Impact Factor: 7.07

KANYI BYOD Security Framework: For Secure Access and Use of Mobile Devices in a BYOD Environment

David Kanyi and **Patrick Ogao*.**

**Department of Geo-Science and Environment*

Abstract

Bring your own device (BYOD) is an IT policy where employees, students, and other people are allowed or encouraged to use their personal mobile devices—and, increasingly, notebook PCs—to access enterprise data and systems. BYOD has brought in a new dimension towards information security in enterprises. Hence new measurers to address the security concerns raised by BYOD implementation must be put in place. There are a number of frameworks developed in this domain of BYOD security. However these frameworks target to solve some security issues and leaves others unaddressed and hence this gap has to be filled by the proposed KANYI BYOD framework. The proposed framework was derived from reviewing existing frameworks and identifying their strengths and weaknesses. The proposed KANYI BYOD Framework borrows from BFS security Framework with a major difference in: advanced devices access to the campus network, Malware detection and prevention, Mobile devices users' categorization and access to servers and rogue access points by disabling Hotspots applications in mobile devices. Simulation methodology (using OPNET version 14.5) was used to test and validate the proposed framework by subjecting the framework network model to a mobile attacker node and putting preventive measures to address the attack and then comparing the simulation results of the various aspects of network performance tested as well as the campus server that was being targeted. We describe the structure and functioning of the framework, security vulnerability tests and discuss the results of the simulation test of the framework.

Keywords: BYOD, BYOD Framework, MDM, Simulation.

International Journal of Networks and Communications 8(4): 106-114.

http://article.sapub.org/10.5923.j.ijnc.20180804.02.html