Kabarak University International Conference on Computing and Information Systems

Monday 22 October 2018 - Tuesday 23 October 2018

KLAW - Conference Center

Book of Abstracts

Contents

Information Security / 1

Security and Privacy of app Permissions on Mobile eServices

Author: Francis LOWU[1]

[1] *BUGEMA UNIVERSITY*

Corresponding Author: hodct@bugemauniv.ac.ug

Eservice provider depends much on mobile app user's data to market their services, to gauge their business growth and compare notes with competitors among many other factors. This paper uses analytical approach to discusses issues that come with the installation and usage of mobile eservice apps on Android devices and how app permissions threaten the security and privacy of users through collecting data and information. This paper was based on the following objectives; to identify security and privacy lapses on eservices, to propose a framework for eservices based on apps permission and user involvement in their development and to discuss and analyze the security and privacy of each app permission on the usage of mobile eservices. To achieve the objectives, using Google play store, different eservice apps were identified, such as mobile banking, ehealth apps among other that have impact on group or individual privacy, a framework was designed to show how app developers and eservice providers can involve users during app development and adoption, app permissions were grouped in sets and analysis was made on each app permission set based on popularity given on Google play store for android eservice apps. The analysis showed that eservice users do not understand the use of app permission and they fear for their security and privacy.

Emerging Technologies / 2

ABIRI: ADDRESSING PASSENGER MANIFEST MANAGEMENT CHALLENGES FOR PUBLIC SERVICE VEHICLES IN KENYA

Author: Moses Thiga[1]

Co-author: Vincent Chebon [1]

[1] *Kabarak University*

Corresponding Authors: mthiga@kabarak.ac.ke, vchebon@kabarak.ac.ke

Passenger manifests are critical in the transport sector as they provide critical information to the transport providers and the government on the volumes and value of business transacted as well as to insurance companies in the event of accidents necessitating compensation of victims. However, the public service transport sector in Kenya and particularly the medium distance providers do not have systems in place to accurately and consistently capture this information. The passenger manifest automation process often times requires the development of software systems, the procurement of additional hardware, installation of networks, training of personnel and attracts significant costs in the ongoing maintenance of these systems. The process and costs are often times out of the reach of a majority of medium distance public service transport providers in Kenya. This study undertook to examine the options available for the effective and affordable automation of the passenger manifests for these public service vehicles. The approach identified and adopted the use of the cloud to host the system in order to allow for universal and convenient access, the use of a mobile application whose use is simple and the use of a pay per use approach in order to spread the costs of development and maintenance of the system. A system prototype using the rapid prototyping approach was developed and evaluated for its potential use in the sector. The approach was found to be convenient given that the users would pay for the development or maintenance of the system progressively and not upfront. Additionally, the use of existing devices in the form of smartphones that most users possess as well as the mobile phone networks which provide coverage across the country was found to significantly reduce barriers to adoption of the system.

Computational Methods / **4**

The Exponentially Modified Gaussian Function As A Tool For Deconvolution Of Astroparticle Physics Data

Authors: Livingstone Ochilo[1]; Markus Risse[2]; Alexey Yushkov[2]

[1] *Jaramogi Oginga Odinga University of Science and Technology*

[2] *University of Siegen*

Corresponding Authors: yushkov.alexey@gmail.com, livingstone.ochilo@gmail.com, risse@hep.physik.uni-siegen.de

The Pierre Auger Observatory has recorded more than two million events of ultra-high energy cosmic rays. In seeking to interpret the data recorded for the events, it is necessary to simulate the interaction of primary cosmic rays with the atmosphere. One of the softwares that is available for this kind of simulation is CONEX. In this study, CONEX is used to simulate various compositions of primary cosmic rays, whose interactions with the atmosphere result in air showers, with a distribution of depths of shower maximum (Xmax), which is treated as the true distribution. Smearing this distribution with a known σ gives the "measured" distribution. By using the Exponentially Modified Gaussian (EMG) function, we have obtained deconvoluted distribution which is generally in good agreement with the original distribution.

