# Design and Implementation of Cloud Computing Security and Privacy System

**Mohamed Ismail[1], Ashraf GasimElsid[2]**

Faculty of Telecommunication and Space Technology Engineering, Africa street , Khatroum, Sudan

*Corresponding authorE-mail:3bqrinoo@outlook.com*

***ABSTRACT*** —Cloud computing is architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Salesforce.som and Microsoft etc This paper is aimed to introduce the history of cloud computing and service model of it, and present cloud computing security issues and challenges, and discuss the privacy of cloud computing with explain the data security laws and regulations around the world, then design secured approach for the cloud with the virtual machines and database using open source software (OpenStack) and explain the recommended tips that should be followed to secure the cloud.

for target classification is proposed.

***Keywords—Cloud Computing, Virtual Machine,Private Cloud , IaaS, OpenStack***

## I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud model promotes five essential characteristic, three service models, and four deployment models. The five essential characteristics are; on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. The three service models are; Cloud Software-as-a-Service (SaaS), Cloud Platform-as-a-Service (PaaS), and Cloud Infrastructures- a-Service (IaaS), together called as the SPI model.

Cloud computing provides a variety of computing resources From servers and storage to enterprise applications such as email, security, backup/DR, voice, all delivered over the Internet.

The Cloud delivers a hosting environment that is immediate, flexible, scalable, secure, and available – while saving corporations money, time and resources. [2]

## II. METHODOLOGY

According to NIST the cloud model is composed of three service models and four deployment model:

- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

And the Model:

- Private Cloud
- Public Cloud
- Hybrid Cloud
- Community Cloud

### A - Cloud Computing Main Security Issues:

- **Integrity:** Integrity makes sure that data held in a system is a proper representation of the data intended and that it has not been modified by an authorized person. When any application is running on a server, backup routine is configured so that it is safe in the event of a data-loss incident. Normally, the data will backup to any portablemedia on a regular basis which will then be stored in an off-site location [3].
- **Availability:** Availability ensures that data processing resources are not made unavailable by malicious action. It is the simple idea that when a user tries to access something, it is available to be accessed. This is vital for mission critical systems. Availability for these systems is critical that companies have business continuity plans (BCP‟s) in order for their systems to have redundancy [3]
-

- **Confidentiality:** Confidentiality ensures that data is not disclosed to unauthorized persons. Confidentiality loss occurs when data can be viewed or read by any individuals who are unauthorized to access it. Loss of confidentiality can occur physically or electronically. Physical confidential loss takes place through social engineering. Electronic confidentiality loss takes place when the clients and servers aren't encrypting their communications [3].

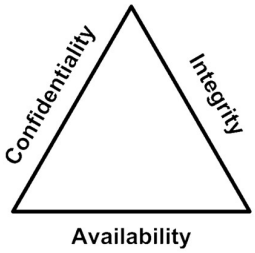


**Figure 1**: **Cloud Computing Main Security Issues**

### 1. Cloud Computing Challenges

The current adoption of cloud computing is associated with numerous challenges because users are still skeptical about its authenticity. Based on a survey conducted by IDC in 2008, the major challenges that prevent Cloud Computing from being adopted are recognized by organizations are as follow:

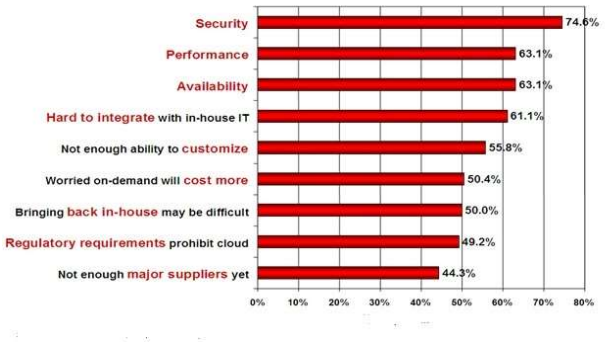


**Figure 2**: **IDC Survy**

A. **Security:** It is clear that the security issue has played the most important role in hindering Cloud computing acceptance. Without doubt, putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, and botnet (running remotely on a collection of machines) pose serious threats to organization's data and software.[3]

B. **Costing Model:** Cloud consumers must consider the tradeoffs amongst computation, communication, and integration. While migrating to the Cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication, i.e. the cost of transferring an organization's data to and from the public and community Cloud and the cost per unit of computing resource used is likely to be higher.[4]

C. **Charging Model:** The elastic resource pool has made the cost analysis a lot more complicated than regular data centers, which often calculates their cost based on consumptions of static computing. Moreover, an instantiated virtual machine has become the unit of cost analysis rather than the underlying physical server.[4]

D. **Service Level Agreement (SLA):** Although cloud consumers do not have control over the underlying computing resources, they do need to ensure the quality, availability, reliability, and performance of these resources when consumers have migrated their core business functions onto their entrusted cloud. In other words, it is vital for consumers to obtain guarantees from providers on service delivery.[4]

E. **What to migrate:** Based on a survey (Sample size = 244) conducted by IDC in 2008, the seven IT systems/applications being migrated to the cloud are: IT Management Applications (26.2%), Collaborative Applications (25.4%), Personal Applications (25%), Business Applications (23.4%), Applications Development and Deployment (16.8%), Server Capacity (15.6%), and Storage Capacity (15.5%).[4]

F. **Network Security:** Network security is the any protection of access, misuse, and hacking of files and directories in a computer network system. Some of the most common threats to a network include viruses, worms, spyware, and adware and identity theft. One of the most important aspects of network security is the multiple layers of security. There is no single package or system that will offer complete protection against every threat to your network.

