Management Issues with Cloud Computing

Akinlolu Olumide Akande
Department of Information Systems
University of Cape Town
Private Bag X3, Rondebosch 7701,
South Africa
+27723135908
Akinlolu.Akande@uct.ac.za

Nozuko Aurelia April
Shosholoza Meyl
Platform 24
Cape Town Station
Cape Town
8001, South Africa
+27764408281
NApril2@metrorail.co.za

Jean-Paul Van Belle
Department of Information Systems
University of Cape Town
Private Bag X3, Rondebosch 7701,
South Africa
+27 21 650 4256
Jean-Paul.VanBelle@uct.ac.za

ABSTRACT
Cloud computing is becoming popular and many organizations are considering the adoption of cloud computing because of its promise of convenient, on demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction [22]. Although Cloud computing has many benefits and has the ability to increase an organizations return on investment, there are many issues such as ethical issues, security issues, data lock-in, lack of standardization, customization, technology bottlenecks, strategy issues etc. which are preventing managements of organizations from adopting cloud computing. As a result of this, it is important for managements of these organizations to be aware of the issues with cloud computing that could affect their implementation success. In order to identify the issues and propose ways to resolve these issues, this paper discusses the different management issues with cloud computing that have been identified by literature and suggests possible ways to resolve them. This paper also suggests that proper investigation into these issues and how to resolve them will increase management's confidence in cloud computing and ensure successful adoption and implementation of cloud computing.

Keywords
Cloud computing, organizations, issues, management, standardize, authorize

1. INTRODUCTION
Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [3]. Cloud computing has become prevalent among organizations looking for a cheaper way to access needed infrastructure, service, and/or applications [14]. This has changed organizations perception of software's, infrastructures and development platforms [19]. This paper aims to give an overview of cloud computing and different management issues that organizations face during cloud computing implementation and to make possible suggestions that could help resolve these issues.

Cloud computing is classified into different categories which are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) based on their delivery models [13]. SaaS allows the user to be able to use applications running on a cloud infrastructure from a provider without having to worry about the management or control of cloud infrastructures such as servers, storage, network, operating systems, storage, and other infrastructures that supports cloud computing [19]. PaaS provides the consumer with the capability to create their own services and applications with the support of services, programming languages and tools supported and provided by the platform provider [12] [19]. IaaS uses virtual machine to provide consumers with storage, networks, processing power, and other important computing resources which allow the consumer to deploy and run their applications and software [12] [19]. Cloud computing offers benefits such as flexibility, elasticity, scalability of infrastructure, reliability, broad network access, on-demand service provisioning, economies of scale, cost effectiveness, and increases speed of time to market [19]. Although cloud computing offers many benefits to organization, management of cloud computing can be challenging as it poses many issues to organizations [18].

The following section will discuss information systems management issues with cloud computing and the directions the issues may take in the coming five years. Suggestions are also made about possible ways in which these issues can be resolved to ensure that organizations reap maximum benefit from cloud computing.

2. INFORMATION SYSTEMS MANAGEMENT ISSUES WITH CLOUD COMPUTING
The management of cloud computing raises many information systems management issues which includes ethical (security, availability, confidentiality and privacy) issues, legal and jurisdictional issues, data lock in, lack of standardized service level agreements (SLA's), customization, technological bottlenecks , strategy issues, implementation issues, reputation fate sharing, dependence on the internet, quality of service, integration issues, change management, transparency, energy management, workload management, disaster recovery, insecure application programming interface, malicious insiders, risk management, and performance measurement**.** Each of these management issues will be discussed in details below.

2.1 Ethical Issues

Cloud computing presents important ethical issues like security, confidentiality, privacy, integrity, and availability because the service providers have an ethical duty to protect data and information stored in their data center for the customer organization [15]. Each of the ethical issue is discussed in details below.

2.2 Security

Security involves confidentiality, integrity and availability which aid the development of secure systems. There is so much concern about security within cloud computing environment [19]. Literature has revealed that security is the biggest management issue with cloud computing. Applications and data being hosted by service providers are prone to vulnerabilities from unauthorized parties [4]. Security measure should be taken to prevent unauthorized access to data, applications, software, and hardware.

