Conference Proceedings

Kabarak University International Conference on Computing and Information Systems

14th -15th October 2019

KLAW Conference Center, Kabarak University, Kenya

Sponsored by

Contents

Agent Based Computational Model For Memory Retention: A Focus On Children With Dyslexia 1

Evaluating the Feasibility of Using Classifiers in Detecting Social Engineering Fraud .. 11

Weaknesses and Security Obstacles in The Application of MANETs for Provision of Smart Health Care 18

Towards a Unique, Secure, and Robust Wireless Local Area Network Device Identifier 28

Data breach challenges facing Kenyan Ecommerce 39

Artificial Neural Network Power Demand Forecasting Model for Energy Management a Case Study of Kabarak University 53

Machine Learning Sms Spam Detection Model 62

Agent Based Computational Model For Memory Retention: A Focus On Children With Dyslexia

Lucy Atieno, Abuodha
Technical University of Kenya, P.O. Box 0200, Nairobi, 52428, Kenya
Tel: +254 0722 966025, Email: lucyabuodha@gmail.com,lucy.abuodha@tukenya.ac.ke
University of Kenya, 52428, Nairobi, 0200, Kenya

Abstract

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 a questionnaire. Results from the computational tool will be analyzed using descriptive statistical techniques.

Keywords: Dyslexia, Memory Retention, Agent Based Computational tool.

1. Introduction

Learning disability (LD) causes a person to have trouble learning and using certain skills. The skills most often affected are reading, writing, listening, speaking, reasoning, and doing math[1]. There are different types of learning disabilities, the most common ones include dyscalculia, dyslexia and dysgraphia as stated by [2] Research by [3], states that dyslexia is defined as an unexpected difficulty in reading and spelling in relation to cognitive ability, education, or professional status". 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 [4]. Memory Retention is the ability the skill of the human mind to hold information in the brain for various durations, depending upon the type of memory and stimulus, repetitions in recall, levels of attention, and emotion [5]. Memory retention is used both in the working memory partly and the long term memory. The distinction between immediate memory (or working memory) and long-term memory has been fundamental to understanding how the brain has organized its memory functions [6]. Immediate memory refers to the limited amount of information that can be held in mind when material is presented for learning. Working memory refers to the capacity to maintain this limited amount of information through active rehearsal, usually across a relatively short time interval [7]. Long-term memory refers to what can be recalled from the past when the information to be learned no longer occupies the current stream of thought, either because immediate memory capacity was exceeded or because attention was diverted from the memoranda. They're 2 main types of memory as follows: short-term memory is the competency to store evidence, data, and information momentarily for seconds before it is amalgamated into the long-term memory ,which is the used for competency to learn new material and recall this material after some time has passed[8]. Holmes et al [9] describes that Poor Working Memory impairments are associated with a wide range of developmental disorders of learning. Children with poor working memory function are at very high risk of educational underachievement. Working memory is used for many functions among many others problem solving and remembering tasks. Working memory is key for academic performance, and a useful prospective indicator of academic performance [4]. Study shows that without appropriate intervention, poor working memory in children, which is thought to be genetic, can affect long-term academic success and prevent children from achieving their potential [4]. The aim of this study to propose an agent-based computational model for pupils with dyslexia, this will be achieved by reviewing existing models and memory retention techniques. The objective of this research is to come up an agent-based memory retention computational model that will help in memory retention and implement it on dyslexic children.

2. Problem statement

One of the key levels of learning is knowledge. Knowledge is the level where the learners can remember and recall what they have learnt. Dyslexia is a neurologically-based, often familial, disorder which interferes with the acquisition and processing of language and manifests as a difficulty in reading written word and spelling (Barton 2015). Children with dyslexia suffer from lack of memory retention which affects their learning (Archibald &Gathercole, 2007). 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 as stated by (Linda, 2012). Reading is a cognitive process that involves constructing meanings of words. Reading forms a way of school going children to learn (Eric, 2018). Memory retention allows the preservation of learning, which means without memory retention there is no learning. Different memory strategies are applied by teachers in the classroom to enhance memory retention, which includes practice at retrieval, repetition, memory cues, visual images, assessments, chunking information (Thorne, 2006; Halpen, 2003). 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, this is according to (Rello et al.,2014; Lexia,2017; Nessy,2017). 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 (Schmidt 2018).

Intelligent Agents based approach have also been used in memory retention among the dyslexic learners. The Intelligent Agents become key in learning environment because of its adaptive nature as it automatically customizes itself to its users based on previous experience. Their nature allows to evaluate the learners understanding to adapt the lessons accordingly. They also have the ability to work together with other Agents to achieve a common goal .Their collaborative nature allows them to modify request, ask clarifications to certain request which is important in a learning environment. Agent becomes key in the learning environment because of its dynamic nature, which allows them to make intelligent decisions based on each learner (Essay, 2013). The Intelligent Agent tools are Intelligent Assistive Reading System which can help school-aged readers who have dyslexia to improve their reading and understanding (Andreas, 2007). Different studies have been carried out on the deployment of Intelligent Agent on enhancement of memory retention (Schneider et al, 2007; Kelly, 2012).The studies showed that Intelligent Agents plays a key role during learning by ensuring adaptive approach to the learners 'needs, providing them with feedback as well as motivating the learner. However for memory retention to take place, key memory strategies such as repetition and practice at retrieval are significant. (Park et al, 2016).

3. Objectives

The general objective of this study is to develop an agent based memory retention computational model that will help in memory retention and implement it on dyslexic children.

Specific Objectives

a) To propose an agent based computational model for pupils with dyslexia, this will be achieved by reviewing existing models and memory retention techniques.

b) Implement the model as a computerized learning tool and test it using experimental method.

c) To determine the effect of memory retention strategies on dyslexic children

4. Literature Review

Researchers have associated successful memory retention must have key memory strategies, they are (a) Retrieval practice (b) Repetition and (c) Feedback according to[30]. Retrieval practice is the act of trying to recall information without having it in front of you. Cognitive psychologists have been comparing retrieval practice with other methods of studying strategies like review lectures, study guides, and re-reading texts. Research shows that nothing cements long-term retention as powerfully as retrieval practice [11].Different studies have shown great impact of retrieval practice on memory retention. The studies includes [12] [13] [14] however retrieval practice works better with other key memory strategies [15] [16] [17][18]. According to Maria et al. [19] defines feedback as information regarding performance outcomes and learning processes and plays a major role in educational performance. It is an essential component of learning [20] and the most powerful single influence on student achievement and one of the most frequently applied psychological interventions [21]. Agrawal [16] suggests that if students retrieve the wrong information, the practice won't be much good unless they find out the right information, so be sure to give them feedback as they go.

Repetition is another very important memory strategies that should be used with the other key strategies in enhancing Memory Retention. According to Willis [22] explains that through repetition of learning more dendrites are developed and strengthened in an area of the brain relevant to this learning and as an outcome we become more efficient in applying this knowledge and it is also argued that practice and rehearsal make learning stick [23].

Research has shown that implementing key memory strategies in educational settings can dramatically improve memory retention in student learning [24].However research shows that these key memory strategies have never been incorporated together and implemented in Dyslexia learners. One significant aspect of memory retention is the ability to enhance memory retention to normal students [25] as well as learners with learning disabilities [26].

Intelligent Agents then becomes crucial because of its characteristics [27] [28] and the nature of in the dyslexic learners. This study concentrates on how Intelligent Agents can be integrated together with the key memory strategies to enhance memory retention.

a) Use of Intelligent Agent on feedback:

Intelligent agents are preferred due to their high degree of self-determination capabilities and their capability to decide for themselves when, where, and under what condition to perform their actions, Feedback is critical for facilitating a comfortable learning environment and assists learners during their learning. Research shows the importance of feedback using intelligent Agents to learners, intelligent Agents can be used to provide feedback in collaborative learning. Feedback in the study is an essential help in collaborative learning by motivating the students and encourage group discussions. Intelligent Agents can use feedback to measure the level of participation of learners' As well as acts as an intervention by the instructor as well as allowing the students to gauge themselves and improve their engagement[29].This study explains that learning process in classic understanding is teacher versus learner (fulltime studies) relationship. This learning process brings the best results on the condition that the teacher is able to respond to all the questions and provide immediate feedback. Immeadiate Feedback can be integrated into Intelligent Tutoring System, thereby making sure that the learner has really mastered the material and not just guessed the previous answer [30]. If the feedback between Intelligent Agent and the learner is provided, better training results are achieved [31] [32].The Intelligent Agents will instantly corrects the mistakes made by the learner, knowledge of the student becomes deeper and wider [33].

b) Use of Intelligent Agent on repetitions:

Children with dyslexia have special learning skills and most of the time only specialized institutions can support their reading difficulties. The study used intelligent Agents to propose a reading system for dyslexic children with personalized attention, through customized presentation of reading materials [34].Intelligent Agent provides personalized assistance. This proves to be really helpful for children with dyslexia, as it combines speech recognition, state recognition via image and error type profiling via adaptive and personalized support. Intelligent agent can offer standardized training with a certain number of repetitions for all of the words. This training was inflexible and in a certain sense also inefficient. Some users might need more repetitions, while others might require fewer. It is important to take care of important facts during training such as cognitive abilities as well as impeding factors such as dyslexia [35].

c) Use of Intelligent Agent on retrieval at practice:

Research shows that for the students to learn better, the students were given less or more materials, deepening on their performance. The study showed that by allowing the undergraduate students to perform students practice exercises before given a new set of questions. The Intelligent Agent as a teacher Agent monitored the students throughout their learning, even after doing more exercises and the student was still not performing as accepted, the teacher will physical have sessions with students. This study emphasizes that students learn better by practising more exercises as opposed to any other learning strategies [36]. According to Tumenayu et al. [37] shows the educational games development with an Agent-Based Technology by using intelligent pedagogical agents can intervene to offer hints, assistance and suggestions when the learner is lacking knowledge. In this paper he describe the possibilities of using pedagogical agents to infer learner's motivation and emotional state as they allow communication and interaction in a digital learning environment.

The study presents the relevance of Pedagogical agent's technology as an approach in enhancing the interactive learning in a game based environment. The agents uses competence activations interventions ,which activates the temporary inactive skill eg remembering, as well as competence acquisition interventions, which allow the educational game Agent to conclude lack any skills, which the Agent provides on behalf of the learner. This Agent also provides problems solving support via hints and indications that will bring the learner closer to the solution as well as progress back. It uses games to enhancing learning among by providing assistance by giving answers to learners when they can't answer questions as well as motivate learner by appraisal. The benefits of Artificial Intelligence in education have been lauded for many years [34].Different intelligent tutoring system has been used in education both through mobile and web based application, encompassing different learning strategies. Despite Intelligent Agents been key in learning, research shows that no study has been done on Intelligent Agents using memory strategies on dyslexic learners.

d) Agent base computational Model

The facilitations discussed above where used to develop an Agent based computational Architecture shown below. The architecture consists of the student model as well as the Domain Model. Different Knowledge Data Base Module will work together with agents to create the Agent based computational Model. The two module Domain Models and Student Model. In the Student Model the knowledge the system has about the student (profile and interaction with the system) is represented. The model is composed of two knowledge databases (KDBs). (1) The Profiles KDB that stores the necessary personal information of the student to control his access to the system. They also store the level as well as the presentation styles of the students. The students are assigned different levels depending on their learning rhythm. (2) The Learning KDB stores parameters such as the exercises and tests proposed so far to the students, the exercises, the pages of notes visited and the scrolls performed on those pages and the reinforcement material prepared by the Pedagogic Module. In the Domain Model the knowledge about the contents to be taught is stored. This model consists of four KDBs: (1) the game KDB incorporates the gaming pages that have been prepared for teaching on the matter, (2) the Tests KDB stores the battery of test questions related to the matter, (3) the Exercises KDB stores the battery of exercises on the matter, and, (4) the Reinforcement KDB contains the information used by the Pedagogic Module to prepare the material to be shown when a student needs to be reinforced.

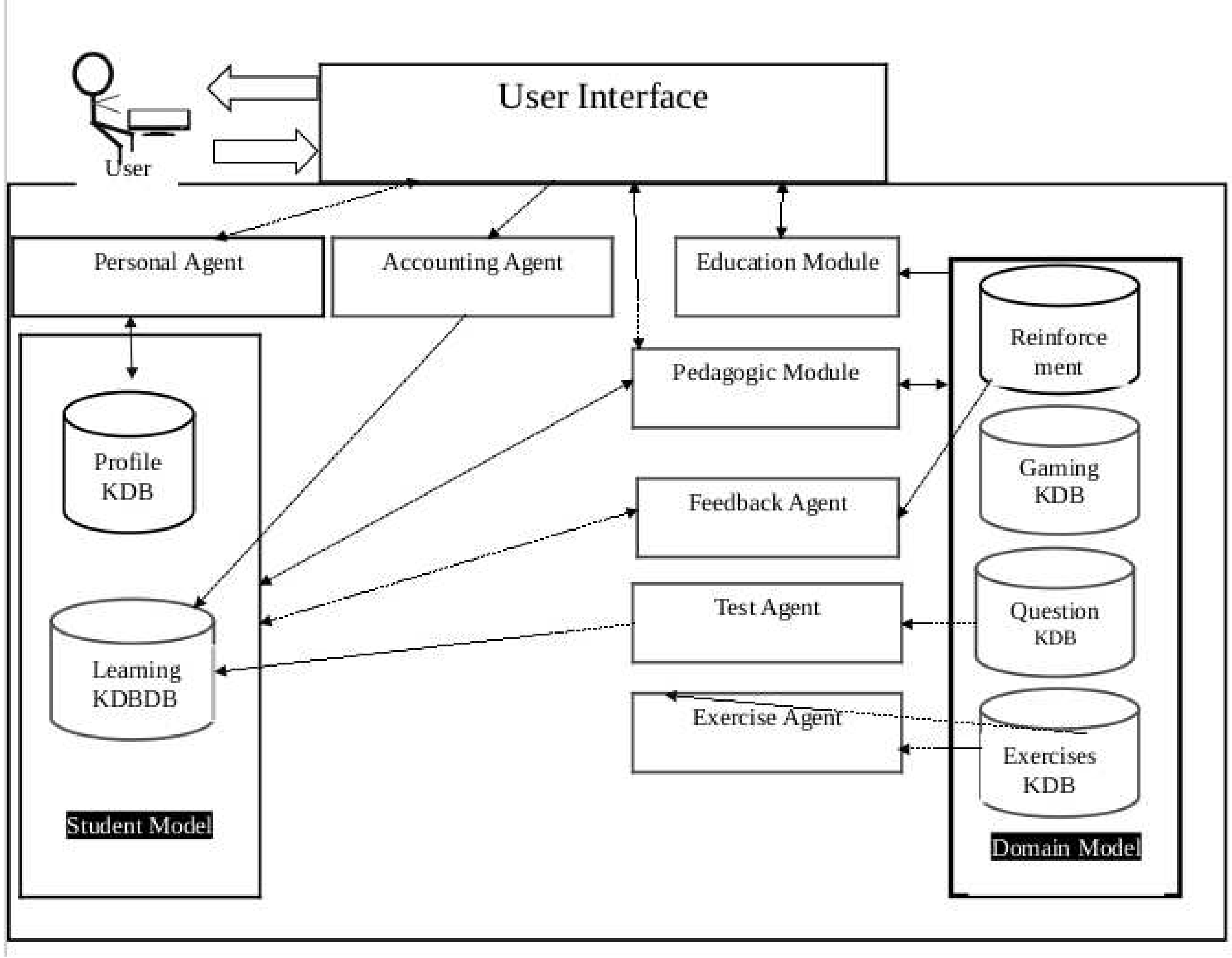


Fig 1. Agent based Computational Architecture

5. Methodology

This paper will adopts two different types of research design:

Experimental design aims to establish the existence of a cause and effect relationship between variable. This study determines to show the correlation between the independent variables (Repetition, Feedback and retrieval practice) and the dependent variable (Memory retention).The experiment will have two groups, one will be the experimental group and the other group will be the control group. The research intends to put in a place an agent based computational tool for dyslexic learners, the learners will use the tool for exercises, tests and exams .The learners will undertake pretest at the beginning of the study and then a post test at the end of the study. The results of the both the control group and the experimental group will be analyzed using ANOVA and then results will be represented in form of tables.

Descriptive design -The researcher will design an open ended questionnaire which will be rolled out to the teachers. These questions will relate on what the teacher observed with the children during learning, when using Agent based computational tool. Interviews (with the teachers) will also conducted before the experiment with the aim of gathering data on what processes entails learning on a day to day basis .This will include;

a) Curriculum development,

b) Mode of teaching and learning,

c) Usage of technology with children with dyslexia,

d) Learning materials and content,

e) How lessons are conducted

6. Results

Results for this study will be mainly from the agent based computational tool. We intend to document the entire process, exercises, quizzes and then the main exam. The study intends to contribute to computational models for dyslexic learners. The study will employ the agent based computational tool on dyslexic learners to determine whether memory retention will be realized. The study aims to help dyslexic learners realise their dream of achieving their academic success.

7. Recommendations and future works

The Architecture works well for collaborative mobile learning based on Moodle Learning Management System. While there is room for improving this architecture, we will also consider implementing it on other mobile learning platforms. Also the architecture may be modified to capture the aspect of agents working together by sharing their information to improve the learning effect on collaborative platforms. Results for this study will be mainly from the agent based computational tool. We intend to document the entire process, exercises, quizzes and then the main exam. The study intends to contribute to computational models for dyslexic learners. The study will employ the agent based computational tool on dyslexic learners to determine whether memory retention will be realized. The study aims to help dyslexic learners realise their dream of achieving their academic success.

8. Conclusions

One of the most recent policy documents in education is Sessional Paper No. I of 2005 on a Policy Framework for Education, Training and Research, through this document the government intend to ensure that all children eligible for primary schooling have opportunity to enrol, remain in school to learn and acquire quality basic education, based on its commitment to achieve Education for All (EFA) by 2015.To achieve this there is need to ensure that learners with learning disabilities especially dyslexia can achieve their dreams achieve and reach their life potential. The Agent based computational model will ensure successful transition of dyslexic learners through education. .

References

[1] National Dissemination Center for Children with Disabilities (NICHCY) Available: https://www.fhi360.org/projects/national-dissemination-center-children-disabilities-nichcy.

[2] Learning Disabilities Association of America (Online).Available: https://ldaamerica.org/types-of-learning-disabilities.[Accessed on 15th May 2019]

[3] Lyon, G.R., Shaywitz, S.E. & Shaywitz, B.A. Ann. of Dyslexia (2003) 53: 1. https://doi.org/10.1007/s11881-003-0001-9

[4] Archibald, L.M.D., & Gathercole, S. E. (2007). The complexities of complex span: Specifying working memory deficits in SLI. *Journal of Memory and Language*, *57*, 177–194.

[5] Endel Tulving(2002)Episodic Memry:From Mind to Brian.Annual Review of Psychology,53,1-25

[6] Larry.R.Squire (2009). Memory and Brain Systems: 1969–2009. Journal of Neuroscience 14 October 2009, 29 (41) 12711-12716; DOI: https://doi.org/10.1523/JNEUROSCI.3575-09.2009

[7] Baddeley, A. and Hitch, G. (1974). Working memor. *The psychology of learning and motivation: advances in research and theory*, 8.

[8] Reber P.J., Beeman M., Paller K.A. (2013) Human Memory Systems: A Framework for Understanding the Neurocognitive Foundations of Intuition. In: Schmorrow D.D., Fidopiastis C.M. (eds) Foundations of Augmented Cognition. AC 2013. Lecture Notes in Computer Science, vol 8027. Springer, Berlin, Heidelberg

[9] Joni Holmes , Susan E. Gathercole ,Maurice Place , Darren L. Dunning , Hilton, Julian.(2009), Working memory deficits can be overcome: Impacts of training and medication on working memory in children with ADHD, https://doi.org/10.1002/acp.1589

[10] https://www.verywellmind.com/great-ways-to-improve-your-memory-2795356

[11] McDaniel, M. A., Thomas, R. C., Agarwal, P. K., McDermott, K. B., & Roediger, H. L. (2013). Quizzing in middle school science: Successful transfer performance on classroom exams. *Applied Cognitive Psychology*, *27*, 360-372. *A journal article on how retrieval practice improves students' transfer to new information in 7th and 8th grade Science.*

[12] Roediger HL , Butler AC. The critical role of retrieval practice in long-term retention, Jan;15(1):20-7. doi: 10.1016/j.tics.2010.09.003. Epub 2010 Oct 15.

[13] Jeffrey D.Karpickle, Henry Roediger, (2008).The critical importance of Retrieval For Learning.

[14]Jeffrey D .Karpicke, Janell F.Blunt,Megan A.Sumeracki(2016)Retrieval-Based Learning: Positive effects of Retrieval Practice in Elementary school Children. Frontiers in Psychology 7(104), DOI: 10.3389/fpsyg.2016.00350

[15] Steven C. Pan &Timothy C. Rickard.(2017) Does Retrieval Practice Enhance Learning and Transfer Relative to Restudy for Term-Definition Facts? American Psychological Association 017 1076-898X/17/$12.00 http://dx.doi.org/10.1037/xap0000124

[16] Roediger, H. L. III, Agarwal, P. K., McDaniel, M. A., & McDermott, K. B. (2011). Test-enhanced learning in the classroom: Long-term improvements from quizzing. *Journal of Experimental Psychology: Applied, 17*(4), 382-395.http://dx.doi.org/10.1037/a0026252

[17] Pooja Agarwal, Patrice M Brian, Roger Chamberlain (2012) The Value of Applied Research: Retrieval Practice Improves Classroom Learning and Recommendations from a Teacher, a Principal, and a Scientist Educational Psychology Review 24(3) DOI: 10.1007/s10648-012-9210-2

[18] Nicole A.M.C Goossens,Gino Camp, Peter PJ; Verkoeijen,Rolf A Zwaan, (2014)The Benefit of Retrieval Practice over Elaborative Restudy in Primary School Vocabulary Learning, Journal of Applied Research in Memory and Cognition 3(3) DOI: 10.1016/j.jarmac.2014.05.003

[19] Maria cutumisu, Daniel L Schwartz. (2017) The impact of critical feedback choice on students' revision, performance, learning, and memory. Computers in Human Behavior DOI: 10.1016/j.chb.2017.06.029

[20] Emma Mulliner, Matthew Tucker (2015) Feedback on feedback practice: perceptions of students and academics Assessment & Evaluation in Higher Education. DOI: 10.1080/02602938.2015.1103365

[21] Yigali Attali, Don Powers, (2010) Immediate Feedback and Opportunity to Revise Answers to Open-Ended Questions, Educational and Psychological Measurement 70(1):22DOI:0.1177/0013164409332231

[22] Shula chiat,Penny Roy(2007) The Preschool Repetition Test: An Evaluation of Performance in Typically Developing and Clinically Referred Children Journal of Speech Language and Hearing Research 50(2):429-43 DOI: 10.1044/1092-4388(2007/030)

[23] Yigali Attali, Don Powers, (2010) Immediate Feedback and Opportunity to Revise Answers to Open-Ended Questions, Educational and Psychological Measurement 70(1):22-35 DOI: 0.1177/0013164409332231

[24] Nate Kornell, Lisa.k son (2009) Learners choices and beliefs about self-testing.

