Cloud Computing Security: An Investigation into the Security Issues and Challenges Associated with Cloud Computing, for both Data Storage and Virtual Applications

Hamisu Alhaji Ali
Department of Computer Science
School of Sciences, Mai Idris Alooma Polytechnic,
P.M.B 1020 Geidam Yobe State
hageidam@gmail.com

ABSTRACT: ***In recent years, cloud computing has developed from the promising business concept that it used to be, to one of Information Technology (IT) industry's most developing section. Now that the world economy was hit by recession, the victims of this tragedy continually understand that by just out-sourcing or tapping the cloud resources, a package of virtualise, elastic, instant on-demand provision, and scalable; infrastructure, platform, and software can be access fast and easy inform of services at a negligible amount via the internet. However, as individuals and organizations embarked on the course of deploying their information and data into the cloud, anxieties are beginning to develop on whether the cloud environment is safe. This research provides an overview of the cloud deployment model, the services they offer and discusses the security issues and challenges of cloud computing in both data storage and virtual applications/servers.***

Keywords: Cloud computing, security, risks, issues, deployment models, virtualization, service delivery models.

I. INTRODUCTION

United State National Institute of Standard and Technology (NIST) henceforth referred to as NIST in Jansen (2011) defined cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction". In addition, NIST proposed four cloud computing deployment models, three service delivery models, and five features of cloud computing .

The year 2009 saw the overwhelming international economic deterioration as felt across large number of industries amongst which is information technology industry. However, even at that time, there were groups showing expectation in the centre of all the confusion. A distinguished IT analyst, Gartner, foresees that cloud computing would be the fundamental origin of development in IT spending, "increasing over 20% year-on-year to global revenues of $56bn in 2009 and surging to $130bn by the year 2013" (Rhoton, 2010, p.3).

Moreover, the current development of cloud computing has desperately changed everyone's understanding of infrastructure architecture, software delivery and deployment models (Zissis and Lekkas, 2012). Cloud computing has developed from being a propitious business conception to one of the quick developing section of IT industry (Subashini and Kavitha, 2011).

Considerable researches were conducted on the security issues and challenges of cloud computing. Nonetheless, this research work investigates the security issues and challenges specific to cloud-based environment, focusing on data storage and virtual applications/servers. Moreover the research has also discussed the cloud computingdeployment models, service delivery models and analysed the risks of using these models. Furthermore, mitigations have been proposed against the cloud computing security threats.

II. RELATED WORK

Cloud computing deployment models

Jamil and Zaki (2011) described three types of cloud models, namely; Private cloud, Public cloud, and Hybrid cloud. Rani and Marimuthu (2012) outlined four major types of cloud computing deployment models as; Private cloud, Public cloud, Hybrid cloud, and Community cloud (see figure 1 below).

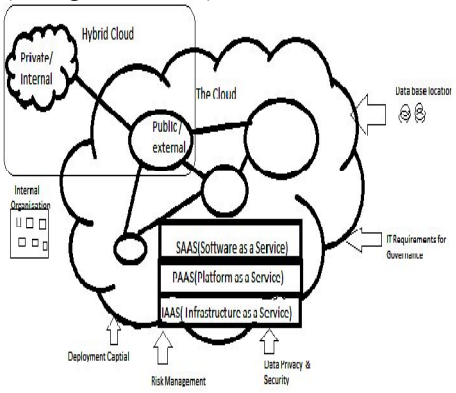


Figure 1;Miniature of cloud computing deployment models (Kumar, 2012)

IRJECE

Private cloud

Carlin and Curran (2011) described private cloud as a cloud environment that emulate cloud computing concept by means of private networks. In private clouds, the infrastructures are hosted internally within the datacentre of an organization. Moreover, it varies from public cloud because organization manages their cloud applications and resources synonymous to intranet. On the other hand, users face a huge expenditure, in that they need to provide the infrastructure and management needed to run the cloud. Yet, Private cloud give clients full control on how data is being managed as well as the measures taken to secure the environment.