2.2.1 Confidentiality and Privacy

Confidentiality means that only an authorized person will have access to data. In cloud computing, the chances that data will be accessed by an unauthorized person are increased as a result of many users using the same resources such as memory, networks, data, and programs [15] [19]. The fear of losing or exposing confidential and sensitive organizational data to a third party due to the increased number of parties, devices and applications on the cloud is also an important IS management issue in cloud computing [1] [19]. These could lead to breach of data confidentiality as current data retention strategies over the Internet platform have been proved not to be efficient [17]. There have been frequent issues of unauthorized access to user accounts as a result of weak access control and Application Programming Interface (API) infrastructures [17] which makes confidentiality and privacy one of the top IS management issues with cloud computing.

Privacy means that control of disclosure of personal information lies with the information owner [19]. Privacy is a serious management issue with cloud computing because data might be saved in numerous locations within a country or even in different countries which poses a bigger risk of confidentiality and privacy breach [19]. Another problem with this issue is that there are legal challenges towards privacy issues involved in data stored in the cloud across different countries because each country have their own laws and jurisdiction regarding confidentiality and privacy [19]. This becomes a serious information systems management issue because it is difficult to determine which country's law to apply in case of breach of privacy.

2.2.2 Integrity

Integrity means only an authorized person can make changes to data, software, and/or hardware [19]. There are many users sharing the same resources in the cloud, as a result authorization is very important because authorization ensures that only the necessary permissions are given to a user to gain access to read, modify, or update data [19]. In a case where an employee who is unhappy decides to delete or make unnecessary changes to data, it may be difficult to identify the perpetrator as fingers might be pointed to the service provider [19].

Authentication can help resolve this issue as the user with such permissions can easily be identified. It is very difficult for an organization to check the data handling practices of the cloud service provider and confirm that their data is being handled in a lawful way [8].

2.2.3 Availability

Availability means that data, software, and/or hardware will be accessible and usable on demand [19]. Availability also means that the system should continue working without any interruptions even when there is a breach of security [19]. Service providers cannot guarantee availability because cloud computing requires internet services to function and if there is a problem with internet, cloud computing services will also be affected, hence the issue of availability becomes an important information systems management issue .

Researchers and organization and continuously researching on security, confidentiality and privacy, integration, and availability issues and these issues may no longer be serious issues in the coming five years.

The legal and jurisdiction issues related to cloud computing implementation will now be discussed.

2.3 Legal and Jurisdictional

Legislative and jurisdictional issues are very important Information Systems management issues in cloud computing because of the possibility of data centers being located in locations with different jurisdictions [8]. There is an urgent need for law makers to come up with useful regulations which will help in determining the applicable legislation in cases where data is located in different jurisdictions [8]. Legal and Jurisdictional issues with regards to cloud computing are being discussed by different countries and the different law makers. This issue may be resolved before the next five years.

Data lock-in as a result of lack of standardization of application programming interfaces across different platforms from different service providers will be discussed next.

2.4 Data lock in

The application programming interfaces (API's) for cloud computing are not standardized and moving from one service provider to another might be difficult [1]. The lack of standardization of user interface gives rise to management issues such as the fear of uncertainty that the provider might go out of business, price might increase, as well as reliability issues which may arise as a result of data lock in [1]. The possible solution to this issue is the standardization of API's to enable users to move freely from one service provider to another without the fear of possible data lock in [1]. Data lock-in issue may be resolved before the next five years as service providers are working towards a standardized API which will allow customer

Conference'13, December 1–2, 2013, Wuhan, China.

organization to migrate their data and applications easily from one service providers' platform to another.

There is also a need for standardized service level agreement (SLA) to ensure that agreed level of service is reached by the service provider at all the time. The lack of standardized SLA's for cloud computing will now be discussed because it is also an important management issue with cloud computing.

2.5 Lack of standardized service level agreements (SLA's)

There are different variety of SLA's in cloud computing market because of the different definitions of cloud computing resources which are often described through different non standardized resources such as execution time, inbound bandwidth, outbound bandwidth, CPU cores, and processor type [12]. The difference in the application programming interfaces and service providers also makes it difficult to have a standardized SLA [12]. There is a need for service providers and users to standardize SLA's that will guide their business relationship and help to ensure delivery of agreed services and infrastructure. Reference [20] has a different view of SLA's because they believe that cloud computing provides guaranteed quality of service (QoS) through SLA's with users on the issues of availability, serviceability, performance, operation, billing, and penalties whenever there is a violation of the SLA. The view of reference [20] is correct but it does not prove that there is standardization as it specifies that the SLA will be between the service provider and the user which will be for the needs of that specific user. Reference [12]'s view is directed towards having an SLA that can be used for different users without much changes. Lack of standardized SLA will no longer be an issue in the next five years because organizations are having better understanding of cloud computing as the technology evolves.

