Kabarak University International Conference on Computing and Information Systems

Contribution ID: **31** Type: **Research Paper**

AN ARCHITECTURE FOR DETECTING INFORMATION TECHNOLOGY INFRASTRUCTURE POLICY VIOLATIONS IN A CLOUD ENVIRONMENT

Organizations are increasingly aware of the business value that cloud computing brings and are taking steps towards transition to the cloud.Many organizations consider the deployment of different types of protection systems to curb the various malicious activities.Despite the use of protection systems to detect any malicious activities,some users still find ways to violate some of the laid down IT infrastructure AUPs.Many cloud security research focus on enforcing standard access control policies typical of centralized systems,such policies often prove inadequate.Developing an architecture would assist network administrators to automatically detect IT infrastructure policy violation in a cloud environment.Deploying Intrusion detection and prevention system which is an integrated model that consists of two techniques(AD) and(SD) is used.An architecture uses software agents as its core components to collect evidence across cloud environment.Whenever any user is in the cloud environment and doing anything regarded as unacceptable,it automatically blocks the site.The objectives that guided this research included,establishing the level of awareness of cloud environment policy,determine technical and non-technical causes of policy violation in the cloud environment,explore mechanisms to enable self-protection of the cloud infrastructure and develop an architecture to detect and identify an attack in the real time traffic.Descriptive research which involved developing research questions based on existing theory, and design Science Research methodology was used to detect and identify an attack in the real time.The architecture captured any policy violation in the cloud environment when using any IT infrastructure.Stratified sampling technique was used to get 132 respondents out of a population of 467.The research data was collected using questionnaires as the main research instrument of the study.Collected data was coded and analyzed using statistical package for social sciences (SPSS) in order to draw out conclusions and recommendations based on the research objectives and findings of the study.
Keywords:Architecture, Policy violation, IT infrastructure, Cloud environment, Detect

Primary authors: Ms OGINGA, Ruth; Dr MAGHANGA, Christopher; Prof. MUSAU, Felix

Session Classification: Emerging Technologies

Track Classification: Emerging Technologies