**Many Flavors of Cloud Computing**

**SaaS – Software as a Service**

• Network-hosted application

 **DaaS – Data as a Service**

• Customer queries against provider’s database

 **PaaS– Platform as a Service**

• Network-hosted software development platform

 **IaaS – Infrastructure as a Service**

• Provider hosts customer VMs or provides network storage

 **IPMaaS – Identity and Policy Management as a Service**

• Provider manages identity and/or access control policy for customer

 **NaaS – Network as a Service**

• Provider offers virtualized networks (e.g. VPNs)

* It has been proved that it is impossible to satisfy consistency, availability, and partitioned-tolerance simultaneously.
* Companies can lower the cost of equipment management.
* Essential characteristics of cloud computing include on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

**Brewer’s CAP Theorem**

CAP-Consistency, availability, partition tolerance Using ACID

**Information Security in Clouds**

HAIL is a distributed cryptographic system, which allows a set of services to assure a client that a stored file is intact and retrievable. It is a remote-file integrity checking protocol and ensures file availability against adversaries. Proofs of retrievability prevent users’ data from corruption or irretrievability.

**Problems\Risks in cloud security**

There are several “cloud formations” - or forms of cloud computing. Each offers different characteristics, varying degrees of flexibility, different collaborative opportunities, and different risks. Thus one of the key challenges that businesses face when considering cloud computing as an option is to determine how to choose the cloud formation best suited to their various types of business operations.

First, it is necessary to classify your data so as to know what rules must apply to protecting

it:

• it’s sensitivity - must it only exist at specific trust levels? If so, which?

• What regulatory/compliance restrictions apply – e.g. Must it stay within your national

boundary? Does it have to stay in Safe Harbours? etc.

We can only meet this requirement if we have universally adopted standards for:

• a data classification model that is sufficiently easy for all originators of data to use –

for example the G8 Traffic Light Protocol2.

• an associated standard for managing trust levels

• standardised metadata that signals to “cloud security” what security needs be applied

to each item of data.

With an understanding on what security you need to apply to your data, you’re in a position

to decide:

• what data and processes to move to the Clouds

• at what level you want to operate in the Clouds? Cloud models separate layers of

business service from each other, for example, Infrastructure / Platform / Software /

Process.

• which Cloud Formations are best suited to your needs.

1. The first attacker is someone who was able to breach the access control provided

by the cloud provider, possibly by stealing your cloud access credentials or

exploiting vulnerabilities in the cloud access control infrastructure.

2. Attacker #2 is coming from another server in the same customer account within

the cloud; this may be a server which belongs to a different project of the same

customer and that should not receive access to the data. This attacker might have

legitimate access to Virtual Server 2, or may have breached it using, for example,

one of the thousands of known Web application vulnerabilities.

3. Another potential threat is coming from an insider (attacker #3) within the cloud

provider’s network.