Kabarak University International Conference on Computing and Information Systems

Contribution ID: **41** Type: **Research Paper**

Evaluation of mechanisms that enable self-protection on policy violation in cloud Infrastructure

Cloud computing is an emerging paradigm that involves all the basic components of computing such as end-user machines (PCs), communication networks, access management systems and cloud infrastructures. According to Gartner, while the hype grew exponentially during 2008 and continued since, it is clear that there is a major shift towards the cloud computing model and that the benefits may be substantial (Gartner Hype-Cycle, 2012). Cloud deployment models have similar internal infrastructure, but vary in their policies and user-access levels. Clouds bring out tremendous benefits for both individuals and enterprises. Clouds support economic savings, outsourcing mechanisms, resource sharing, any-where any-time accessibility, on-demand scalability, and service flexibility. Clouds minimize the need for user involvement by masking technical details such as software upgrades, licenses, and maintenance from its customers. Clouds could also offer better security advantages over individual server deployments. Since a cloud aggregates resources, cloud providers charter expert security personnel while typical companies could be limited with a network administrator who might not be well versed in cyber security issues. However,as the shape of the cloud computing is emerging and developing rapidly both theoretically and in reality, the cloud security, data and cloud infrastructure and privacy issues still pose significant challenges. It still lacks mechanism to enable itself from policy violation. In this work, we describe various mechanisms that would enable self-protection on policy violation in cloud infrastructure. In particular, we discuss five critical mechanisms: IDS, Cyberoam, Federated Identity Management System, firewall and honeypot. Some solutions to mitigate these attacks on these mechanisms are also proposed along with a brief presentation on the future trends in cloud computing deployment. Finally we evaluate these mechanisms based on the data collected from users on in case they know how to protect their data in cloud environment.
Keywords: Policy violation, cloud infrastructure, evaluating and self-protection

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

Session Classification: Emerging Technologies

Track Classification: Emerging Technologies