Another important management issue with cloud computing is customization as organizations are concerned with applications and services that are customizable for their specific business in order to differentiate them from their competitors. Customization issues will now be discussed.

2.6 Customization

Customization is also an important IS management issue because organizations like to customize their applications and services as they believe it makes them unique and gives them a competitive edge over competitors [7]. The sharing of resources by different users in cloud computing prevents service provider from being able to customize their services to suit the different customer needs [7]**.** Customization is an important management concern because of the need for uniqueness. [20], have a contrary view to that of reference [7] because they said that users can customize and personalize their computing environments like software installation, and network configuration. It is therefore the organizations responsibility to investigate further and find out about which service provider offers the kind of customization they desire before choosing a service provider.

Technological bottleneck is another important management issue with cloud computing. Organizations need to procure technologies that will support cloud computing to be efficient in their cloud computing implementation. Technological bottleneck will be discussed below.

2.7 Technological bottlenecks

Cloud computing requires organizations to upgrade their existing technology in terms of new data structures in order for them to be able to handle dynamic and large amounts of data, new file systems, and storage technologies [6]. The upgrading of existing technologies will involve buying of new technologies and getting rid of old unnecessary one's that are not needed for cloud computing. This is an important management issue because management has to decide on an efficient and economical way to achieve this without incurring too much cost. Technological bottlenecks will not be an issue if organizations can acquire all the necessary technology that supports cloud computing or upgrade their existing technologies to meet cloud computing requirements.

Cloud computing is associated with strategy issues as it requires a number of change in an organization.

Strategy issues and change management will be discussed next.

2.8 Strategy issues

The introduction of cloud computing will bring about a change in the organizations Information Technology (IT) structure [11]. Some of the questions that need to be answered to resolve the strategy issues are: What type of cultural change does the organization need, how will the change be addressed, and how will the organization prevent employee resistance of cloud computing [11]. One of the possible changes in the IT structure due to the introduction of cloud computing could be the downsizing of Information Technology (IT) department as most of the work done by the IT department will now be done by the cloud computing service providers [8]. This can also lead to a decrease in job satisfaction of technical staffs, support care staff , and sales and marketing staff as most of the technical roles will be taken up by third party service provider and technical staffs will only be left to do some reporting work and resolving issues with third party service providers [8]. This is a sensitive issue because employees may not accept cloud computing because of the fear of losing their job or being reduced to support personnel's whose job will be to log complaints to the service provider [8]. The question of whether the organization has skilled IT professionals with experience to manage cloud computing is also an important strategic issue [10]. The effect of cloud computing on organization culture and how well the management is able to address this issues and convince the employees to accept cloud computing will be influential in determining the success or failure of their cloud computing implementation [11].

2.9 Change Management

The implementation of cloud computing brings about a change in the way organizations carry out their daily activities. The process of change management is therefore a serious management issue because it will determine the success of the organizations cloud computing implementation [4]. Proper change management practices should be put in place in order to overcome issues as a result of change. Strategy issues and change management issues will not be an issue in the coming five years if organizations can develop necessary strategies and come up with adequate change management strategies.

Implementation issues are also important management issues as the success of implementation will bring about the desired change through cloud computing to the organization. Implementation issues will be discussed in the following section.

2.10 Implementation Issues

Organizations find it difficult to determine which of their data should be moved into the cloud and which should remain on the organizations traditional system [8]. Organizations are also concerned about how to migrate their data into the cloud without any interference in their businesses during migration. Organizations are also faced with the issue of how to integrate their traditional in-house applications with cloud applications [8]. Implementation issue will be resolved by the next five years when the API issue is resolved and movement across different API's is enabled.

Organizations on the same cloud can affect one another's reputation as any problem caused by one of the organizations will be traced to the shared resources which will have necessary consequences on other organizations. The issue of reputation fate sharing will be discussed in the next section.

