Kirinyaga University

Tel: +254 701562092, +254 728499650, +254 709742000/30
P.O. Box 143-10300 Kerugoya.

Email: info@kyu.ac.ke
Website: www.kyu.ac.ke

SCHOOL OF PURE AND APPLIED SCIENCES
DIVISION OF RESEARCH, INNOVATION AND GRANTS (DRIG)

A seminar by: ***Dr. James Mwikya Reuben***
Department of Pure and Applied Sciences, Kirinyaga University

Cloud Computing Security Threats, Mitigation and Framework for Real-Time Applications: A Theoretical Review

27TH April, 2021| 9:00 – 10:00 AM
Venue: Virtual

Abstract

At this moment in time, when small and medium scale businesses (SMBs) and large scale enterprise face an economic downturn, the labour and capital required for stand up servers and license software may be prohibitive an accelerated shift to the cloud seems inevitable. With maturity of cloud computing in year 2019, security is still a key cloud concern also for late adopters in Sub-Saharan Africa. Cloud provider achieve economic of scale by building a large data center and then sharing resources to all the customers. Due to the shared environment, customers information and data are exposed to all forms of vulnerabilities and threats, there is a need for provider to ensure that every customer is identified, and that non should have the ability to see or change another customer's data. Organizations are worried on how to develop adequate mitigation strategies for effective control measures and to balancing common expectation between cloud providers and cloud users. First to identify common threats and link them with some compromising attributes in cloud computing, secondly to provide mitigation techniques and their impacts in cloud computing practice and finally propose frameworks for identifying threats due to vulnerabilities in cloud computing. The study adopted a systematic literature review in cloud computing environment. Study Result reveal that threats identified are; Misconfiguration,

Unauthorized Access, Insecure Interfaces/APIs, Hijacking of Accounts, Lack of Visibility, External Sharing of Data, Malicious Insiders, Cyber-attacks; Denial of Service Attacks ,Data Loss/Leakage, Data, Privacy/ Confidentiality, Accidental Exposure of Credentials, Incident Response, Data Sovereignty and Control Legal and Regulatory Compliance. The mitigation practices would include Data storage protection; Patches and updates; Intrusion detection system (IDS) and Intrusion prevention system (IPS); Security plan; Threat management system; Virtual machine monitor; Security policies; Risk assessment and management; Behavior-based; Service level agreement (SLA); Audit and compliance; Privacy impact assessment (PIA); IT Security; Software security; Encryption; Incident response plan; Performance and capacity management; Firewall, security certificate, Testing and evaluation; Authentication and Session Management. The frameworks for identifying threats include Automated Patches Generation; PolyVaccine; CSP Controls Life Cycle; Zero-day Attack Signature Management Infrastructure (ZASMIN); and Integrating some IDS and VM Management.

DRIG COMMITTEE

Contact person: Dr Dickson M Kinyua –DRIG Chairman
(dkinyua@kyu.ac.ke)