Proposing a model of Inter-University Collaboration System Using Cloud Computing Infrastructure

S.C. Echezona, H. C. Inyiama

Abstract: ***The need for research collaborations in Higher Educational and Further Educational world-wide gave rise to National Research and Education Network (NREN). In Nigeria however, many attempts towards the creation of NREN have been made. Some aimed at Development of a platform on which contents can be applied later, such as NUNet. Others were aimed at the development of in-house proprietary contents that may later be integrated with the platform being developed, such as, Nigeria Universities Management Information System (NUMIS). Despite the efforts expended, none of these projects could be fully realized. Uwadia C. et al, (2003), pointed out a number of risk factors that posed a serious challenge to realizing an integrated and sustained network for research and education. The researcher modeled a system based on public cloud that will handle problems of cost flights, expertise and availability, as well as, curb problems of project duration and Total Cost of Ownership (TCO).***

Keywords: NREN, Cloud Computing, Managed Computing, EDUroam, TCO.

I. INTRODUCTION

There is a paradigm shift in the technology that powered most of the existing Education and Research initiatives such as, Joint Academic Network (JANET), China Education and Research Network (CERNET), Nigeria University Network (NUNET), etc. Technology has experienced a dramatic leap with accompanying reduction in the cost of setting up and maintenance. Before now, collaborations can only be achieved through on-premise interconnection of nodes, where the hardware (processors, memory, etc.,) are hosted and managed by the user. Then with the internet came the use of web sites that stand between the served data (the data store) and the user. With internet's wider reach, there is minimal cost compared with the predecessor – the self managed. Even with the internet and web technology, most organizations still develop and maintain their resource in-house, thereby replicating the efforts. Chief Information Officers (CIOs), noticed that this has a number of setbacks, such as, cost of setup of computing facilities, power consumption for each separate node, maintenance cost, and most importantly, it discourages green computing, as there is bound to be more carbon foot-prints, Morgan Stanley, (2011).

In a bid to reduce most of these setbacks, scale-up and scale-out techniques were considered. Scale-up - when the computing power can be increased or scaled-up by increasing the capacity of such components (the memory, the processor, etc.), at the same time expending the same power consumption rate. This scale-up technology gave rise to virtualization. That is, multiple software running on separate partitions of the same hardware when the system is busy. When not very busy however, some system intensive software that require more attention will incorporate the free partitions and hence have access to larger memory space and greater chunk of the processor time. The software that handles these processes is called a hypervisor. VMware is an example of such implementation. This is the technology adopted in such systems that run private cloud. Morgan Stanley, (2011).

For scale-out, rather than increase the power of one system to run many software at the same time, independent and less powerful systems in the form of nodes are linked to use their resources to handle huge jobs. So that, one job can run on one or more nodes at a time. This is the concept of grid computing. Public cloud uses the technology of grid, the major difference being that the grid is used by research institutions, which is used for private purposes, while public cloud is commercially made available by the public cloud providers to provision hardware, software, application programs and other computing facilities in an elastic fashion depending on demand and need. The subscriber pays as he uses. Essentially the rates are relatively low, reminiscent of the mobile telephony in Nigeria where you recharge minimally as you go. Providers of public cloud charge for two services: Storage in gigabytes and bandwidth in giga bits per second.

With the development of computing system in the 70's, computer bureau were responsible for provisioning of computing facilities (through batch processing), then in the 80's came the Internet Service Providers, providing wireless access to computer services. Users can now create web sites to data centers online. Finally, Public Cloud Providers now replace ISPs providing in addition to other services Software as a Service, Platform as a Service, and Infrastructure as a Service, and by extension, anything as a Service. From this development, the researcher believes that the phobia surrounding cloud computing is artificial since computing is simply evolving as usual. Earlier users must have had similar phobia for batch processing and internet since they equally do not have complete control over their software artifacts.

II. OBJECTIVES

The following objectives will be met in this research:

- Propose the use of cloud model to design and implement National Education and Research Network for Nigeria, captioned EIS.
- Used an Object Oriented Design Methodology (UML) to analyze and design the system.

Manuscript Received on July, 2013.

S.C. Echezona, Lecturer, Computer Science Department, University of Nigeria, Nsukka.

H. C. Inyiama, Lecturer, Electronic and Computer Engineering Department, Nnamdi Azikiwe University Awka.

- Designed a model to suit Nigeria Educational Information System (EIS).
- Reviewed security issues as it concerns cloud computing.

