**ASSOSA UNIVERSITY**



**COLLAGE OF COMPUTING AND INFORMATICS**

**DEPARTMENT OF COMPUTER SCIENCE**

**GROUPE ASSIGMENT**

**ON**

**Traditional clod computing security**

**Prepared by:**

**Name**  **ID**

Gashaw Tarko ETR/877/06

Kibri Alem ETR/911/06

Mekides Abebe ETR/926/06

Mhiret Akele ETR/940/06

Tizita Tesfya ETR/1007/06

Submitted to:Azeze

Submitted date:12/8/2009

**Traditional clod computing security**

First,Cloud computing is Internet-based computing, where by shared resources, software, and information are provided to computers and other devices on demand, like the electricity grid. Cloud computing is a recently developing paradigm of distributed computing. The Concept Cloud computing is Internet ("cloud") based development and use of computer technology ("computing"). It is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet.

The traditional security paradigm refers to a realist construct of security in which the referent object of security is the state. The prevalence of this theorem reached a peak during the Cold War. For almost half a century, major world powers entrusted the security of their nation to a balance of power among states. In this sense international stability relied on the premise that if state security is maintained, then the security of citizens will necessarily follow. Traditional security relied on the anarchistic balance of power, a military build-up between the United States and the Soviet Union (the two superpowers), and on the absolute sovereignty of the nation state. States were deemed to be rational entities, national interests and policy driven by the desire for absolute power. Security was seen as protection from invasion; executed during proxy conflicts using technical and military capabilities.

The security in a traditional setting is accomplished by the use of firewalls,  
Internet protocols, policies for access control, virus protection, and auditing, with all of  
these things being controlled by local administrators.

In a traditional setting, access control is handled by policy and is locally  
managed, whether it be username/password or a token of some sort or a combination  
(Chandramouli). It is also often based on a user’s role in the organization.

Firewalls are either hardware or software, that by policy, protect a computer  
system or network from unauthorized users and protect against intruders. A firewall  
limits the data that can pass through it, both incoming and outgoing, and can block or  
allow any and all traffic, based on rules set by the network administrator (Office of  
InformationTechnology).  
Network protocols determine how data is sent over the network, to and from the  
internet. There are several, such as HTTP, TCP/IP, SMTP and Internet Protocol  
Security (IPSec). IPSec is a suite of policies that use cryptographic security to protect  
data as it travels throughout the internet. IPSec is the standard for basic internet  
security. Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer  
(SSL), are also protocols that provide secure communication over the Internet. These  
protocols operate above the transport layer. SSL, which was developed by Netscape,  
uses a cryptographic system that uses two keys to encrypt data for transmission over  
the Internet. One key is a public key known to everyone and the second key is a secret  
key that is only known to the recipient of the message. The Internet Explorer and  
Netscape Navigator both support SSL, and by convention any URL that begins with  
https: instead if http: represents an SSL connection (Brook).  
Confidentiality, Integrity, and Availability (CIA), create a triad that is a security  
model. This model serves commonly serves as the standard on which security is based.  
The CIA triad is a security model that serves to assist in the development of security  
policy and can be used to identify problems in security. The goal of security of a system  
is to protect a system while ensuring the confidentiality of the data, the integrity of the data and the availability of both the data and the system (Brook, CIA Triad: Managing  
and Controlling Risk) The CIA triad is also sometimes called PAIN, which stands for  
privacy, availability and/or authentication, integrity, and non-repudiation. Privacy and  
confidentiality are closely linked and are referenced to as meaning that the data being  
transferred is only available for the intended party and this can be accomplished by  
using encryption. Integrity refers to being able to say with confidence that the data has  
not been intercepted and tampered with during transmission and non-repudiation refers  
to the ability to ensure that a user can be confident of the origin of data and the sender  
cannot deny. This is accomplished by use of digital signatures (International  
Organization for Standardization (ISO)).

Traditional Computing. If you own the server, you  have incurred some capital expenditure (e.g. cost of the server, hiring admins, and physical rent etc.)capex and recurrent operational expenditure (e.g. power and cooling, admin wages, software and hardware upgrades). This cost is almost constant regardless of whether the server is fully utilized or not.  Otherwise, if you use the traditional web hosting infrastructure that predates the cloud era, well, though you may have eliminated the capex, there are still other issues.

* You are storing your files and data with other users with often conflicting objectives. The lack of isolation exposes you to the risk of security and poor performance.
* You also probably pay a fixed charges regardless of how much of your bandwidth or storage portion  you actually use.
* The way you subscribed to storage is not 'automatic', i.e. if you need more storage you have to inform the administrator and then you wait for them to upgrade your subscription etc. Even if it seems like automatic, in almost all cases, there is some human system admins doing the dirty work at the back-end.

In a traditional networking setup, the server is fixed in hardware and if you want to scale up to more users than the current hardware can support, you would have to spend more money for upgrades and there would still be a limit. But with the cloud computing infrastructure, multiple servers are already in place at the get go. They then use virtualization to provide only the resources that a specific user needs which gives it great scalability from the very tiny need in resources of personal businesses to massive corporate resource needs, a cloud provider is able to scale resources without problems and the client will only need to pay for what they use. In traditional networking you need pay for everything, the hardware plus the installation and maintenance, or even just rent it for a monthly fixed price, even if you only need a little bit of resource.In the traditional model of computing, both data and software are fully contained on the user's computer; in cloud computing, the user's computer may contain almost no software or data (perhaps a minimal operating system and web browser, display terminal for processes occurring on a network).

In a traditional computing environment for internet usage, the set up includes the  
servers, routers, switches hubs and computers and all policies, access control and  
security is handled in-house. The infrastructure is on-site and all aspects of security are  
left to the local administrators, from updates to audits to backups.

In a traditional setting, encryption can be used when passing data from one point to  
another. This encryption is generally implemented through Internet Protocol Security (IPSec).  
This is a traditional type of encryption that uses standards created by the Internet Engineering  
Task force (IETF) and it is based on network architecture (Search Security: Network Encryption).

Data Recovery in a traditional setting is dependant on either hot, warm or cold  
sites and is costly to maintain. It is costly due to the fact that the organization must run  
multiple servers in order to ensure that all data is backed up and not at risk of being lost. Also, in traditional shared hosting you are sharing a single server with many  
other users. Any security issues with the shared host will directly impact your business.  
For example, problems on the shared host can cause your website to go down for long  
periods. Therefore, with traditional shared hosting we face problems such as lack of  
support, lack of control, and risk of poor performance (Edward, 2009). Private cloud  
computing provides several advantages over traditional Internet, especially for large organizations.

**Security risk of traditional computing**

* Managed by polices to protect computing environment
* Locally managed
* Infrastructure on site encryption
* Based on CIA security model
* Use of digital certificates
* Use of anti-virus and ante-malware
* Use of fiurewalls auditing
* Cost of data recovery
* Service recovery time