2.11 Reputation Fate Sharing

The problem of reputation fate sharing arises when one organization sharing the same resources with other organizations has a bad reputation and this affects other organizations [16]. This is a major management issue because organizations will not like the activities of other organizations to affect them as they have their own integrity to protect. An example of reputation fate sharing was when the FBI agents in Unites states raided a data center because there was a suspected cybercrime being committed from hardware in the data center [16]. Because of that, the operations of all the organizations sharing that data center was halted during the period that the FBI agents were looking for evidence for the cybercrime case. Another example is was when attackers managed to subvert Amazon EC2 and sent a large amount of SPAM to be sent out from the Amazon Cloud [16]. The incident forced Amazon to change its policies and request additional security steps for users to access the system [16].

Another important management issue is cloud computing's dependent on the internet. This issue is discussed in details below.

2.12 Dependence on Internet

The dependence of cloud computing on the internet is a serious management issue because if there is any problem with the internet, cloud computing will be affected. Cloud computing depends on internet to function properly [16]. If there is no internet connection, it automatically means cloud computing cannot function. Slow internet connections will also affect service delivery of cloud computing. In order to resolve this issue, customer organizations should endure they subscribe to a reliable internet service provider who will guarantee consistent, fast and reliable internet connection. Organizations can also have back up internet connections like wireless connections which they can automatically switch to when their main internet connection is down. Dependence on the internet may not be resolved in the coming five years as there is no alternative to the internet.

Quality of service which is also an important management issue will be discussed in the following section.

2.13 Quality of Service

The quality of service offered by the service provider is an important management issue because organizations are concerned about moving their important applications to the cloud of they are uncertain about the ability of the service providers to commit to the high quality of service [11]. Quality of service issue will be resolved in the coming five years once the service level agreement for cloud computing has been standardized.

Another important management issue is transparency which is required from the service provider to gain the trust of customer organizations. This issue will be discussed in the following section.

2.14 Transparency

Cloud service provider does need to disclose their security policies, design, practices, and relevant security measures in daily operations to their customers as this will help cloud service providers gain customers trust [4]. SLA's should contain services to be delivered, performance, tracking and reporting, problem management, legal compliance, resolution of disputes customer duties, security responsibility, and confidential information termination as this will help ensure that the agreed service level is reached [4]. Transparency issue may be resolved in the next five years if it is discussed in the SLA and the service provider is opened to the customer organizations.

Energy management, which is an issue that mainly lies with the service providers' management, will be discussed next.

2.15 Energy Management

Data centers have been found to consume high amounts of energy. "It has been estimated that the cost of powering and cooling accounts for 53% of the total operational expenditure of data centres" [21]. The continuous growth of computing applications and data requires larger servers and disks for fast and efficient processing. An important management issue for service providers is to find a way to lower the energy consumption of the data centers [2]. The increase in energy consumption is a serious management issue as it can increase the Total Cost of Ownership (TCO) and reduce the return on investment (ROI) of cloud infrastructures [2]. Energy management could be resolved in the coming five years through the use of proper workload management and energy saving technologies like virtualization which will reduce the number of physical servers and in turn reduce energy consumption.

Another management issue which is solely on the service provider's side is workload management. This issue is discussed in the following section.

2.16 Workload management

Service providers also face the issue of workload management because they need to be able to share the available resources among their different customers to meet the changing demands of their customers. Efficient workload management will help in the maximization of resources and reduce waste [2]. Efficient workload management will also help to reduce energy consumption because unused resources can be turned off or switched to energy saving mode. Workload management issue may be resolved in the coming five years if efficient algorithms are developed to allocate workload to the resources and maximize resource usage.

Disaster recovery is also an important management issue. This issue is discussed below.

2.17 Disaster recovery

Management is concerned with the continuity of their business and the possibility of fully recovering from a disaster [4]. This leaves management with issues of trying to establish whether the service provider has necessary disaster recovery and business continuity plans in place should there be a loss of data, software, or hardware as a result of a disaster. Disaster recovery management issue may be resolved in the coming five years if appropriate plans such as data backup are put in place and incorporated into the SLA.

Insecure application programming interfaces (API's) and integration issues are other important management issues in cloud computing. These issues are discussed in the following sections.

2.18 Insecure application programming interfaces (API's)

Cloud computing users unable to monitor events associated with API use and incomplete log data to enable reconstruction of management activity. The available security control mechanism may also not be adequate to combat API hacks. This may lead to unauthorized people gaining access to privileged data and functionalities [9]. This issue may be resolved in the coming five years through standardization of API's.