Emerging Technologies / **5**

A SERIAL NUMBER BASED IDENTIFICATION MODEL FOR A COMPUTER IN A WIRELESS LOCAL AREA NETWORK

Authors: John Chebor[1]; Simon Maina Karume[2]; Nickson Menza Karie[1]

[1] *Kabarak University*

[2] *Laikipia University College*

Corresponding Authors: nmkarie@kabarak.ac.ke, smkarume@gmail.com, jchebor@kabarak.ac.ke

With today's technological evolution, wireless networks have become very common for organizations, homes and public places. Besides, wireless devices seem to fill our daily lives with wireless "hotspots" emerging almost everywhere both in offices, airports, cyber cafes, sports venues and even in coffee shops. For any device to be authenticated and authorised to use any of the wireless network services, it must first be identified. Once a device has been identified, it may then be authenticated and authorized to have access to the wireless network resources. One of the biggest challenges with implementing wireless networks, though, is implementing the identification of the wireless devices. Apart from port numbers and IP addresses at application and network layers respectively, devices in a network use MAC addresses for identification at the physical layer. However MAC addresses can be altered thereby compromising the security, robustness and uniqueness qualities of a device identifier. This study therefore examined the inbuilt access and use of a serial number prototype system as an alternative method of identifying devices in a network. The model was constructed using evolutionary prototyping and proof of concept methods through test runs and was found to actually identify a device in a network based on a computer's serial number. It is then recommended that prototype be scaled up and adopted as network device identification method
Key Words: Computer, Serial Number-Based Identification, Wireless Local Area Network

Artificial Intelligence / **7**

Improving the Performance of Network Intrusion Detection Based on Hybrid Feature Selection Model

Author: joseph chahira[1]

Co-authors: Moses Thiga [2]; joseph siror

[1] *university*

[2] *Kabarak University*

Corresponding Authors: jmbugua80@yahoo.com, josephsiror@yahoo.com, mthiga@kabarak.ac.ke

Improving the Performance of Network Intrusion Detection Based on Hybrid Feature Selection Model

Abstract
Due to the high dimensionality of the network traffic data, it is not realistic for an Intrusion Detection System (IDS) to detect intrusions quickly and accurately. Feature selection is an essential component in designing intrusion detection system to eliminate the associated shortcoming and enhance its performance through the reduction of its complexity and acceleration of the detection process. It eliminates irrelevant and repetitive features from the dataset to make robust, efficient, accurate and lightweight intrusion detection system to be certain timelines for real time. In this paper, a novel feature selection model is proposed based on hybridising feature selection techniques (information gain, correlation feature selection and chi square). In this experiment the performance of the proposed feature selection model is tested with different evaluation metrics which includes: True Positive rate (TR), Precision (Pr), false positive rate (FPR), on NSL KDD dataset with four different classificaton techniques i.e. random forest, Bayes, J48, Parts. The experimental results showed that the proposed model improves the detection rates and also speed up the detection process.
Key words Intrusion detection, Performance, hybrid, feature selection, classifier.

Emerging Technologies / 8

Practices, Challenges and Approaches for Software Project Risk Management in Kenyan County Governments

Author: Mercy Kilisio[None]

Co-author: Moses Thiga [1]

[1] *Kabarak University*

Corresponding Authors: mthiga@kabarak.ac.ke, mkilisoi@kabarak.ac.ke

In the recent past the county governments in Kenya have embarked on an aggressive drive to automate their processes and systems in an effort to improve service delivery to their citizens, improve revenue collection and better management of resources. Part of these efforts have been the initialization of software projects that have either required the development of bespoke software or the acquisition and customization of existing products from vendors. However, it has not always been smooth sailing for these projects as they often delayed, experience cost overruns and experience scope creep occasioned by the materialization of various risks in the projects. This study examined the practice of risk management at the Nakuru county government ICT department in order to establish the specific risks facing software projects at the county level, the challenges faced in managing them and proceeds to make specific recommendations for risk management at the county level for software projects risk management.
Keywords: county government, risk management, software project

Computational Methods / 13

Ab initio calculation of structural and electronic properties of 3c-Silicon Carbide: Density functional calculations

Author: Perpetua Muchiri[1]

Co-authors: George Amolo [1]; Nicholas Makau [2]; Korir Kipronoh [3]; Valid Mwalukuku [2]

[1] *Technical University of Kenya, Department of Physics & Space Sciences, P.O. Box 52428-00200, Nairobi.*