[25] Jeffrey D Karpicke(2016) A powerful way to improve learning and memory

[26] Gagne Theories (2008). *Conditions of learning* (R. Gagne). http://tip.psychology.org/gagne.html

[27] Charles R. Dyer [2003] Intelligent Agents

[28] Russell, S. J. and Norvig, P. (2003). Artificial Intelligence: a Modern Approach. Prentice Hall, 2nd edition

[29] Njenga, Stephen & Oboko, Robert & I Omwenga, Elijah & Maina, Elizaphan. (2017). Use of Intelligent Agents in Collaborative M-Learning: Case of Facilitating Group Learner Interactions. International Journal of Modern Education and Computer Science. 10. 18-28. 10.5815/ijmecs.2017.10.03.

[30] Janis Dabolins, Janis Grundspenkis, (2014) The Role of feedback in Intelligent Tutoring system.

[31] Giannandrea, L. (2013). A literature review on Intelligent Tutoring Systems and on student profiling . Atee Conference.

[32] Ido Roll, Vincent Aleven, Bruce M. McLaren, Kenneth R. Koedinger. (2014) Improving students' help-seeking skills using metacognitive feedback in an intelligent tutoring system

[33] Manuela Macedonia, Iris Groher, Friedrich Roithmayr (2011) intelligent virtual agents as language trainers facilitate multilingualism Front Psychol. 2014; 5: 295. Published online 2014 Apr 14. doi: 10.3389/fpsyg.2014.00295

PMCID: PMC3995038

[34] Drigas, Athanasios & Ioannidou, Rodi-Eleni. (2012). Artificial intelligence in special education: A decade review. International Journal of Engineering Education.

[35] Gascueña, José & Fernández-Caballero, Antonio. (2005). An Agent-based Intelligent Tutoring System for Enhancing E-Learning/E-Teaching. Int J Instr Technol Dist Learn. 2

[36] Jose Gacuena,Antonio Fernandez-collabero,(2005) Anagent-based Intelligent Tutoring System for Enhancing/e-Teaching.

[37]Ogar Ofut Tumenayu, Olga Shabalina, Valeriy Kamaev and Alexander Davtyan (2014)Using Agent-Based Technologies to enhance Learning in Educational Games1. International Conference e-Learning 2014

Evaluating the Feasibility of Using Classifiers in Detecting Social Engineering Fraud

Clifford Kengocha
Kabarak University, 13 P.O. Box Private Bag, Kabarak, 20157, Kenya
Tel: +254 721681468, Email: cogeto@kabarak.ac.ke

Abstract

Social engineering fraud is among the most notorious forms of fraud through which people continue to lose money and sensitive information. 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 the possibility of using natural language processing and machine learning to automate the detection of voice-based social engineering fraud. Outcomes of the study can be used to develop automated real-time SEF detection systems.

Keywords: Machine learning, social engineering fraud, natural language processing, classifier

1. Introduction

Social engineering fraud (SEF) refers to any form of fraud that involves tricking victims to divulge sensitive information or authorize payments (Meinert, 2016). Before the mass penetration of information and communication technologies, such fraud occurred through face-to-face interactions. However, today, this form of fraud can be conducted over the phone, email or using messaging services. Phone-based SEF is particularly common as it takes relatively shorter times to get responses from victims and thus, complete the attack successfully (Nturibi, 2018). While it may be easy for some people to detect attempts to defraud them, it remains difficult for the elderly, illiterate or otherwise less-knowledgeable individuals to identify an impending fraud.

Various interventions including blacklisting suspect phone numbers and tightening law enforcement have been forged in attempts to control the problem. A particularly noteworthy effort in the prevention of related frauds is the introduction of voice biometrics by a Kenyan mobile money service provider to facilitate customer identification (Chetalam, 2018). This service allows customers to use their voices as a factor of authentication, thereby, preventing impersonation attacks. Nonetheless, the tricks and tactics used by swindlers keep changing such that countermeasures have not been effective. Therefore, there is a need to enhance existing measures or develop new approaches to address the problem.

One of the promising solutions to this problem is the use of machine learning to continuously collect data on phone-based fraud instances and use it to identify new events. Classifiers can be used for this purpose. Classifiers are a type of supervised machine learning algorithms that use input data sets to categorise new observations. Unlike regression algorithms which approximate the closeness of a given sample to an expected output, classifiers provide either "match" or "no match" outputs only. Thus, they have a chance of incorrectly classifying an observation. Nevertheless, this type of machine learning has been extensively applied in image classification problems with significant success (Litjens et al., 2017). This paper evaluates the applicability of the technology in voice classification to detect SEF.

2. The Problem

The high prevalence of social engineering fraud has resulted in substantial financial losses to end consumers and reputation damage to service providers. If this situation persists, the uptake of mobile money transfer technology may decline resulting in economic stagnation. Additionally, it may impact the adoption of other technologies by affected end users.

3. Objectives

The main aim of this research was to evaluate the feasibility of using classifiers to detect voice-based social engineering fraud. This aim was achieved by addressing the following objectives:

f) To identify and define indicators of looming fraud (IOLF) in voice calls.
g) To establish an approach for classifying SEF using indicators of looming fraud.
h) To establish the potential accuracy of classifiers in categorizing a call as fraudulent.
i) To recommend applications and areas improvement of the approach.

4. Literature review

Given that social engineering, in general, is an old problem, there exists vast literature on the subject. Some researchers have even developed appliances that help to minimize risks associated with social engineering. This literature review provides an analysis of relevant literature aimed at identifying the gaps in addressing social engineering fraud.

Social Engineering Detection

Social engineering is an art of deception. In the context of this study, it involves tricking an individual in attempts to lead them to provide information or authorize a payment. Its use in leading individuals to authorize payments, such as transferring money, has been noted with concern in the recent past (Castle et al., 2016). In US Patent 9,123,027, Srivastana, Walker and Olson present methods and systems for detecting social engineering in emails. The invention by the three scholars involves the extraction of both semantic and non-semantic data items from an email message. Semantic data refers to the meanings of the words used while non-semantic data refers to other properties of the email such as the sender's address. Using this approach, the researchers developed a functional appliance that can detect some level of social engineering in emails (Srivastana, Walker & Olson, 2015). This study indicates the significance of semantic data in computer-aided detection of malicious communication.

The use of natural language processing techniques in detecting social engineering has also been researched. Sawa, Bhakta, Harris and Hadnagy (2016) identify questions and commands in speech as two fundamental components of natural language. By processing natural language to extract questions and commands, the scholars theorize that it is possible to identify questions directed at obtaining sensitive information or commands intended at leading a user to perform unintended actions. Their approach involves comparing extracted questions and commands against a blacklist of common tricks. The authors reported a high rate of detection accuracy with few false positives. This research is consistent with Castle et al.'s patent inasmuch as both employ the use of semantic data extracted from a communication occurring in a natural language. Therefore, it is evident that using natural language processing to extract semantic data is a feasible method for obtaining indicators of looming fraud.

In another study, Bhakta and Harris further explore the concept of using semantic data items in the identification of IOLFs. Since a robust detection approach should be applicable to a variety of attack vectors, the authors propose the use of a topic blacklist to identify a potential fraud communication. According to their model, an attack is detected if a topic in a communication matches a topic on the blacklist (Bhakta & Harris, 2015). One of the major challenges with this approach is the difficulty in describing blacklist topics. Options for defining an unambiguous blacklist may be limited to keyword identification and the detection of word sequences. Clearly, this method would result in a non-exhaustive list of entries in the blacklist which will likely result in low detection rates. However, the method can be improved by allowing ambiguous definition of topics then adding another layer of verification to address the ambiguity. For instance, if a topic is identified as ambiguous, a non-semantic data item, such as the caller's phone number, can be used in the next step to rate its suspiciousness. The feasibility of using both semantic and non-semantic properties is evidenced in Castle et al.'s patent discussed above. Therefore, one can conclude that the concept of using predefined topic blacklists is a valid parameter for describing IOLFs.

Data quality is another factor that affects the success of machine learning systems. Poor data quality negatively impacts machine learning. As such, a high quality set of training data is paramount to the success of this approach. Quality data can be defined as data that exhibits consistency. Excessive heterogeneity in a data set can make it difficult for a machine learning system to accomplish its objectives. Similarly, excessive heterogeneity can result in relatively high error rates. A classifier, which is a typical machine learning system, is trained by running two sets of data through the algorithm until it can acceptably identify the set to which a given data sample belongs. In the context of this study, such data can be effectively obtained from users who can recognize fraudulent calls, either by recalling a similar incident or otherwise. Heartfield and Loukas (2018) aver that such social engineering training data for machine learning can be reliably obtained from end users. In a concept they dubbed as human-as-a-security-sensor, the researchers implemented Cogni-Sense, a prototype application for Microsoft Windows that "enables and encourages users to report semantic social engineering against them" (2018). The researchers conduct an experiment to test the effectiveness of Cogni-Sense deploying human sensors. They defined at least one user report as the criterion for detection. From the experiment, the scholars reported to have found less than 10% missed detections when human sensors are used compared to 81% where only technical sensors are used. There could be some variations in the rate of effectiveness of the sensors, but nevertheless, their study demonstrates the validity of collecting machine learning data from users.

Adedoyin et al. (2017) also evaluate the use of case-based reasoning, an application of machine learning, to predict fraud in mobile money transfer. Case-based reasoning is also a type of classification. Unlike in previously evaluated literature, Adedoyin et al.'s research does not refer to social engineering. Nevertheless, the researchers identify classification as one of the valid methods of predicting fraud. In case-based reasoning, past cases and their solutions are stored. When a similar or approximate case is encountered in future, the algorithm will use the past decision to predict the value of the expected output. This study further demonstrates that classification has the potential use in detecting fraud including social engineering fraud.

Voice-Based Authentication

Voice based authentication is increasingly being adopted as an alternative to password authentication. In the context of social engineering fraud, the major advantage of voice-based over passwords is the difficulty in executing impersonation attacks. As such, it has been proposed as a more secure approach to authenticating users prior to authorizing financial transactions in mobile money transfer platforms (Chetalam, 2018). However, it must be noted that social engineering fraud attack vectors are not limited to impersonation. In fact, a significant proportion of these attacks aim at influencing an authorized user to perform an unintentional action. Therefore, without undermining the effectiveness of voice-based authentication, using voice biometrics in place of passwords may not fully address the problem. Regardless of the inadequacy of voice biometrics in addressing fraud, it demonstrates that speaker recognition is a practical approach to identifying users. This conclusion revives the idea of using non-semantic properties in detecting IOLFs. In other words, it suggests that potential fraud can be detected simply by identifying the voice of the caller. In a given scenario, assuming the concept of human sensors is implemented, a swindler can be detected effortlessly if they have been reported before as a potential con-person.

This literature review has analysed current research on social engineering fraud and the different approaches researchers are using to attempt to solve the problem. The use of both semantic and non-semantic data items has stood out as a potential method of identifying indicators of looming fraud. Additionally, the use of predefined blacklists has been seen as an effective, though limited, approach to defining IOLFs. To improve the quality of training data and hence, the effectiveness of machine learning, literature has shown that using human sensors to report suspect cases can result in high detection efficiency. All these studies strongly suggest that a combination of these technologies can be used to effectively address voice-based social engineering fraud.

5. Methodology

Methods –Literature Review

This study used a literature review approach to address its objectives. To recap, the study aimed at evaluating the effectiveness of using classifiers to detect voice-based social engineering fraud. The study required an analysis of literature from diverse subjects in social engineering, machine learning and natural language processing. Consequently, the literature divided into the following subjects:

ii) Social engineering detection –Literature on social engineering detection was essential in identifying existing solutions and the challenges faced in addressing the problem. Observations from this field of study were also useful in defining IOLFs.

iii) Automated fraud detection –literature from this field of study was included to focus on addressing the use of classifiers in identifying IOLFs.

iv) Machine learning and natural language processing: Literature from this field of study was expected to address the use of natural language processing techniques in extracting semantic data from communications. It also tackled the feasibility of extracting useful non-semantic data from speech, such as data that can be used to distinguish a speaker.

Conceptual Framework

Conclusions from the literature review strongly suggested that a combination of (i) the use of both semantic and non-semantic data; (ii) the use of predefined topic blacklists; and, (iii) the use of human sensors to report suspected or actual cases of fraud, could be effective in detecting voice-based social engineering fraud. This conclusion is represented in the following illustration.

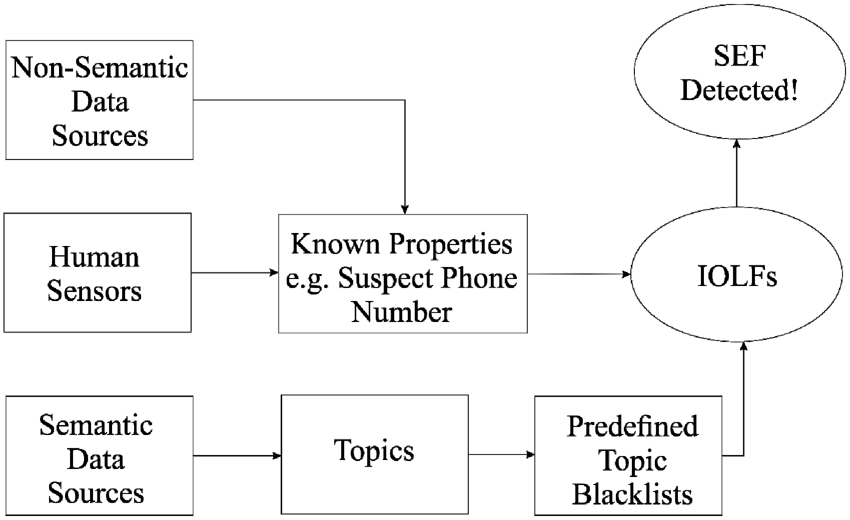

Non-Semantic Data Sources
SEF Detected!
Human Sensors
Known Properties e.g. Suspect Phone Number
IOLFs
Semantic Data Sources
Topics
Predefined Topic Blacklists

Fig. 1: Illustration showing the interaction of human sensors, semantic and non-semantic data sources and predefined topic blacklists in the automated detection of social engineering fraud

6. Results

This study was set to establish the extent to which the detection of social engineering fraud can be automated. In this quest, literature was systematically reviewed to address the objectives outlined initially. From the review, the following results were obtained:

- Indicators of looming fraud (IOLFs) can be obtained from both semantic and non-semantic data items. These may include reported phone numbers, names, aliases or specific tricks.
- Classification of SEF using IOLFs can be achieved using combination of (i) both semantic and non-semantic data; (ii) predefined topic blacklists; and, (iii) human sensors to report suspected or actual cases of fraud.
- The accuracy of any such classifier as above would largely depend on the data sources provided for training. More homogeneous data sets would result in higher accuracy of the classifier. It was also observed that the use of classifiers in other problem areas such as image classification have proven successful. Additionally, the

study found that the use of human sensors, as opposed to technical systems, can drastically improve the quality of data used for training the classifier.

7. Recommendations and Areas for Further Study

The outcomes of the study suggest feasibility and a high likelihood of success in the application of automated detection of social engineering fraud. The approach and objectives of the study were specific aimed at its application in detecting voice-based social engineering fraud. However, some of the discussions and results could be applied in frauds that use other attack vectors such as email. The findings can only be applied by both phone service providers and end-user application developers.

Although the research extensively covered the problem area, there are areas of study that could not be addressed due to limited scope. First, the definition of IOLFs is a continuous process which improves as more data is collected and tested. Therefore, the study recommends that further research be conducted to develop a more robust definition of IOLFs. Secondly, the study did not examine different classification approaches. It should be noted that different classification algorithms have varying applicability and accuracy. Therefore, it would be important to explore which algorithms are best suited for this application. This can only be achieved through tests with actual systems and actual data to compare the efficiency of different algorithms.

8. Conclusions

The study was successful insofar as it was able to determine that classifiers can be used in the automated detection of voice-based social engineering fraud. Some of the key concepts that would facilitate such tasks include the use of semantic and non-semantic data items, predefined topic blacklists and human sensors. Regardless of the success of the research, a few areas of further study were identified. These include strategies for widening the definition of IOLFs and further examination of suitable algorithms for this application.

References

Nturibi, B. M. (2018). A Mobile Money Social Engineering Framework for Detecting Voice & SMS Phishing Attacks-A Case Study Of M-Pesa (Doctoral dissertation, United States International University-Africa).

Litjens, G., Kooi, T., Bejnordi, B. E., Setio, A. A. A., Ciompi, F., Ghafoorian, M., & Sánchez, C. I. (2017). A survey on deep learning in medical image analysis. *Medical image analysis*, *42*, 60-88.

Castle, S., Pervaiz, F., Weld, G., Roesner, F., & Anderson, R. (2016). Let's Talk Money: Evaluating the Security Challenges of Mobile Money in the Developing World. In *Proceedings of the 7th Annual Symposium on Computing for Development* (p. 4). ACM.

Srivastava, M. K., Walker, W. A., & Olson, E. A. (2015). *U.S. Patent No. 9,123,027*. Washington, DC: U.S. Patent and Trademark Office.

Sawa, Y., Bhakta, R., Harris, I. G., & Hadnagy, C. (2016, February). Detection of social engineering attacks through natural language processing of conversations. In *2016 IEEE Tenth International Conference on Semantic Computing (ICSC)* (pp. 262-265). IEEE.

Bhakta, R., & Harris, I. G. (2015). Semantic analysis of dialogs to detect social engineering attacks. In *Proceedings of the 2015 IEEE 9th International Conference on Semantic Computing (IEEE ICSC 2015)* (pp. 424-427). IEEE.

Chetalam, L. J. (2018). *Enhancing Security of Mpesa Transactions by Use of Voice Biometrics* (Doctoral dissertation, United States International University-Africa).

Adedoyin, A., Kapetanakis, S., Samakovitis, G., & Petridis, M. (2017, December). Predicting fraud in mobile money transfer using case-based reasoning. In *International Conference on Innovative Techniques and Applications of Artificial Intelligence* (pp. 325-337). Springer, Cham.

Meinert, M. C. (2016). SOCIAL ENGINEERING: The Art of Human Hacking. *American Bankers Association. ABA Banking Journal*, *108*(3), 49.

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

Kirori Mindo [1] , Moses M Thiga [2] , Simon M Karume [3]
Department of Computer Science and Information Technology, Kabarak University, Kenya
[1]Tel: +245721864816. Email: kirori@kabarak.ac.ke
[2]Tel: +254720780468, Email: mthiga@kabarak.ac.ke
[3]Tel: +245722499397, Email: smkarume@laikipia.ac.ke

Abstract

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.

1. Introduction

It is reported that smart healthcare devices experience twice the number of cyber security attacks as opposed to other industries. FortiGuard Labs that provides cyber security defence mechanisms reported that healthcare experienced an average of 32,000 intrusion cyber security attacks per day in 2017. This is in comparison to 14,300 attacks in other industries (Adefala, 2018). A recent cyber-attack regarded as the biggest distributed denial-of-services attack ever experienced, a botnet of thousands of hacked IOT smart devices redirected traffic to a European based webserver in 2018 with packets exceeding one terabit per second (Liu, Jin, Hu, & Bailey, 2018).

It was recently reported by Ars Technica (Urquhart & McAuley, 2018) that hackers wrestled control over various IOT devices including cameras, routers and other IOT devices and initiated several DDoS attacks, which propagated data exceeding 300 Gbps In 2014, a children's Boston Hospital was a victim of a consistent DDoS attack, whereby hackers against Justina Pelletier at that time withheld at the hospital in Boston against her parents' wishes, were seeking her release. (Hongach, 2018). Recently an NSA cyber weapon - WannaCry was spread across the world, it infected several 200,000 Windows based machines which included systems at more than 45 hospitals in the United Kingdom. Various medical devices and technology-based healthcare devices were affected too, Forbes has learned (Kao & Hsiao, 2018). Orangeworm hackers have also been recorded to have attacked X-Ray and MRI Machines by targeting critical systems executed by major international health companies based in the United States, Europe, and Asia with a key focus on the healthcare devices (Arapi, 2018).

2. The Problem

Security of smart healthcare devices that provide mission critical support in healthcare is extremely vital. These devices, which run on MANETs, are such that their physiognomy lacks the adequate capability to devise robust systems to shield themselves against eavesdropping, malicious attacks, packet sniffing and other security threats. There is a great need to dissect and expound on these weaknesses and vulnerabilities that creates obstacles limiting the uptake of smart devices in healthcare.

3. Methodology for the Identification of Existing Weaknesses and Security Obstacles in The Application of MANETs For Provision of Smart Health Care.

A literature review study was carried out to examine and identify the weaknesses and security obstacles in the application of MANETs in the provision of Smart Health. The following were the objectives of the literature review;

i) To identify weaknesses if any, within the MANET ecosystem as a consequence of the device(s) physiognomy.

ii) To identify the various risks and attacks that can happen or be experienced within the MANET ecosystem as a result of the weaknesses identified.

The literature review was premised on the following empirical research questions.

- To what degree do the weaknesses within a MANET ecosystem contribute to vulnerability?
- To what extent does the weaknesses of MANET devices and the ecosystem, contribute to risks and expose the devices, data and network to attacks.
- To what magnitude do the various weaknesses contribute to loss of confidentiality and availability of the devices and/or data?

4. Literature Review.

The following some of the common attacks in internet of things as presented by various authors

i. Leakage of Information (Confidentiality)

Data and information collected and transmitted by the smart devices within an MANET wireless sensor network is susceptible to leakage. Data and information from these devices is easily leaked since there lacks sufficient data encryption that is applied either between gateway and sensors or between the sensors themselves. In addition, user authentication to prevent un-authorized access and/or enable detection of unwanted and unauthorized parties is often weakly implemented (Rath et al, 2018).

ii. Denial of Service and/or Distributed Denial of Service (Availability)

This is a common attack that denies users from accessing the system(s) and information when and if they require it. This DOS/DDOS attack targets a device by using malicious unwanted response requests thereby draining resources and rendering the device unable to respond to genuine user requests. While no data is leaked or exposed, it is very disastrous as it makes systems unusable and renders data/information un-useful as a result for the period of the attack (Dhindsa and Bhushan, 2019).

iii. Falsification (Integrity)

This attack happens when a wireless device is in communication with the gateway and the attacker successfully captures the collect packets in transition and alters the fields containing routing information. As a result, the attacker can access the information therein and alter, leak or destroy the data/information as a whole. Most SSL mechanisms have the capability to protect against this type of attack, while unauthorized devices that gain access should be entirely blocked. Most of these attacks happen as passive eavesdropping and/or traffic analysis. Hostile silently listen the communication (Ngomane, Velempini and Dlamini 2018).

5. Research Methodology for Identifying the Weaknesses and Security Obstacles in the Application of MANETs for Provision of Smart Health Care.

