Security Threats and Challenges in Cloud Computing Application

Abdulrahman Saidu
Department of Computer Science, Federal Polytechnic Bali, Taraba State Nigeria
abdulrahmansaidu@gmail.com

Abstract

Security issues and challenges is the major concern of data storage on cloud. The paper discuses the most recent vulnerable security threats in cloud computing, which will enable both end users and cloud providers to take necessary measures. In particular, the paper makes critical evaluation on various challenges that impede successful hosting of data on cloud such as lack of data confidentiality and integrity, inadequate policy to manage security threats, software vulnerability, inadequate access to client information, loss of data, breach of trustworthiness and cloud compatibility issue. .The paper aims to discover the most susceptible security threats and issues in cloud computing environment. Also, the paper provides some recommendations that will enhance the security challenges of cloud computing application.

Keywords: *Cloud computing, Security, threats, challenges, application and data.*

INTRODUCTION

The application of cloud computing is receiving fast recognition from various stakeholders due it importance. (Masud *et al*., 2012, Pocatilu *et al*., 2009, 2010a, 2010b, Greenhow, *et al*., 2009, Ramgovind, *et al*., 2010, Leavitt, 2009& Dong, *et al*., 2009). Cloud computing is an informal expression used to describe different types of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet (Carrol *et al*., 2012 and Leavitt, 2009). This means that Cloud computing is a type of computing that relies on sharing computing resources rather than having local services on personal devices to handle applications. Additionally, cloud computing can be seen as a computing model based on networks especially the Internet, whose task is to ensure that users can simply use the computing resources on demand and pay money according to their usage by a metering pattern like water and electricity consumption (Masud *et al*., 2012). Therefore, cloud computing can be referred as storing and sharing data over internet through various cloud application tools. The aim of this paper is to discover the most susceptible security threats and issues in cloud computing environment. This will provides an opportunity for stake holders to take necessary measures for enhancing security in cloud storage.

TYPES OF CLOUD COMPUTING

Some researchers reported that there are four types of cloud such as private, public , hybrid and community cloud(Kulkarni, *et al*., 2012 and Dillon & Chang 2010) reported).With slight contrast other researchers reported that cloud include: private, public, hybrid and virtual private cloud(Zhang & Boutaba 2010). In the other hand some studies carried out by (Ramgovind, *et al.*, 2010, Sabahi, 2011, and Ramya & Ramya 2013) reported that there are three type of cloud (private, public hybrid cloud).

a. *Private cloud:* - this type of cloud is operated solely within a single organization, and managed by the organization or a third party regardless whether it is located premises or off premise (Dillon & Chang 2010).In slight contrast, it is used and own by an organization internally, anyone within the organization can access the data, services and web application except for outside users (Kulkarni, *et al*., 2012).Zhang & Boutaba (2010), reaffirmed the above assertions and added that, a private cloud provides the upmost degree of control over performance, trustworthiness and security.
b. *Public cloud:* - this is used by the public cloud consumers and the cloud service provider has the full ownership of the public cloud with its own policy, value and profit costing, and charging model (Dillon & Chang 2010). Similarly, it is for the public where resources such as web applications and web services are shared over the internet for users. (Kulkarni, *et al*., 2012).Zhang & Boutaba (2010), confirmed the above authors and further that public clouds lack fine-grained control over data, network and security settings, which hinders their effectiveness in various commercial activities.
c. *Hybrid cloud:* -This kind of cloud consist of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data application probability (e.g., cloud bursting for load-balancing between clouds (Dillon & Chang 2010). Likewise, it is reported by (Kulkarni, *et al*., 2012) Hybrid cloud is a combination of two or more clouds (public, private, and community) in which multiple internal or external suppliers of cloud services are used. In contrary to the above statements, Zhang & Boutaba (2010) reported that, hybrid cloud is a combination of public and private cloud models that tries to address the limits of each method. The further that it provides additional flexibility compared to public and private clouds. Precisely, hybrid cloud offers strong control and security over application data than public cloud.
d. *Community Cloud:* - This type of cloud is operated by several organizations jointly construct and share the same cloud infrastructure as well as policies, requirements, values and concerns (Dillon & Chang 2010). The authors added that, the cloud infrastructure could be hosted by a third-party vendor or within one of the organizations in the community. Kulkarni, *et al*., (2012) equally, reported that it is a mixture of two or more clouds, which is shared among organizations for single reason (mainly security concern) and managed by third party or within. They added that its cost is less compare to public cloud but more than private cloud.