[2] *Computational Material Science Group, Physics Department, University of Eldoret, P.O. Box 1125-30100, Eldoret, Kenya.*

[3] *Moi University, Physics Department, P.O. Box 3900-30100, Eldoret, Kenya.*

Corresponding Authors: wanimak@yahoo.com, koriro1208@gmail.com, vmwatati@yahoo.com, pshiroh2015@gmail.com, georgeamolo862@gmail.com

Silicon Carbide has become one of the promising materials that can be used for electronic and optical applications. This is as a result of its superior properties among them structural, thermal, chemical,electronic and mechanical. This material is among the prominent systems that exhibits several polytypism. It has more than 200 polytypes and among them is 3C polytype which has attracted more
attention due to its favorable electronic properties. SiC is used in microelectronic devices such as high-power and high-temperature applications. However, a deep understanding of the physical properties of SiC is necessary due to technological problems that need to be addressed before the material can be
used in the production of electronic devices. This work reports both the structural such as bond length, lattice parameter and electronic properties of cubic Silicon Carbide (3C). The theoretical calculations were carried out using Ab initio approach based on Density Functional Theory framework within
Generalized Gradient Approximation using Perdew, Burke and Ernzerhof exchange correlation functional using Ultrasoft pseudopotential as implemented in Quantum ESPRESSO computer code. The lattice parameter was found to be overestimated by +0.66% when compared to the experimental value of 8.24 bohr while the bulk modulus was underestimated by 11.25%. The band structure was determined using Γ, X, W K, L, W Γ high symmetry points. Cubic Silicon Carbide was found to have an indirect band gap of 1.34 eV between X and Γ which is underestimated by the Density Functional Theory calculations. The system exhibit a small band gap indicating it is a semiconductor necessary in technological and industrial applications.

Computational Methods / 14

Computational methods in Materials Science studies

Author: James Sifuna[1]

Co-authors: George Amolo [2]; George Manyali [3]

[1] *The Technical university of Kenya*

[2] *The Technical University of Kenya*

[3] *Masinde Muliro University of Science and Technology*

Corresponding Authors: sifunajames@gmail.com, georgeamolo862@gmail.com, georgemanyali@gmail.com

Recent years have seen a great improvement in the field of Density Functional Theory (DFT) calculation of the structure and properties of crystalline materials. There are several reasons underlying the present successful application of DFT to materials science: Faster and faster computers, software improvements and theory advancement. Based on these three pillars, we the computing scientists are now fully able to understand the properties and performance of real materials. We are also able to explore the immense realm of the virtual materials in their quest for novel materials. Indeed, high-throughput techniques for the search of new crystal structures and the screening of band structure traits have become very popular in the field of computational materials science. Despite these, many challenges are still to be faced. Common to all computational materials scientists is the unquenchable thirst for higher speed and better accuracy in DFT calculations. This paper aims to present recent advances in the theory and computational methods in DFT calculation of materials as well as to highlight computational results on negative thermal expansion in cubic scandium triflouride in comparison to experimental and other theoretical studies.

Emerging Technologies / 16

A Scalable Zigbee WPAN for waterflow Telemetry

Authors: Kirori Mindo[1]; Moses Thiga[1]; Simon Karume[2]

[1] *Kabarak University*

[2] *Laikipia University*

Corresponding Authors: skarume@laikipia.ac.ke, kirori@kabarak.ac.ke, mthiga@kabarak.ac.ke

Water and Sewerage service providers in Africa have encountered challenges in proficient collection of water billing data from customer's meters. This necessitates the need to implement a proper data collection mechanism that can be implemented remotely, effortlessly, and accurately. A Zigbee WPAN-to-WAN solution for water meter data collection is thus a viable solution. The objective was to design, implement and evaluate a scalable Zigbee Mesh WPAN model for remote water meter reading. This paper presents a model, prototype and project for a water meter sensor network based on IEEE 802.15.4 Zigbee standard. The resulting WPAN network allowed collection of data logged from the water meter sensors in real time remotely and accurately. The PPDIOO lifestyle approach was used to develop the model, prototype and guided project set-up. The model, prototype and project developed in this study will serve to inform the development of Zigbee water meter networks with data collected consumed by third party software solution providers for purposes of analyzing, organizing and reporting.