The literature review study exposed numerous weaknesses that hinder adoption of MANETs in healthcare due to the nature of these devices and their physiognomies. The results identified the security weaknesses in MANETs that have inhibited rapid adoption in smart devices for provision of healthcare, as follows.

i. Weakness 1: Distributed Operation

One of the characteristics of MANETs is that they have no centralized control of network operations. This lack of coordination can bring addressing conflicts, routing and data loops. This results from the lack of a well-coordinated defence mechanism as shown (Inzillo, Serianni and Quintana, 2019)

ii. Weakness 2: Multi-Hop routing

Devices in MANETs forward packets via an intermediate node thus bringing up possibility of eavesdropping and man in the middle attacks. Due to their mobile nature, a device that requires to remotely forwards packets to a neighbouring hopping device, which can turn out to be a malicious device, or one that is not authorized to handle the traffic (Zhang et al., 2018).

iii. Weakness 3: Light Weight Terminals

These devices in MANETs are considered Light Weight Terminals with Low CPU capability, low power storage and small memory size. Thus they do not have the ability to provide robust security and protection. Low CPU capability translates to their inability to run high key security algorithms. Low power storage is a weakness that can cause the device to deplete its power resource once overworked by malicious attacks. In addition, its small memory size incapacitates it from running robust security systems (Kamakshi and Kumar, 2018).

iv. Weakness 4: Shared Physical Medium

MANETs ecosystem is by nature a wireless shared medium propagated by CSMA/CA for purposes of collision avoidance due to the shared nature of the physical medium. These devices are thus visible to other devices on the same channel and or any devices with sniffing capability. Further, attacks like MAC addressing snooping are easily propagated in such an environment (Kamakshi and Kumar, 2018).Results.

v. Weakness 5: Limited bandwidth

Devices in MANET ecosystems mainly exhibit a small packet data size, which propagates bandwidth with a data rate of upto 250kbit/s. This is quite limiting as compared with other devices as those on Wireless Fidelity. This also means that a large case of DDOS on such an ecosystem can easily clog the network (Delkesh and Jamali, 2019).

vi. Weakness 6: Dynamic topology

There is a rapid and dynamic topology change, due to the mobility of the devices in MANETs. This brings upon disturbed trust among nodes, due to their reconfiguration and reorientation to new networks and unfamiliar intermediary devices (Chaudhary and Shrimal, 2019).

vii. Weakness 7: Routing Overhead

Intermediary devices within the MANET ecosystem experience a lot of routing information overhead due to the dynamic networks and mostly stale routes. There are also numerous and unnecessary routing overhead as a result which clog and slow up route resolution functionalities (Garikipati and Rao, 2019).

viii. Weakness 8: Hidden terminal problem

The hidden terminal problem is a common phenomenon which multiplies transmissions thus resulting to collision of packets in some cases. This hidden terminal can also lead to packet losses due to transmission errors. Collisions and packet losses especially in UDP communication are considered expensive since UDP is an un-reliable protocol without strategies for recovery in data loss (Tomar et al., 2019).

ix. Weakness 9: Wireless Radio

Devices in MANETs communicate over wireless links thus suffer from electro-magnetic interference, uni-directional links and frequent path breaks due to mobility of nodes which can lead to loss of data or duplicate frames. (Das and Pal, 2019).

x. Weakness 10: Mobility

By the fact that they have dynamic mobility, this nature brings about induced route changes and frequent route changes which can cause data loss. This would have dire consequences especially when this technology is applied to monitor healthcare for users whom their lives depend on monitoring devices (Fatima et al., 2019).

xi. Weakness 11: Battery constraints

Most MANET devices rely on batteries to provide power. If the device experiences DDOS attacks, it can lead to draining of battery resources and thus result to broken links or dead links which lead to data loss (Singh et al., 2018).

xii. Auxiliary Security Weakness

The nature of these devices in MANETs is auxiliary node cooperation which can lead to exposure to numerous security attacks. Devices are required to first corporate with similar devices within the ecosystem, while cautious connectivity is discouraged. As a result, a device looking to gather reconnaissance data, finds cooperative devices (Aldaej, 2019).

6. Results.

The table below summarises the identified weaknesses and vulnerabilities through which various threats take advantage of to attack the MANET.

Table 1: Summary of MANET Vulnerabilities that propagate security threats.

No	Weakness	Vulnerability	Attack / Risk /	Source
a)	Distributed Operation	No centralized control of the network operations	Each node is a relay	(Inzillo, Serianni and Quintana, 2019)
b)	Multi-Hop routing	Packets forwarded via an intermediate node	Eavesdropping	(Zhang et al., 2018)
c)	Light Weight Terminals	Low CPU capability, low power storage and small memory size	Non-Robust systems	(Kamakshi and Kumar, 2018)
d)	Shared Physical Medium	Wireless communication	Medium accessible to other entities	(Kamakshi and Kumar, 2018)
e)	Limited bandwidth	Lower capacity	Lower throughput	(Delkesh and Jamali, 2019)
f)	Dynamic topology	Rapid Topology change	Disturbed trust among nodes	(Chaudhary and Shrimal, 2019)
g)	Routing Overhead	Dynamic networks	Stale routes and unnecessary routing overhead.	(Garikipati and Rao, 2019)
h)	Hidden terminal problem	Multiple transmissions	Collision of packets Packet losses due to transmission errors High packet loss	(Tomar et al., 2019)
i)	Wireless Radio	EMI interference	Uni-directional links, frequent path breaks due to mobility of nodes.	(Das and Pal, 2019)

j)	Mobility	induced route changes	Frequent route changes which can cause data loss.	(Fatima et al., 2019)
k)	Battery constraints	Restricted power source	Lack keep alive	(Singh et al., 2018)
l)	Auxiliary Security threats	node cooperation	Exposure to numerous security attacks.	(Aldaej, 2019).

7. Validation of the Results.

Following the general literature review on security weaknesses in the application of MANETs for the provision of Smart Health care, there was need to perform validation of the results recorded above, to ascertain that malicious attacks like DDOS do happen on MANETS easily. This section was achieved through using Proof of Concept methodology.

The main objective of this section was to interrogate whether, by taking advantage of weaknesses in MANETs, the following activities can be achieved;

j) To verify if a DDOS can be easily propagated within a MANET.

k) To verify if a Blackhole attack can be carried out within a MANET.

A MANET network was implemented on Linux, to review the performance of devices so as to validate and ascertain the results of the desk research. This network was setup without any intrusion detection scheme implemented so as to note and review the weaknesses that can cause loss of confidentiality, availability and integrity thus inhibit the application of MANET for provision of smart health care. The Figure 4 below shows the MANET set up without any security IDS and the various malicious attacks that were experienced.

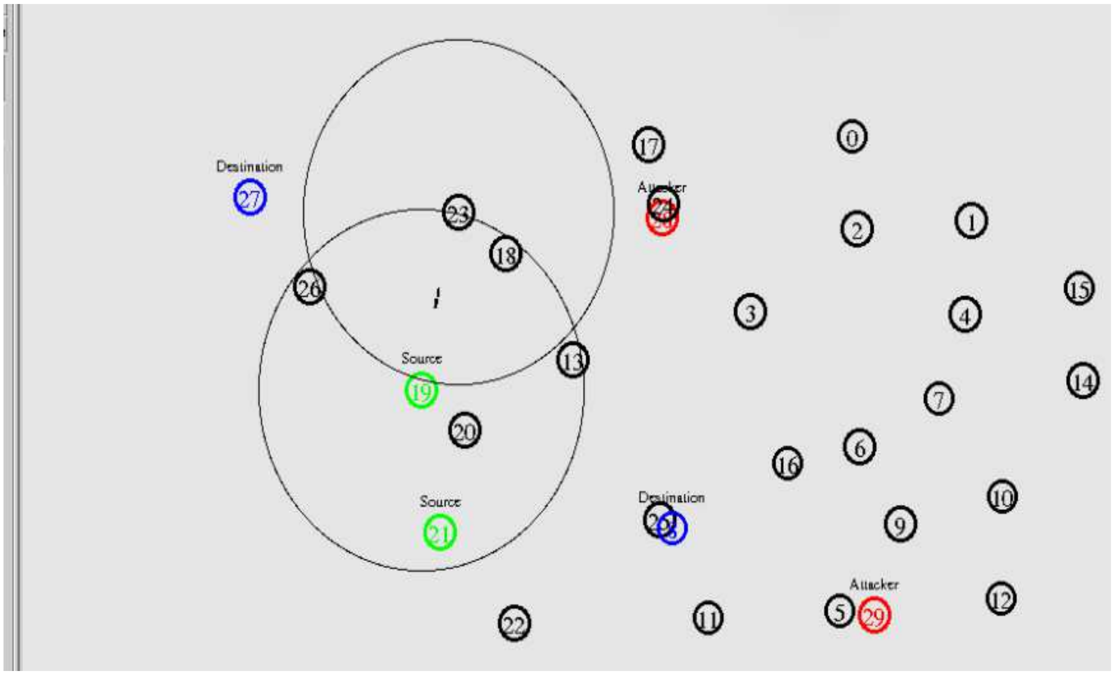


Figure 1: An open vulnerable MANET

The various devices in the above network propagated data using Bluetooth, with two source (19 and 20) and two destination devices (26 and 27). Two other devices were configured as malicious nodes which are required to propagate DDOS and blackhole attacks on the MANET.

Running the network above, the experiment enabled the deployment of two types of malicious data in DDOS and blackhole attacks, which were feasible and that run successfully. As a result, there was a high propagation of duplicate packets on the network. This is extremely dangerous, since an attacker can take advantage of this gap and launch data interception, man in the middle attacks, packet replay as well as packet delay.

Following the ability to propagate these attacks, the experiment above confirms that, if replayed in a real-world environment, it can have serious ramifications to healthcare users. These includes and especially those ailing patients with heart beat monitors, pacemakers, blood pressure monitors can bring life threatening consequences. Table 4 below shows the various malicious packets that were successfully permeated and their anomalous characteristic.

Table 2: Malicious Packets permeated into the MANET successfully.

No	Data Type	Disposition	Vulnerability	Attack
1	ICMP	High Rates	DDOS	Availability
2	TCP	Black hole	Reconnaissance	Confidentiality

Table 4 above, shows that MANETs are vulnerable and thus propagate two types of attacks against confidentiality and availability as shown above by Blackhole and DDOS attacks. Blackhole attacks on a network, can affect the data in two ways;

- A malicious node transmits an erroneous RREP (Route Replay) message to the source device; masquerading as the shortest path to the destination thus packets are forwarded to the malicious node.
- In another scenario, incoming or outgoing traffic can be redirected to a blackhole (or a dev/null) without the source device knowing that the traffic did not reach its intended destination

In both cases above, a third party can receive unauthorized or unsolicited packets leading to both loss of confidentiality and/or availability of data. DDOS can be disastrous since systems, data or routes can be completely unavailable to devices, people or systems that direly need them.

8. Recommendations.

Subsequent to the validation of general literature review on security weaknesses and obstacles in the application of MANETs for the provision of Smart Health care, there emerged observable and feasible recommendations which are enumerated below. The resulting design would take cognizance of the weaknesses in IDS systems for MANET and ensure that MANETs design should not introduce a window for added vulnerabilities to the system and should be self□managed to monitor and identify both hardware and software abnormalities and modifications spontaneously. The following are key areas to apply when designing a secure IDS system for MANETs.

- The Smart MANET IDS should have ability to identify intrusions by taking cognizance of unfamiliar device addresses;
- The Smart MANET IDS should not permit TCP sessions that are initiated by devices outside its network to get into fruition;
- The Smart MANET IDS should detect the intrusions with low processing and communication overhead;
- The Smart MANET IDS should identify scenarios that cause high resource usage in CPU, Ram and bandwidth within the ecosystem;
- Dynamic network topology and mobility of MANET devices should not affect the detection accuracy of the Smart IDS MANET system;

Conclusion.

This paper discussed the literature review on weaknesses that inhibit application of MANETs for smart health. The literature provided vital knowledge on various other researchers' experiences that will guide the design, implementation and evaluation of a fused machine learning intrusion detection model for the provision of smart health care in MANETS.

The results showed that existing intrusion detection methods are mainly built for compute-intensive systems and mainly and most commonly, for networks with a rigid architecture and topology. MANET are mobile and deployed in a scattered fashion, with a frequent change in network topology which translates from their continuously changing addresses schemes, depending on the hosting network that they plug into. As a consequence, therefore, these devices must consistently reconfigure their routes. As such, MANETs and devices in MANETs lack a central controlling system thus must perform these tasks on their own. As a result of both the literature review and validation of the same, the following research questions were answered;

- The various weaknesses within a MANET ecosystem do contribute to vulnerabilities within the MANET ecosystem.
- These weaknesses of MANET devices and the ecosystem, exposes the devices, data and network to attacks.
- Attacks are experienced within the MANET ecosystem do contribute to loss of confidentiality and availability of the devices and/or data.

References

Adefala., L (2018, March 06). Healthcare Experiences Twice the Number of Cyber Attacks As Other Industries. Fortinet Labs. Retrieved from https://www.fortinet.com/blog/business-and-technology/healthcare-experiences-twice-the-number-of-cyber-attacks-as-othe.html.

Aldaej, A. (2019). Enhancing Cyber Security in Modern Internet of things (IoT) Using Intrusion Prevention Algorithm for IoT (IPAI). IEEE Access.

Arapi, K. (2018). The Healthcare Industry: Evolving Cyber Threats and Risks (Doctoral dissertation, Utica College).

Chaudhary, A., & Shrimal, G. (2019). Intrusion Detection System Based on Genetic Algorithm for Detection of Distribution Denial of Service Attacks in MANETs. Available at SSRN 3351807.

Das, S., & Pal, S. (2019). Analysis of Energy-Efficient Routing Protocols in Mobile Ad Hoc Network. In Advances in Computer, Communication and Control (pp. 285-295). Springer, Singapore.

Delkesh, T., & Jamali, M. A. J. (2019). EAODV: Detection and removal of multiple black hole attacks through sending forged packets in MANETs. Journal of Ambient Intelligence and Humanized Computing, 10(5), 1897-1914.

Dhindsa, K. S., & Bhushan, B. (2019). Flow-based Attack Detection and Defense Scheme against DDoS Attacks in Cluster based Ad Hoc Networks. International Journal of Advanced Networking and Applications, 10(4), 3905-3910.

Fatima, M., Bandopadhyay, T. K., & Gupta, R. (2019). Unconventional Prediction Algorithm for Quick Route Convergence and Stability in MANET. In Computing, Communication and Signal Processing (pp. 409-418). Springer, Singapore.

Garikipati, V., & Rao, N. N. M. (2019). Secured Cluster-Based Distributed Fault Diagnosis Routing for MANET. In Soft Computing and Signal Processing (pp. 35-51). Springer, Singapore.

Hongach Jr, W. J. (2018). Mitigating Security Flaws in the TCP/IP Protocol Suite (Doctoral dissertation, Utica College).

Inzillo, V., Serianni, A., & Quintana, A. A. (2019). A secure adaptive beamforming mechanism exploiting deafness in direcional beamforming MANET. In Signal Processing, Sensor/Information Fusion, and Target Recognition XXVIII (Vol. 11018, p. 110181F). International Society for Optics and Photonics.

Kamakshi, Y. L., & Kumar, M. M. (2018). A Novel Approach to Secure Route Discovery for Dynamic Source Routing in MANETs.

Kao, D. Y., & Hsiao, S. C. (2018, February). The dynamic analysis of WannaCry ransomware. In Advanced Communication Technology (ICACT), 2018 20th International Conference on (pp. 159-166). IEEE.

Liu, Z., Jin, H., Hu, Y. C., & Bailey, M. (2018). Practical Proactive DDoS-Attack Mitigation via Endpoint-Driven In-Network Traffic Control. IEEE/ACM Transactions on Networking, (99), 1-14.

Ngomane, I., Velempini, M., & Dlamini, S. V. (2018). The detection of the spectrum sensing data falsification attack in cognitive radio ad hoc networks. In 2018 Conference on Information Communications Technology and Society (ICTAS) (pp. 1-5). IEEE.

Rath, M., Swain, J., Pati, B., & Pattanayak, B. K. (2018). Network Security: Attacks and Control in MANET. In Handbook of Research on Network Forensics and Analysis Techniques (pp. 19-37). IGI Global.

Singh, P., Gupta, S., Sejwal, L., & Mohan, A. (2018). Power Issues of MANET. In Information and Communication Technology (pp. 123-128). Springer, Singapore.

Tomar, R. S., Sharma, M. S. P., Jha, S., & Chaurasia, B. K. (2019). Performance Analysis of Hidden Terminal Problem in VANET for Safe Transportation System. In Harmony Search and Nature Inspired Optimization Algorithms (pp. 1199-1208). Springer, Singapore.

Urquhart, L., & McAuley, D. (2018). Avoiding the internet of insecure industrial things. Computer Law & Security Review, 34(3), 450-466.

Zhang, M., Yang, M., Wu, Q., Zheng, R., & Zhu, J. (2018). Smart perception and autonomic optimization: A novel bio-inspired hybrid routing protocol for MANETs. Future Generation Computer Systems, 81, 505-513.

.

Towards a Unique, Secure, and Robust Wireless Local Area Network Device Identifier

John C. Chebor[1], Simeon M. Karume[2] and Nelson B. Masese[3]

[1]Kabarak University, P.O. Box Private Bag, Kabarak, 20157, Kenya
Tel: +254 0721416894, Email: jchebor@kabarak.ac.ke

[2]Laikipia University, P.O. Box 1100-20300, Nyahururu, Kenya
Tel: +254 0722499397, Email: smkarume@gmail.com

[3], [1]Kabarak University, P.O. Box Private Bag, Kabarak, 20157, Kenya

Tel: +254 0727171725, Email: NMasese@kabarak.ac.ke

Abstract

With today's technological evolution, wireless networks have become very common for organizations, homes and public places. For any device to be authenticated and authorized to use any of the wireless network services, it must first be identified then 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. This study therefore examined uniqueness, security and robustness characteristics of MAC in relation to a device serial number in order to establish a suitable network device identifier. In order to achieve this, test runs through a proof of concept method by using *Advanced IP Scanner* and *getmac* command line tools. Advanced IP Scanner was used to determine the security, hence robustness of the identifiers while *getmac* was used to determine the uniqueness of the identifiers. The run tests indicated that a MAC address can actually be spoofed and altered rendering the MAC address not unique, insecure and unreliable. On the contrary, a computer's serial number is hard-coded in the hardware only and therefore cannot be spoofed and altered making it unique, secure and reliable. The researcher recommends that a study be conducted on how a device serial number can be used as network device identifier

Key Words: Network device, MAC Address, Serial Number, Identifiers, Wireless Local Area Network

1. Introduction

Wireless LANs (WLAN) also known as Wireless Fidelity (Wi-Fi) or 802.11 standards is a type of a local area network that allows users access network services using mobile devices (wireless stations) such as laptops, personal digital assistants and even smartphones (Dordal, 2018). The wireless stations use a base station usually an access point (AP) as an entry point to the network services. Unlike wired LANs that use cables or wires as transmission media, WLANs uses radio wave frequencies to transmit information over the local area network.

WLAN comes with a number of benefits as compared to wired LANs, notably mobility, rapid deployment, reduction in infrastructure and operational cost, flexibility, and scalability (Raji, 2014; DHS, 2017; Wallace, 2018). Due to these benefits hotpots are now virtually found everywhere; in enterprises, at homes, and in public places. Wireless devices such as laptops, personal digital assistants and even smartphones come with WiFi features integrated into them. Despite the numerous benefits that come with wireless LANs, network insecurity has become a thorn in the flesh for proprietors of such kind of networks. Singh & Sharma (2017), point out that an attacker simply needs to be within the range of the WLAN access point to intrude into the network as opposed to wired LANs where an attacker requires physical access to the LAN or remotely use porous firewall systems to gain access to the LAN. WLANs are therefore easily targeted by attackers through spoofing, denial of service, eavesdropping, man-in-the-middle, masquerading, message modification, message replay and traffic analysis (Stallings, 2011; DHS, 2017; Wallace, 2018), describes the reasons for the threats as default configurations, network architecture, encryption weaknesses, and physical security. Garska, (2016), identifies identification, authentication, and authorization as the essential functions in providing the required services in a network.

For authentication and authorization hence accounting to take place, devices in a network must first be identified. According to Takahashi *et al.* (2010), devices in a network can only be explicitly identified by their port numbers, IP address, and MAC address. But whereas MAC addresses are used by messages to identify actual physical destination and source network addresses, IP addresses are used by information to be effectively routed from network to network in an internetwork. On the other hand, port numbers are used specifically to identify processes running on sending and receiving stations (Kurose & Ross, 2013).

Problem Statement

Existing identification methods at the OSI model include the physical address (MAC address) at the data link layer, the logical address (IP address) at Network layer, the Port address at Transport layer and the application specific address at the application layer. Whereas MAC addresses are used by messages to identify actual physical destination and source networks, IP addresses are used by information to be effectively routed from network to network in an internetwork. On the other hand, port numbers are used specifically to identify processes running on sending and receiving stations while application address is for identifying different instances of the same application (Kurose & Ross, 2013).

Apart from the absence of identifiers at the physical layer of the OSI reference model, MAC addresses, which are used to identify the physical source and destinations addresses, are not universally unique across networks, they are easily spoofed and altered to aid in spoofing attacks. In addition, MAC addresses are coded on the network hardware and a copy is replicated in the operating system when the system starts to facilitate network troubleshooting and configuration. This copy of the MAC address is the one that is usually spoofed. Furthermore, all the identifiers (MAC address, IP address, Port number and application-specific address) are pointers to locations rather than the device itself.

Research Objectives

The main aim of the study was to investigate the suitability of a MAC address in relation to a serial number as a wireless LAN device identifier. The specific objectives are:

i) To establish the characteristics of wireless device identifiers

ii) To analyse the suitability of a MAC address in relation to a computers serial number network device identifier

iii) To recommend a suitable network device identifier

Related Work

An identifier, according to Hoffer *et al.* (2009), is an attribute (or a combination of attributes) whose value distinguishes instances of an entity type (device) from another. Coulouris *et al.* (2012) further cites examples of identifiers as could be a code (identification number, serial number, ISBN) name (domain name) or an address (IP, MAC, Port Number or an application specific address). An attribute should possess uniqueness, universality, collectability, security, data dependence, robustness and mnemonic (Danev *et al.* 2015; Lavassani *et al.* 2010; and Leo, 2004) qualities to be a good identifier. Whereas uniqueness ensures that no two devices have the same identifier value, universality ensures that devices in the same space have an identifier, collectability is the ability of an identifier to be captured from existing systems, security ensures availability, integrity and confidentiality of an identifier, data dependence is the ability of an identifier to be associated with other device attributes, robustness or reliability or permanence is the ability of an identifier not to vary with time and mnemonic defines a standard and meaningful structure of the identifier.

Application specific addresses are addresses that are designed for a specific application geared towards user-friendliness. Also referred to as persistent identifiers (Richards *et al.* 2011), the application specifies identifier is permanently assigned to an object. Examples of application specific addresses include e-mail address such as deanset@kabarak.ac.ke and a universal resource locator (URL) such as kabarak.ac.ke. Whereas an e-mail address defines the recipient of an e-mail, a URL is used to find a document on the internet.

Such addresses or locators fundamentally play a crucial role in enabling internet users easily finds information on the internet (Commer, 2013). This is more so as the internet has a huge amount of information which makes it difficult to find. Labelling the files or objects in a way of application-specific addresses, therefore, makes it easy to find a specific object or file. The addresses, however, get changed to the corresponding port and MAC addresses of the sending computer.

Port numbers are numbers on hosts/devices that identify sending and receiving processes. According to Lee, (2010), port numbers are usually captured when a system requests for a page with usernames and password details. Process identification in communication is crucial because a host could be running several applications. Although port numbers can be used in conjunction with other numbers, namely, IP address and MAC address to identify a host, port numbers can pause as threat to network security. Intruders can use a port scanner that listens to well-known port numbers so as to detect services running on a system, therefore can easily break into the system (Canavan, 2012).