Public cloud

According to Metri and Sarote (2011) public cloud is a cloud model in which the computing infrastructure is housed by the cloud proprietor on his premises. The user has no idea or say on the location of the infrastructure, and any organizations can utilise and share the infrastructure. Public cloud is cost effective because management cost are shared and distributed between organizations or businesses and large number of individual users (Kumar, 2012).

Hybrid cloud

According to Bowen (2011) hybrid cloud infrastructure is the combination of two or more clouds (private, public or community) which remain separate bodies, yet put together through an authoritative mechanism or standard technology that permits portability of application and data (e.g., 'load-balancing in cloud bursting'). Furthermore, the internal services are firewall protected and can be access by authorized stakeholders only, while the external services are accessible to the general public. Furthermore, organizations can host applications that are critical on a private cloud and use public cloud for applications with minimal security requirement (Sabahi, 2011).

Community cloud

Community cloud model as the name implies, is for a particular community formed by many organizations that have common goals (Cheng and Lai, 2012).

Cloud computing service delivery models

Mathisen (2011) is of the opinion that cloud service delivery models are fundamentally classified into three.

Software as a Service (SaaS)

Software as a service is the delivery of software to users of cloud computing over the internet through browsers, the most common uses of SaaS are; email-client, antivirus, and word processors. Users utilised this model to carryout business and social computing task via internet and pay for the service and not the software used. Moreover, SaaS has control the usual desktop problems of compatibility, upgrading, installation problems, etc. Yet, SaaS architecture is particularly tailored to cater for multiple users simultaneously (multi-tenancy) (Kuyoro'Shade, Frank and Oludele, 2011).

Platform as a Service (PaaS)

PaaS is identical to SaaS, however, platform as a service provides full development framework, from design down to implementation and testing. PaaS makes it possible for developers to out-source virtual development frameworkinform of instant on-demand service via internet and use it to develop and deploy application using tools and programming languages supported by vendor (Rani and Marimuthu, 2012). In addition, PaaSprovides an Integrated Development Environment (IDE) that supports a full application development life-cycle (planning, design, building application, deployment, testing and maintenance).

Infrastructure as a Service (IaaS)

IaaSdelivers computing infrastructure as services inform of Virtual Machine (VM) that has all the resources needed by the developer. In addition, a user can request for Infrastructure or resources needed over the internet through web-browser and pay for the usage rather than buying the software, network tools, servers, datacentre and the expertise needed to handle them. Furthermore, since cloud services are extremely flexible, a client can automatically shrink or grow the number of VMs running at a particular time (Ertaul, Singhal and Saldamli, 2011).

Characteristics of cloud computing

NIST in Che et al. (2011) mentioned five fundamental features of cloud computing; virtualized resource pool, broad network access, rapid elasticity, on-demand self-service, and measured service. A client can request for computing resources as an instant on-demand service without human intervention.Capabilities are accessed via network that permits the use of different types of platform (laptops, PDAs and mobile phones). Moreover, computing resources are pooled to provide services to many customers using multi-tenant protocols and capabilities that are vigorously allocated and reallocated based on client request.

Jurisdiction issues in cloud computing

The ability to store, share, and localize data in large number of countries as please by the service provider is a significant feature of cloud computing. However, a company relinquishes authority over its data as soon as it chooses to use cloud computing. Consequently, the company will find it difficult to ensure proper security of data and information as different jurisdictions in which the data resides have different legislative laws (e.g., the United State stored communication Act and Patriot Act are threats to privacy and confidentiality of data) (Yves and Andre, 2010).

IRJECE

In Libya for example, encryption is forbidden unless Government is supplied with the decryption software, while in China, the government has been given unlimited access to all types of data by local laws. Nevertheless, data protection laws (European Union data protection directives) that provide rights and safeguards to individuals on how personal data are processed have been enacted in all the 27 EU member states. Other non EU States such as; Argentina, United Arab Emirate (UAE), Hong Kong, Canada, Israel, and Russia also enacted data protection laws unanimous to the European Union model (Ward and Sipior, 2010).