Emerging Technologies / 25

A CONCEPTUAL FRAMEWORK FOR IMPLEMENTING CLOUD ERP SYSTEM IN A DEVELOPING COUNTRY LOCAL GOVERNMENT: A CASE OF UGANDA

Authors: David Mpanga[1]; Christopher Maghanga[2]; Rabah Kefa[2]

[1] *Bugema University*

[2] *Kabarak University*

Corresponding Authors: cmaghanga@kabarak.ac.ke, krabah@hotmail.com, dmpangabiz@gmail.com

Increased demand for efficiency and effectiveness in service delivery has made the implementation of information systems and the demand for access to real time information no longer a requirement unique to private sector or large public sector entities. Local government entities like municipalities are also challenged to provide services with similar efficiency and effectiveness. Successful implementation of an ERP system depend on a number of factors, the framework adopted when implementing the ERP is one of the factors that is critical. Implementing ERP system in local governments in developing countries should also take into account the fact that developing countries lack sufficient technological infrastructure, ERP implementing skills, adequate funds, and have unique political influences unlike developed countries. Cloud ERP provides a platform where local governments in developing countries could successfully implement ERP within prevailing constraints. An exploratory methodology involving focus groups was used to understand the information systems context of municipalities in a developing country, Uganda. Existing ERP implementing frameworks were reviewed, and a conceptual framework to successfully implement a cloud ERP system in a developing country local government is proposed. The understanding of ERP implementing framework/methodology will enable decision makers and ERP vendors reduce on total or partial failure rate of ERP implementation in developing country local governments.
Key words: ERP, Cloud ERP, ERP implementing framework, Local government ERP, ERP implementation

Emerging Technologies / 26

A Web Based Inter Institution Model for Lecturer's Teaching Workload Monitoring in Kenyan Institutions of Higher Learning

Author: Evans Maoncha[1]

Co-authors: Simon Maina Karume [2]; Moses Thiga [3]

[1] *Ombati*

[2] *Laikipia University College*

[3] *Kabarak University*

Corresponding Authors: mthiga@kabarak.ac.ke, smkarume@gmail.com, evansmaoncha@gmail.com

Part-time lecturing is a familiar engagement that many lecturers in Kenya undertake. Lecturers are assigned lectures in multiple independent learning institutions and there is no platform to foster inter-university communication regarding the shared lecturers' employment state, tenure and lecturing obligations. Commission for University Education has guidelines set to limit the maximum lecturer workload and yet there is no way in which Commission for University Education monitors and regulates inter institution lecturers' teaching workload. There's the need to employ technology to address this problem. Tutor management software available in the market today have no provision to monitor cross-campus lecturers' workload but rather concentrate on the business aspect of automating scheduling, recruitment and billing for tutor companies. A critical survey of previous studies and current technologies associated to lecturers' workload management was conducted. This helped establish and highlight the technological gaps to be filled by a web-based model for lecturer's teaching workload monitoring in Kenyan institutions of higher learning. The methodology adopted by this research is a mixed research methodology, in particular the concurrent triangulation methodology. Proof of concept methodology was applied to develop and test the model. The research questions were answered through an experiment that entailed engaging industry experts in a validation exercise. The model's properties that were validated included confidentiality, integrity, availability, user interface and viability. During focus groups, participants acknowledged the need to monitor lecturers' workload to help in policy formulation and ultimately improve lecturers' competency. Feedback received from a chief part of the participants also indicated that the model would be an efficient tool in addressing the workload problem. Further research should be undertaken to identify how the number of students taught by a lecturer and the type of course which a lecturer teaches may be used to corroborate lecture hours in quantifying a lecturer's teaching workload.