SERVICE LAYERS OF CLOUD COMPUTING

Cloud computing operate under three basic service layers which comprised the of Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) (Ramya, 2015; Matthew, 2015; Masud *et al.*, 2012;Pocatilu, *et al*, 2009;Kulkarni, *et al*, 2012; Pocatilu, *et al.*, 2010a;Ramgovind, *et al.*, 2010; Dillon & Chang 2010 and Al Noor, *et al.*, 2010). Each of these categories achieve a specific goal and support different outputs for organizations and individuals throughout the universe.

Software as a Service (SaaS)

Kulkarni *et al*., (2012) reported that, SaaS is run by cloud service providers through internet and mostly used by organization. This assertion was supported by (Matthew 2015; Goel *et al*., 2011; Ramgovind *et al*., 2010 and Low, *et al*., 2011). Mathew and Goel *et al*., added that the applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email) or a program interface. Similarly, SaaS is a process by which different software applications are provided by the application service provider as a rental over the internet, leveraging cloud infrastructure and services released by Salesforce.com (Low, *et al*., 2011). Likewise, Software‘s are provided as a service to the clients according to their requirement and enables the clients to use the services that are hosted on the cloud server (*Shaikh & Haider*, 2011)

Platform as a Service (PaaS)

In this category, a client is provided with the ability to install onto the cloud infrastructure, consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The client does not manage or control the underlying cloud infrastructure (network, servers, operating systems, or storage), but has control over the installed applications and perhaps configuration settings for the application-hosting environment (Matthew, 2015). Similarly, according to Shaikh & Haider (2011)Clients are provided platforms access, which enables them to put their own customized software‘s and other applications on the clouds. In contrast to this Kulkarni *et al*., (2012) reported that PaaS is a tool (windows, LINUX) used by developers for developing Websites without installing any software on the system, and can be executed without any administration expertise.

Infrastructure as a Service (IaaS)

In IaaS, a client is provided with processing, storage, networks and other fundamental computing resources where the customer can deploy and run arbitrary software, which can include operating systems and applications (*Shaikh & Haider*, 2011 and Matthew, 2015). The customer does not manage or control the underlying cloud infrastructure (network, servers, operating systems, or storage), but has control over operating systems, storage and deployed applications; and maybe restricted control of select networking components (Matthew, 2015). In support of this statement, Low, *et al.*, (2011) and Kulkarni *et al*., (2012) reported that IaaS is operated, maintained and controlled by cloud service providers that support various operations like storage, hardware, servers and networking. Low, *et al.*, added that service providers own the equipment and is responsible for housing it. Stability and reliability of the IaaS is guarantee through hardware and software virtualization technologies (Dong, *et al*., 2009)

CLOUD COMPUTING APPLICATION TOOLS

The role cloud computing application in teaching and learning processes can be delivered in several ways. In an article written by Thomas (2011) on potential of cloud computing application in scholarship of teaching and learning found that Google docs and Microsoft SkyDrive are among the vital tools for effective delivery of knowledge. However, the limitation of the study is lack of an indication as which methodology was used. An investigation carried by Cachin *et al.*, (2009) on trusting the cloud confirmed the findings of Thomas (2011) and further revealed that Amazon S3, Amazone EC2, Google Apps, Nirvanix Cloud NAS and Apple Mobile Me are application tools for cloud computing. Mobile Me allows users to synchronous common applications that run multiples devices. Generally, these tools allow easy collaboration with colleagues. However, the authors argued that risk was involved over releasing control of client data and the availability of online service is the major concern due to downtime as reported recently with Google Mail, Hotmail, Amazon S3 and Mobile Me. The key drawback on this research, the proposed solution to security issue raised on cloud storage is yet to be implemented. In support of both Thomas (2011) and Cachin*et al*. (2009), a similar research carried out by Ramya (2015) found several cloud computing application tools such as Dropbox, Apple iCloud, Google drive, Microsoft One Drive, Amazon Cloud drive, and Box. These cloud application tools support cloud storage, file synchronization and collaboration. Dropbox is a modern workspace designed to reduce busywork for one to focus on the things that matter.