Virtualization

Among the essentials characteristics of cloud computing is the ability to elastically shrink or grow storage capability or computing ability according customer demand, which is possible through virtualization technology. Virtualization is the process of abstracting computer resources from the underlying infrastructure. The application layer that provides virtualization is known as hypervisor or Virtual Machine Monitor (VMM) (Kong, 2011). Moreover, virtualization is the technology that permits cloud scalability, multi-tenancy and elasticity among others. It uses physical cloud resources particularly server and partition it into smaller virtual resources known as virtual machines.

Furthermore, virtualization offers the essential abstraction required to make sure that business services and applications are not bound directly to the underlying infrastructure (storage, servers or networks) that provides them, e.g., the Amazon's EC2 (Gurav and Shaikh, 2010). In addition, virtualization is basically the technology that permits a single server or PC to run many operating systems concurrently. This enables cloud users to run software or applications that are intended for distinct operating system on one machine rather than using different hardware for each operating system.

Cloud computing issues and challenges

A contemporary survey conducted by the Cloud Security Alliance (CSA) and Institute of Electrical and Electronics Engineers (IEEE) in kuyoro,Shade, Frank and Oludele (2011) symbolizes that, enterprises are keen to embrace cloud computing but security is required both to hasting the acceptance of cloud computing on a broad scale and to respond to regulatory drivers.

Furthermore, a survey by International Data Corporation (IDC) on cloud computing issues and challenges in Popovic and Hocenski (2010) also shows that security is the main challenge that hinders the wider adaptation of cloud computing by businesses and organizations (see figure 2 below). In addition, the survey also claimed that cloud computing is configuring the future of information technology; however, lack of conforming environment is having sensational effect on thedevelopment and wider acceptance of cloud computing.

Data storage security

Due to the multi-tenancy background of cloud computing, enterprise's data hosted on the cloud are kept in collocated manner alongside other customer's data in a shared environment, whereneither the exact location of enterprise's data nor the actual sources of other customer's data is known to them.

Consequently, there are several security concerns and uncertainties surrounding the cloud data storage system in term of data integrity, availability, and confidentiality (Pearson and Benameur, 2010). Some of which include;

Centralized facilities

Because cloud computing implements storage inform of a centralised facility, it will potentially be an interesting target for cyber attackers or criminals. This has constantly been the case with any important resources or computing assets. Any vulnerable organization may be used as "bot" to attack other organizations which shares the environment and facilities with it, a successful

Cloud attack could or will affect thousands or even millions of organizations and individual (due to multi-tenancy and data collocation) (Pearson and Benameur, 2010).

Multi-tenancy

Multi-tenancy presents another burden or concerns either because of potential operation failure in data isolation mechanism or rollback operation from a backup system. Multi-tenancy also lead to other storage risk such as; data leakage, seizure, and "bot" threat.

System complexity

Cloud storage systems are normally implementations of complex software and hardware. Hence there are concerns about potential destruction of data or exposure to unauthorised owners as a result of catastrophic failure or system malfunction.

Data integrity

Ensuring that data is only change or alters in accordance with authorized transaction, usage, or operation (transfer, retrieve, storage, etc.) is what is referred to as integrity. However, this is not certain in the world of cloud computing as there is not yet a universal standard for ensuring data integrity (Eartual, Singhal and Saldamli, 2009).

Unauthorised usage

Some of the cloud vendors could use clients data in order to earn revenue mostly targeting advertisement, and although it is part of the standard of cloud business model, the owner will be extremely displease where the situation involve confidential record (medical, account, etc.) or resale of comprehensive sales record to other customer which are competitors to the client

IRJECE

Virtualization security

Cloud computing is a new way of using the internet which is access through web browsers, and virtualization as defined in section 2.5 is the abstraction and isolation of the computing resources from the underlying infrastructure (hardware) thereby making the promise of cloud computing realisable. Consequently, the cloud environment will be vulnerable to all types of internet and browser attacks (hacking, frauds, distributed denial of service attack, SQL injection attack, man in the browser attack, cross-site scripting attack, session hijacking, man in the middle attack, packet sniffing, port scanning, IP spoofing, etc.). This is because virtualization has now exposed the cloud to cyber-attacks by simplifying the complex and sophisticated security found in traditional on-premise data centres.

