**COS700 Research Project**

T Bester1, MT Dlamini1,2, HS Venter1

1University of Pretoria, Pretoria, South Africa

2University of Kwazulu-Natal, Durban, South Africa

**Abstract:**The increased availability of computing resources in conjunction with the success of the Internet has put the cloud computing paradigm at the cutting edge of a digital revolution. Cloud computing offers benefits such as high availability, on demand access from anywhere on any device at any time, cost saving, scalability and etc. Cloud computing also offers a new business model that outsources computing resources to a shared third party infrastructure.Cloud computing services can be classified into infrastructure as a service (IAAS), platform as a service (PAAS) and software as a service (SAAS). Delivering infrastructure, platforms or software as a service requires a high level of virtualization and implementation of virtual machines. Virtual machines are created, clustered together and operated via a hypervisor. A hypervisor or virtual machine monitor creates a virtual platform for virtual machines and manages the execution thereof. Cloud computing offers resources and services to users regardless of physical or geographical boundaries at any time of day or night. However, the cloud as one of the most promising technology developments of this century is hampered by a string of security challenges which has led to its low adoption rates, more especially for public cloud infrastructure. The low adoption rate of public clouds indicates that the business world is hesitant to make the necessary move to cloud computing due to perceived security challenges and vulnerabilities.

Hence, this research proposes a dynamic risk-based authentication mechanism.SecuringIT-resources that are hosted on a public cloud requires risk-based authentication.The proposed solution assigns a certain risk profile to each authentication attempt. The risk profile determines the complexity of the challenge. A high risk profile requires a strong challenge and a low risk profile requires a user name and password. This paper argues that authentication on the cloud can be improved by implementing a risk profile for each authentication attempt, as stipulated above. For example logging in from your work computer in business hours is a lower risk than logging in from an unknown mobile device in different country in the middle of the night. With a low risk authentication attempt, the proposed system would require a normal user to authenticate with name and password only and this would suffice for just that particular scenario. However, as the risk increases so does the difficulty of the authentication challenge; for example, a one-time pin (OTP), supervisor authorization etc would be required on top of the usual username and password. There is a need to improve authentication systems in order to assure prospective users that public cloud computing can give them competitive edge without exposing their confidential data to unnecessary risk of falling into the wrong hands of unauthorized third parties and threating their business bottom line.