SECURITY AND RELIABILITY ISSUES IN THE DEPLOYMENT OF CLOUD COMPUTING SYSTEM

Araoye, Olalekan I.
Dept. of Computer Studies, The Federal Polytechnic, Ado-Ekiti, Ekiti State, Nigeria
araoyek@yahoo.com

Akintoye, Kayode A.
kintos20@yahoo.com

Abstract
The Cloud Computing (CC) is a new computer paradigm that provide Computer services in the form of services on demand, accessible from anywhere, anytime and by anyone. It aims to provide reliable, customized, dynamic computing environments focused towards better quality of service and IT infrastructure availability without much financial burden. There are numerous security issues for Cloud Computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. In this paper we explore security and reliability issues that are involved in deploying a secured and reliable Cloud Computing system.

Keywords: Cloud Computing, Networks, Database, Operating System, Resource Scheduling

1.0 Introduction
Cloud Computing is a concept proposed by several researchers [2], which consists to incorporate and to use several Cloud Computing Service Providers to provide a uniform resource interface for the client. The cloud offers several benefits like fast deployment, pay-for-use, lower costs, scalability, rapid provisioning, rapid elasticity, ubiquitous network access, greater resiliency, hypervisor protection against network attacks, low-cost disaster recovery and data storage solutions, on-demand security controls, real time detection of system tampering and rapid re-constitution of services[4]. The Cloud Computing came in lime light in 2007, its popularity has increased swiftly since then due to its ability to offer flexible dynamic IT infrastructures, good Quality of Service, computing environments and configurable software services [3]. Although Cloud Computing has attracted much attention but still there are no widely accepted definition for it. Several reasons have contributed to this situation [1]:

- Cloud Computing involves researchers and engineers from various backgrounds, e.g., grid computing, software engineering and databases. They work on this computing from their own and different viewpoints.
- Technologies which enable Cloud Computing are still in progressing stage, for example, Web 2.0 and Service Oriented Computing.
Existing computing clouds still lack large scale deployment and usage, which would finally justify the concept of CC. understand

The Cloud Computing is a concept that combines several technologies to deliver different services. It is a passage from the Computer to the Internet. Users are no longer owners of their Computer Servers but may gain many services Online scalable without having to manage the underlying infrastructure, often complex. Companies in this context would no longer need for clean rooms or servers or computer scientists. All applications are leased and run through the browser or application servers.

2.0 Cloud Computing Architecture

Architecture of Cloud Computing mainly comprises of four layers: Application, Platform, Infrastructure, and Hardware as shown in figure 1 below. These four layers facilitate three different types of cloud services, that’s Software as a Service, Platform as a Service and Infrastructure as a Service. These layers are described in detail as follows

i. Software as a Service (SaaS):
This provides typically hosts and manages a given application in their own data center and makes it available to multiple tenants and users over the Web. Some SaaS providers run on another cloud provider’s PaaS or IaaS service offerings. Oracle CRM On Demand, Salesforce.com, and Netsuite are some of the well-known SaaS examples.

ii. Platform as a Service:
Platform as a Service (PaaS) is an application development. It facilitates development and deployment of applications without the cost and complexity of buying and managing the underlying infrastructure, providing all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available from the Internet. This platform consists of infrastructure software, and typically includes a database, middleware and development tools. A virtualized and clustered grid computing architecture is often the basis for this infrastructure software. Some PaaS offerings have a specific programming language or API. For example, Google AppEngine is a PaaS offering where developers write in Python or Java. EngineYard is Ruby on Rails. Sometimes PaaS providers have proprietary languages like force.com from Salesforce.com and Coghead, now owned by SAP.

iii. Infrastructure as a Service:
Infrastructure as a Service (IaaS) is the delivery of hardware (server, storage and network), and associated software (operating systems virtualization technology, file system), as a service. It is an evolution of traditional hosting that does not require any long term commitment and allows users to provision resources on demand. Unlike PaaS services, the IaaS provider does very little management other than keep the data center operational and users must deploy and manage the software services themselves--just the way they would in their own data center. Amazon Web Services Elastic Compute Cloud (EC2) and Secure Storage Service (S3) are examples of IaaS offerings.
3.0 Cloud Computing Model

The Cloud Computing model has three main deployment models which are:

1. Private cloud
2. Public cloud
3. Hybrid cloud
4. Community cloud

1. Private cloud

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization’s internal enterprise data centre. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud.

2. Public cloud

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

3. Hybrid cloud

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both public and private clouds.
Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems. Hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services. It can also describe configurations combining virtual and physical, collocated assets - for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter.

4. Community cloud The cloud infrastructure is shared among a number of organizations with similar interests and requirements. This may help limit the capital expenditure costs for its establishment as the costs are shared among the organizations. The operation may be in-house or with a third party on the premises.

4.0 Security Issues In Cloud Computing
In traditional data centres, IT managers put procedures and controls in place to build a hardened perimeter around the infrastructure and data they want to secure. This configuration is relatively easy to manage, since organizations have control of their servers’ location and utilize the physical hardware entirely for themselves.

In the private and public cloud, however, perimeter boundaries blur and control over security diminishes as applications move dynamically and organizations share the same remotely located physical hardware with strangers.