Issues in adopting cloud computing technology

According to the distinguished IT analyst 'Gartner' (2008) in Heiser and Nicolett (2008) there are seven main issues that needs to be addressed before adopting cloud computing infrastructures, namely; Privilege user access, Regulatory compliance, Data location, Data segregation, Data recovery, Investigative support, and Long-term viability.

Risk of adopting cloud computing infrastructure

According to SAN Institute (SysAdmin Audit Networking and Security) in Bisong and Rahman (2011), "risk is the potential harm that may arise from some current process or from some future event, while risk management is the process of understanding and responding to factors that may lead to failure in the confidentiality, integrity or availability of an information system".

III. METHOD

The materials used are books, e-books, journals, e-journals, conference papers, magazines and symposium, which were accessed from the Wolverhampton university library catalogue and other reputable databases, such as ACM digital library, Science direct, Computer sources, EBSCO host research, Safari, etc. The research evaluate, analyse, compare, contrast and summarise the ideas and opinions of the various authors and provides an overview of the cloud computing deployment models, the services they offer, and the security issues and challenges facing these services, particularly data storage and virtual applications/servers.

IV. RESULTS AND EVALUATION

Research questions:

1. What are the specific security issues and challenges in a cloud computing environment?
2. How can these security threats be avoided or mitigated and user re-assured?

The researcher has successfully answered both questions to some extend by given an elaborate detail of the security issues and challenges of cloud computing. Moreover, the research has make itclear to its audience that most of the security threats been perceived related to cloud computing are not peculiar to cloud computing, but are rather general network security threats.

Furthermore, the questions were not answered well because of lack of adequate literatures on the subject matter. Most of the available literature focused on general network security threats and other internet security related issues. However, the research was able to discuss some security threats that are specific to cloud computing; which are posed as a result of multi-tenancy, virtualization, and jurisdictions issues. Therefore, the research has only answered both questions partially, because, question number two depends on question one and can only be answered well if question one is fully addressed.

Nevertheless, two encryption methods (Identity-based encryption and Homomorphicencryption) were proposed so asto mitigate or even stop the threats. The confidentiality, integrity, and privacy of data would be protected by applying these encryption methods, yet meaningful and reasonable computation can be perform on the data although it is encrypted (Kumar, 2012).

Objectives

Four objectives have been set up as follows in order to help the researcher answer the research questions and achieve the research aims;

1. To investigate the security issues and challenges in cloud computing.
2. To analyse the main security risks in a cloud computing system.
3. To determine the security deficiencies and qualify the benefits of cloud computing.

The research has met the above objectives by providing an elaborate discussion of the security issues and challenges associated with cloud computing environment. Furthermore, the study has enumerate and analysed the main security risks in cloud computing. In addition, security shortcomings of cloud computing have been determined and way forward were suggested to help improve the security of cloud domain.

V. CONCLUSION

In this paper, an elaborate discussion of cloud computing deployment models, the services they offer and the security issues and challenges affecting the system was provided. Furthermore, security threats affecting information and network in cloud computing were highlighted.

In addition, the research has clarified issues surrounding cloud computing security and enumerates some of the real cloud computing security issues as oppose to the

IRJECE

perceived ones and suggest mitigation against the threats. Furthermore, cloud computing risks were analysed using risk analysis table in which the risk, its probability of occurrence, and possible impact on organization were compared and analysed.

A large number of researches were conducted about cloud computing security, but most of the issues discussed are general network security threats and not unique to cloud computing. Because cloud computing is a new way of using the internet which is access through web browsers, it is vulnerable to all internet and browser attacks.Nevertheless, the research was able to highlight some attacks that are unique to cloud computing which are mostly due to the cloud's multi-tenancy, data collocation and virtualization nature as well as unstable data centres.

Moreover, it is hopeful that further research would focus more on this and also discover other security issues that are unique to cloud computing in order to provide a more elaborate, thoroughand precise discussion of the cloud computing security issues (real not perceived) so that the cloud would be secure, safe, conforming, and acceptable to governments,universities, and businesses.

