Kabarak University International Conference on Computing and Information Systems 2019

Monday 14 October 2019 - Tuesday 15 October 2019

KLAW - Conference Center

Book of Abstracts

Contents

General Papers / 2

Data breach challenges facing Kenyan E-commerce

Author: Elvine Saikwa[1]

Co-author: Moses Thiga [2]

[1] *Student*

[2] *Kabarak University*

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

E-commerce in Kenya continues to grow in leaps and bounds driven largely by increased affordability of smartphones, greater internet penetration and affordability and the very extensive automation of government services at the national and county government levels. The success stories and positive impacts in the form of greater convenience, efficiency, increased business revenues and improved revenue collections among others are well known. However, the practice has experienced a great number of challenges most of which have gone unreported and undocumented making it difficult for ecommerce practitioners to learn from the challenges of their counterparts. This study sought to develop a structured body of knowledge on the specific aspect of data breaches in the ecommerce practice in Kenya and examined the occurrences of these breaches, their impacts and further proposes actions for consideration by the practitioners in the sector.

Keywords:

ecommerce, data breach, information security

3

AGENT BASED COMPUTATIONAL MODEL FOR MEMORY RETENTION: A FOCUS ON CHILDREN WITH DYSLEXIA

Author: Lucy Abuodha[1]

[1] *PHD student*

Corresponding Author: lucyabuodha@gmail.com

Memory retention can be defined as a process by which both working memory and long term memory preserves knowledge so that it can locate, identify and retrieve it in the future. Children with dyslexia suffer from lack of memory retention. They suffer from reduced mental ability, which affects the series such language acquisition, mathematical difficulties and many more. Different interventions have been implemented using computing technologies to aid memory retention among the dyslexic children. Computing techniques such as gaming, assessments and motivation are employed to improve the reading and spelling skills of learners. Unfortunately the computing techniques tend to address either one or the other of these needs being either enabling or instructional. Such computing technologies up to now, have not been designed to respond to personalized feedback from the learner and to personalize the system in line with the user's performance. In view of this, the paper discusses, the use of Intelligent Agents that will help design an adaptive learning support system together with key memory strategies to enhance memory retention. This study will design an Agent based computational model that will be implemented using a computational tool that will be used by dyslexic learners. The computational tool will be used to test grade 3 students in a school in Nairobi County. Data will also be collected using questionnaire. Results from the computational tool will be analyzed using descriptive statistical techniques.
Keywords— Dyslexia, Memory Retention, Agent Based Computational tool

Keywords:

888888

4

Evaluating the Feasibility of Using Classifiers in Detecting Social Engineering Fraud

Author: clifford kengocha[1]

[1] *kabarak university*

Corresponding Author: cogeto@kabarak.ac.ke

Social engineering fraud is among the most notorious forms fraud through which people continue to lose money. Its increasing prevalence is negatively affecting strides made in mobile and digital banking. Despite efforts in creating public awareness, its mitigation has not been effective as the tricks used by swindlers keep evolving. Virtually all existing solutions to the problem are based on human interventions such as manually reporting and blacklisting phone numbers. This approach is slow and inefficient due to the huge number of incidents reported relative to the limited existing human resource capacity. This paper presents an evaluation of the feasibility of using classifiers to detect voice-based social engineering fraud. Findings suggest that the use of speaker recognition, speech recognition and classifiers can automate the detection of voice-based social engineering fraud. Outcomes of this research can be used to develop a system that can automatically detect when a criminal is attempting to defraud a user over the phone.

Keywords:

Artificial intelligence, social engineering fraud, voice recognition, classifier, reasoning system

General Papers / 11

Weaknesses and Security Obstacles in The Application of MANETs for Provision of Smart Health Care

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

The use of smart devices in provision of healthcare provides numerous benefits. Use of technology in the healthcare profession has generally led to faster diagnosis, lower costs, health workers and research collaboration, reliable services, efficient and effective healthcare systems as well. The provision of smart healthcare services is dependent on MANETs. While technology is particularly indispensable, security of the systems and data remains a critical challenge that hinders the accelerated adoption of smart health care. It is reported that smart healthcare devices experience twice the number of cyber security attacks as opposed to other industries. These attacks and are made possible due to the weaknesses and nature of smart devices in MANETS. These weaknesses give rise to security obstacles that inhibit the adoption of smart health care. There is need to investigate these weaknesses and obstacles in the application of MANETs for provision of smart health care. This study will describe and enlighten the various obstacles so as to aid guide on the best practices for provision of secure Smart Healthcare. This research used a desk research of general literature review methodology. The results identify the various weakness and outline commensurate vulnerabilities as well as attacks that take advantage of these vulnerabilities. Ultimately this research gives design recommendations that can be incorporated in providing ways to seal these gaps.

Keywords:

MANET, Smart Heath Care, IOT, DDos, Cyber Attacks.