III. METHODOLOGY

The methodology adopted is Object Oriented Analysis and Design (OOAD) using Unified Modeling Language (UML). Use Case diagram with Sequence diagram and Activity diagram were used to model many perceived use cases, etc. Figure 1 through figure 5 are examples of these.

Use case problem 1

Research materials available in the EIS can be accessed by the industrialists who are registered with the EIS. They may not know the location of the research materials they will need prior to a search, can have opportunity for a feedback when a result of interest is obtained. Design a use case scenario. The solution is shown in Figure 1.

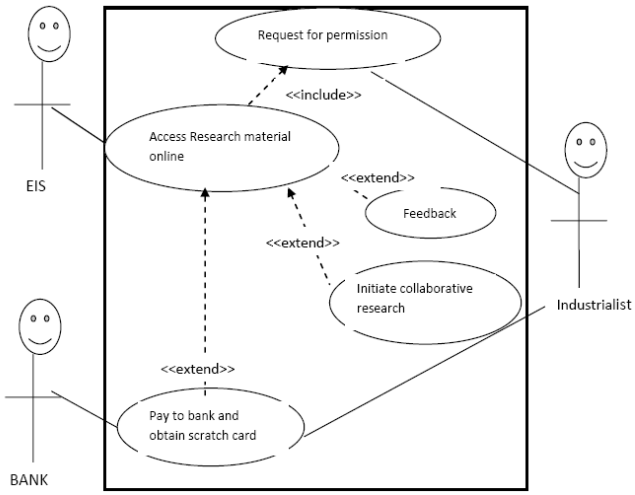

Figure 1: Use case diagram for problem 1

Use case problem 2

Develop a use case scenario of inter-university collaborations, where staff from different universities can collaborate with colleagues in their research works. They can use some of the tools for communication, such as, blog, email, chat room, and audio/video-conferencing. The solution is shown in figure 2.

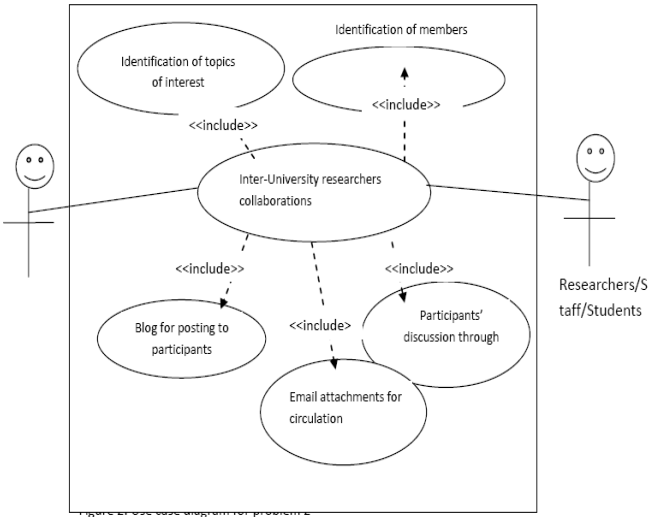

Figure 2: Use case diagram for problem 2

Other use case scenarios could not be included because of space limitation.

The activity diagram of use case of problem 1 is given in figure 3, while figure 4 shows its sequence diagram.

