and multimedia technology; 2011. p. 401–6.
Ramgovind S, Eloff MM, Smith E. The management of security in cloud computing. In: Proceedings of the IEEE international conference on cloud computing; 2010. p. 1–7.
Rao S, Perry C. Convergent interviewing: a starting methodology for an enterprise research program. In: Hine D, Carson D, editors. Innovative methodologies in enterprise research. Northampton, Massachusetts: Edward Elgar; 2007.
Reed A, Rezek C, Simmonds P. Security guidance for critical areas of focus in cloud computing v3.0. Cloud Security Alliance (CSA); 2011.
Ren K, Wang C, Wang Q. Security challenges for the public cloud. Proc IEEE Internet Comput 2012;16(1):69–73.
Saeed I, Juell-Skielse G, Uppström E. Cloud enterprise resource planning adoption: motives and barriers. In: International conference on research and practical issues of enterprise information systems; 2011. p. 99–122.
Saini SL, Saini DK, Yousif JH, Khandage SV. Cloud computing and enterprise resource planning. In: Proceedings of the world congress on engineering, London, U.K.; 2011.
Sakka MA, Defude B, Tellez J. Document provenance in the cloud: constraints and challenges. In: Proceedings of the 16th EUNICE/IFIP WG 6.6 conference on networked services and applications: engineering, control and management; 2010. p. 107–17.
Savu L. Cloud computing: deployment models, delivery models, risks and research challenges. In: International conference on computer and management; 2011. p. 1–4.

Schilling J. On the pragmatics of qualitative assessment: designing the process for content analysis. Eur J Psychol Assess 2006;22(1):28–37.
Schoo P, Fusenig V, Souza V, Melo M, Murray P, Debar H, et al. Challenges for cloud networking security. In: Mobile networks and management, social informatics and telecommunications engineering, 68. New York: Springer; 2011. p. 298–313.
Shea BJ, Grimshaw JM, Wells GA, Boers M, Andersson N, Hamel C, et al. Development of AMSTAR: a measurement tool to assess the methodological quality of systematic reviews. BMC Med Res Methodol 2007;7:10.
Shen Z, Li L, Yab F, Wu X. Cloud computing system based on trusted computing platform. Proc IEEE Int Conf Intell Comput Technol Autom 2010;1:942–5.
Smith AE. Automatic extraction of semantic networks from text using Leximancer. Paper presented at the North American Chapter of the Association for Computational Linguistics — Human Language Technologies, Edmonton, Canada; 2003.
Smith AE, Humphreys MS. Evaluation of unsupervised semantic mapping of natural language with Leximancer concept mapping. Behav Res Methods 2006;38(2):262–79.
Sohan Y, Zeng H. Cloud: a computing infrastructure on demand. In: Proceedings of the 2nd international conference on computer engineering and technology, Chengdu, China; 2010.
Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 2011;34(1):1–11.
Suleiman B, Sakr S, Jeffrey R, Liu A. On understanding the economics and elasticity challenges of deploying business applications on public cloud infrastructure. J Internet Serv Appl 2012;1–21.
Takabi H, Joshi J, Ahn G. Security and privacy challenges in cloud computing environments. Proc IEEE Secur Priv 2010;8(6):24–31.
Tan X, Ai B. The issues of cloud computing security in high-speed railway. In: International conference on electronic and mechanical engineering and information technology (EMEIT); 2011. p. 4358–63.
Tian LQ, Ni Y, Lin C. Evolution of user behaviour trust in cloud computing. Int Conf Comput Appl Syst Model 2010;7:567–72.
Tripathi A, Parihar B. E-governance challenges and cloud benefit. VSRD Int J Comput Sci Inf Technol 2011;1(1):29–35.
Tweneboah-Koduah S. Knowledge management: critical factor for successful implementation of e-government applications. In: Proceedings of the 12th European conference on E-government, Spain; 2012. p. 713–21.
Vaquero LM, Rodero-Merino L, Caceres J, Lindner M. A break in the clouds: towards a cloud definition. ACM SIGCOMM Comput Commun Rev 2008;39:50–5.
Velte T, Velte A, Elsenpeter R. Cloud computing: a practical approach. Int J Sci Eng Res 2010;3(8):1–6.
Verma A, Kaushal S. Cloud computing security issues and challenges: a survey. In: Proceeding of Springer international conference on advances in computing and communication; 2011. p. 445–54.
Wang J, Mu S. Security issues and countermeasures in cloud computing. In: Proceedings of the IEEE international conference on grey systems and intelligent services (GSIS); 2011. p. 843–6.
Wang L, Tao J, Kunze M. Scientific cloud computing: early definition and experience. In: Proceedings of the 10th IEEE international conference on high performance computing and communications, Dalian, China; 2008.
Wang W, Rashid A, Chuang HM. Toward the trend of cloud computing. J Electron Commer Res 2011;12(4): 238–42.
Weber RP. Basic content analysis. Newbury Park, CA: Sage Publications; 1990.
Wei Y, Blake M. Service-oriented computing and cloud computing: challenges and opportunities. Proc IEEE Internet Comput 2012;14(6):72–5.
Weinhardt C, Anandasivam A, Blau B, Stosser J. Business models in the service world. IT Prof 2009;11:28–33.
Wyld D. Risk in the clouds? Security issues facing government use of cloud computing. Innovations in computing sciences and software engineering; 2010. p. 7–12.
Xu X. From cloud computing to cloud manufacturing. Robot Comput Integr Manuf 2012;28:75–86.
Yadav N, Singh VB. E-governance: past, present and future in India. Int J Comput Appl 2012;53(7):36–48.
Yang JF, Chen ZB. Cloud computing research and security issues. In: International conference on computational intelligence and software engineering; 2010. p. 1–3.
Zheng XP. Study on the opportunities and challenges of the cloud computing for Chinese medium-sized and small enterprises. In: International conference on E-business and E-government, Shenzhen; 2011. p. 1–4.
Zou B, Zhang H. Toward enhancing trust in cloud computing environment. In: The second international conference on control, instrumentation and automation; 2011. p. 364–6.