ACKNOWLEDGEMENT

This work was supported by Federal government through Tertiary Education Trust Fund (TETFUND).

REFERENCES

[1] Bisong, A. and Rahman, M. S. (2011) An overview of the security concerns in enterprise cloud computing. *International Journal of Network Security and its Applications* [online]. **3**(1), pp. 30-45 [Accessed 02 September 2012]. Available at: <http://arxiv.org/ftp/arxiv/papers/1101/1101.5613.pdf>.

[2] Bowen, A. J. (2011) Cloud Computing: issues in data privacy/security and commercial considerations. *The Computer and Internet Lawyer* [Online]. **28**(8), pp. 1-4 [Accessed 09 May 2012]. Available at: <http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=de61a872-6a3b-4dc8-8cdf-5e51cf7cc29a%40sessionmgr114&vid=5&hid=122>.

[3] Carlin, S. and Curran, K. (2011) Cloud computing security. *International Journal of Ambient Computing and Intelligence (IJACI)* [online]. **3**(1), pp. 14-19 [Accessed 06/may/2012]. Available at: <http://www.ijest.info/docs/IJEST11-03-04-129.pdf>.

[4] Cheng, F.C. and Lai, W.H. (2012) The Impact of Cloud Computing Technology on Legal Infrastructure within Internet—Focusing on the Protection of Information Privacy. *Procedia Engineering* [online]. **29** pp. 241-251 [Accessed 29/05/2012]. Available at: <http://www.sciencedirect.com/science/article/pii/S1877705811065386>.

[5] Che, J., Duan, Y., Zhang, T. and Fan, J. (2011) Study on the Security Models and Strategies of Cloud Computing. *Procedia Engineering* [online]. **23** pp. 586-593 [Accessed 29/05/2012]. Available at: <http://scholar.google.co.uk/scholar?q=Study+on+the+security+models+and+strategies+of+cloud+computing&hl=en&as_sdt=0%2C5>.

[6] Ertaul, L., Singhal, S. and Saldamli, G. (2009) Security Challenges in Cloud Computing. *California State University, East Bay.Academic paper http://www.mcs.csueastbay.edu/~lertaul/Cloud% 20Security% 20CamREADY.pdf* [online]. [Accessed 20/06/2012]. Available at: <http://www.mcs.csueastbay.edu/~lertaul/Cloud%20Security%20CamREADY.pdf>.

[7] Gurav,U. and Shaikh,R. (2010) Virtualization: a key feature of cloud computing *Proceedings of the International Conference and Workshop on Emerging Trends in Technology* ACM [online]. pp. 227-229 [Accessed 06/06/2012]. Available at: <http://scholar.google.co.uk/scholar?hl=en&q=Virtualization+%E2%80%93+A+key+feature+of+cloud+computing&as_sdt=1%2C5&as_sdtp=>.

[8] Heiser, J. and Nicolett, M. (2008) Assessing the security risks of cloud computing. *Gartner Report* [online]. pp. 2-6 [Accessed 02/07/2012]. Available at: <http://cloud.ctrls.in/files/assessing-the-security-risks.pdf>.

[9] Jamil, D. and Zaki, H. (2011) Cloud Computing Security. *International Journal of Engineering Science* [online]. **3**(4), pp. 3478-3483 [Accessed 06/may/2012]. Available at: <http://scholar.google.co.uk/scholar?q=cloud+computing+security&hl=en&as_sdt=0%2C5>.

[10] Jansen,W. A. (2011) Cloud Hooks: Security and Privacy Issues in Cloud Computing *System Sciences (HICSS), 2011 44th Hawaii International Conference on* [online]. IEEE, pp. 1-10 [Accessed 12/may/2012]. Available at: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5719001&tag=1>.

[11] Kong, J. (2011) AdjointVM: a new intrusion detection model for cloud computing. *Energy Procedia*[online]. **13** pp. 7902-7911 [Accessed 29/05/2012]. Available at: <http://www.sciencedirect.com/science/article/pii/S187661021103952X>.