An IP address is number assigned to a host or a router in the internet for identification and location of the device as stated by Tanenbaum, (2011). An IPv4, which is currently in use (Kurose & Ross, 2013), is composed of four dotted decimal notation (example 243.246.0.28) each part range between 0 and 255. Depending on the class or the subnet mask of the IP address, some parts (first) belong to network identification and the other parts (usually from the second part) belong to host identification. IPv4 was designed to use 32-bit address space (Shay, 2004). This translates to 2^{32} or approximately four (4) billion addresses which is not sufficient for the global needs. Actually, the numbers were projected to have been exhausted by 2013 (IEEE-USA, 2009). A temporary solution of conserving IP address used by network administrators in apart from organizational LANs, has also found use in residential and wireless LANs, is the use of DHCP (Kurose & Ross, 2013). DHCP assigns devices IP addresses on demand, therefore two devices can use the same IP address but on different occasions.

MAC address also known as LAN address or a physical address is a number used to identify a network adaptor on a LAN. As Kurose & Ross, 2013 puts it "it is not hosts and routers that have link-layer addresses but rather their adapters (that is, network interfaces) that have link-layer addresses." In other words, a MAC address is used not by devices but by information to identify a particular physical network like an Ethernet network. A device with multiple interfaces has multiple corresponding MAC addresses. Kurose & Ross, 2013 further puts it that the management of MAC address space is the prerogative of IEEE internet standard. This then implies that different adaptors from different manufacturing companies cannot have the same MAC address. Furthermore, the possibility of a MAC address being spoofed renders it not unique, variant and therefore unreliable.

Methodology

Out of all the characteristics of an identifier, security, robustness and uniqueness characteristics compromised the suitability of a MAC address as an identifier. Security, robustness and uniqueness qualities were therefore analysed using *Advanced IP Scanner* and *wmic* command line tools through test runs. *Advanced IP Scanner* was used to test security and consequently reliability of a computer's serial number and a MAC address. Similarly, *wmic* command line tool was used to test the uniqueness characteristics of the identifiers whose results are presented in the section next.

Results

Characteristics of a Network Device Identifier

The characteristics that define the suitability of an identifier as were established from the related work section of this study were uniqueness, universality, collectability, data dependent, security (availability, integrity, and confidentiality), robustness and mnemonics. As compared to the other identifier characteristics, security, robustness and uniqueness characteristics were established to compromise the suitability of MAC address. The three requirements were examined as follows

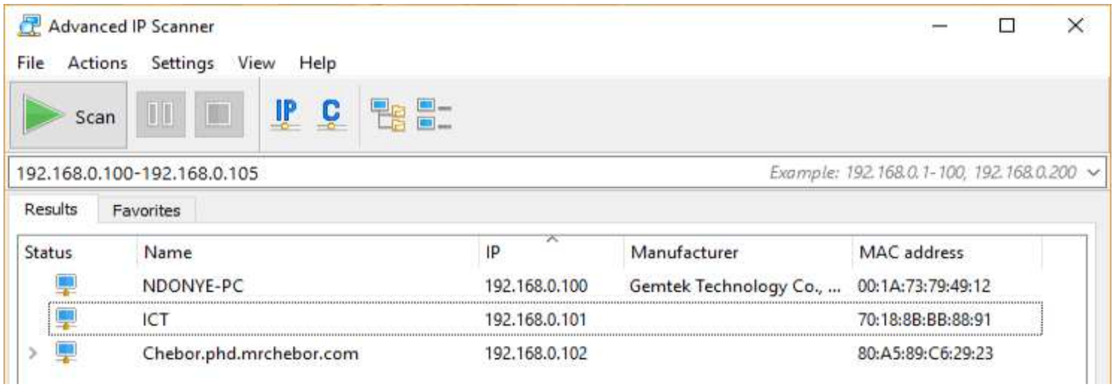
Suitability of MAC Address as Physical Layer Network Identifier

Security of a MAC Address

Availability, confidentiality and integrity aspects of security determine the suitability of a MAC address.

Confidentiality of a MAC Address

Confidentiality of an identifier is the degree of how an identifier can be disclosed to an unauthorized entity (Paulsen & Byers, 2019). Although measures have been put in place to protect the confidentiality of a MAC address by coding it into the network hardware, as a network device identifier, attackers would always have a way of getting it unauthorized. *An Advanced IP scanner* tool, for instance, can be used by an intruder to access MAC address of all devices connected to the network. To demonstrate this, the researcher created a test network of three computers and then the scanner was run from one of the computers. The results are presented in figure 1 below



192.168.0.100-192.168.0.105

Example: 192.168.0.1-100, 192.168.0.200

Status	Name	IP	Manufacturer	MAC address
	NDONYE-PC	192.168.0.100	Gemtek Technology Co., ...	00:1A:73:79:49:12
	ICT	192.168.0.101		70:18:8B:BB:88:91
	Chebor.phd.mrchebor.com	192.168.0.102		80:A5:89:C6:29:23

Figure 1: MAC Address Spoofing

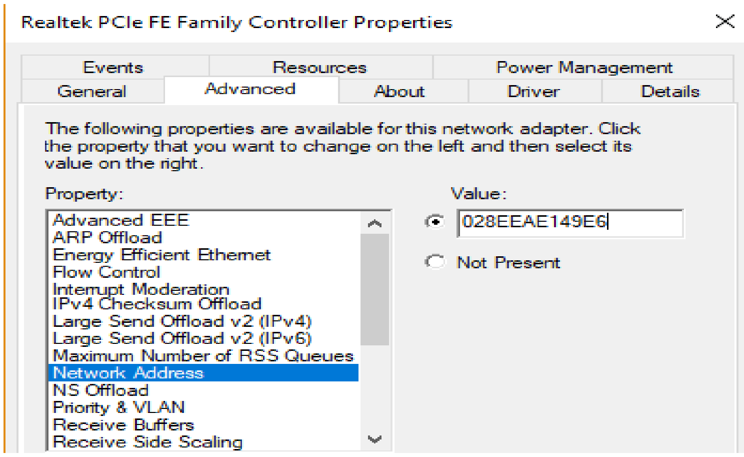
As demonstrated in the results in figure 1 above, the scanner collected and displayed all the MAC addresses of the networked computers. This may result in the following flaws

i) If the network is designed to use MAC filters to allow or block network access based on valid existing MAC addresses, then an attacker may use a MAC address spoofed using the advanced IP scanner to gain access to the network
ii) When an attacker knows ones MAC address then they can use it to track a user
iii) If the valid MAC address device and the spoofed MAC address device log onto a network simultaneously, the addresses conflict with each other resulting in miscommunication and inconvenience on the valid device end.

The integrity of a MAC Address

A MAC address is usually hard-coded or 'burned' into the network hardware; therefore, it is difficult to alter it. However, a copy of the MAC address in the system software can easily be modified by an attacker to suit the valid MAC addresses spoofed. To demonstrate this, the following procedure was used to alter the researcher's computer MAC address and results illustrated in figure 2 below:

i) Open System Properties window
ii) Click on Device Manager
iii) Click on the plus sign preceding Network Adaptors list on the dialog that appeared
iv) Select the card whose MAC address is to be altered
v) Right click on the network adaptor and select Properties
vi) Click on the Advanced tab
vii) Click on Network Address option in the list provided
viii) Type the six-digit code in the Value field after selecting the radio button
ix) Click OK



Realtek PCIe FE Family Controller Properties

The following properties are available for this network adapter. Click the property that you want to change on the left and then select its value on the right.

Property:

Advanced EEE
ARP Offload
Energy Efficient Ethernet
Flow Control
Interrupt Moderation
IPv4 Checksum Offload
Large Send Offload v2 (IPv4)
Large Send Offload v2 (IPv6)
Maximum Number of RSS Queues
Network Address
NS Offload
Priority & VLAN
Receive Buffers
Receive Side Scaling

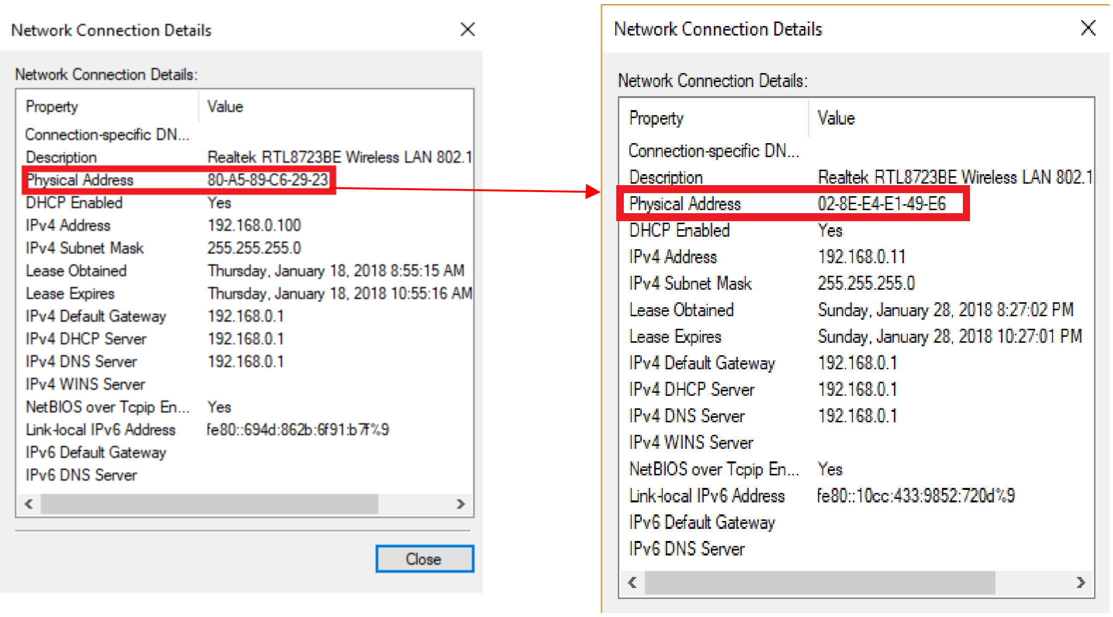
Value:

● 028EEAE149E6

○ Not Present

Figure 2: MAC address copy in system software

The altered MAC address is illustrated in figure 3 below. The first part of the figure shows the original MAC address 80-A5-89-C6-29-23 of the researcher's computer before and after it was altered using the procedure described figure 2 above to 02-8E-E4-E1-49-E6.



Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Realtek RTL8723BE Wireless LAN 802.1
Physical Address	80-A5-89-C6-29-23
DHCP Enabled	Yes
IPv4 Address	192.168.0.100
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Thursday, January 18, 2018 8:55:15 AM
Lease Expires	Thursday, January 18, 2018 10:55:16 AM
IPv4 Default Gateway	192.168.0.1
IPv4 DHCP Server	192.168.0.1
IPv4 DNS Server	192.168.0.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::694d:862b:6f91:b7f%9
IPv6 Default Gateway	
IPv6 DNS Server	

Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Realtek RTL8723BE Wireless LAN 802.1
Physical Address	02-8E-E4-E1-49-E6
DHCP Enabled	Yes
IPv4 Address	192.168.0.11
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Sunday, January 28, 2018 8:27:02 PM
Lease Expires	Sunday, January 28, 2018 10:27:01 PM
IPv4 Default Gateway	192.168.0.1
IPv4 DHCP Server	192.168.0.1
IPv4 DNS Server	192.168.0.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::10cc:433:9852:720d%9
IPv6 Default Gateway	
IPv6 DNS Server	

Figure 3: MAC Address before and after alteration

Both results were viewed through the following procedure:

a) Click on Control Panel then Network and Sharing Centre
b) Click on any one of the active networks
c) Click on the Details button on the general tab of the active network window
d) Which leads to Network Connection Details shown in figure 3 above

Availability of a MAC Address

Availability aspect of security as defined earlier on (Paulsen & Byers, 2019), refers to the accessibility and usability of an identifier upon demand by an authorized user. Availability ensures that the identifier works properly and that its service is available to valid users when needed. In ideal scenarios, a MAC address is usually made available by having a copy in the operating system as illustrated in figure 5 above. However, the effect of the possibility of altering a MAC address compromises the availability of a MAC address.

Robustness of a MAC Address

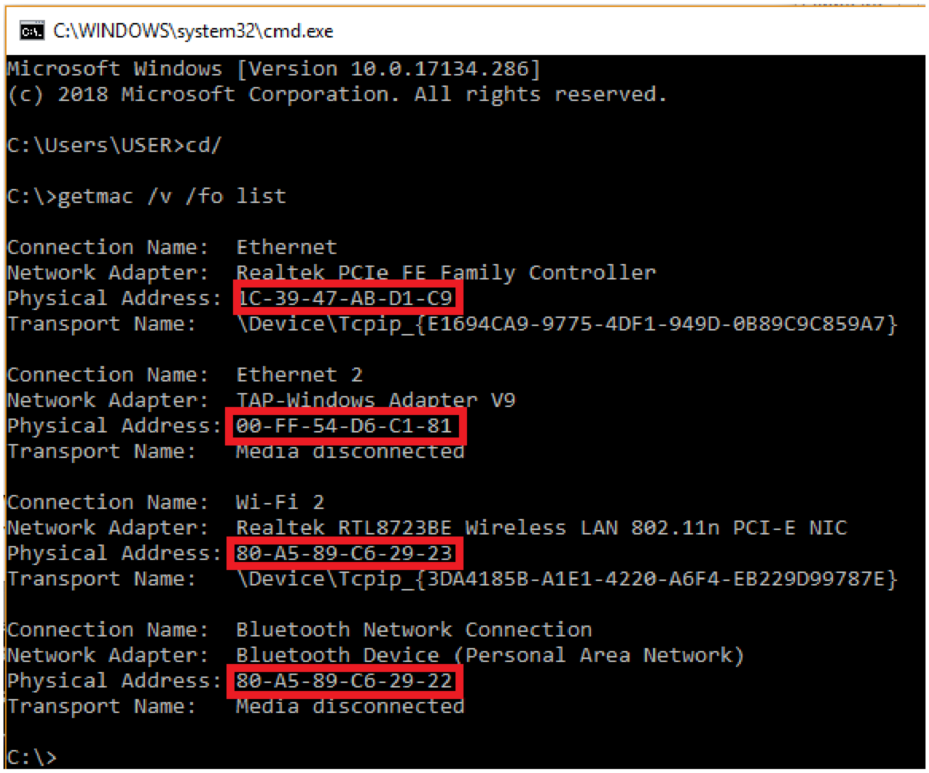
Robustness characteristic of an identifier refers to the ability of an identifier to function or continue functioning well in unexpected situations (Microsoft Corporation, 2018). Closely related to robustness characteristic of an identifier, are performance and reliability characteristics. Answers to the questions; does the MAC address remain invariant over time? Is a MAC address reliable? is it able to function as intended over a given period time under specified conditions? enable establish the robustness of a MAC address.

The answers to these questions are based on fact that the initial intention of encoding MAC address in the network hardware is to make it independent from the operating system supposedly rendering it permanent and hard to alter (Cardenas, 2003). However, due to some valid and invalid reasons, a copy of the MAC dress in the operating system can be altered as shown in figure 6 below. Good reasons for changing a device MAC address include testing out networks for configurations, security applications or new protocols, workarounds and nefarious means. For whichever reasons in changing a MAC address, it leads to the conclusion that a MAC address is not permanent, unreliable and therefore not robust.

The Uniqueness of a MAC Address

The fact that the MAC address is assigned to each network interface controller (NIC) card by the manufacturer makes it unique only to a particular interface. Furthermore, vendors are given a range of MAC addresses that can be assigned to their products by the IEE (Iwaya, 2015). This way, MAC address assignment is controlled such that no different adaptors can have the same address even if they are from different manufacturers. However, a device can have more than one network interface hence even though MAC address can actually uniquely identify a network interface, it doesn’t necessary uniquely identify a device.

One case in mind is an instance where a networked computer could contain multiple interfaces for Wi-Fi, Bluetooth and Ethernet adaptors. As illustrated in figure 4 below, a node can contain several MAC addresses. In this particular case, for instance, the node in question contains four interfaces with corresponding four MAC addresses. This was obtained by running the *getmac* command on the command prompt of the computer in question.



```
Microsoft Windows [Version 10.0.17134.286]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\USER>cd/

C:\>getmac /v /fo list

Connection Name:   Ethernet
Network Adapter:   Realtek PCIe FE Family Controller
Physical Address:  1C-39-47-AB-D1-C9
Transport Name:    \Device\Tcpip_{E1694CA9-9775-4DF1-949D-0B89C9C859A7}

Connection Name:   Ethernet 2
Network Adapter:   TAP-Windows Adapter V9
Physical Address:  00-FF-54-D6-C1-81
Transport Name:    Media disconnected

Connection Name:   Wi-Fi 2
Network Adapter:   Realtek RTL8723BE Wireless LAN 802.11n PCI-E NIC
Physical Address:  80-A5-89-C6-29-23
Transport Name:    \Device\Tcpip_{3DA4185B-A1E1-4220-A6F4-EB229D99787E}

Connection Name:   Bluetooth Network Connection
Network Adapter:   Bluetooth Device (Personal Area Network)
Physical Address:  80-A5-89-C6-29-22
Transport Name:    Media disconnected

C:\>
```

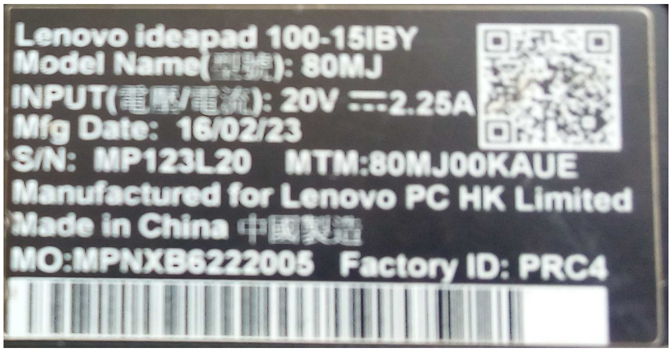
Figure 4: One computer with a number of MAC addresses

The possibility of a MAC address being spoofed is yet another case of a MAC address that makes it not to uniquely identify a device. If a device MAC address is altered for whatever reason, the likelihood of another device having the same address is imminent. As such, it cannot be assumed that a MAC address definitely identifies the device uniquely.

A Computer's Serial Number

- *Computer's Serial Number Location*

Just like in any other product, a computer has its serial number tagged as part of the serialization of the product. Perhaps the only extraordinary thing is that the number is placed strategically on the computer to simply frustrate snoopers from finding it. One would, therefore, more than often find it usually tagged beneath the computer or staged somewhere beside it. Figure 5 below shows an illustration of a laptop model details that include the serial number in a tag.

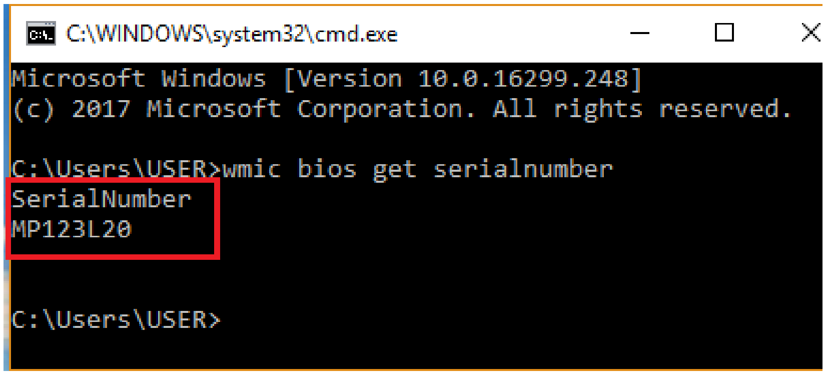


Lenovo ideapad 100-15IBY
Model Name(型號): 80MJ
INPUT(電壓/電流): 20V ⎓2.25A
Mfg Date: 16/02/23
S/N: MP123L20 MTM:80MJ00KAUE
Manufactured for Lenovo PC HK Limited
Made in China 中國製造
MO:MPNXB6222005 Factory ID: PRC4

Figure 5: Serial Number tag on a laptop model

Although tagging of computer serial number is the norm to serializing computers, it is a practice common to products including computers. This way, identifiers that use scanners such as bar code readers can be used to capture their identification details.

Alternatively, modern laptop models have their serial numbers coded into their basic input-output (BIOS) chips. This makes it possible for the identifier to internally be accessed and so, it can be processed for a given desired function. The first line of accessing a computers serial number is generally by running the command *wmic bios get serial number* at the systems command line interface. The serial number for the author's laptop, for instance, can be obtained as shown in figure 6 below;



```
Microsoft Windows [Version 10.0.16299.248]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\USER>wmic bios get serialnumber
SerialNumber
MP123L20


C:\Users\USER>
```

Figure 6: Serial number of a laptop obtained from system BIOS using the wmic command

The encoding of a serial number in a computer's hardware rather than just tagging it on a surface makes it possible to manipulate the serial number. This way, a model that can access the serial number internally and use it to identify the device is made possible.

- *Characteristics of a Computer's Serial Number*

The mere fact that a computer's serial number is hard-coded on the hardware without a copy in the system software alone renders it hard to be spoofed. It then implies that the serial number in normal circumstances cannot be altered and therefore unique, secure and reliable. It is only in some rare cases that the serial number can be altered. But this requires that a computer system has to turned off, any power lines disconnected, any static electricity discharged, computer case opened, disconnect the CMOS battery, wait for roughly 30 seconds (to completely ensure that the CMOS power is completely drained) then the process is done in reverse to revert back to original state (Derekyoung, 2017). This way, all original CMOS settings such as custom CMOS settings, BIOS password, time and date, as well as the motherboard serial number are lost. The system then generates a new system data that includes a serial number when booted.

Conclusions and Recommendations

The mere fact that MAC address can be spoofed and altered affects robustness and uniqueness attributes of a MAC address due to the fact that apart from it being hard-coded in the hardware, it has a copy of the MAC address in the system software. Uniqueness factor problem is more compounded due the possibility of multiple network interfaces attached to a computer results to multiple MAC address for the same computer thus compromising the uniqueness quality of a MAC address as an identifier. On the hand, a computer's serial number is hard-coded in the hardware only and therefore cannot be spoofed and altered making it unique, secure and reliable.

This study then recommends for a further research on how a serial number may be used for identifying a device in a wireless network. One way of realising this recommendation could be by conducting a study towards an algorithm, a model and a prototype that can access a computer's number remotely and use it as an identifier. Progressive systems can as well be developed that would consequently use the computer's serial number as an identifier for authentication, authorization and accounting (AAA) to the network resources.

REFERENCES

Canavan, J.E. (2012). *Fundamentals of Network Security,* Artech House, Boston, London.

Cardenas, D.E., (2018), MAC Spoofing: An Introduction, *GIAC Security Essentials Certification (GSEC),* https://www.giac.org/paper/gsec/3199/mac-spoofing-an-introduction/105315, Accessed on 07/07/2019

Comer, E.D., (2013), *Internetworking with TCP/IP Volume One,6th Edition*, Pearson, USA

Coulouris, G., Dollimore, J., Kindberg, T. and Blair, G., (2012), *Distributed Systems, Concepts, and Design*. Fourth Edition, Addison Wesley.

Danev, B., Zanetti, D. and Capkun, S., (2015), On physical-layer identification of wireless devices, *Computing Surveys* Volume: 45 Issue: 01.

