

# COS700 Research Project

Tjaart Bester

May 5, 2014

## 1 Abstract:

Cloud computing is a new paradigm that offers a wide variety of benefits such as high availability, access from anywhere on any device at any time, resources on demand, cost saving, etc. Security concerns have been cited as one of the biggest challenges to this new paradigm. Clarification of these security concerns will help identify real security risks which in turn will help decision maker make more informed decisions about cloud computing.

## 2 Introduction:

The march of progress has seen the price of computing resources such as storage and CPU power become ever cheaper. With the increased availability of such computing resources and in conjunction with the success of the internet the new paradigm cloud computing is at the cutting edge of a digital revolution. Bringing benefits such as high availability, access from anywhere on any device at any time, resources on demand, cost saving, scalability etc. Cloud computing resources may be clustered to offer public, private or hybrid networks. Private cloud: also known as internal or corporate cloud. A Private cloud is infrastructure created for a single entity but managed by a third party cloud service provider. Public cloud: is open to the general public over the internet on a pay-per-usage system. Hybrid cloud: is a combination of atleast one public and one private cloud.

Cloud computing services can be classified into infrastructure as a service (IAAS), platform as a service (PAAS) and software as a service. Cloud computing also offers a new business model that outsources computing resources and software to a shared third party infrastructure.

Delivering infrastructure, platforms or software as a service requires a very high level of virtualisation and implementation of virtual machines. Virtual machines are created, clustered together and operated via a Hyper Visor. With such a high level of virtualisation at the core of cloud computing, the physical separation of Systems and infrastructure is no longer possible. By removing the physical separation which served to reinforced security and authentication in other paradigms.

Placing systems, sensitive and critical information into a public cloud in the middle of a hostile and open network (the internet) is seen as a risk that most companies are unwilling to take. The following section we will look at motivation.

### **3 Motivation:**

Cloud computing offers resources and services to users regardless of physical or geographical boundaries at any time of day or night. For example a pharmaceutical company may move their stock control and manufacturing scheduling systems to a public cloud. This will give their sales representatives across the world access to current stock levels and production schedules in real time. The move to cloud computing will allow greater monitoring and improvement to the company's logistical infrastructure. But the information contained within this system would also be very valuable to competitors trying to secure a competitive edge in the market. Ensuring that this information is only accessible to the authorized parties is hampered by the high use of virtualisation with the cloud paradigm, competing companies systems and information might reside next to each other within the cloud. This possible proximity and removal of physical separation has raised the requirement to ensuring effective and adequate user authentication. Delivering an authentication model to match the potential of the cloud will make the new paradigm more attractive to companies and businesses. The following section we will look at the problem.

## **4 Problem:**

Taking a look at traditional paradigms in authentication for public or hosted services/resources we see a reliance on physical separation and access only allowed through a fortified proxy. With cloud computing the hosted system or service is no longer within the confines of a company's local network but located in the cloud. Thus we see the need for effective and adequate authentication for resources, information and systems of varying importance within the public cloud is required. How to implement authentication for device independent paradigm such as Cloud Computing?

The following section we will look at objectives.

## **5 Objectives**

Investigate how device identification can be incorporated into user and system authentication within the cloud.

Investigate measures to improve user and system authentication on the cloud.