[12] Kumar, A. (2012) World of Cloud Computing & Security. *International Journal of Cloud Computing and Services Science (IJ-CLOSER)* [online]. **1**(2), pp. 53-58 [Accessed 01/07/2012]. Available at: <http://scholar.google.co.uk/scholar?hl=en&q=cloud+computing+security+threats+and+responses+by+sabahi&as_sdt=1%2C5&as_sdtp=>.

[13] Kuyoro'Shade, O., Frank, I. and Oludele, (2011) A. Cloud Computing Security Issues and Challenges. *International Journal* [online]. **3**(5), pp. 247-253 [Accessed 10/may/2012]. Available at: <http://cscjournals.org/csc/manuscript/Journals/IJCN/volume3/Issue5/IJCN-176.pdf>.

[14] Mathisen,E. (2011) Security challenges and solutions in cloud computing *Digital Ecosystems and Technologies Conference (DEST), 2011 Proceedings of the 5th IEEE International Conference on* [online]. IEEE, pp.208-212 Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5936627>.

[15] Metri, P. and Sarote, G. (2011) Privacy Issues and Challenges in Cloud computing. *International Journal of Advanced Engineering Sciences and Technologies* [online]. **5**(1), pp. 5-6 [Accessed 07/may/2012]. Available at:

REJECT

<http://ijaest.iserp.org/archieves/9-M16-31-11/Vol-No.5-Issue-No.1/1.IJAEST-Vol-No-5-Issue-No-1-Privacy-Issues-and-Challenges-in-Cloud-computing-001-006.pdf>.

[16] Pearson,S. and Benameur,A. (2010) Privacy, security and trust issues arising from cloud computing *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*. [online]. Ieee, pp.693-702[Accessed 21/may/2012]. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5708519>.

[17] Popovic,K. and Hocenski,Z. (2010) Cloud computing security issues and challenges *MIPRO, 2010 Proceedings of the 33rd International Convention* [online]. pp. 344-349 [Accessed 20/04/2012]. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5533317>.

[18] Rani, A.M.G. and Marimuthu, A. (2012) A Study on Cloud Security Issues and Challenges. *International Journal* [online].**3**(1), pp. 344-347 [Accessed 01/07/2012]. Available at: <http://www.ijcta.com/documents/volumes/vol3issue1/ijcta2012030164.pdf>.

[19] Rhoton, J. (2010) *Cloud computing: explained.* 2nd ed. London: Recursive Ltd.

[20] Rittinghouse, J. W. and Ransome, J. F. (2010) *Cloud computing: implementation, management, and security*. ; London: CRC Press.

[21] Sabahi,F. (2011) Virtualization-level security in cloud computing *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on* [online]. IEEE, pp. 250-254 [Accessed 21/may/2012]. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6014716>.

[22] Subashini, S. and Kavitha, V. (2011) A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications* [online]. **34**(1), pp. 1-11 [Accessed 12/may/2012]. Available at: <http://www.sciencedirect.com/science/article/pii/S1084804510001281>.

[23] Ward, B.T. and Sipior, J.C. (2010) The Internet jurisdiction risk of cloud computing. *Information Systems Management* [online]. **27**(4), pp. 334-339 [Accessed 21/may/2012]. Available at: <http://www.tandfonline.com/doi/pdf/10.1080/10580530.2010.514248>.

[24] Yves, G. and Andre, L. (2010) Cloud computing: decision about switching to cloud computing should be based on sound practices despite any limitation. *AC Magazine* [online]. **143**(4), pp. 37 [Accessed 18 July 2012]. Available at: <http://scholar.google.co.uk/scholar?q=diving+into+the+cloud&hl=en&as_sdt=0%2C5>.

[25] Zissis, D. and Lekkas, D. (2012) Addressing cloud computing security issues. *Future Generation Computer Systems* [online].**28**(3), pp. 583-592 [Accessed 07/may/2012]. Available at: <http://ac.els-cdn.com/S0167739X10002554/1-s2.0-S0167739X10002554-main.pdf?_tid=7c4c080dd12b41750ed694c7cbe33b93&acdnat=1340290616_7de89fd0dd004c72bc8985e7191c7

IRJECE