2.19 Integration Issues

Organizations prefer to implement the hybrid model in order to have control over their important and sensitive data and infrastructure [3]. The less sensitive data is then migrated to a public cloud. Managements find it difficult to integrate their in-house infrastructure and service provider's infrastructure because of the different API's which makes the infrastructure incompatible [1]. Standardization of API's will also help resolve these issues in the coming five years.

Malicious insiders, risk management, and performance measurement which are also important management issues with cloud computing are discussed in the following sections.

2.20 Malicious insiders

An employee of the service provider may also cause a security breach because the employee may have access to confidential data and services which may then be exposed to unauthorized third parties. This is a serious management issue for service providers because they have an ethical duty [9]. This issue may be resolved in the coming five years if service providers include appropriate remedies in the employment contract in case of a breach by the employee.

2.21 Risk Management

Cloud computing exposes organizations to a wide range of risks most of which has been discussed earlier in this paper. The management of these risks is a serious issue because the success of cloud computing implementation depends on proper management, reduction, and mitigation of risks associated with cloud computing [5]. This issue may be resolved in the coming five years through the implementation of available risk management practices such as disaster recovery planning.

2.22 Performance measurement

Measuring the service delivery level of service providers is a serious management issue for organizations to determine whether the service provider meeting the agreed service level as stipulated in the SLA [4]. This issue may be resolved in the coming five years if clear measurement goals are defined in the SLA.

Figure 1 is a conceptual model of management issues with cloud

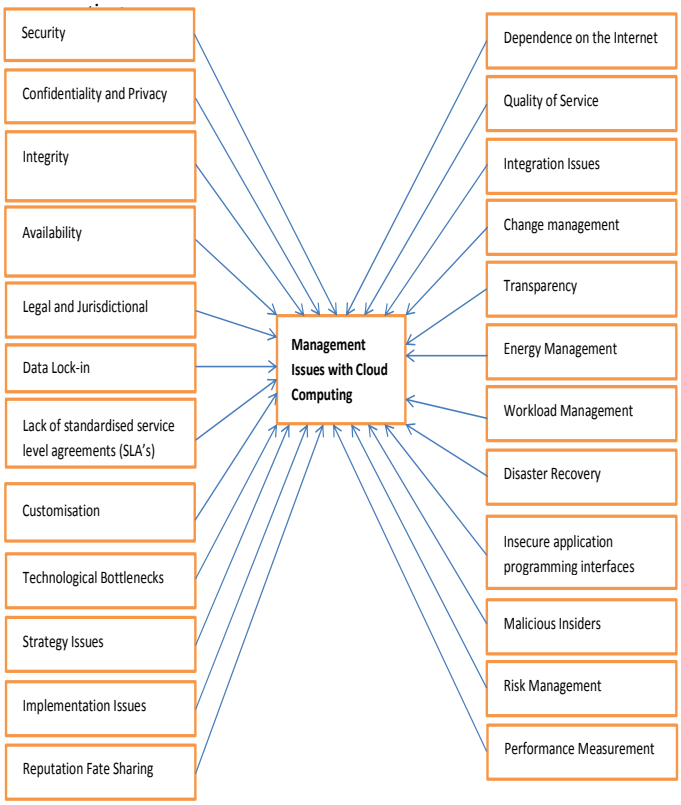

Figure 1: Conceptual Model of Management Issues with Cloud Computing

3. CONCLUSION

Cloud Computing promises a better cloud computing experience for organizations in the future. The limitations of cloud computing such as security issues, confidentiality and privacy issues, strategic issues, availability, data lock-in etc. will no longer be a serious management issue in future as researchers and organizations are consistently looking for solutions to this issues. To make cloud computing more secure and save, control measures should be put in place to mitigate security risks. This paper provides an overview of IS management issues with cloud computing as a guideline to assist management in the implementation of cloud computing. Risks should be thoroughly considered to ensure integrity, privacy, data and application availability in the cloud.

Consideration should be given to risks to ensure completeness, integrity and availability of applications and data in the cloud

4. ACKNOWLEDGMENTS

Our thanks to God for giving us grace to complete this work. We would also like to thank Chief and Mrs Oladapo Akande for their advice and guidance towards the success of this work. This

research is supported by National Research Foundation of South Africa (NRF).

5. REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. . A. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "Electrical Engineering and Computer Sciences, University of California at Berkeley," 10 February 2009. [Online]. Available: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf. [Accessed 12 July 2013].