Emerging Technologies / 30

Enabling Secure Maternal Health Information Exchange using Blockchain

Author: Antony G. Musabi[None]

Co-authors: Moses Thiga [1]; Simon M. Karume [2]

[1] *Kabarak University*

[2] *Laikipia University*

Corresponding Authors: mthiga@kabarak.ac.ke, amusabi@kabarak.ac.ke, smkarume@gmail.com

According to UH2030 (2018), medical facilities in Kenya have made efforts to adopt Electronic Health Records systems. However, lack of secure means to share the sensitive personal health records curtails the potential inherent in the shared electronic health records which includes provision of historical health information that is critical to facilitate better informed medical decisions. Concerns for confidentiality of patients' records must be adequately addressed through measures such as data encryption and patient mediated records access. A cloud based blockchain solution accessed using mobile devices would reliably address these concerns and result in access to better quality maternal healthcare services in Kenya. The main objective of this study is to develop a Blockchain distributed ledger model for Enabling Secure Maternal Health Information Exchange. The proposed solution

targets inter health facilities within Kenya, then the data protection and access to information acts of Kenya would suffice at this stage. Simulation of records would work initially to demonstrate to target pilot facilities how the system works before scaling to a live pilot phase. Distributed Ledger Technologies (DLT), and specifically blockchain, have the potential to address these and more challenges: Information security, Costs, Enhanced Privacy and Improved Auditability.
The Overall methodical process to be adopted for the study will be that developed by the Kenya Ministry of Health for the development of mHealth solutions. The implementation process provides for stakeholder involvement in the identification of priority issues and areas of intervention as well as their subsequent involvement in the development and system testing activities.

Key words: Electronic Health Records systems, Blockchain, mHealth, Distributed Ledger Technologies (DLT).

Emerging Technologies / 31

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

Authors: Ruth Oginga[None]; Christopher Maghanga[None]; Felix Musau[None]

Corresponding Authors: musaunf@gmail.com, cmaghanga@kabarak.ac.ke, roginga@kabarak.ac.ke

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

Artificial Intelligence / 34

ARTIFICIAL NEURAL NETWORKS BASED POWER LOAD FORECASTING.

Author: Francis Komen[1]

Co-author: Moses Thiga [1]

[1] *Kabarak University*

Corresponding Authors: mthiga@kabarak.ac.ke, fkomen@kabarak.ac.ke

The current demand for power to fuel the economies of nations is at stake due to the ever increasing demand of electricity compared to low power generation levels .This demand is attributed the accelerated economic growth in respective countries. Power generating companies are struggling to meet high demand with power unreliability in developing nations. This indicates a big challenge of balancing load demand with the generated power capacities. There is dire need for countries across the world to carry out continuous load forecasting assessment for adequate management of their scarce power resources. Therefore, research in load forecasting is a critical component for cost effective power supply management. Load forecasting plays a key role in reducing generation costs and improves the reliability of the power system. This paper proposes a Multi-Layer Perceptron (MLP) with back propagation algorithm as a learning strategy to train the neural network to intelligently asses power demand to enable cost effective power generation. The artificial neural network will assist in online monitoring systems where voltage and current is supplied to the network as input. The key feature of engaging (MLP) neural networks is its accuracy in assessing the variations that will affect predicted load. The results of medium term load forecasting are will be obtained from on-line applications. The performance of the proposed method will be evaluated by comparing the test results with the actual expected values. Experimental science approach will be used to achieve the concept viability.
Keywords: Back propagation, artificial neural networks, multilayer perceptron, Medium Term Power Load Forecasting (MTPLF)

Information Security / **36**

SECURITY ISSUES ON THE IMPLEMENTATION OF ELECTRONIC DATA INTERCHANGE BETWEEN HUDUMA CENTERS AND GOVERNMENT AGENCIES IN KENYA

Authors: NIXON NYAMBANE[1]; Moses Thiga[2]

[1] *N.O.N*

[2] *Kabarak University*

Corresponding Authors: nixonnyambane@gmail.com, mthiga@kabarak.ac.ke

Electronic data interchange has emerged as one of the core features of many organizations. It has revolutionized the ways in which organizations interact with customers, employees, suppliers and partners. Implementation of electronic data interchange system in organizations can positively and negatively impact the organization's performance. Huduma center was one of the vision 2030 flagship project that started in 2013.Its aim was to access and pay for government services electronically in order to cut corruption and bureaucracy some of the amalgamated services offered by huduma Kenya include: birth certificates, national identity cards, passports, registration of business names, and applications for marriage certificates, drivers' licences, police abstracts.Inorder to access the services offered, Huduma center has to share and interchange data with government agencies that have records i.e. record of births stored in the birth registry in various districts in Kenya, In the process of sharing huduma center faces security issues. This paper will focus on the security issues on the implementation of electronic data interchange between huduma centers and the government agencies in Kenya. The study will adopt descriptive case study research design. The target population under study will be the various departments in different huduma center using the electronic data interchange. The research will use the purposeful sampling procedure to collect data from the various departments of huduma centers in Kenya through a sample of key informants. On completion of data collection process, the questionnaires will be sorted, coded and then analyzed. Analysis of the data will be done using frequency and percentages. The statistical tool that will be used will be excel.

