Contribution ID: **17** Type: **Abstract for Research Paper**

Security Framework for Internet of Things Based on 4G Communication

Internet of Things, a revolutionary paradigm, is burgeoning in ubiquitous wireless systems allowing autonomous communications fueled by wireless sensor nodes and intelligent nodes. The incessant dynamic advancement in deployment of Internet of Things (IoT) for 4G systems has resulted to enhancement in in-depth networking inspection, network indicator analysis and network evaluation through intelligent tracking, intelligent identification and monitoring. The objective of this study was to design a security framework for internet of things based on 4G communication and elucidate its implications. The study identified security breaches of IoT in telecommunication systems and designed SFIT4G (Security Framework for Internet of Things based on 4G Communication), a security framework to decouple the emerging security threats. The SFIT4G architecture comprising of sensing, application and network layers was characterized by resilient processing, intelligent sensing and robust transmission of signals between nodes in 4G. The study used EM3G (Existing Methods Based on 3G) analysis model on the transmission speeds with emphasis on security performance during communication then compared to existing security architectures of internet of things.

Primary authors: Dr MUGO, David Muchangi (University of Embu); Mr LOTENGAN, KELVIN ESINYEN (University of Embu); Dr WAITHAKA, Stephen Titus (Kenyatta University)