4.1 Areas of Security
The following areas need to be secured in Cloud Computing for liability use

i. Multi-Tenancy
Cloud Computing users share physical resources with others through common software virtualization layers. These shared environments introduce unique risks into a user’s resource stack. For example, the cloud consumer is completely unaware of a neighbour’s identity, security profile or intentions. The virtual machine running next to the consumer’s
environment could be malicious, looking to attack the other hypervisor tenants or sniff communications moving throughout the system. Because the cloud consumer’s data sits on common storage hardware, it could become compromised through lax access management or malicious attack. In a joint paper published in November 2009 by MIT and UCSD entitled “Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds,” the authors exhibited the possibility of a side-channel attack in a cloud environment in which an attacker would be able to implant some arbitrary code into a neighbour’s VM environment with little to no chance of detection. In another scenario, a security bulletin from Amazon Web Services reported that the Zeus Botnet was able to install and successfully run a command and control infrastructure in the cloud environment.

ii. Data Mobility and Control
Moving data from static physical servers onto virtual volumes makes it remarkably mobile, and data stored in the cloud can live anywhere in the virtual world. Storage administrators can easily reassign or replicate users’ information across data centers to facilitate server maintenance, HA/DR or capacity planning, with little or no service interruption or notice to data owners. This creates a number of legal complications for cloud users. Legislation like the EU Privacy Act forbids data processing or storage of residents’ data within foreign data centers. Careful controls must be applied to data in cloud computing environments to ensure cloud providers do not inadvertently break these rules by migrating geographically sensitive information across political boundaries. Further, legislation such as the US Patriot Act allows federal agencies to present vendors with subpoenas and seize data (which can include trade secrets and sensitive electronic conversations) without informing or gaining data owners’ consent.

iii. Data Remanence
Although the recycling of storage resources is common practice in the cloud, no clear standard exists on how cloud service providers should recycle memory or disk space. In many cases, vacated hardware is simply re-purposed with little regard to secure hardware repurposing. The risk of a cloud tenant being able to gather pieces of the previous tenants’ data is high when resources are not securely recycled. Resolving the issue of data remanence can frequently consume considerable negotiating time while establishing service agreements between an enterprise and a cloud service provider.

iv. Data Privacy
The public nature of cloud computing poses significant implications to data privacy and confidentiality. Cloud data is often stored in plain text, and few companies have an absolute understanding of the sensitivity levels their data stores hold. Data breaches are embarrassing and costly. In fact, a recent report by the Cloud Security Alliance lists data loss and leakage as one of top security concerns in the cloud. Recent laws, regulations and compliance frameworks compound the risks; offending companies can be held responsible for the loss of sensitive data and may face heavy fines over data breaches. Business impacts aside, loose data security practices also harm on a personal level. Lost or stolen medical records, credit card numbers or bank information may cause emotional and financial ruin, the repercussions of which could take years to repair. Sensitive data stored within cloud environments must be safeguarded to protect its owners and subjects alike.
4.2 SOME OTHER SECURITY ISSUES IN CLOUD COMPUTING

i. **Data Security**: The enterprise data is stored outside the enterprise boundary • Security vulnerabilities in the application • Malicious employees

ii. **Network Security**: All data flow over the network needs to be secured in order to prevent leakage of sensitive information. This involves the use of strong network traffic encryption techniques. Malicious users can exploit weaknesses in network security configuration to sniff network packets.

iii. **Data Locality**: The customer does not know where the data is getting stored. Certain types of data cannot leave the country because of potentially sensitive information.

iv. **Data Integrity**: In a distributed system, there are multiple databases and multiple applications -One of the biggest challenges with web services is transaction management -At the protocol level, HTTP (Hyper Text Transfer Protocol) does not support transactions or guaranteed delivery.

v. **Data Segregation**: Data of various users will reside at the same location • Intrusion of data of one user by another becomes possible in this environment • This intrusion can be done either by hacking through the loop holes in the application by injecting client code into the SaaS system.

vi. **Data access**: A company will have its own security policies based on which each employee can have access to a particular set of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users.

vii. **Data breaches**: Since data from various users and business organizations lie together in a cloud environment breaching into the cloud environment will potentially attack the data of all the users (6)

5.0 **Data Security Model**

All the data security technic is built on confidentiality, integrity and availability of these three basic principles. Confidentiality refers to the so-called hidden the actual data or information, especially in the military and other sensitive areas, the confidentiality of data on the more stringent requirements. For cloud computing, the data are stored in "data center", the security and confidentiality of user data is even more important. The so-called integrity of data in any state is not subject to the need to guarantee unauthorized deletion, modification or damage. The availability of data means that users can have the expectations of the use of data by the use of capacity.

![Fig 3: Security Model in Cloud Computing](image-url)
6.0 Conclusion
As enterprises make plans to deploy applications in private and public cloud environments, new security challenges need to be addressed. Optimal cloud security practices should include encryption of sensitive data used by cloud-based virtual machines; centralized key management that allows the user (and not the cloud provider) to control cloud data; and ensuring that cloud data is accessible according to established enterprise policies.

REFERENCE