G. **Data Location:** Customers may not know the physical location of the server used to store and process their data and applications. Cloud computing technology allows cloud servers to reside anywhere. From a technology standpoint, location becomes mostly irrelevant.

H. **Data Protection:** Data is stored in a shared environment in cloud i.e. in a shared environment data is located with other customer's data. Data types that are stored in cloud can vary and to keep data away from unauthorized users access control as well encryption are the only choices.

I. **Identity and Access Management:** Managing identities and access control for enterprise applications remains one of the greatest challenges facing IT today. While an enterprise may be able to leverage several cloud computing services without a good identity and access management strategy, in the

long run extending an organization's identity services into the cloud is a necessary prerequisite for strategic use of on-demand computing services.

J. **Backup and Recovery issues:** Cloud Computing servers are place where users store all the sensitive enterprise data and regular backup of the user data needs to be done as a fault tolerant mechanism and recover case of disasters where original data is destroyed.

## 2. Result of Approach

We have used OpenStack, so OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources throughout a datacenter, all managed through a dashboard that gives administrators control while empowering their users to provision resources through a web interface.

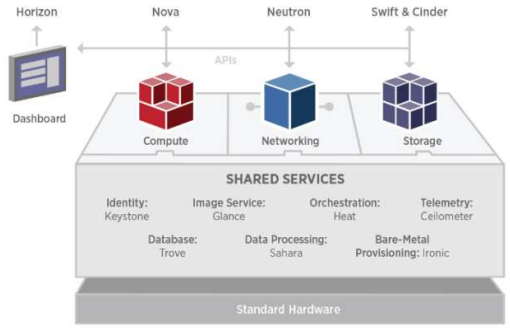


**Figure 3**: Archtcutre of OpenStack

**Network Side**

- We used OVS (Open VSwitch) in all Servers to manage the network in the virtual environment.
- In OVS we separated the network traffic by using Bridge and port technology.
- In network service (Neutron) we used two interface to provide internal and external connectivity.

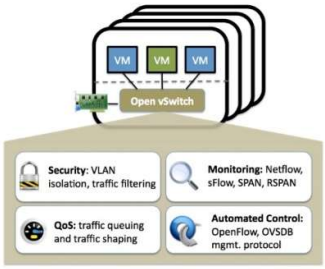


**Figure 4**: OVS Featrues

**Compute Node Side**

- We installed Nova Service (in OpenStack) to support creating virtual machines.
- In Hypervisor we used KVM (Kernel-based Virtual Machine) technology to build the visualization.
- We created multi node as a clustering to achieve High availability (HA).
- To provide security for hypervisor we used **IP Tables** technology.

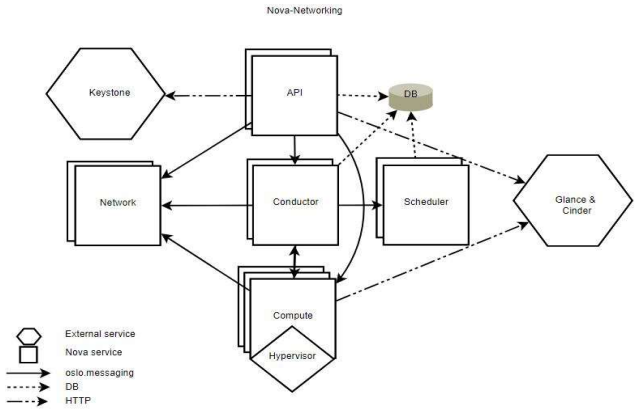


**Figure 5**: Nova Desgin

## 3. Conclusion and Recommendations

This work we discussed cloud computing security issues and challenges, privacy of cloud computing, then we design an approach to be applicable in every private cloud by using OpenStack software.

Cloud computing is the most modern technology so lots of issues are remained to consider. It has many open issues some are technical that includes scalability, elasticity ,data handling mechanism, reliability, license software, ownership, performance, system development and management and non-technical issues like legalistic and economic aspect. Cloud computing still unknown "killer application" will establish so many challenges and solutions must develop to make this technology work in practice. So this research is not stop here much work can be done in future.

The design model presented in this research is the initial step and needs more modifications; however it can provide the basis for the deeper research on security and privacy deployment of cloud computing for the research community working in the field of Cloud Computing.

For future work study we recommend to follow the below steps to make sure that you have secured cloud:

- Install and maintain firewall configuration. A firewall should be placed at each external network interface and between each security zone within the cloud.

- Do not use vendor supplied defaults for passwords and other security parameters.
- Research into standardized SLAs and liability provisions could lead to greater accountability.
- Ensure that no unnecessary functions or processes are active.
- Ensure patch management.
- Protect encryption keys from misuse or disclosure

**References**

[1] Peter Mell Timothy Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology".

[2] C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser."Business Models in the Service World."IT Professional, vol. 11, pp. 28-33, 2009.

[3] F. Gens.,"New IDC IT Cloud Services Survey: Top Benefits and Challenges", IDC eXchange, Available: [Feb. 18, 2010.