A research conducted by Husain *et al*. (2010) reported Map Reduce is currently an evolving tool for cloud computing in handling large amount of data. The authors further outlined that Scholars and enterprises have applied Map Reduce technology for web indexing search, data mining and semantic web. According to the researchers Semantic Web technologies are being developed to present data in a more effective way which can be retrieved and understood by both users and machine. In another research conducted by Calheiros *et al*. (2011) developed a Cloud Sim toolkit for modeling and simulating extensible Clouds. It is a suitable research tool that can manage the difficulties arising from simulated environments. Therefore, it refers as a platform for modeling and simulation of cloud computing infrastructures and services. The study suggested future work that will incorporate new pricing and provisioning policies to Cloud Sim, to offer a built-in support to simulate the currently available Public clouds. In support of this finding Nurmi *et al*., (2009) built an EUCALYPTUS system which allow administrators and researchers to deploy an Infrastructure as a Service (*IaaS*) for user-controlled virtual machine creation and control upon existing resources.

EVALUATION OF SECURITY CONCERN IN CLOUD COMPUTING PLATFORM

One of the major concern of cloud computing is the safety of the data. Many researchers have revealed the security concern of storing data on cloud atmosphere (Pocatilu, *et al*, 2010a,Sabahi, 2011,whycliff, *et al.*, 2016, Al Zain, *et al.* 2012, Han & Zhang, 2012, Mathew, 2015, Cachin *et al.* 2009, Minqui Zhou,*et al.* 2010, Ramgovind, *et al*. 2010, kresimirpopovic *et al.* 2010, Rewagad & Pawar, 2013, and Shaikh, & Haider, 2011). Despite the benefits of cloud computing for storing data, the cloud is not completely safe or trustworthy since it could be compromised or illegally accessed by an unauthorized third party. In cloud computing environment, security issues could be divided into four types: safety problems caused by virtual technology; root authority of the data center; data security and consistency; and problems prompted by modern technology (Han & Zhang, 2012). A similar study by Goel,*et al*.(2011)supported the above findings.

1. Breach of Trustworthiness

One of the biggest concern of cloud computing is the security issues of data because both data and the software are placed on isolated servers that is not guarantee from smash or vanish without any cautions (Pocatilu, *et al.*, 2010a, Sabahi, 2011 and sheikh & Haider, 2011). This finding was supported by Wycliff (*et al.*, 2016) who revealed that data security has always remained a major issue in cloud application since data are scattered at various places all over the globe. Similarly, Al Zain *et al. (*2012), reported that in everyday computing, security is one of the most acute aspects to be considered and it is no less important for cloud computing due to the sensitivity and significance of data stored in the cloud.

Recent studies reveled that stored data on cloud platform are liable to leakage by unauthorized users. In study conducted by Shaikh, & Haider (2011) on security threats in cloud computing that aimed to identify the most vulnerable security threats in cloud computing, revealed that the most concern security issues are data loss, leakage of data, client‘s trust, user‘s authentication, malicious users handling, wrong usage of cloud computing and its services, and hijacking of sessions while accessing data. Some these challenges are confirmed by Mathew (2013) who reported that cloud data is unreliable and customer lacks control on their data. Shaikh, & Haider further reported that there is no security standards available for securing cloud computing. This point out that a lot of researches are needed to secure data on cloud storage. Studies conducted by Cachin*et al.* (2009), Minqui Zhou *et al.* (2010), kresimirpopovic *et al.* (2010) and Popović & Hocenski (2010) reaffirmed the above findings. Likewise, Kumar &Kumar (2013) added that data breaches and other attacks are resulted from negligent authentication, week password, and poor key or certificate management. This findings is supported by Chen *et al.*, (2010) who revealed that password weakness is among the security challenge of cloud computing. Kumar &Kumar recommended that clients should use multifactor authentication and encryption to protect against data breaches.

1. Lack of Data Confidentiality and Integrity

Mathew (2015) examined the trends, benefits and challenges being encountered for adopting cloud computing in Nigerian Universities. An empirical research via questionnaire was used to generate data for the study. The study found challenges of cloud computing adoption in Nigerian University as shown in the table below

Table 1: Challenges of using Cloud Computing Adoption in Nigerian Universities (Mathew, 2015).