[2]A. Beloglazov, J. Abawajy and R. Buyya, "Energy-aware resource allocation heuristics for efficient management of data centers for Cloud computing," *Future Generation Computer Systems*, vol. 28, no. 1, p. 755–768, 2012.

[3] E. D. Canedo, R. T. de Sousa Junior and R. de Oliveira, "Trust model for reliable file exchange in Cloud Computing," *International Journal of Computer Science & Information Technology (IJCSIT)*, vol. 4, no. 1, pp. 1-18, 2012.

[4] M. Carroll, A. Van der Merwe and P. Kotzé, "Secure Cloud Computing: Benefits, Risks and Controls," in *Information Security South Africa*, Rosebank, 15 - 17, August 2011.

[5] P. G. Dorey and A. Leite, "Commentary : Cloud computing e A security problem or solution?," *Information Security Technical Report*, vol. 16, no. 1, pp. 89 - 96, 2011.

[6] S. Goel, R. Kiran and D. Garg, "Impact of Cloud Computing on ERP implementations in Higher Education," *International Journal of Advanced Computer Science and Applications*, vol. 2, no. 6, pp. 146-148, 2011.

[7] A. Joint and E. Baker, "Knowing the past to understand the present - issues in the contracting for cloud based services," *Computer Law and Security Review*, vol. 27, no. 1, pp. 4 0 7 - 4 1 5, 2011.

[8] A. Khajeh-Hosseini, D. Greenwood and I. Sommerville, "Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS," in *IEEE 3rd International Conference on Cloud Computing*, Florida, 5 - 10 July, 2010.

[9] T. M. Khorshed, S. A. Ali and S. A. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," *Future Generation Computer Systems*, vol. 28, no. 1, pp. 833 - 851, 2012.

[10] A. Lin and N.-C. Chen, "Cloud computing as an innovation: Percepetion, attitude, and adoption," *International Journal of Information Management*, vol. 1142, no. 1, pp. 1 - 8, 2012.

[11] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang and A. Ghalsasi, "Cloud computing - The business perspective," *Decision Support Systems*, vol. 51, no. 1, p. 176–189, 2011.

[12] M. Maurer, V. C. Emeakaroha, I. Brandic and J. Altmann, "Cost–benefit analysis of an SLA mapping approach for defining standardized Cloud computing goods," *Future Generation Computer Systems*, vol. 28, no. 1, pp. 39 - 47, 2012.

[13] S. C. Misra and A. Mondal, "Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding Return on Investment," *Mathematical and Computer Modelling*, vol. 53, no. 1, pp. 504 - 521, 2011.

[14] S. Paquette, P. . T. Jaeger and S. C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," *Government Information Quarterly*, vol. 27, no. 1, pp. 245 - 253, 2010.

[15] V. Ratten, "Entrepreneurial and ethical adoption behaviour of cloud computing," *Journal of High Technology Management Research*, vol. 1, no. 1, pp. 1 - 11, 2012.

[16] J. C. Roberts II and W. Al-Hamdani, "Who Can You Trust in the Cloud? A Review of Security Issues Within Cloud Computing," in *Information Security Curriculum Development Conference*, Kennesaw, October 7 - 9, 2011.

[17] D. Teneyuca, "Internet cloud security: The illusion of inclusion," *Information Security Technical Report*, vol. 16, no. 1, pp. 102 - 107, 2011.

[18] X. Wang, Z. Du and Y. Chen, "An adaptive model-free resource and power management approach for multi-tier cloud environments," *The Journal of Systems and Software*, vol. 85, no. 2, pp. 1135 - 1146, 2012.

[19] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 1, pp. 583 - 592, 2012.

[20] L. Wang, G. Von Laszewski, M. Kunze and J. Tao, "Cloud Computing: a Perspective Study," *New Generation Computing*, vol. 28, no. 2, pp. 137 - 146, 2010.

[21] M. Ahmed, A. S. M. R. Chowdhury, M. Ahmed and M. M. H. Rafee, "An Advanced Survey on Cloud Computing and State-of-the-art Research Issues," *International Journal of Computer Science Issues*, vol. 9, no. 1, pp. 201 - 207, 2010.

[22] T. Dillon, C. Wu and E. Chang, "Cloud Computing: Issues and Challenges," in *24th IEEE International Conference on Advanced Information Networking and Applications*, Perth, Australia, 20 - 23 April, 2010.