Derekyoung, (2017), How to Change a BIOS Serial Number, *Itstillworks,* https://itstillworks.com/how-to-change-a-bios-serial-number-10394.html, Accessed on 20/06/2019

DHS, (2017), A Guide to Securing Networks for Wi-Fi (IEEE 802.11 Family), *Department of Homeland Security (DHS),* Version 1.0 First Release, https://www.us-cert.gov/sites/default/files/publications/A_Guide_to_Securing_Networks_for_Wi-Fi.pdf, Accessed on 20/07/2019

Dordal, P.L., (2018), An introduction to Computer Networks, *Loyola University Chicago,* http://intronetworks.cs.luc.edu/current/ComputerNetworks.pdf, Accessed on 03/08/2019

Garska, K., (2016), Higher Education's Unique Identity and Access Management Challenges, *Identity Automation*, https://blog.identityautomation.com/higher-educations-unique-identity-and-access-management-challenges, Accessed on 10/04/2019

IEEE-USA. (2009). Next Generation Internet: IPv4 Address Exhaustion, Mitigation Strategies and Implications for the U.S. *IEEE-USA White Paper,* https://www.ieeeusa.org, Accessed on 24/11/2015

Kurose, J.K. and Ross K.W., (2013), Computer *Networking: A Top_down Approach Featuring the Internet*, *6th Edition*, Addison Wesley

Lavassani, K.M., Movahedi, B. and Kumar, V., (2010), Identification in Electronic Networks: Characteristics of e-Identifiers, *Eight International Conference on Electronic Commerce (ICEC)*, 2006, Fredericton, New Brunswick, Canada

Lee, T., (2010), Securing your Meru Network, *Meru Networks White Paper*, Accessed on 19/09/2014

Leo, R.V., (2004), Predicting consumer intentions to use on-line shopping: the case for an augmented technology acceptance model**,** *Information & Management,* 41, 747-762

Microsoft Corporation, (2018). *Microsoft Computer Dictionary*, 6th Edition. Microsoft Press, USA

Paulsen, C. and Byers, R., (2019), Glossary of Key Information Security Terms, National Institute of Standard and Technology (NIST), NISTIR 7298 Revision 3

Raji, M.O., (2014), Design and Implementation of Wireless Network, *Research Gate*, https://www.researchgate.net/publication/269295509_DESIGN_AND_IMPLEMENTATION_OF_WIRELESS_NETWORK, Accessed on 13/04/2019

Richards, K., White, R., Nicoleson, N. and Pyle, R., (2011), A Beginner's Guide to Persistent, Identifiers, *Global Biodiversity Information Facility,* http://links.gbif.org/persistent_identifiers_guide_en_v1.pdf, Accessed on 1/7/2015

Shay, W. A., (2004), *Understanding Data Communication and Networks*, *Third Edition*, Thomson Learning

Singh, R. and Sharma, P.T., (2017), On the IEEE 802.11i security: a denial-of-service perspective, *Security Comm. Networks*; 8:1378–1407, DOI: 10.1002/sec.1079

Stallings, W., (2011), *Network Security Essentials, Applications and Standards*, *Fourth Edition*. Pearson Education, New Jersey, USA

Tanenbaum, A. S., (2011), *Computer Networks, 4th Edition*, Pearson Education, USA

Takahashi, D., Xiao, Y., Zhang, Y., Chatzimisios, P. and Chend, H., (2010), IEEE 802.11 user fingerprinting and its applications for intrusion detection, *Computers and Mathematics with Applications*, 60 (2010) 307_318

Wallace, K., (2018), Wireless LAN Security, *Kevin Wallace Training*, https://www.kwtrain.com/blog/wlan-security, Accessed on 13/04/19

Data breach challenges facing Kenyan Ecommerce

Elvine Saikwa[1], Moses Thiga [2]
[1]Kabarak University, P.O. Box Private Bag, Kabarak, 20157, Kenya
Tel: +254 719153128, Email: esaikwa@kabarak.ac.ke
[2]Kabarak University, P.O. Box Private Bag, Kabarak, 20157, Kenya
Tel: + 254 720780468, Email: mthiga@kabarak.ac.ke

Abstract

E-commerce in Kenya continues to grow in leaps and bounds mainly driven 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

1. Introduction

Ecommerce is sharing business information, maintaining business relationships and conducting business transactions by means of telecommunications networks (Zwass, 1998). The systems and communication networks used should be secure from potential attack vectors that can lead to data breaches. A data breach is a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion (Rouse, 2017). Any organization should, therefore, take appropriate measures to protect its computer systems from attacks. In order to protect itself from attacks, an organization would have to implement the information security principles in its systems. Although taking appropriate measures does not guarantee a hundred percent security, and this has made it possible for hackers to attack and compromise systems and services.

Across the world, organizations and governments have experienced data breaches, and some of them have been reported while others have not. In Kenya, some organizations have experienced data breaches but we still do not have a body of knowledge on the breaches This study therefore sought to develop a body of knowledge so that eCommerce practitioners who have not been affected by data breaches can learn from the experiences of their counterparts and this would enable them to be better prepared to protect their systems from probable attacks.

2. Objectives

The main objective of this study is to document the nature of data breaches that organizations have experienced in Kenya.

3. Problem statement

Data breaches have been occurring in Kenya and they have been reported. Unfortunately, we still do not have a detailed body of knowledge where eCommerce practitioners can refer to so that they can learn from their counterparts. This study, therefore, sought to come up with a knowledge base of data breaches that have occurred in Kenya.

4. Literature review

Many organizations across the world, whether private or government have experienced data breaches that have led to loss of information worth billions of dollars. Besides information, organizations have also lost huge amounts of money for litigation and price hive offs when they were sold to other companies (Yahoo and Uber have been the biggest victims). Yahoo is a search engine, subject directory, and web portal (Collins, 2018) while Uber is a technology platform that uses its Uber application to connect driver-partners and riders (Uber, 2018). Clients belonging to those organizations have also had their personal information like credit card numbers and social security numbers compromised. According to (Kan, 2017), Yahoo experienced the largest ever breach in the history of the world, considering that over 3 billion user accounts were compromised. In addition, banking institutions like JP Morgan Chase, Heartland Payment Systems, Equifax, government institutions like the US Office of Personnel Management and private businesses like Adult Friend Finder Network, Sony, eBay , Uber, RSA Security have not been spared either (Armerding, 2018).After these attacks, a company like Yahoo forced password reset for all its users and introduced three-factor authentication of username, password and a verification code that is sent to users who try to login into their accounts. This indicates that no organization in the world is immune from these cyber-attacks. It is therefore not surprising that Kenya has also been a victim of data breaches.

In the recent past, the Government of Kenya, decided to automate most of its services and this is evidenced by eCitizen, iTax, National Transport and Safety Authority portal, online registration of students sitting for national examinations, among others. “The more we adopt IT and the more data we put online, the more we will see cyber-attacks targeted at the government in Kenya. The problem is, we are not secure,” Mr William Makatiani managing director of IT security firm Serianu said (Mumo, 2016). It is because of Kenya not being secure from cyber-attacks that we decided to investigate data breaches that organizations have experienced. We will look at the nature of the breaches, the loses they incurred after the violations and recommend appropriate measures to take so that an organization can protect itself from such attacks.

5. Methodology

In conducting the study, a critical evaluation of literature on data breaches in Kenya was used. The data obtained provided a basis for the study. Additionally, for ethical reasons, names of people were anonymized. For example, if a person’s name was Bob, it was changed to Anonymous person one.

6. Results

i) Kenya Revenue Authority (KRA)

The authority is charged with the responsibility of collecting revenue on behalf of the Government of Kenya. In the year 2017, they made discoveries that may have led to data breaches. The first one was when detectives discovered a hidden laptop at KRAs network chambers that was connected to using port 11 (Kamau & Cherono, 2017). The fraudster, accused person one, who was a former employee at KRA, planted the laptop which enabled him to siphon money into his account in addition to allowing access of crucial data by cybercriminals which led to the taxman losing millions of shillings (Ombati, 2017).

The other discovery was when they lost Sh3,985,663,858 through an attack that was propagated by interfering with the tax collector computer systems (Kakah, 2017; Okoth, 2017) over a period of one year between March 2016 to March 2017. The prosecution lawyer, prosecutor one, informed the court that the printout data seized from the suspect would fill a room measuring 30 by 40 feet. They also said that the analysed data indicated that the accused, accused person two had been working with suspects outside the country. According to (BBC, 2017), he is part of an international network involving expatriates from the United States and other countries that steals money from several state bodies using high tech equipment and software.

In the year 2018, the taxman sued internet giant Google over a mystery hack (Wasuna, 2018) that prompted investigations. Investigator one of KRA's DCI unit said that unauthorised email address on more than one occasion performed tasks reserved for the taxman officers and it infringed on the information security of KRA (Fayo, 2018; Muthomi, 2017)(Kakah, 2018). The mystery hacker may have probably accessed millions of data on taxpayers and he/she could have used the information to solicit for money from taxpayers who had avoided paying taxes.

ii) Safaricom PLC

Safaricom is one of the leading mobile network operators in Kenya and this is evidenced by the net profit of around Sh 55 billion in the year ending March 2018 (Kubania, 2018). Nevertheless, they have not been spared by hackers. In 2017, a mobile subscriber for Safaricom lost Sh260,000 through unauthorized sim swap (Mumo, 2017), though the money was later refunded. This was discovered after Safaricom detected suspicious activity on its network and their risk management unit caught the intrusion before it could escalate (Mumo, 2017; Kangethe, 2017). When investigations were done, the hack was associated with a Safaricom staff account

Similarly, in 2018, between the dates of 24th and 30th April, they suffered another attack. This time, an attacker by the name Attacker one, unlawfully sent 24,258,730 million queries to the Safaricom App system using a laptop and mobile phone with a Safaricom line with the intent to defraud Safaricom (Bocha, 2018; Karanja, 2018). The requests were not normal based on the historical data of the accused.

iii) Banks

Regrettably, banks have also been victims of cyber-attacks. In the year 2008, Equity bank was subjected to a social engineering attack when one of its staff was told over the phone to transfer money from an account that belonged to a company called Dyer and Blair to a fraudster (Ochieng, 2017). The client lost Sh 26,250,250.

In the year 2013, the Central Bank of Kenya website was subjected to a denial of service attack by a group called the Gaza Hacker Team (Nguta, 2013). Although, the website was restored at 11 pm, critical services like the exchange rate was severely affected during the attack.

In January 2015, the infamous hacker, accused person two and an accomplice accused person three were arraigned before a court of law and they were charged with hacking into NIC Bank database in December, 2014 (Okuttah, 2015). They later demanded to be paid 200-Bitcoins which was valued at KSh 6.2 million at that time. Failure to that would lead to them exposing confidential information (Agoya, 2015) which could have led to extortion of money from the clients whose information had been disclosed.

In January, 2018, National Bank of Kenya confirmed that they had lost Sh 29 million through a data breach. Initially, there had been reports in the social media they had lost between Sh 150 million and 340 million. National bank through its twitter handle said that unauthorized people gained access to several accounts and siphoned off money before the bank detected and froze the accounts (Alushula, 2018). The bank also assured customers that their accounts had not been affected (Macharia, 2018).

iv) Ministry of Foreign Affairs

The government of Kenya confirmed that the Ministry of Foreign Affairs had been hacked and as a result, the hackers were able to get access to some data which was classified as open (Mutambo, 2016). The Anonymous claimed responsibility for the hack and said that they acquired one terabyte of data and they would be releasing it in the dark web in phases (Waqas, 2016). The data dump contained confidential and non-confidential pdf and docx files from the ministry server including email conversations, letters of conversation related to weapon clearance in Namibia ,details about a business collaboration between Kenya and Oman, documents discussing state officials visit to Kenya, security related communication, international trade agreements and letters discussing the security situation in (South)Sudan where government forces are fighting the Sudan People's Liberation Army (SPLA). Surprisingly, it contained an alert email from an ICT administrator warning them of a phishing campaign that could compromise their staff ID and he even shared a screenshot of an email sent by the hackers (Waqas, 2016).

v) Ministry of Defence

Anonymous claimed responsibility of taking control of the ministry of defence twitter account and a senior ranked military official. This was confirmed through their twitter handle Anon_0x03. Two hours after the account had been restored, they regained control of the accounts (Mumo, 2016; Ombati, 2016; Munyori, 2016; Muraya, 2016). The Kenya Defence Forces in an interview with the Nation said that no confidential information been obtained (Mumo, 2016).

vi) National Oil

The Operation Africa banner by the anonymous that is against corruption, child labour and child abuse in March 2016 through the World Hacker Team were at it again. According to (Uzair, 2016), they were able to hijack the database of National Oil Corporation in Kenya and posted data and screen shoot online to prove legitimacy of their claim. The data contained email, usernames, email addresses and along with the user's rank. It also contained a survey by the company (Cimpanu, 2016)

vii) Communications Authority of Kenya (CA)

CA is the state agency that regulates internet resources for public and private entities. It is tasked with protecting all the governments websites from malicious attack (Sunday, 2017). In spite of this, hackers identified as AnonPlus defaced the organizations website together with the National Environment Management Authority (NEMA) website for several hours.

viii) Kenya Police Website

In January 2011, a renowned journalist called Journalist A posted on his twitter account posted that the Kenya police website had been hacked. The website normally contains information about and provided by Kenya's primary national law enforcement body. According to (Constantin, 2011), there was no information about the hacker's motives for targeting the website. The attack only affected the home page but the rest of the links indexed by Google remained accessible.

ix) Office of the President

According to (Waqas, 2015),on 11th May,2015, the official website for president of Kenya was hacked and the home page was replaced with the hacker's information. Indonesian hackers known as Gantengers Crew took responsibility for the hack. During an interview with HackRead, the hackers said that their reason for attacking the website was to show that they were powerful.

x) Office of the Attorney General

In the year 2013, the website of attorney general of Kenya was defaced by the hacker with the handle Dz Mafia of Algeria (Waqas, 2013). They left greetings for their team and curse messages for USA. However, they did not state their motivation for the attack (Waqas, 2013). The website was later restored.

xi) Google Kenya

One would really wonder why a person would even think of hacking google. Nevertheless, the hacker going by the name Tiger-M@te hacked Google.co.ke but he did not give any reason for his attack (Waqas, 2013). The website was later restored.

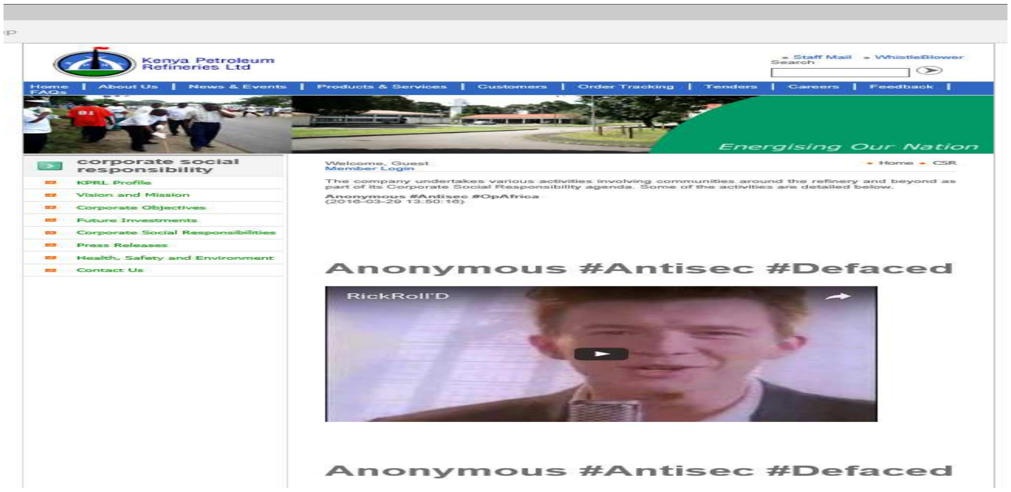
xii) Kenya Petroleum Refineries Limited

The organization was originally set up by Shell and the British Petroleum Company BP to serve the East African region in the supply of a wide variety of oil products. On 29th March, 2016, one of their website pages was defaced by Anonymous under their Operation Africa campaign (Cimpanu, 2016).The hackers did not breach the database or steal anything from the backend but they left a music video.Probably this was a stunt to show their capability.

7. Discussion

In the introduction, we mentioned that some of the data breaches are normally reported. This section discusses the identified breaches.

Among the breaches was defacement of websites. It consists of hacking into a web server and replacing a web page with a new page bearing some sort of message (Samuel, 2004). Some of the indicators of a defaced site is through notification by the hacker on the web pages or a peer. Defaced websites can lead to erosion of consumers' confidence, downtime, disruption of business activities, potential data breach and loss of time and money when restoring the website. This is the most prevalent attack in Kenya. The following images shows how the attacks were manifested.



Kenya Petroleum Refineries Ltd

» Staff Mail » WhistleBlower
Search

Home | About Us | News & Events | Products & Services | Customers | Order Tracking | Tenders | Careers | Feedback | FAQs
Energising Our Nation
corporate social responsibility
KPRL Profile
Vision and Mission
Corporate Objectives
Future Investments
Corporate Social Responsibilities
Press Releases
Health, Safety and Environment
Contact Us
• Home • CSR
RickRoll'D

Welcome, Guest
Member Login

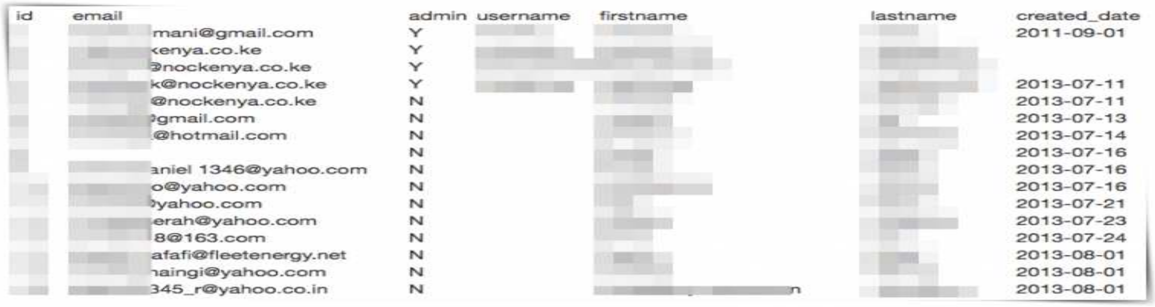
The company undertakes various activities involving communities around the refinery and beyond as part of its Corporate Social Responsibility agenda. Some of the activities are detailed below.

Anonymous #Antisec #OpAfrica
(2016-03-29 13:50:16)

Anonymous #Antisec #Defaced

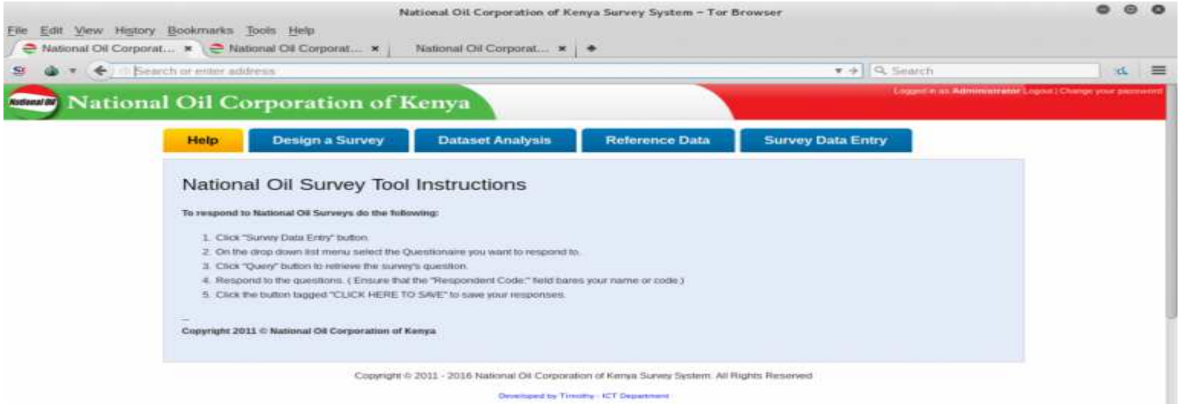
Anonymous #Antisec #Defaced

Figure 2:Kenya petroleum refineries limited defaced webpage



id	email	admin	username	firstname	lastname	created_date
[redacted]	[redacted]mani@gmail.com	Y	[redacted]	[redacted]	[redacted]	2011-09-01
[redacted]	[redacted]kenya.co.ke	Y	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]@nockenya.co.ke	Y	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]k@nockenya.co.ke	Y	[redacted]	[redacted]	[redacted]	2013-07-11
[redacted]	[redacted]@nockenya.co.ke	N		[redacted]	[redacted]	2013-07-11
[redacted]	[redacted]@gmail.com	N		[redacted]	[redacted]	2013-07-13
[redacted]	[redacted]@hotmail.com	N		[redacted]	[redacted]	2013-07-14
[redacted]		N		[redacted]	[redacted]	2013-07-16
[redacted]	[redacted]aniel 1346@yahoo.com	N		[redacted]	[redacted]	2013-07-16
[redacted]	[redacted]o@yahoo.com	N		[redacted]	[redacted]	2013-07-16
[redacted]	[redacted]@yahoo.com	N		[redacted]	[redacted]	2013-07-21
[redacted]	[redacted]erah@yahoo.com	N		[redacted]	[redacted]	2013-07-23
[redacted]	[redacted]8@163.com	N		[redacted]	[redacted]	2013-07-24
[redacted]	[redacted]afafi@fleetenergy.net	N		[redacted]	[redacted]	2013-08-01
[redacted]	[redacted]aingi@yahoo.com	N		[redacted]	[redacted]	2013-08-01
[redacted]	[redacted]345_r@yahoo.co.in	N		[redacted]n	[redacted]	2013-08-01

Figure 3: National oil Kenya hacked website



National Oil Corporation of Kenya Survey System – Tor Browser
File Edit View History Bookmarks Tools Help
National Oil Corporat...
National Oil Corporat...
National Oil Corporat...
Search or enter address
Search
National Oil
National Oil Corporation of Kenya
Logged in as Administrator Logout | Change your password
Help
Design a Survey
Dataset Analysis
Reference Data
Survey Data Entry

National Oil Survey Tool Instructions

To respond to National Oil Surveys do the following:

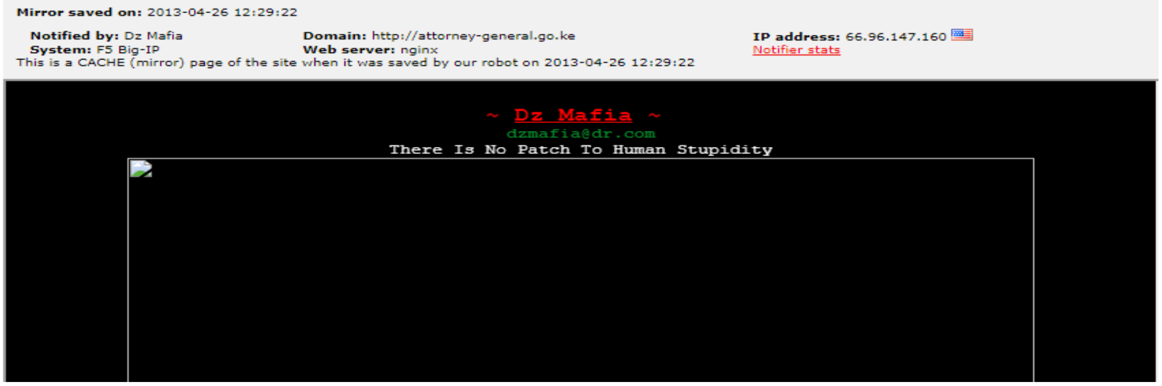
1. Click "Survey Data Entry" button.
2. On the drop down list menu select the Questionaire you want to respond to.
3. Click "Query" button to retrieve the survey's question.
4. Respond to the questions. (Ensure that the "Respondent Code:" field bares your name or code)
5. Click the button tagged "CLICK HERE TO SAVE" to save your responses.