S/N	Challenges of using Cloud Computing in Nigeria Universities	% of Respondents
1	Data insecurity	89.3
2	Unsolicited Advertising	64.6
3	Lock-in	77.6
4	Reluctance to eliminate staff positions	64.6
5	Privacy Concerns	68.9
6	Reliability challenge	64.2
7	Regulatory compliance concerns / User control	80.0
8	Institutional culture / resistance to change in technology	59.2

From the findings above, data insecurity is the highest security challenge follow by regulatory compliance concern/user control. The study indicates that client does not have control over their stored data on cloud and this post major challenge.

In support of the above results, similar studies carried by Cachin *et al.* (2009), Minqui Zhou *et al.* (2010), kresimirpopovic *et al.* (2010) and Lin (2012) disclosed that there are various threats concerning cloud storage security which include: lack of total access to owner information, absence of proper control, inadequate compliance to the law governing cloud storage, lack of data integrity, lack of audit, privacy breach, and poor confidentiality. A study by Ramgovind, *et al.* (2010) on the management of security in cloud computing adoption confirmed the above findings and added that data segregation, recovery, investigative support, long-term viability and data availability are among the challenges of adopting cloud computing application. In support of both Mathew (2015), Minqui Zhou *et al.* (2010), kresimirpopovic *et al.* (2010) and Ramgovind, *et al.* (2010) a study by Rewagad & Pawar(2013) revealed that privacy, confidentiality and integrity are among the forefront of security issues in cloud and it demands a trustworthy computing atmosphere so that data confidentiality can be maintained. In contrast to above findings, a study by carried out by Goel *et al.*, (2011) on the impact of cloud computing on ERP implementations in higher education, discovered challenges of implementing cloud computing for ERP in higher technical education such aselasticity complexity, superstructure emergence, technological bottlenecks, serializability and consistency, programming model; monitoring, analysis and building trust, mobility and provisioning.

2. Inadequate Policy to Manage Security Threats

Lack of proper policy to handling hackers is one of the major concerns of data storage on cloud and many studies have confirmed this statement. (Mathew, 2015, Kumar & Kumar, 2013 and Shaikh & Haider, 2011). This shows that cloud computing lacks proper standardization in their system of operationi.

Similarly, ….(10 security concerns for cloud computing) reported that the Service Level Agreement (SLA) between cloud providers and customers is not provided adequately. The above findings agreed with Lin, (2012) who revealed that legal and contractual issues should be addressed. Dillon & Chang (2010) confirmed Lin, that when customers migrated their core business functions onto their entrusted cloud service providers, there is need to ensure the SLA are adhere in terms quality, availability, reliability, and performance.

3. Software Vulnerability

Cloud is vulnerable. This means that it is possible to perform unauthorized actions by hackers in computer system. This statement is supported by Kumar & Kumar (2013) who reported that organizations share memory, databases, and other resources in close proximity to one another and this create new room for attacks. However, the study suggested that the vulnerabilities can be mitigated with regular vulnerability scanning, prompt patch management and quick follow-up on reported system threats.

4. Inadequate Access to Client Information

In study carried out by Mathew (2015) revealed that clients lack total control on their stored data on cloud. Also, it has been reported that data stored on a cloud service provider's server can potentially be accessed by an employee of that company, and you have no control over it.[ii] Access control is a key concern in cloud computing, because an insider may attack client data which is very risk. In early 2009 an insider was accused of planting a logic bomb on Fanny Mae server, which would have caused enormous destruction if launched. To manage the above problem Lin, (2012) reported that customers need to have full access to their data cloud.

5. Loss of Data

Due to measures taken by cloud providers, loss of data becomes extremely rare (Kumar & Kumar, 2013).However, the authors reported that hackers have being permanently deleting data to harm clients business and cloud data centers are vulnerable to natural disaster. This finding is supported by Shaikh, & Haider (2011) who reported that one of the major concerns of cloud service is loss of data. Similarly, Chen *et al.*, (2010) reaffirmed the above findings that one of the fundamental issues in cloud data storage that data is liable to loss. Kumar & Kumar further recommended that, adequate measures for data backup, off-site storage and disaster recovery should be adhere to best IT practice for business sustainability in case of any disasters. Mathew (2015) reported that data storage on cloud is unreliable. Similarly, Cloud Security Alliance (CSA) has reported that" attacks have surfaced in recent years that targeted the shared technology inside Cloud Computing environment."[ii]

6. Cloud Compatibility Issue

Due to recent advancement of technology that involve in cloud computing, compatibility post issues that affect most of the companies. Challenge arises due to the fact that company would have to replace much of its existing IT infrastructures to make the system compatible on the cloud. However, using hydride cloud solves this problem. In line with this Popović & Hocenski (2010) reported that services provided by one cloud vendor may be incompatible with another vendor's services, if a client decides to move from one to the other (e.g. Microsoft cloud is incompatible with Google cloud).