12

User Interface Design Issues and Challenges Preventing Effective Communication of Personal Health Information to Non-Medical Users

Authors: Laura Cheptegei[1]; Moses Thiga[1]; Elizabeth Okumu[1]

[1] *Kabarak University*

Corresponding Authors: laura.cheptegei@kabarak.ac.ke, eokumu@kabarak.ac.ke, mthiga@kabarak.ac.ke

There is an increasing drive for people other than health care professionals, to participate in the management of their own health and well-being, whether patient or non-patient. The third sustainable development goal concerns good health and well-being, and governments across the world are making efforts to achieve this goal. For instance, the Trump administration started a MyHealthEData initiative that aims to empower patients to take control of their personal health information (PHI). The Kenyan government is also making strides towards the same direction e.g the implementation of the Open source electronic Medical records system (OpenMRS) in public hospitals. These are efforts aimed to improve the quality of health care systems. People will first require access to their PHI in order to participate in the management of their health e.g communicate their health status clearly to relevant people, share their health information with relevant people, make shared-decisions concerning their health care etc. However, this participation might be hindered due to lack of medical knowledge or medical training background and therefore they might not easily make sense of their data; or due to inappropriate presentation of their data on the user interface of the PHI systems which may lead to wrong interpretations and as a result unintended consequences. Therefore, this research seeks to examine the context-of-use of user interface design of PHI systems, in order to identify issues and challenges that prevents effective communication of PHI to non-medical users. A contextual inquiry research method will be carried out to achieve this objective, and the findings of this study is expected to inform the design of a framework that will guide designers of PHI systems in designing user interfaces that will effectively communicate PHI to non-medical users.

Keywords:

User Interface Design. Non-medical Users. Personal Health Information Systems

18

Artificial Neural Network Power Demand Forecasting Model for Energy Management

Author: Francis Komen[1]

Co-authors: Peter Rugiri [2]; Moses Thiga [1]

[1] *Kabarak University*

[2] *Kabarak University*

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

Load forecasting is important in electric power industry. It provides future load demand information necessary for improving decision making thus enhancing reduction of power demand. Currently many world organizations depend on technical expert's knowledge and experience to assess, evaluate and advice on energy conservation and efficiency status. These methods suffer from inaccuracies and bias leading to uncertainty in power generation, supply and high costs of energy. The current adoption and advancement of information technology, application of machines learning and artificial intelligence techniques will provide unbiased and more accurate information on energy efficiency status. The research study developed an Artificial Neural Networks Based Power Demand Forecasting Model for Energy Management (ANNPDFMEM). A Multi-Layer Feed Forward Neural Networks structure was used. The electricity load data was collected from the Kenya Power and Lighting company (KPLC) smart meters for Kabarak University in Nakuru County. The collected data set was divided into 70% training set, 15% validation set and 15% testing set. The model was trained using the Back-Propagation learning algorithm. The smallest Mean Square Error in the training iteration was selected and validated with independent set of test samples. Actual smart meter load data from KPLC was compared against the predicted load. The performance evaluation of the model was done to predict the actual load values. The results obtained a Mean Squared Error (MSE) of 9.5%, and R value of 1. The results indicated high accuracy forming the basis for recommendation for adoption of the (ANNPDFMEM) as a tool for future power demand information. This information platform is important for decision making on energy efficiency and conservation strategies for sustainability and energy management

Keywords:

Load Forecasting, energy demand, Energy management

19

MACHINE LEARNING SMS SPAM DETECTION MODEL

Author: ANDREW KIPKEBUT[1]

[1] *KABARAK UNIVERSITY*

Corresponding Author: akipkebut@kabarak.ac.ke

Millions of shillings are lost by mobile phone users every year in Kenya due to SMS Spam, a social engineering skill attempting to obtain sensitive information such as passwords, Personal identification numbers and other details by masquerading as a trustworthy entity in an electronic commerce. The design of efficient fraud detection algorithm and techniques is key to reducing these losses. Fraud detection using machine learning is a new approach of detecting fraud especially in Mobile commerce. The design of fraud detection techniques in a mobile platform is challenging due to the non-stationary distribution of the data. Most machine learning techniques especially in SMs Spam deal with one language. It is in this background that the study will focus on a client side SMs Spam detection in Kenya's mobile environment for both English and Swahili text messages using machine learning. Naive's Bayes algorithm was used for this purpose because it is highly scalable in text classification. The contributors of Corpus include mobile service providers in Kenya and selected mobile phone users. Machine learning and data mining experiments were conducted using WEKA (Waikato Environment for Knowledge Analysis). The results and discussions are presented in form of descriptive statistics and detection metrics. At the end an android based prototype implementation of the SMs Spam detection model is demonstrated that based on Naive Bayes machine learning algorithm .This model gave an overall classification accuracy of 96.1039% .

Keywords:

Algorithm, Classification, Detection, Machine learning, Naïve bayes, WEKA.