Copyright 2011 © National Oil Corporation of Kenya

Copyright © 2011 - 2016 National Oil Corporation of Kenya Survey System. All Rights Reserved

Developed by Timothy - ICT Department

Figure 4:National oil survey that was exposed

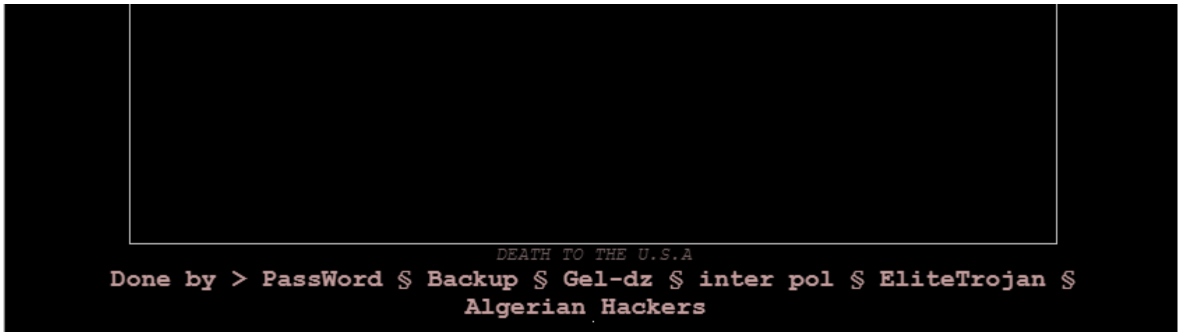


Mirror saved on: 2013-04-26 12:29:22

Notified by: Dz Mafia **Domain:** http://attorney-general.go.ke **IP address:** 66.96.147.160
System: F5 Big-IP **Web server:** nginx Notifier stats
This is a CACHE (mirror) page of the site when it was saved by our robot on 2013-04-26 12:29:22

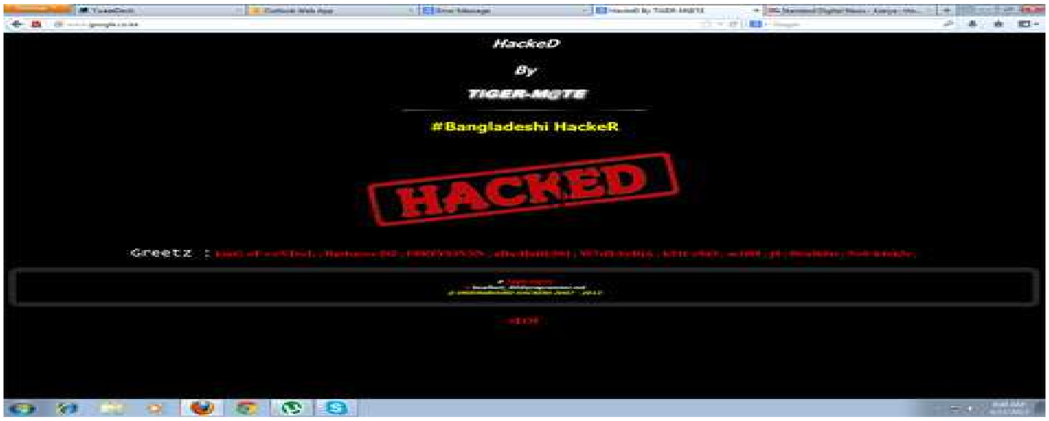
~ Dz Mafia ~
dzmafia@dr.com
There Is No Patch To Human Stupidity

Figure 5: Ag website that was defaced



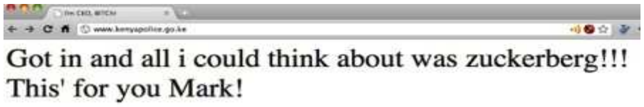
DEATH TO THE U.S.A
Done by > PassWord § Backup § Gel-dz § inter pol § EliteTrojan § Algerian Hackers

Figure 6: Ag website that was defaced



HackeD
By
TIGER-M@TE
#Bangladeshi HackeR
HACKED
Greetz : [illegible]

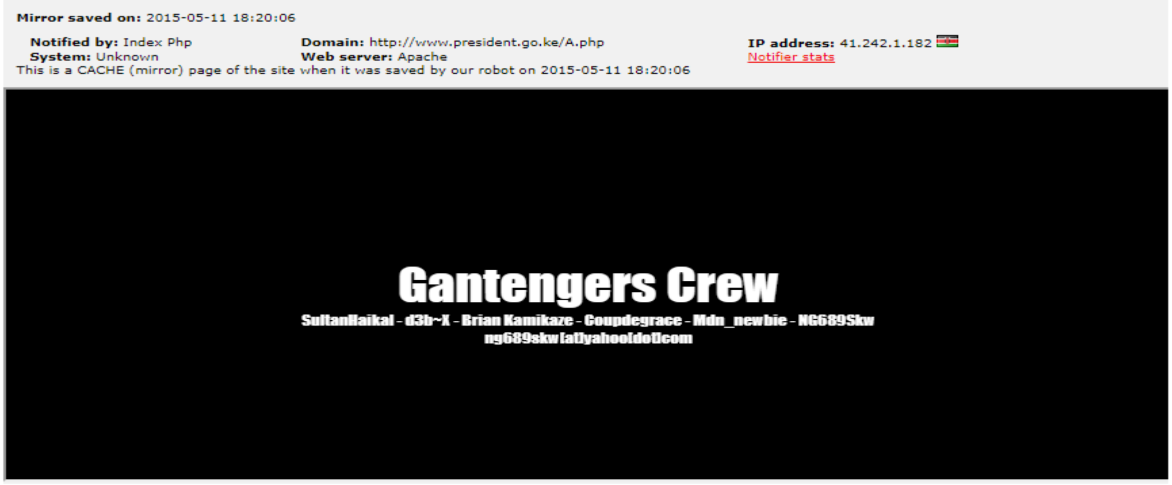
Figure 7: Google website that was defaced



www.kenyapolice.go.ke

Got in and all i could think about was zuckerberg!!!
This' for you Mark!

Figure 8:Kenya police web page that was defaced



Mirror saved on: 2015-05-11 18:20:06

Notified by: Index Php
System: Unknown
Domain: http://www.president.go.ke/A.php
Web server: Apache
IP address: 41.242.1.182
Notifier stats
This is a CACHE (mirror) page of the site when it was saved by our robot on 2015-05-11 18:20:06

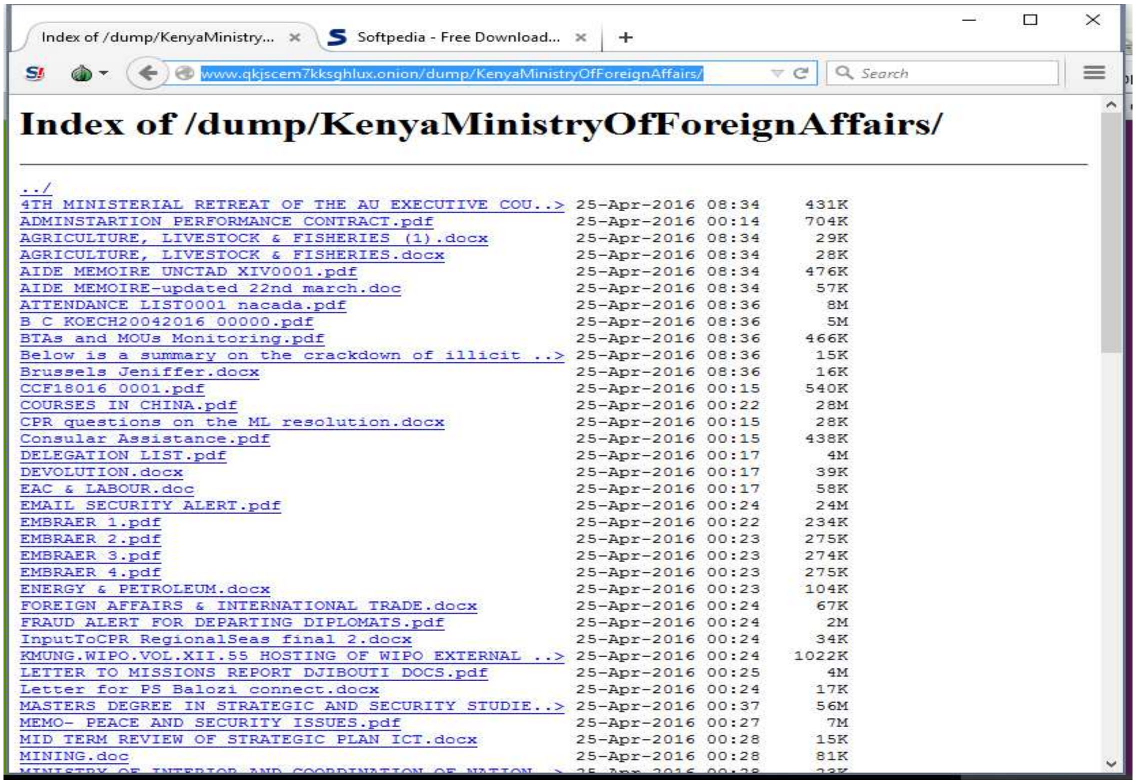
Gantengers Crew
SultanHaikal - d3b~X - Brian Kamikaze - Coupdegrace - Mdn_newbie - NG689Skw
ng689skw[at]yahoo[dot]com

Figure 9: President's web page that was defaced

Insider threats was also another vector of data breaches. It normally happens when an individual working for an organization aide an intruder by allowing him to have unauthorized access to their internal systems. The access is made possible by sharing confidential information like usernames and passwords, installing backdoors in organizational computer systems or allowing remote access of the computer systems. This threat can lead to loss of revenue and personal information of people in an affected organization. Kenya Revenue Authority was a victim of this. They discovered a computer hidden in their network chamber. The computer may have been used to alter tax collection history for individuals, change log books of vehicles, falsify tax payment records, creation and deletion of user accounts, deletion of system logs and transfer of money from KRAs accounts.

Unauthorized sim swap is also another threat. According to Communications Authority of Kenya, it happens when a fraudster in collaboration with a staff at Safaricom or by himself calls you pretending to be an employee of a mobile service provider and asks for your personal identifiable information (PIN). After getting the PIN, he conducts a sim swap and the legitimate sim is switched off and rendered unusable to the owner. The fraudster gets access to all sim services like mobile money transfer, mobile and internet banking, SMS, voice calls and any other data service. Lastly, the fraudster transfers money in the phone or bank accounts. Unauthorized sim swap can mainly lead to loss of money and identity theft.

Phishing was also among the attacks. Phishing happens when an attacker possesses as a genuine entity and asks for confidential information like usernames and password. The confidential information may be obtained when legitimate users are requested to change their passwords or update their records. This happened to the staff working at the ministry of foreign affairs. Such attacks normally lead to compromises of user accounts and exposure of information. The following image shows the information that was exposed after the attack.


Index of /dump/KenyaMinistry...
Softpedia - Free Download...
www.qkjscem7kksghlux.onion/dump/KenyaMinistryOfForeignAffairs/
Search

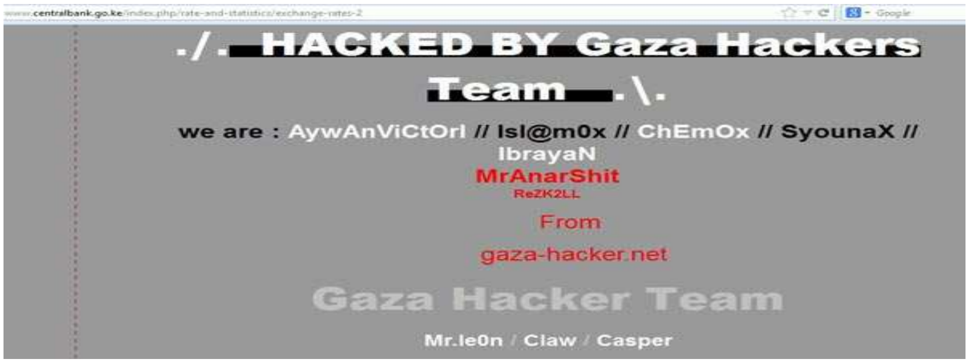
```
Index of /dump/KenyaMinistryOfForeignAffairs/

../
4TH MINISTERIAL RETREAT OF THE AU EXECUTIVE COU..> 25-Apr-2016 08:34    431K
ADMINSTARTION PERFORMANCE CONTRACT.pdf             25-Apr-2016 00:14    704K
AGRICULTURE, LIVESTOCK & FISHERIES (1).docx        25-Apr-2016 08:34     29K
AGRICULTURE, LIVESTOCK & FISHERIES.docx            25-Apr-2016 08:34     28K
AIDE MEMOIRE UNCTAD XIV0001.pdf                    25-Apr-2016 08:34    476K
AIDE MEMOIRE-updated 22nd march.doc                25-Apr-2016 08:34     57K
ATTENDANCE LIST0001 nacada.pdf                     25-Apr-2016 08:36      8M
B C KOECH20042016 00000.pdf                        25-Apr-2016 08:36      5M
BTAs and MOUs Monitoring.pdf                       25-Apr-2016 08:36    466K
Below is a summary on the crackdown of illicit ..> 25-Apr-2016 08:36     15K
Brussels Jeniffer.docx                             25-Apr-2016 08:36     16K
CCF18016 0001.pdf                                  25-Apr-2016 00:15    540K
COURSES IN CHINA.pdf                               25-Apr-2016 00:22     28M
CPR questions on the ML resolution.docx            25-Apr-2016 00:15     28K
Consular Assistance.pdf                            25-Apr-2016 00:15    438K
DELEGATION LIST.pdf                                25-Apr-2016 00:17      4M
DEVOLUTION.docx                                    25-Apr-2016 00:17     39K
EAC & LABOUR.doc                                   25-Apr-2016 00:17     58K
EMAIL SECURITY ALERT.pdf                           25-Apr-2016 00:24     24M
EMBRAER 1.pdf                                      25-Apr-2016 00:22    234K
EMBRAER 2.pdf                                      25-Apr-2016 00:23    275K
EMBRAER 3.pdf                                      25-Apr-2016 00:23    274K
EMBRAER 4.pdf                                      25-Apr-2016 00:23    275K
ENERGY & PETROLEUM.docx                            25-Apr-2016 00:23    104K
FOREIGN AFFAIRS & INTERNATIONAL TRADE.docx         25-Apr-2016 00:24     67K
FRAUD ALERT FOR DEPARTING DIPLOMATS.pdf            25-Apr-2016 00:24      2M
InputToCPR RegionalSeas final 2.docx               25-Apr-2016 00:24     34K
KMUNG.WIPO.VOL.XII.55 HOSTING OF WIPO EXTERNAL ..> 25-Apr-2016 00:24   1022K
LETTER TO MISSIONS REPORT DJIBOUTI DOCS.pdf        25-Apr-2016 00:25      4M
Letter for PS Balozi connect.docx                  25-Apr-2016 00:24     17K
MASTERS DEGREE IN STRATEGIC AND SECURITY STUDIE..> 25-Apr-2016 00:37     56M
MEMO- PEACE AND SECURITY ISSUES.pdf                25-Apr-2016 00:27      7M
MID TERM REVIEW OF STRATEGIC PLAN ICT.docx         25-Apr-2016 00:28     15K
MINING.doc                                         25-Apr-2016 00:28     81K
```

Figure 10: Exposed information from the ministry of foreign affairs

Information systems were also infiltrated. System infiltration happens when unauthorized users gain unauthorized access to an organizations internal system. This access can lead to loss of revenue and confidential information of users and clients of a given organization. National bank of Kenya and Safaricom detected the intrusion using their intrusion detection systems and stopped the attacks. NIC bank received threatening emails of black mail from hackers. KRA found logs of an unauthorised email account that had performed transactions on its systems.

Denial of service is also another attack. It happens when a web server is flooded with requests thereby constricting the bandwidth and making it difficult for legitimate requests to get response. Central bank of Kenya was a subject of this attack which caused a huge disruption of business activities and it resulted in loss of money because clients could not get access to the offered services. Normally, denial of service attack results from poor programming practises or programmer error. The banks main url address http://www.centralbank.go.ke gave a not found response after the attack. The following image shows the response from their website when the attack happened.



www.centralbank.go.ke/index.php/rate-and-statistics/exchange-rates-2

./. HACKED BY Gaza Hackers Team .\.

we are : AywAnViCtOrl // Isl@m0x // ChEmOx // SyounaX // IbrayaN

MrAnarShit

ReZK2LL

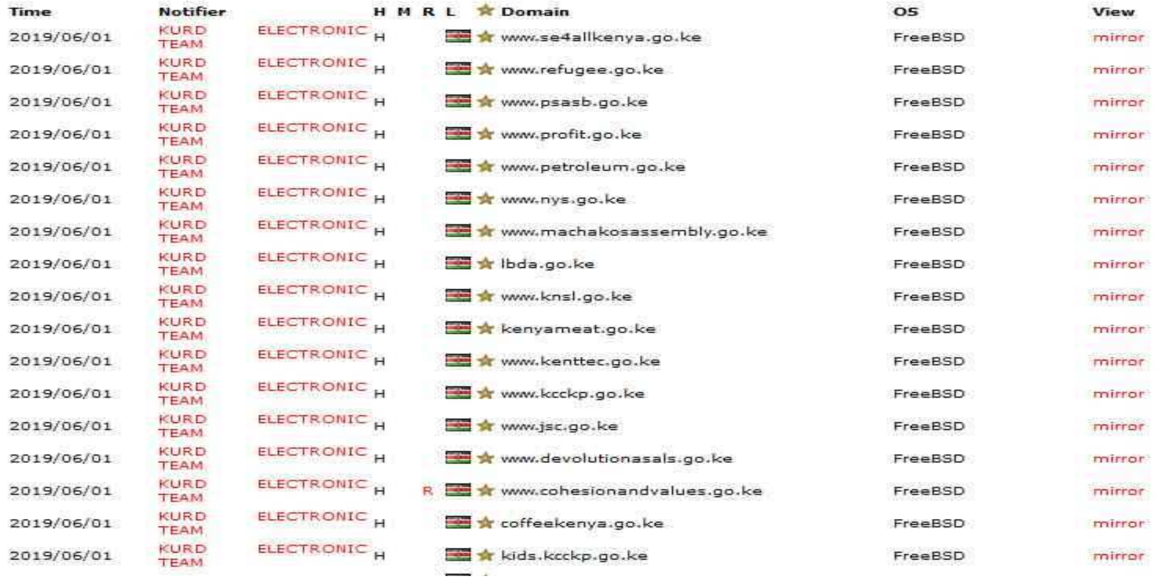
From

gaza-hacker.net

Gaza Hacker Team

Mr.le0n / Claw / Casper

Figure 11: CBK website after the attack



Time	Notifier		H	M	R	L	★ Domain	OS	View
2019/06/01	KURD TEAM	ELECTRONIC	H				★ www.se4allkenya.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H				★ www.refugee.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H				★ www.psasb.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H				★ www.profit.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H				★ www.petroleum.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H				★ www.nys.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H				★ www.machakosassembly.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H				★ lbda.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H				★ www.knsl.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H				★ kenyameat.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H				★ www.kenttec.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H				★ www.kcckp.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H				★ www.jsc.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H				★ www.devolutionasals.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H		R		★ www.cohesionandvalues.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H				★ coffeekenya.go.ke	FreeBSD	mirror
2019/06/01	KURD TEAM	ELECTRONIC	H				★ kids.kcckp.go.ke	FreeBSD	mirror

Figure 12: List of hacked websites in Kenya, 2019. (Source, Zone-H)

Password guessing was also used. It happens when an attacker tries to get access to an account by either guessing or running automated scripts to find any possible combination of password and username. Ministry of Defence in Kenya and a senior ranked military officer in Kenya twitter accounts were subjected to this attack and their account was taken over by hackers. They posted derogative tweets about the military. One of the tweets read "So much poverty in Africa while you are wasting money in guns." This raises the question of whether the real hackers were the militia that the government of Kenya was fighting in Somalia. In addition, during the breach, the number of followers of the military's twitter account increased. Did this mean that the followers subscribed to the ideas of the attackers after getting wind of the breach that had occurred.

Observations

We observed that, after the breaches have occurred, most of the affected organizations do not publicize the data breaches. Additionally, some of the organizations take litigation measures against those found/suspected of trying to get unauthorised access to their information systems. Furthermore, some of the organizations assure their clients that their personal information had not been interfered with. Majority of the organizations affected belong to the government of Kenya.

Lastly, some of the organizations opted to keep quiet about the breaches that they had experienced.

Recommendations

We would like to recommend that, organizations should conduct penetration testing on their systems so that potential vulnerabilities can be identified and patched in order avoid data breaches.

We would also recommend that the government of Kenya should implement proper security policies which would help its institutions to mitigate against data breaches

Conclusion

Data breaches will continue to occur to organizations if they do not take their information security with great concern. Given that most of the affected organizations belong to the government, it is imperative that the government of Kenya takes appropriate measures to secure its systems from any potential attacks.

This study has been able identify organizations that have experienced data breaches and documented how they happened. ECommerce practitioners should take lessons from the discussed data breaches so that they can be able to equip themselves with the necessary knowledge, tools and techniques to deal with data breaches before and after they happen.