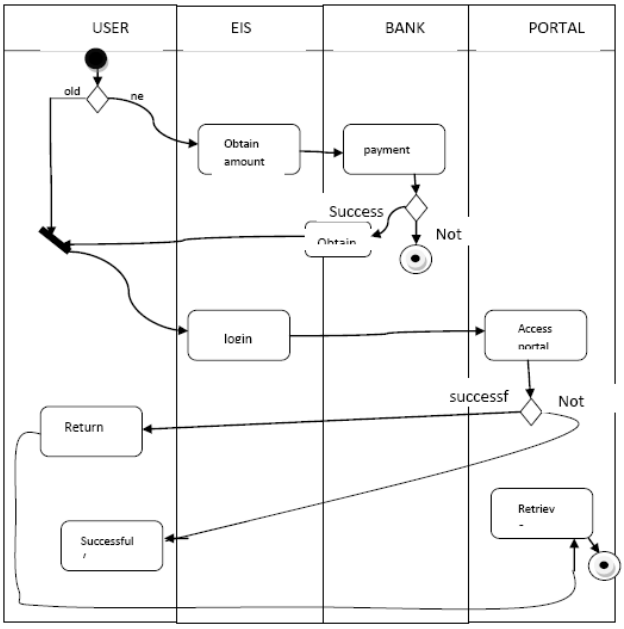

Figure 3: activity diagram of problem 1

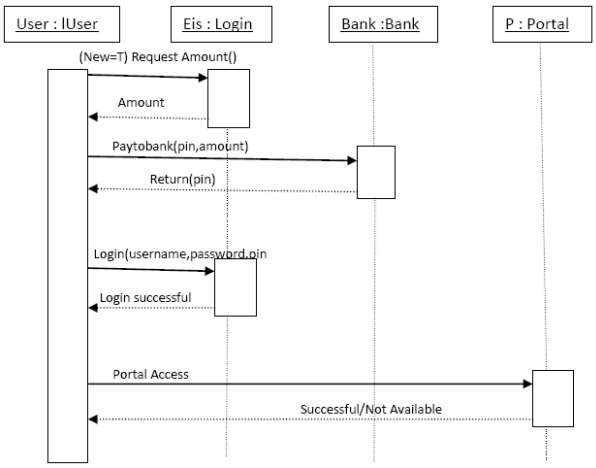

Figure 4: Sequence diagram of problem 1

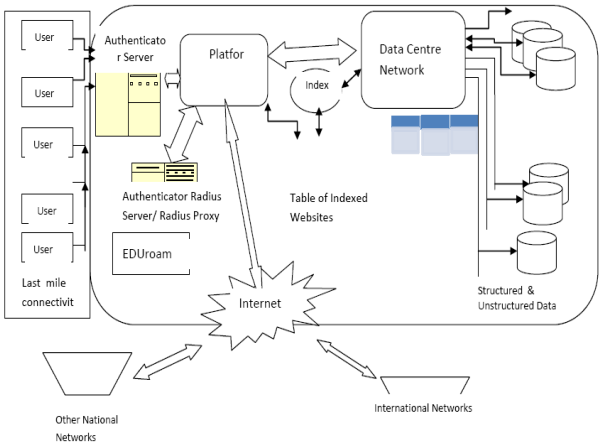

Fig. 5 The perceived model of EIS

This model unlike what obtains from other implementations overseas, has no need for laying fiber optic cables around the country to achieved total connectivity, but exploits the facilities provided by modern IT infrastructure like cloud computing to attain full connectivity speedily with minimal cost and time. There is no time wasted at reinventing the wheel. For instance, the designer at the design stage may not need to know where the data are stored nor the

capacity of the storage; even backup and recovery may no longer be a problem. In fact everything may be offered as a service at minimal costs. Mobile device users are expected to form the major part of users in the system. These are taken care of with the EDUroam software. Even the speed of access (bandwidth) can be provisioned as a service.

According to the design, every class of user is expected to access the EIS software through a single platform (much like a portal's single-sign-on). It is the duty of this platform to accept requests from different users and channel them to the ubiquitous information contained in the EIS. It either channels the request to the unstructured data files or to the structured using the search engine provided within the platform. The researcher looks at the data emanating from the institutions as either unstructured, that is text data that is stored as is without being organized using any data model, and the structured, that is data that is organized using any of the data models such as relational data model etc. Examples of such unstructured data are: Academic research publications, courseware, eBooks, etc. Structured are such data like students personality profile, course registration, student's results, staff data and finance information.

To achieve this, the researcher considered the two options of servicing requests from users to different databases hosting these different classes of data. One option is to replicate the server software among the member databases. This is so as to provide speed and allow each scripting language to have a dedicated connection to a specific database. Figure 6 illustrates this design model. While Figure 7 shows an Agile Engine that solves the same problem with single server software.