Key words: security issues, Electronic data interchange, Huduma center, implementation.

Emerging Technologies / 37

RETSA - Real Time Security Alert

Author: Ronald Yator[None]

Corresponding Author: ronald.yator@gmail.com

Keywords: RETSA, Detectors, Signal, Security, Alert

Abstract: Insecurity is a major challenge in our current world today. Millions of shillings and property has been lost, many lives has been lost due to insecurity. It is high time to embrace innovation and invention of ways to curb the societal problems like this. That is why there is need to come up with faster security alert systems.
This innovation is alert system that notifies the owner or users on an illegal access to their property. Due to this challenge i came up with the (RETSA – REAL TIME SECURITY ALERT) system that notifies the owner or users on an illegal access to their property. The system ensures the property access points are secured with active detectors that signal the main system – (RETSA) to alert the owner of illegal access. It has capabilities of eradicating the cattle rustling by alerting owner when bandits opens or destroy fence of cowshed.
Therefore ensuring that the owner can monitor his property wherever he or she is e.g. outside country, outside the locality.

Emerging Technologies / 41

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

Authors: Felix Musau[None]; Ruth Oginga[None]; Christopher Maghanga[None]

Corresponding Authors: roginga@kabarak.ac.ke, cmaghanga@kabarak.ac.ke, musaunf@gmail.com

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

Conference Plenary / 42

Blockchain Solutions Development

An overiview of what it takes to be a blockchain solutions developer

Conference Plenary / **43**

Legal issues around Blockchain based financial solutions in Kenya

An examination of the legal perspectives to blockchain

Conference Plenary / **44**

The African Blockchain Opportunity

Author: John Karanja [1]

[1] *Bithub Africa*

The prospects for blockchain in Africa

Conference Plenary / **45**

Blockchain – Challenges and prospects for Kenya

A perspective from the AI and Blockchain Taskforce in Kenya

Conference Plenary / **46**

Roundtable on Blockchain in Kenya

Corresponding Author: mthiga@kabarak.ac.ke

A discussion session on issues raised by the speakers

Information Security / **47**

DEVELOPING A THREAT MATRIX FOR SMART MOBILE DEVICES IN A UNIVERSITY NETWORK TOWARDS A SECURE LOCAL AREA NETWORK ECOSYSTEM

Author: Irene Wanja[1]

[1] *Kabarak*

Corresponding Author: irenewanja2003@gmail.com

The need by staff and students to use smart mobile devices in university network is indisputable. This is because they help them to work and study more effectively as well as achieve better work-life balance. However smart mobile devices pose a security challenge as they continue to expand the corporate network unchecked thus increasing the attack surface. This creates a major security burden to security professionals who are supposed to ensure that smart mobile devices adhere with the security policy. The purpose of this study was to propose a solution on how to determine likelihood of threat attack in a university network. The objectives of the study were to evaluate threats introduced to university network through use of smart mobile devices, to develop a threat matrix that computes likelihood of threat attack, to identify security requirements needed for a secure university LAN ecosystem and to test and validate the matrix. Case study research design was adopted. Egerton University was selected as a case study where 384 respondents from all the campuses were targeted. Response rate of 80% was recorded and considered sufficient for the study. The matrix was designed based on five of the ISO 27001's domains which closely relate to operation of smart mobile devices in a corporate network. Regression analysis was used to determine the Functional weights to compute likelihood of attack. The matrix was implemented as a web-based application using Hypertext Preprocessor (PHP) as server-side scripting language, MySQL was employed as a database engine and Bootstrap 4 was used for styling user interface. The developed threat matrix will act as threat and risk assessment tool to provide recommendations that maximize the protection of confidentiality, integrity and availability of university data while still providing functionality and usability of smart mobile devices.