CONCLUSION

The reviewed found that there are number of security issues and threats on cloud storage such as lack of proper policy to govern cloud storage, inadequate access to client information, breach of trustworthiness, technological bottlenecks, lack ICT infrastructure, managerial problems, absence of qualified personal to manage ICT facilities/equipment, lack of data confidentiality and integrity.

RECOMMENDATIONS

- Mutual understanding and collaboration between cloud service providers and clients is highly needed for enhancing cloud security issues.
- Adequate policy for handling cloud services should be provided to ensure safety and security of data on cloud.
- Client should examine security policy before signing contract with cloud providers.
- Client should engage end-to-end monitoring of data over the cloud. This will provide effective control of data by the customers.
- The client should know the type of data encryption that will be applied on their data and control it. For instance there is different between WEP and WPA2.

REFERENCES

Al Zain, M., Soh, B., & Pardede, E. (2012). A New Approach Using Redundancy Technique to Improve Security in Cloud Computing. IEEE.

Al Noor, S., Mustafa, G., Chowdhury, S. A., Hossain, M. Z., & Jaigirdar, F. T. (2010). A proposed architecture of cloud computing for education system in Bangladesh and the impact on current education system. IJCSNS International Journal of Computer Science and Network Security, 10(10), 7-13.

Beckham, J. (2011), 'The Top 5 Security Risks of Cloud Computing' available at: http://blogs.cisco.com/smallbusiness/the-top-5-security-risks-of-cloud-computing/

Chen, Y., Paxson, V., & Katz, R. H. (2010). What's new about cloud computing security? University of California, Berkeley Report No. UCB/EECS-2010-5 January, 20(2010), 2010-5.

Chander *et al*. (2013) International Journal of Advanced Research in Computer Science and Software Engineering Vol 3(5) May -2013, pp. 570-575

Calheiros, R. N., Ranjan, R., Beloglazov, A., De Rose, C. A., & Buyya, R. (2011). CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. Software: Practice and experience, 41(1), 23-50.

Cachin, C., Keidar, I., & Shraer, A. (2009). Trusting the cloud. AcmSigact News, 40(2), 81-86.

Dillon, T., Wu, C., & Chang, E. (2010, April). Cloud computing: issues and challenges. In Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on (pp. 27-33). Ieee.

Goel, M. S., Kiran, R., & Garg, D. (2011). Impact of cloud computing on ERP implementations in higher education. INSTITUTIONS, 5(8).

Husain, M. F., Khan, L., Kantarcioglu, M., &Thuraisingham, B. (2010, July). Data intensive query processing for large RDF graphs using cloud computing tools. In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on (pp. 1-10). IEEE.

Han, D. and Zhang, F. (2012), Applying Agents to the Data Security in Cloud Computing. International Conference on Computer Science and Information Processing (CSIP). IEEExplore Pp. 1126 – 1127

kresimirpopovic and Zeljko Hocenski (2010) Cloud Computing Security and Challenges in MPRO

Kumar, P., & Kumar, L. (2013). Security Threats to Cloud Computing. *International Journal of IT, Engineering and Applied Sciences Research (IJIEASR)*, *2*(1).

Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. Industrial management & data systems, 111(7), 1006-1023.

Lin, G. (2012, April). Research on electronic data security strategy based on cloud computing. In Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on (pp. 1228-1231). IEEE.

Mariana Carroll, Paula Kotzé, Alta van der Merwe (2012). "Securing Virtual and Cloud Environments". In I. Ivanov *et al*. Cloud Computing and Services Science, Service Science: Research and Innovations in the Service Economy. Springer Science+Business Media.doi:10.1007/978-1-4614-2326-3.

Minqui Zhou, Rong Zhang (2010) "Security and Privacy in Cloud Computing: A Survey" In Sixth International Conference on Semantics, Knowledge and Grids.

Rewagad, P. and Pawar, Y. (2003), Using Digital Signature with Differ Hellman Key Exchange and AES Encryption Algorithm to Enhance Data security in Cloud Computing.