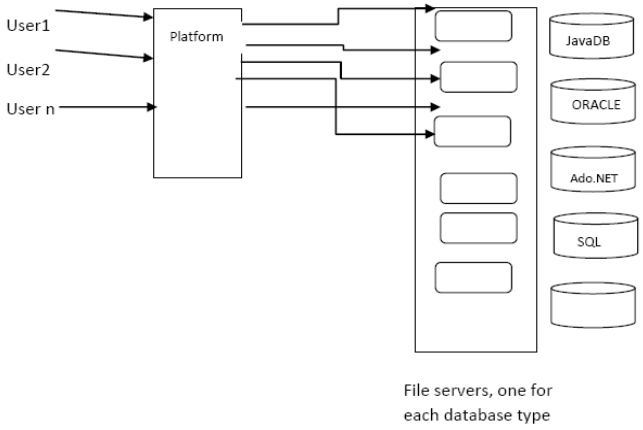

Fig.6 Engine for the selection of desired share resources

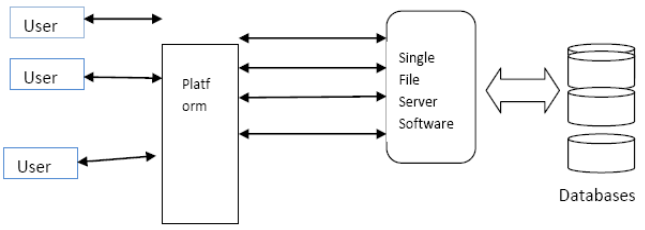

Fig. 7 Agile Engine

Here is a simple algorithm to implement the Agile Search Engine of figure 7:

```
Switch (databaseType)
Case 1:  DB = "mySQL"; MySql ++; break;
Case 2: DB =  "ORACLE" ; ORAC ++; break;
Case 3: DB = "SQL" ; sql++; break;
Case 4: DB = "JavaDB"; Jdb++; break'
Case 5: DB = "Ado.NET"; Ado++; break;
Case n: DB = "Informix"; inf++; break;
Default: return;
Endcase
Conn = DB;
for (int I = 0; I <= n; i++)
SELECT  *
FROM  $table
WHERE condition exist
```

Security issues associated with the cloud

Cloud computing security definition according to Wikipedia: (sometimes referred to simply as "cloud security") is an evolving sub-domain of computer security, network security, and, more broadly, information security, refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing Wikipedia, (Retrieved 2012)There is a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing software, platform, or infrastructure as-a-service via the cloud) and security issues faced by their customers Wikipedia, (Retrieved 2012). In most cases, the provider must ensure that their infrastructure is secure and that their client's data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information, wrote, Winkler Vic., (2011).

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service, Winkler Vic (2011). Virtualization alters the relationship between the operating system and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured, Hickey Carthleen, (2012) Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist, Winkler, Vic., (2011).

Dimensions of cloud security

Correct security controls should be implemented according to asset, threat, and vulnerability risk, Wikipediam (Retrieved 2012). While cloud security concerns can be grouped into any number of dimensions, (Gartner 2010) named seven while the Cloud Security Alliance identifies fourteen areas of concern) these dimensions have been aggregated into three general areas: Security and Privacy, Compliance, and Legal or Contractual Issues.

4.1. Security and privacy

Identity management

Every enterprise will have its own identity management system to control access to information and computing resources. Cloud providers either integrate the customer's identity management system into their own infrastructure, or provide an identity management solution of their own.

Physical and personnel security

Providers ensure that physical machines are adequately secure and that access to these machines as well as all relevant customer data are not only restricted but that access is documented.

Availability

Cloud providers assure customers that they will have regular and predictable access to their data and applications.

Application security

Cloud providers ensure that applications available as a service via the cloud are secure by implementing testing and acceptance procedures for outsourced or packaged application code. It also requires application security measures in place in the production Environment. Privacy
Finally, providers ensure that all critical data (credit card numbers, for example) are masked and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.
Legal issues
In addition, providers and customers must consider legal issues, such as Contracts and E-Discovery, and the related laws, which may vary by country
Business continuity and data recovery
Cloud providers should have business continuity and data recovery plans in place to ensure that service can be maintained in case of a disaster or an emergency and that any data loss will be recovered. Wikipedia, (Retrieved 2012) These plans are shared with and reviewed by their customers.
Logs and audit trails
In addition to producing logs and audit trail, cloud providers should work with their customers to ensure that these logs and audit trails are properly secured, maintained for as long as the customer requires, and are accessible for the purposes of forensic investigation (e.g., eDiscovery).
4.2 Unique compliance requirements.
In addition to the requirements to which customers are subject, the data centers maintained by cloud providers may also be subject to compliance requirements. Using a cloud service provider (CSP) can lead to additional security concerns around data jurisdiction since customer or tenant data may not remain on the same system, or in the same data center or even within the same provider's cloud.
4.3 Legal and contractual issues.
Aside from the security and compliance issues enumerated above, cloud providers and their customers will negotiate terms around liability (stipulating how incidents involving data loss or compromise will be resolved, for example), intellectual property and end-of-service (when data and applications are ultimately returned to the customer). These should be articulated in a Service Level Agreement (SLA).