References

Agoya, V. (2015, 4 10). Meet the man police link to Safaricom, NIC Bank frauds. *Business Daily*. Retrieved from https://www.businessdailyafrica.com/corporate/The-man-police-have-linked-to-Safaricom-NIC-Bank-fraud/539550-2681054-46or3ez/index.html

Alushula, P. (2018, 1 20). National Bank reassures customers after Sh29m fraud. *Standard Digital*. Retrieved from https://www.standardmedia.co.ke/business/article/2001266542/national-bank-reassures-customers-after-sh29m-fraud

Armerding, T. (2018, 1 26). The 17 biggest data breaches of the 21st century. *CSO*. Retrieved from https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

BBC. (2017, 3 22). Kenya Revenue Authority 'lost $39m to hacker'. *BBC News*. Retrieved from https://www.bbc.com/news/world-africa-39351172

Bocha, G. (2018, 5 15). Man in court for trying to hack Safaricom app. *Business Daily*. Retrieved from https://www.businessdailyafrica.com/corporate/companies/Man-charged-for-trying-to-hack-Safaricom-app/4003102-4563176-132uduw/index.html

Cimpanu, C. (2016, 5 30). Anonymous Leaks Employee Details from National Oil of Kenya. *Softpedia News*. Retrieved from https://news.softpedia.com/news/anonymous-leaks-employee-details-from-national-oil-corporation-of-kenya-504671.shtml

Cimpanu, C. (2016, 3 29). Anonymous Rickrolls Kenyan Petrol Refinery as Part of Its Anti-Corporations Op. *Softpedia News*. Retrieved from https://news.softpedia.com/news/anonymous-rickrolls-kenyan-petrol-refinery-as-part-of-its-anti-corporations-op-502325.shtml

Collins, J. (2018, 5 26). What is Yahoo? Yahoo 101. *Lifewire*. Retrieved from https://www.lifewire.com/what-is-yahoo-3483209

Constantin, L. (2011, 1 4). Hacker Defaces Kenyan Police Website in Mark Zuckerberg's Honor. *Softpedia News*. Retrieved from https://news.softpedia.com/news/Hacker-Defaces-Kenyan-Police-Website-in-Mark-Zuckerberg-s-Honor-176141.shtml

Fayo, G. (2018, 6 19). KRA duel with Google in Gmail account hack probe. *Business Daily*. Retrieved from https://www.businessdailyafrica.com/corporate/companies/KRA-duel-with-Google-in-Gmail-account-hack-probe/4003102-4621152-eb47ls/index.html

Kakah, M. (2017, 3 28). Court detains computer geek in Sh4bn KRA case for 40 days. *Daily Nation*. Retrieved from https://www.nation.co.ke/news/Alex-Mutungi-Mutuku-KRA-cybercrime-kenya/1056-3867562-10bq6hvz/index.html

Kakah, M. (2018, 1 31). Google wins order against email search in battle with KRA. *Business Daily*. Retrieved from https://www.businessdailyafrica.com/corporate/companies/Google-wins-order-against-email-search-in-battle-with-KRA/4003102-4286500-egyx30z/index.html

Kamau, J., & Cherono, S. (2017, 3 9). Police bust ring of hackers in multi-million shilling KRA, bank thefts. *Daily Nation*. Retrieved from https://www.nation.co.ke/news/Police-bust-ring-of-hackers/1056-3842558-11h7q5xz/index.html

Kan, M. (2017, 3 2). Yahoo execs botched its response to 2014 breach, investigation finds. *CSO*. Retrieved from https://www.csoonline.com/article/3176181/security/yahoo-execs-botched-its-response-to-2014-breach-investigation-finds.html

Kangethe, K. (2017, 4 6). Safaricom foils elaborate attempt to hack company systems. *CapitalBusiness*. Retrieved from https://www.capitalfm.co.ke/BUSINESS/2017/04/SAFARICOM-FOILS-ELABORATE-ATTEMPT-HACK-COMPANY-SYSTEMS/

Karanja, F. (2018, 5 16). Man charged with unlawful access to Safaricom systems. *Standard Digital*. Retrieved from https://www.standardmedia.co.ke/article/2001280627/man-charged-with-unlawful-access-to-safaricom-systems

Kubania, J. (2018, 5 9). Safaricom full-year profit hits Sh55.3bn, Bob makes comeback. *Business Daily*. Retrieved from https://www.businessdailyafrica.com/corporate/companies/Safaricom-full-year-profit-Sh55-3bn-Bob-makes-comeback/4003102-4552246-14m8rsoz/index.html

Macharia, K. (2018, 1 19). Fraudsters steal Sh29Mn from National Bank of Kenya. Retrieved from https://www.capitalfm.co.ke/business/2018/01/fraudsters-steal-sh29mn-national-bank-kenya/

Mumo, M. (2016, 7 22). Cyber security in the spotlight as hackers infiltrate defence account. *Daily Nation*. Retrieved from https://www.nation.co.ke/business/Cyber-Security-Hacking-KDF-Emmanuel-Chirchir/996-2393516-10j3pduz/index.html

Mumo, M. (2017, 4 6). Two men charged with hacking into Safaricom system. *Business Daily*. Retrieved from https://www.businessdailyafrica.com/corporate/Two-men-charged-with-hacking-Safaricom-system/539550-3880240-140vv0az/index.html

Munyori, W. (2016, 7 21). Group hacks defence forces Twitter account. *Daily Nation*. Retrieved from https://www.nation.co.ke/news/Group-hacks-defence-forces-Twitter-account/1056-2392622-format-xhtml-r58cnaz/index.html

Muraya, J. (2016, 7 22). Kenya military Twitter accounts ‘captured’ again. *CapitalNews*. Retrieved from https://www.capitalfm.co.ke/news/2014/07/kenya-military-twitter-accounts-captured-again/

Mutambo, A. (2016, 4 28). Govt admits hackers stole data from Foreign Affairs ministry. *Daily Nation*. Retrieved from https://www.nation.co.ke/news/Govt-admits-hackers-stole-data-at-Foreign-Affairs-ministry/1056-3180962-90t2wyz/index.html

Muthomi, K. (2017, 2 1). Google Kenya battle State in digital privacy suit. *Standard Digital*. Retrieved from https://www.standardmedia.co.ke/business/article/2001268029/google-battle-state-in-digital-privacy-suit

Nguta, J. (2013, 7 22). Central Bank of Kenya website hacked. *Standard Digital*. Retrieved from https://www.standardmedia.co.ke/business/article/2000089020/central-bank-website-hacked

Ochieng, A. (2017, 12 23). Banks vulnerable to theft by staff, not just tunnel diggers. *Daily Nation*. Retrieved from https://www.nation.co.ke/news/Banks-vulnerable-to-thefts-by-staff/1056-4239424-13tjigjz/index.html

Okoth, B. (2017, 3 22). This man Mutuku: Inside opulent lifestyle of man, 28, charged with loss of KRA's Ksh4 billion. *Citizen Digital*. Retrieved from https://citizentv.co.ke/news/this-man-mutuku-inside-opulent-lifestyle-of-man-28-charged-with-loss-of-kras-ksh4-billion-161518/

Okuttah, M. (2015, 4 10). Meet the man police link to Safaricom, NIC Bank frauds. *Business Daily*. Retrieved from https://www.businessdailyafrica.com/corporate/The-man-police-have-linked-to-Safaricom-NIC-Bank-fraud/539550-2681054-46or3ez/index.html

Ombati, C. (2016, 7 23). KDF Twitter account hacked yet again. *Standard Digital*. Retrieved from https://www.standardmedia.co.ke/article/2000129139/kdf-twitter-account-hacked-yet-again

Ombati, C. (2017, 3 11). How Kenyan banks lost Sh30 billion in two years to tech savvy criminals. *The Standard*. Retrieved from https://www.standardmedia.co.ke/business/article/2001232241/how-kenyan-banks-lost-sh30-billion-in-two-years-to-tech-savvy-criminals

Rouse, M. (2017, 12). Data breach. *TechTarget*. Retrieved from https://searchsecurity.techtarget.com/definition/data-breach

Samuel, A. W. (2004). *Hacktivism and the Future of Political Participation (Doctoral dissertation).* Cambridge, Massachusetts: Harvard University .

Sunday, F. (2017, 1 7). Shame as Kenya's Internet regulator website hacked. *Standard Digital*. Retrieved from https://www.standardmedia.co.ke/business/article/2000228978/shame-as-kenya-s-internet-regulator-website-hacked

Uber. (2018, 1 1). What is Uber? *Uber Help*. Retrieved from https://help.uber.com/h/eac2e43e-af42-4521-a042-2982c18664af

Uzair, A. (2016, 6 1). Anonymous Linked Team Hacks Kenyan Oil Firm Against Police Brutality. *HackRead*. Retrieved from https://www.hackread.com/anonymous-hacks-kenyan-oil-firm-against-police-brutality/

Waqas, A. (2013, 4 30). Attorney General of Kenya Website Hacked by Dz Mafia Algerian Hacker. *HackRead*. Retrieved from https://www.hackread.com/attorney-general-of-kenya-website-hacked-by-dz-mafia/

Waqas, A. (2013, 4 15). Google Kenya Hacked and Defaced by Tiger-M@te Hacker. *HackRead*. Retrieved from https://www.hackread.com/google-kenya-hacked-and-defaced-by-tiger-mte-hacker/

Waqas, A. (2015, 5 13). President of Kenya Website Hacked by Indonesian hackers. *HackRead*. Retrieved from https://www.hackread.com/kenya-president-website-hacked-indonesia-crew/

Waqas, A. (2016, 4 28). Anonymous Leaks 1TB of Data from Kenya' Ministry of Foreign Affairs. *HackRead*. Retrieved from https://www.hackread.com/anonymous-hacks-kenya-ministry-foreign-affairs/

Waqas, A. (2016, 4 28). Anonymous Leaks 1TB of Data from Kenya' Ministry of Foreign Affairs. *HackRead*. Retrieved from https://www.hackread.com/anonymous-hacks-kenya-ministry-foreign-affairs/

Wasuna, B. (2018, 2 1). Taxman, Google Kenya in court battle over mystery KRA hack. *The Star*. Retrieved from https://www.the-star.co.ke/news/2018/02/01/taxman-google-kenya-in-court-battle-over-mystery-kra-hack_c1706694

Zwass, V. (1998). *Structure and Macro-level Impacts of Electronic Commerce: From Technological Infrastructure to Electronic Marketplaces.* McGraw-Hil

Artificial Neural Network Power Demand Forecasting Model for Energy Management a Case Study of Kabarak University.

Francis Komen[1], Moses Thiga[2], Peter Rugiri[3]
[1]Kabarak University P.O. Box Private Bag, Kabarak, 20157, Kenya
Tel:+254 721 327 274, Email: fkomen@kabarak.ac.ke
Tel:+254 720 780 468, Email: mthiga@kabarak.ac.ke
Tel:+254 722 691 163, Email: PRugiri@kabarak.ac.ke

Abstract

World governments face challenges of increasing rate of power consumption and energy insecurity. There is need for countries to increase supply sustainability by reduction of demand through energy efficient investments. 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 biasness 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 is 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, Energy efficiency, Artificial Neural Network, Demand Response.

1. Introduction

In Kenya the effective power generation capacity as at the end of December 2018 is 2,200 megawatts (MW) while demand is at 1,859MW (ERC, 2018).There is insufficient spinning reserve which is a risk to power reliability on the interconnected system which may cause a total system collapse (black outs).The Kenya energy act No. 1 of 2019 section 200 (h),202 (1) on establishment of energy consumption benchmarks requires power consumers to monitor energy consumption in buildings and to implement measures to reduce energy consumption to acceptable levels. Kenyan gazette notice on Energy management Regulations 2012 requires consumers consuming more than 15,000 Kilowatt-hours (KWH) of monthly electricity to put in place measures to reduce their consumption by 50%. The affected facilities are among commercial buildings, hotels, institutions and industries. (Ngila & Group, 2015).

Currently the power consumers know their consumption status based on the monthly electricity bills. This data does not give a clear picture of future consumption trends that can enable power reduction decisions. The problem is inability to anticipate future demand with high accuracy. There are few studies that have developed simple, elaborate and accurate load forecasting model. Power consumers therefore need to evaluate and know their consumption behaviour based on historical data in order to effectively manage their power consumption. This can be achieved through power demand forecast. The forecast output will help in, power system planning, energy efficiency management and ensuring good quality of life. This forms a basis for the study and development of an artificial intelligence model to Power Demand Forecasting. A month a-head load demand forecasts will provide decision support. Future load prediction will enable the power system operators ensure an equilibrium between energy demand and electricity supply.

A case study of Kabarak University, where over a million shillings is spent monthly on electric energy bills. This study area is chosen because it is a designated consumer institution by the regulatory authority under section 187-188 of the energy act 2019 (Oyedepo, 2019). The University management has instituted an Energy management committee whose mandate is to develop a university energy policy. The goal is to improve implementation energy efficiency and conservation programs for university sustainability. It endeavours to plan energy saving strategies, monitor energy consumption and implement measures to reduce consumption within the University. This will lead to KABU earning compliance to Energy Act No.1 of 2019 sections (200-205) of Kenya published in 12th March 2019.The institution currently uses the expert knowledge in planning and implementation of energy efficiency and power reliability measures. Therefore, there is need for load forecasting information to enable the institution make energy saving decisions based on information.

2. The Problem

Electric energy being enabler to sustainable development goals calls for a stable, reliable and affordable power supply. There is a rising concern over inefficiency and reliability of power supply in Kenya. The erratic power consumption is causing a challenge in ensuring efficiency and reliability of power supply. To reduce this power inefficiency and improve reliability, ERC has set policy regulations on demand reduction targets for large power consumers. Kabarak University (KABU) is among large power consumers earmarked by the current Energy and Petroleum Regulatory Authority (EPRA). Its average consumption both high rate and low rate is 35,000 Kilowatt-hours (KWH) translating to over one Million shillings monthly.

The Energy regulator expects that this category of consumers shall comply with the Energy Policy Act. It is a regulatory requirement for consumers to earn compliance through implementation of energy saving measures by cutting down its current consumption by 50% according Energy Act published in March 2019.KABU management has made commitment to improve energy efficiency for University sustainability and compliance to these energy regulations through the University energy policy. However, it lacks a tool that can provide information about future consumption critical for making informed decisions on ways to reduce their consumption and energy management. Knowledge of prior load demand patterns will enable power consumers make strategic planning on implementation of energy reduction measures.

Therefore, this research addressed this problem by designing Artificial Neural Network Based Power Demand Forecasting Model for Energy Management (ANNPDFMEM). The purpose of ANNPDFMEM has been achieved by forecasting electricity demand for one day up to one week ahead. Thus, enables the power consumers to use this information for decision making on; planning, demand reduction strategies, energy management and ensuring good quality of life.

3. Objectives

The main objective of this research study is to develop an Artificial Neural Networks Based Power Demand Forecasting Model for Energy Management a case of Kabarak University. The model will provide a solution to power consumption monitoring and prediction of one day a-head power demand. The specific objectives contributing to this objective are;

- To design an Artificial Neural Networks Based Power Demand Forecasting Model for Energy Management.
- To implement an Artificial Neural Network Based Power Demand Forecasting Model for Energy Management.
- To evaluate the accuracy of the Artificial Neural Networks Based Power Demand Forecasting Model for Energy Management.

4. Literature Review.

4.1 Power Demand forecasting.

Power Demand Forecasting is categorized into three types based on period of time. Short term forecast are load predictions ranging from few minutes to hours up to one week (Barbieri, Rajakaruma et al. 2017). Medium Term Load Forecasts range from one week to one year period (Ahmad and Chen 2018). Long term Forecasting are predictions that range from one year and beyond (Carcedo and Garcia 2017). This load demand information is used as baselines in decision making for energy management. It is important in balancing electricity generation with its demand for maximum efficiency and power reliability. Power consumers use their demand forecasting information to plan for energy conservation measures that lead to reduction of energy consumption and increasing energy efficiency (Barbieri, Rajakaruma et al. 2017).

A study on weather sensitive demand model was developed for small utilities in North Cyprus. It is showed that independent variables including price of electricity, number of customers, tourists and population are significant in estimating the future peak demand of electricity (Mirlatifi 2015).Researchers have also forecasted the demand for electricity using approaches such as Adaptive Neuro Fuzzy Inference System (ANFIS) for prediction of electricity demand in India for the period during 2013 to 2020 (Saravanan, Kannan et al. 2015).Artificial Neural Network (ANN) was applied for forecasting a day ahead electricity price in Spain(Panapakidis and Dagoumas 2016),Decision Support System (DSS) has been utilized for taking decision in a competitive electricity market based on various factors, Hybrid Model used for forecasting electricity demand in china for the period 2016-2020 (Liang and Liang 2017)

A study that made a forecast on the World's green energy demand up to the year 2050 used a feed forward back propagation ANN technique, results showed lower errors and better performance (K. Ermis, 2007). Bilgili in his study applied ANN, Linear Regression

(LR) and Non Linear Regression (NLR) to forecast electricity demand for residential and industrial sector of Turkey. Results were compared between the ANN, LR and NLR showed actual data and the predicted results were almost the same, also the performance values of the ANN method were better than performance values of the LR and NLR models. A study by Adams built econometric model of the Chinese energy economy, it forecasted Chinese energy demand and imports up to 2020, ANN showed superior results (G. Adams and Y. Shachmurove, 2008).Kialaskaki and Reisel developed a model for energy demand forecasting for United States, they compared results from Multiple Linear Regression Models and ANN models, ANN was chosen based on the good ANN model evaluation parameter (Reisel, 2014)

5. Results

5.1 Design of ANNBPDFMEM;

The model design process systematically followed a design science approach of five steps as collecting power consumption data, pre-processing data, building the forecasting network model, training the model and finally testing the model. . A feed forward artificial neural network structure was designed because it had a good ability to map nonlinear functions (Taravat, 2015)

5.2. Data collection and pre-processing process;

Kabarak University electricity consumption data was collected from Kenya Power and lighting Nakuru. Historical power consumption for the period January to June 2019 data and current data for the period July -August 2019.The hourly active power in kilowatts (KW), Daily total energy consumption measured in KiloWatts-Hour (KWH) was collected and stored in excel file format. Hourly temperature in degrees Celsius data was collected from Nakuru meteorological station and stored in spread sheets. Data was pre-processed using the mapminmax function in MatLab toolbox. Data was normalized and randomized before presenting to the model network. The input vector was normalized so as to be in acceptable standard range. The output vector was be normalized into its original format.

5.3 Design of model network

We chose to design a multilayer neural network with three layers. The first layer had four input parameters, the hidden layer to have 10 neurons and the output layer to have one output neuron. A sigmoid symmetric transfer function was used on the output. The model structure is as on the figure 1:

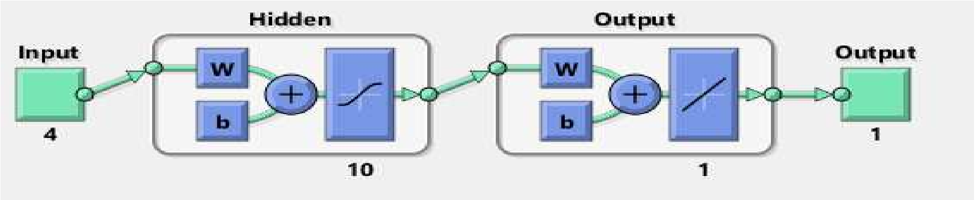
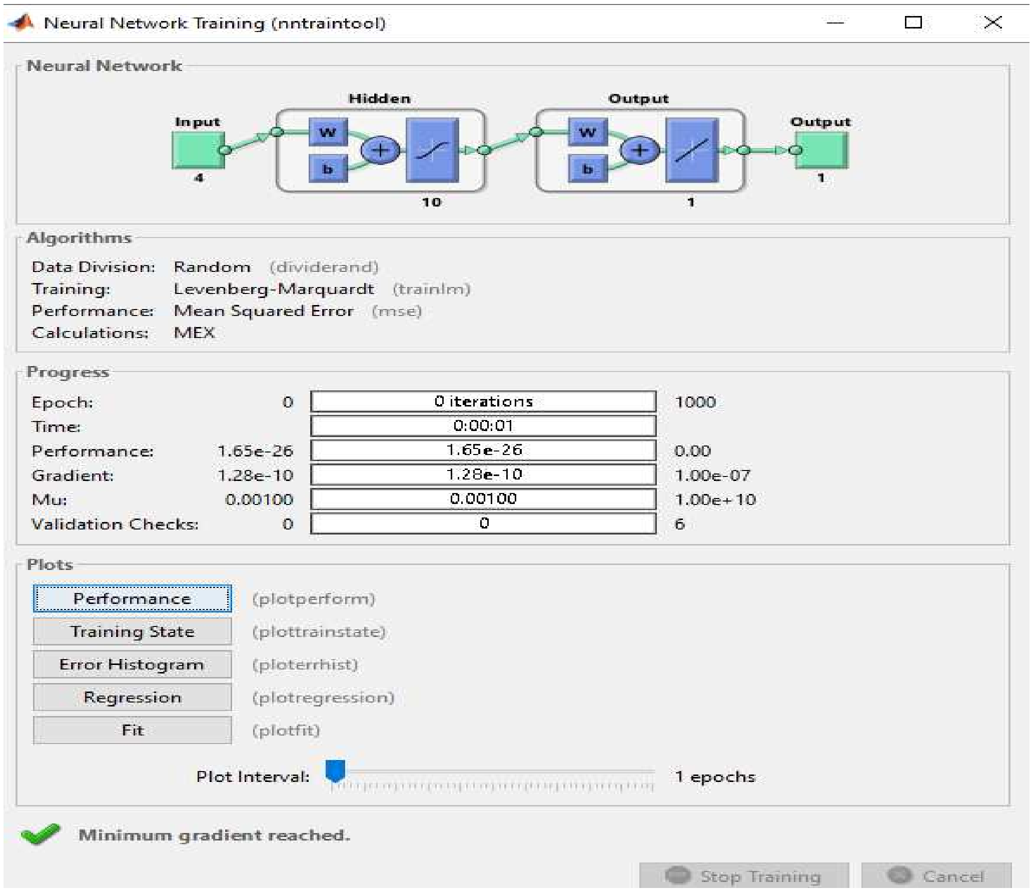


Figure 1: Artificial Neural Network Structure (Matlab, 2018a)

5.4 Model network training.

In this process a number of iterations were done to come up with the most accurate model for demand forecasting. Back-Propagation training algorithm method was used since it had proven effective results and accuracy needed for the network (Hanan A. Akar a. F., 2016).

A delta learning rule was used in this study. The acquired data set was split into the Training set and testing set. Training was the process of adjusting the weights of the neuron to the desired accuracy. The training set was 70%, 15% and 15% testing set. The best model had a network structure of four input neurons, hidden layer neurons, one output neuron.



Neural Network Training (nntraintool)

Neural Network
Input
4
Hidden
W
b
10
Output
W
b
1
Output
1

Algorithms

Data Division: Random (dividerand)
Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)
Calculations: MEX

Progress

Epoch:	0	0 iterations	1000
Time:		0:00:01	
Performance:	1.65e-26	1.65e-26	0.00
Gradient:	1.28e-10	1.28e-10	1.00e-07
Mu:	0.00100	0.00100	1.00e+10
Validation Checks:	0	0	6

Plots
Performance (plotperform)
Training State (plottrainstate)
Error Histogram (ploterrhist)
Regression (plotregression)
Fit (plotfit)
Plot Interval:
1 epochs

✓ Minimum gradient reached.

Figure 2: model training window.

Training Algorithm results table 1

	Samples number	Network structure	Levenberg-Marquardt training Algorithm.		Bayesian Regularization Algorithm		Scaled Conjugate function Algorithm	
	Samples number	Network structure	MSE	R Value	MSE	R Value	MSE	R Value
Model 1								
Training	1534	[4 6 1]	59314.51	0.812	48536.73	0.855	61243.11	0.813
validation	331	[4 6 1]	59072.94	0.820	0.00	0.855	66336.83	0.808
Testing	331	[4 6 1]	78849.72	0.811	50221.43	0.858	73567.84	0.769
Model 3								
Training	1534	[4 20 1]	33518.16	0.905	33517.62	0.904	56021.43	0.826
validation	331	[4 20 1]	40890.87	0.849	-	-	56495.72	0.838
Testing	331	[4 20 1]	42537.20	0.884	31882.70	0.904	67646.72	0.809

Model 4								
Training	50	[4 10 1]	9.5138	0.999	2.23	0.970	709.78	0.979
Validation	11	[4 10 1]	501.24	0.994	0.00	0.000	341.34	0.904
Testing	11	[4 28 1]	11.47	0.999	2.06	0.899	1348.45	0.924

Table 1: Table showing training algorithm results

It was observed that Levenberg-Marquardt had the best training algorithm as from table 1. Mean squared Error is the defined as the squared difference between outputs and targets. The best was model 7 with lower values which is desirable. Zero values indicate no error. Regression R values is a measure of how close the correlation between output and targets, the model achieved an R value of 1 indicating a close relationship among variables while R value of zero indicates a random relationship.

5.5 Model evaluation.

The trained ANNBPDFMEM model was tested against unseen data for the period 1st August, 2019.The model posted good prediction accuracy when compared with the actual values. The ANNBPDFMEM evaluation showed the following results train performance of 2.9985, Validation performance of 9.39998 and test performance of 9. 399. This showed the model is good for prediction with accuracy.