International Conference on Communication System and Network Technologies IEEExplore Pp. 437 - 438

Veeraju Gampala, SrilaskhmiInuganti, SatishMuppidi, “Data Security in Cloud Computing with Elliptic Curve Cryptography” vol. 2 Issues 3, July, 2012.

Dong, B., Zheng, Q., Yang, J., Li, H., &Qiao, M. (2009, July). An e-learning ecosystem based on cloud computing infrastructure. In Advanced Learning Technologies, 2009. ICALT 2009. Ninth IEEE International Conference on (pp. 125-127). IEEE.

Pocatilu, P., Alecu, F., & Vetrici, M. (2010a). Cloud Computing Benefits for E-learning Solutions. Oeconomics of Knowledge, 2(1), 9-14.

Greenhow, C., Robelia, B., & Hughes, J. E. (2009). Learning, teaching, and scholarship in a digital age Web 2.0 and classroom research: What path should we take now?. Educational researcher, 38(4), 246-259.

Masud, M. A. H., & Huang, X. (2012). An e-learning system architecture based on cloud computing. System, 10(11).

Matthew, F.T., 2015. Cloud Computing In Education—A Study of Trends, Challenges and an Archetype for Ef-fective Adoption in Nigerian Universities. Information Communication Technology (ICT) Integration to Educational Curricula: A New Direction for Africa, p.119.

Nurmi, D., Wolski, R., Grzegorczyk, C., Obertelli, G., Soman, S., Youseff, L., &Zagorodnov, D. (2009, May). The eucalyptus open-source cloud-computing system. In Cluster Computing and the Grid, 2009. CCGRID'09. 9th IEEE/ACM International Symposium on (pp. 124-131). IEEE.

Pocatilu, P., Alecu, F., & Vetrici, M. (2010b). Measuring the efficiency of cloud computing for e-learning systems. WSEAS Transactions on Computers,9(1), 42-51.

Pocatilu, P., Alecu, F., & Vetrici, M. (2009, November). Using cloud computing for E-learning systems. In Proceedings of the 8th WSEAS international conference on Data networks, communications, computers (pp. 54-59). World Scientific and Engineering Academy and Society (WSEAS).

Popović, K., & Hocenski, Ž. (2010, May). Cloud computing security issues and challenges. In MIPRO, 2010 proceedings of the 33rd international convention (pp. 344-349). IEEE.

Ramgovind, S., Eloff, M. M., & Smith, E. (2010, August). The management of security in cloud computing. In Information Security for South Africa (ISSA), 2010 (pp. 1-7). IEEE.

Ramya, R., & Ramya, K. (2013). Cloud computing.

Saidu, A., Clarkson, M. A., & Mohammed, M. E-Learning Security Challenges, Implementation and Improvement in Developing Countries: A Review.

Shaikh, F. B., & Haider, S. (2011, December). Security threats in cloud computing. In Internet technology and secured transactions (ICITST), 2011 international conference for (pp. 214-219). IEEE.

Sabahi, F. (2011, May). Cloud computing security threats and responses. In Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on (pp. 245-249). IEEE.

Thomas, P. Y. (2011). Cloud computing: A potential paradigm for practicing the scholarship of teaching and learning. The Electronic Library, 29(2), 214-224.

Wycliff, O. J., Saidu, A. & Adamu S. (2016). Enhancement of Data Security in Cloud Computing: Issues and Challenges. IOSR Journal of Computer Engineering 18(2) 12-17

Weihai, P.R. (2013), Data Security in Cloud Computing. The 8th International Conference on Computer Science and Education (ICCSE) IEEExplor. Pp. 811- 813 Columbo, Sri Lanka

Wang, Q., Wang, C., Ren, K., Lou, W. and Li, J. (2011). Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing IEEE Transactions on Parallel and Distributed System Vol. 22, No. 5, Pp. 848 – 849.

Kulkarni, G., Chavan, N., Chandorkar, R., Waghmare, R., & Palwe, R. (2012, October). Cloud security challenges. In *Telecommunication Systems, Services, and Applications (TSSA), 2012 7th International Conference on* (pp. 88-91). IEEE. APA

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications, 1(1), 7-18.

[i] http://mobiledevices.about.com/od/additionalresources/tp/The-Risks-Involved-In-Cloud-Computing.htm accessed 17/09/13

[ii] http://blogs.cisco.com/smallbusiness/the-top-5-security-risks-of-cloud-computing/ accessed 17/09/13