IV. SUMMARY

What the researcher has done so far can be summarized as follows:

- Proposed the use of cloud model to design and implement National Education and Research Network for Nigeria, captioned EIS
- Used Object design methodology (UML) to analyze and design the system..
- Proposed a model to suit Nigeria Universities
- Reviewed security issues as it concerns cloud computing.

V. CONCLUSION

This research has shown that most of the phobia expressed on cloud computing as regards security is unfounded, since throughout the history of computing, CIO's have been migrating from on-premise computing to managed computing. This is because of the drive to reduce cost of computing services. However, like all other computing processes, security in cloud must be kept in perspective, since it is still vulnerable to attacks from many sources which include:

- Hackers including illegal access to data through sql injection).
- Multi-tenancy (where cotenant may willfully attempt to gain access to another's database.
- The presence of additional layer of software called hypervisor that make a powerful machine a virtual machine, etc.

RECOMENDATION

This write-up having reviewed various attempts at initiating a NREN in the country and their weaknesses, especially when it borders on cost, expertise, project duration and green computing, affirms that the cloud artifact if suitable Service Level Agreement and other IT related security issues are set up and applied, will do better.
Also, the reason why most implementations go moribund is because the designer usually starts from the scratch (in-house design). This will always reinvent the wheel. Ideally, a system tested and trusted can be bought off the shelf and customized at minimal cost, time and expertise. Or outright negotiation with the clouds providers for services

REFERENCES

1. Chand-Ji Wang, Jian-PingWu (2010) Application of peer to peer technology in CERNET, Network Research Centre, Tsinghua Unkiversity Beijing, China.
2. Cloud Computing Security Policies You must Know. CloudComputingSec. 2011. Retrieved 2011-12-13.
3. Cloud Computing Front and Centre" Forrester Research. 2009-11-18. Retrieved 2010-01-25.
4. Communication commission of Kenya (UK) http://www.ck.go.ke
5. Gartner," Seven cloud-computing security risks". InfoWorld. 2008-07-02. Retrieved 2010-01-25.
6. Goggig Greg (2005):Virtual Nation: The Internet in Australia Sydney, UNSW press pp: 33. ISBN 978-0-86840-503-2
7. Hickey, Kathleen."Dark Cloud Study finds security risks in virtualization".. Government Security News. Retrieved 12 February 2012.
8. http:www.cloudsecurityalliance.org.giudance.csguid.v3.0/pdf
9. Jim Roche, Jim Ghadbane, Karthryne Anthonisen (2011): Canada's Advanced Research and innovation Network, 2011 strategic road map for Australian Research Infrastructure Discussion paper, eResearch Infrastructure expert Working Group, 13th April, 2011.
10. Kennedy Aseda (2009): Kenya Education Network Infrastructure, (Current and Future Infrastructure Potential and Emerging possibilities)
11. Kenya Education Network KENET (HTTP://www;kenet.or.ke
12. Security Guidance for Critical Areas of Focus in Cloud Computing. Cloud Security Alliance. 2011. Retrieved 2011-05-04.
13. Swamp computing aka Cloud Computing Web Security Journal. 2009-12-28. Retrieved 2010-01-25.
14. Wik, Philip (2011-10).Thunderclouds Managing SOA- Cloud Risk Service Technology Magazine. Retrieved 2011-21-21.
15. Winkler, Vic.oncerns", Technet Magazine, Microsoft. Retrieved 12 February 2012.
16. Winkler, Vic (2011). *Securing the cloud: Cloud Computer Security Technologies and Tactics.*. Waltham, MA USA: Elsevier. pp. 59.ISBN Securing the Cloud Cloud Computer Security Techniques and Tactics.
17. Winkler, Vic (2011): Securing the Cloud" Cloud Computer Security Techniques and Tactics. Waltham, MA USA: Elsevier. pp. 65, 68, 72, 81, 218–219, 231, 240.ISBN 978-1-59749-593-9
18. Uwadia C, et al, (2006): Risk factors in the collaborative development of Management Information System for Nigerian Universities, Information Technology for Development, InterScience, Wiley Periodicals Inc. vol. 12(2) 91-111 (2006).