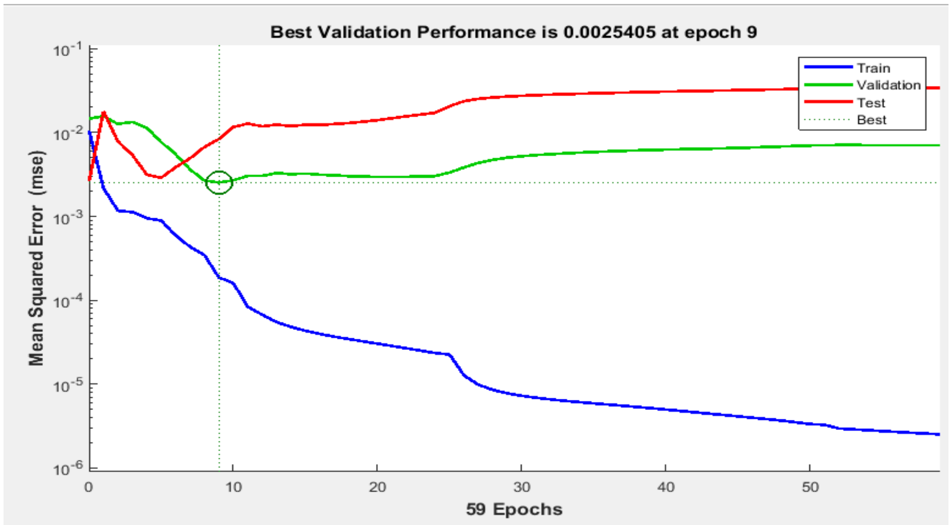


Figure 3: Model evaluation.

We observed that the ANNPDFMEM achieved best validations at after nine training iterations.From figure 4 below we observed that KABU consumption is high during weekdays as compared to weekends.Also high consumption is witnessed during mid day and evening due to optimum operation activity e.g computer lab operation and lighting loads.

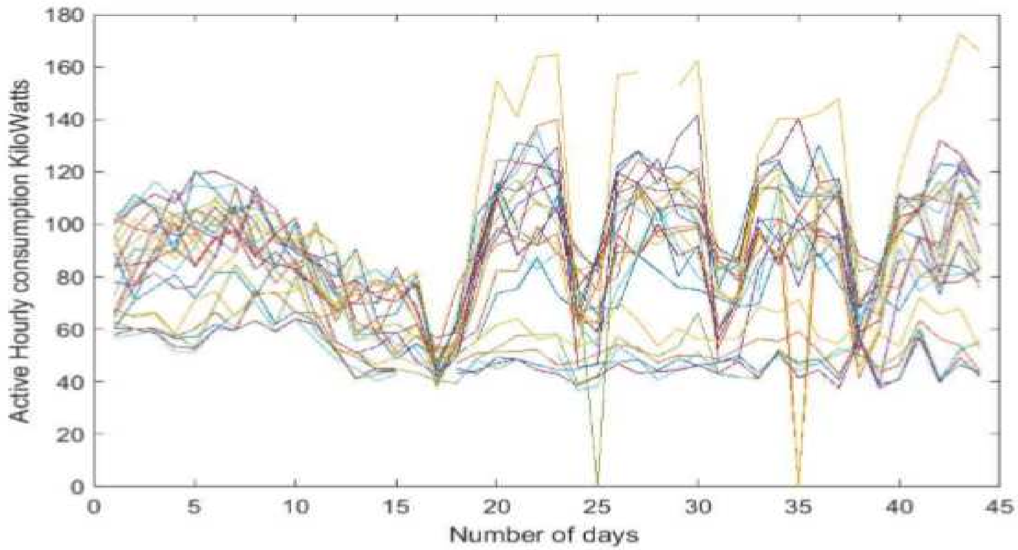


Figure 4 consumption loads analysis evaluation plot.

6. Results.

The model was designed and trained using Kabarak University electricity consumption data. It was observed that Levenberg training algorithm was the best with a MSE of 9.5 with an R value of 1 as from table 1.A network structure with smaller samples of training data proofed to train well as compared with large data sample set. The developed model showed that a Forward Neural Network layer used in this study with a BP training algorithm is able to learn well and can be used for forecasting.

The KPLC smart meter measured load data for Kabarak University was compared with the model predicted load table 2. It is seen that the model prediction is close to the actual load with 0.11% Mean absolute percentage error.

Date	Actual load (Mwh)	Predicted load (Mwh)
2019-08-14 12:00:00	1.43068	1.61195
2019-08-13 12:00:00	1.90032	1.92356
2019-08-12 12:00:00	1.97488	2.24838
2019-08-11 12:00:00	2.06650	1.09758
2019-08-10 12:00:00	2.06650	1.28328
2019-08-09 12:00:00	2.08826	1.78486

Table 2: Load forecast results.

MAPE= ({(sum of Actual-Sum of predicted)/Total Actual}/Duration) = 0.11%.

6.1 challenges in power demand forecasting.

The challenges of power fluctuations and blackouts deteriorates the forecasting accuracy of the model, this will be mitigated by normalization of raw data.

7. Recommendations and areas of further study.

7.1 Recommendations

The forecasting in future should focus on additional parameters to improve on the model accuracy and provide more information on power demand trends.

7.2 This research area presents a gap which needs further research on effects of student school days on institutional power demand to provide more insights on improving energy efficiency and conservation. This will provide information for decision making on improved energy management.

8. Conclusion.

Artificial Neural Networks power demand forecasting model proof to accurately predict a day a-head power demand. Institutions of higher learning will benefit in adoption of this study by way of prediction of their short-term power demand and use the power consumption information to make informative decisions to reduce consumption and hence cutting down their power bills.

References.

Abadi, M., Barham, P., Chen, Z., Davis, A., Dean, J., Ghenawat, S., et al. (2016). A system for large scale machine learning. *In proceedings of the 12th USENIX Symposium on operating systems Design and Implementation*, PP16,265-283.

Ahmad, T., & Chen, H. (2018). Short Term Focasting of cooling and Heating Load Demand in building enviroment with data mining based approaches., (pp. 266,460-476).

al., F. C. (2015). *Keras.* Retrieved from github: https://github.com/keras-team/keras. (2015)

Alemu H.Z, W. (2018). FeedForward Neural Networks with Hidden Layer Regularization Method., (pp. 10,525).

Al-Wakeel, A. J. (2017). k-means based load estimation of domestic smart meter measurements. *Applied Energy*, P.333-342.

Amasyali, K. a.-G. (2018). A review of data driven building energy consumption prediction studies. *Renewable and Sustainable Energy Reviews*, 1192-1205.

Amasyali, K. a.-G. (2018). A review of data-driven building energy consumption prediction studies. *Renewable and Sustainable Energy Reviews*, 1192-1205.

Amasyali, K. a.-G. (2018). A review of data-driven building energy consumption prediction studies. *Renewable and Sustainable Energy Reviews,*, P.1192-1205.

Jain, R. e. (2014). Forecasting energy consumption of multi-family residential buildings using support vector regression: Investigating the impact of temporal and spatial monitoring granularity on performance accuracy. *Applied Energy*, 168-178.

Jetcheva, J. (2014). W.Neural network model ensambels for building-level electricity load forecasts., (pp. 84,214-223).

Jian C.L., Y. (2015). Non-Divergence of Stocholastic Discrete Time Algorithms for PCA neural Networks. *IEEE Trans.*, 394-399.

K. Ermis, A. M. (2007). "Artificial neural network analysis of world green energy. *Energy Policy, vol. 35*, 1731-1743.

Khajure S., M. S. (2016). Future Weather Forecasting Using Soft Computing Techniques., (pp. 402-407).

Khuntia, S. e. (2016). Time-horizons in the planning and operation of transmission networks: an overview. *IET Generation, Transmission & Distribution,*, P.841-848.

Zor, K. T. (2017). A state-of-the-art review of artificial intelligence techniques for short-term electric load forecasting. *In Energy (IYCE), 2017 6th International Youth Conference*, (pp. pp. 1-7).

Machine Learning Sms Spam Detection Model

Andrew Kipkebut[1], Moses Thiga[2] Elizabeth Okumu[3]
School of Science , Engineering and Technology
Kabarak University, P.O. Box Private Bag, Kabarak, 20157, Kenya
Tel: +254 0719499615, Email: akipkebut@kabarak.ac.ke

Abstract

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 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 .The results and discussions are presented in form of descriptive statistics and detection metrics, the model registered an overall classification accuracy of 96.1039% .

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

1.0 Introduction

The goal of machine learning is to improve the performance of a computer program with experience. There are a lot of tasks that can be solved using machine learning, including speech recognition, playing games, automatic driving of a vehicles, anomaly detection medical diagnosis and data mining (Sinclair, C., Pierce, L., & Matzner, S. (1999). A range of algorithms have been invented for machine learning, that uses the fields of artificial intelligence, probability, statistics, information theory, neurobiology and others. Some of these algorithms include decision trees, Support Vector machines (SVM), Artificial Neural Networks (Almomani, et al., (2013)), Naïve Bayes algorithm, Decision trees among others. Machine learning is a fascinating field of artificial intelligence where investigation on how computer agents can improve their perception, cognition, and action with experience. Mansfield Devine (2017) defined SMS phishing (SMS Spam) as a form of criminal activity that uses social engineering techniques in an attempt to harvest credentials such as passwords, PINs (personal identification numbers) and other details by masquerading as a trustworthy entity in an electronic communication using Short Message Service (SMS)

1.1 Statement of the problem

SMS spam is real and a growing problem largely due to the availability of very cheap bulk pre-pay SMS packages and the fact that SMS stimulate higher response rates as it is a trusted and a personal service. The Short Messaging Service (SMS) mobile communication system is attractive for criminal gangs for a number of reasons i.e. it is easy to use, fast , reliable and affordable technology (Delany S. J , Buckley M,& Greene D ,2012). The presence of lack of a unifying model is perceived as a hindrance to the further development of the field of machine learning especially in Sms spam detection. Many approaches proposed, regardless of their effectiveness, focus on a specific aspect or language and most of them do not have integrated approach and are not exhaustive.

1.3 Main objective

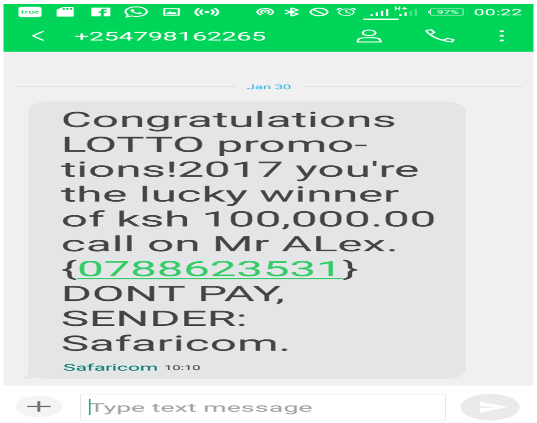
The main objective of this research is to evaluate a machine learning Sms Spam detection model.

1.4 Specific objectives

- To develop Spam detection model that can be used to detect Spam messages in Kenya .
- Demonstrate the use of machine learning in classifying messages as either Spam or not.
- To test the machine learning model through the use of a prototype.

2.0 Literature Review

Mobile phones have completely changed the way people communicate and interact. You can call, send text messages, read emails, play games as well as read and edit documents on the fly. Today, the mobile phone has become part and parcel of many people’s lives. Leaving the house without your cell phone is like leaving your brain at home, some people may not function without the phone. According to Joo J.W, Moon S.Y, & Singh S, (2017) SMs Spam has continued to grow and evolve in popularity as a social engineering tool for cybercriminals. SMs Spam can trick the user into clicking on a link in a text message which can lead the user to entering personal data. The objective is to gain access to sensitive information like usernames and passwords. Additionally, many SMs Spam messages will include links with malware waiting on the other side for anyone who clicks on them. If you click on the infected web site link , it may download malware, which compromises your mobile device or the web site will ask you to input personal information such as, social security number, credit card type, credit card number and PIN etc. If you call the phone number given, it will sound very official and will ask you to input personal information such as, Identification number, credit card type ,digital wallet pin among others. An SMs Spam text message is determined on the basis of the basic attribute of the text message. Whether the text message includes a Universal Resource Locator(URL) or a telephone number or just plain sentences (Kang, S. & Kim, S., 2013) as shown in figure 1.



Congratulations LOTTO promotions!2017 you're the lucky winner of ksh 100,000.00 call on Mr ALex. {0788623531} DONT PAY, SENDER: Safaricom.

Figure 1: An SMs Spam example (source, Researcher).

2.1 Naïve Bayes classifier

As stated by Russell Stuart & Norvig Peter (2016) Naive Bayes classifiers are a family of simple probabilistic classifiers based on Bayes' theorem with strong independence assumptions between the features. It has been studied extensively since the 1950s., and was introduced under a different name into the text retrieval community in the early 1960s, it remains a baseline method for text categorization, the problem of judging messages as belonging to one category or the other (such as spam or legitimate) with word frequencies is used as features. With appropriate pre-processing, it is competitive in the classification domain with more advanced methods including support vector machines (Rennie J, Shih L ,Teevan J,& Karger D, 2003).

Naive Bayes (NB) is a classifying algorithm as shown in figure 2 uses data about prior events to estimate the probability of future events. Typically it's best applied to problems in which the information from numerous attributes should be considered simultaneously in order to estimate the Probability of an outcome. While many algorithm typically ignore features with weak effects, this technique uses all available info to subtly change predictions (Raghav Bali, Dipanjan Sarkar ,& Brett Lantz ,2013). Most of the current spam email detection systems use keywords to detect spam emails. These keywords can be written as misspellings eg: baank or bannk instead of bank. Misspellings are changed from time to time and hence spam email detection system needs to constantly update the blacklist to detect spam emails containing misspellings (Renuka & Hamsapriya,2010).A Naive Bayes classifier will converge quicker than other models, it requires less training, it is easy to build and particularly useful for very large data sets. Along with simplicity, Naive Bayes is known to outperform even highly sophisticated classification methods. Although the independence assumption may seem sometimes unreasonable, its performance is usually reasonably good, even for those cases (Romero, 2010).It is called Naïve classifier because its assumes independent features.

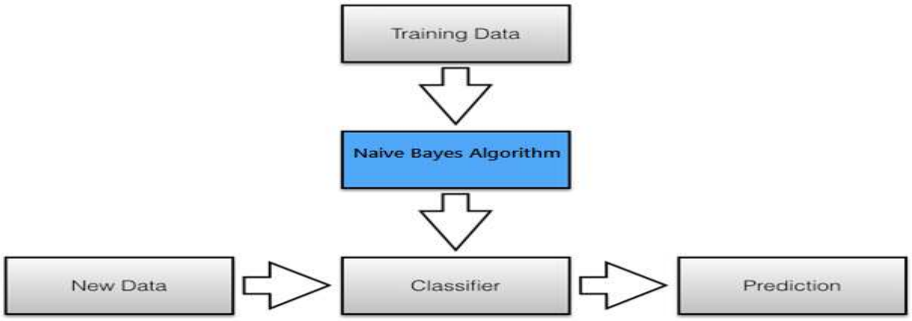


Figure 2 Naïve classifier approach (Sebastian Raschka, 2014)

.2.2 Conceptual Design

Yadav et al.,(2011) provides an approach is similar to Deng & Peng (2006) in that they propose a client side Naive Bayes filter which uses the occurrence of keywords that appear in spam messages to determine a spam score. Messages that score above a certain threshold are labelled as spam. Their solution also requires user feedback to confirm and correct errors made by the classifier and therefore their filter can learn new spam keywords from client reports to a central server, which are in turn pushed out to other clients. The research will be informed by the conceptual design in figure 3. The data is pre-processed which includes formatting of the data, then trained using Naïve Bayes ML algorithm after which its tested and lastly classified to determine which class they belong to.

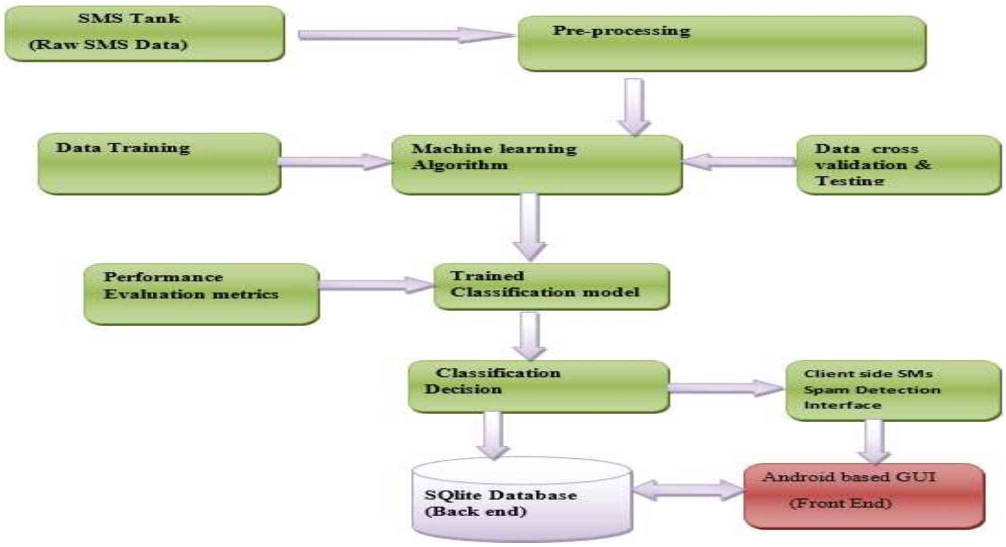

SMS Tank
(Raw SMS Data)
Pre-processing
Data Training
Machine learning Algorithm
Data cross validation & Testing
Performance Evaluation metrics
Trained Classification model
Classification Decision
Client side SMs Spam Detection Interface
SQlite Database (Back end)
Android based GUI
(Front End)

Figure 3 : Conceptual Design Source Researcher

3.0 Methodology

This chapter provides a description of the approaches that were adopted in carrying out the research . Naive Bayes algorithm that uses Bayes theorem as shown in formula below was used for detecting whether a message is Spam or not.

$$P(spam \mid word) = \frac{\mathrm{P(spam).P(word|spam)}}{\mathrm{P(spam).P(word|spam) + P(non-spam).P(word|non-spam)}}$$

Several measurement methods were typically used for comparing results of classification Some of these methods included precision, recall, accuracy, true positive, false negative, true negative and false negative-rates (B.K. Bharadwaj & S. Pal, 2011).Machine learning experiments were employed in this research using WEKA. WEKA (Waikato Environment for knowledge analysis) an Open source data mining tool written in Java programming that can be used for collection of machine learning algorithms data, data pre-processing, classification, regression , clustering and visualization. It contains a collection of visualization tools and algorithms for data analysis and predictive modelling, together with graphical user interfaces (Hall M, Frank E, Holmes G, Pfahringer B, Reutemann P, & Witten I. H, 2009).

3.1 Prototype development.

The SMs Spam detection prototype development involves an iterative SDLC (Software development life cycle) , a process of dividing software development into distinct steps that contains finite activities , the steps include ,Problem definition, Data collection , Data preparation, spot check on algorithm, Training of the model ,Evaluation of model performance , data visualization and prototype implementation. On these activities there is a lot of flexibility. The greatest thing in using automated tools is that you can always go back a few steps (iteration) and insert a new transform of the dataset and re-run experiments in the intervening steps to see what interesting results come out and how they compare to the experiments executed before. The algorithm was trained on the training dataset and evaluated against the test set. This involves selecting a random split of data (66% for training, 34% for testing).

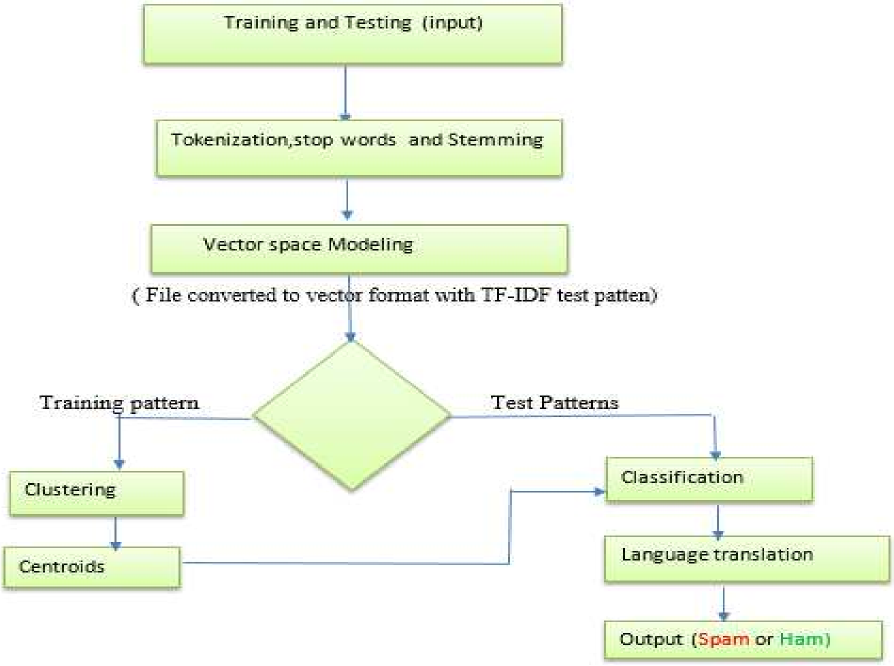


Fig 4 Flow chart of the proposed prototype

The flow chart in Fig 4 involves training and testing of the data , Tokenization , stop words and stemming, Vector space modelling using TF-IDF transformation. This will result into a training pattern and a test pattern that will be used for classification. Clustering was also done in order to group the messages as either spam or Not , this was done using K – means Clustering algorithm.

4.0 Results Findings and Discussions

This chapter gives an overview of the results, findings and discussions .An experiment was done to examine 1001 SMS as Spam or not a Spam. This analysis was done with reference to the three objectives aforementioned in the research objectives. These findings were used to explain the results and future work. WEKA tool was used to read stored SMS data from a file and was further structured for the learning algorithm interpretation.

4.1 Data Testing

A test data (Artff file) containing 322 instances (1/3 of total 1001 instances) with missing class(?) was used to test the full training data. Stemming was done using potter stemmer algorithm, This generated 1115 keyword based attributes that include Cash, safaricom ,win, bank among others,the Table 1 gives a the summary of keywords which includes its mean, standard deviation weighted sum and precision for each class.The naives bayes algorithm correctly classified 962 instances and incorrectly classified 39 of the 1001 instances which gives a percentage of 96.1039% and 3.8961% respectively. It leads to an accuracy of 96.1039% as shown in Table 2 and Table 3, from the confusion matrix the naïve bayes r learner was able to get 207 +755 correct classifications, and made 22+17 mistakes , this is fairly good compared to the nature of the algorithm.

Table 1 Some keyword -attribute statistics

Attribute	**Class**	
safaricom	**Spam(0.22)**	**Ham (0.78)**
Mean	0.0214	0
Std deviation	0.627	0.5327
Weight Sum	224	777
Precision	3.1928	3.1928

Table 2 Evaluation on training Set

Correctly classified instances	962	96.1069%
Incorrectly classified instances	39	3.8961%
Kappa statistic	0.8887	
Mean absolute error	0.0439	
Root Mean Squared error	0.1769	
Relative absolute error	12.6162%	
Root relative squared error	42.4404%	
Total number of instances	1001	

Table 3 Detailed accuracy by Class

Weighted Avg	**TP Rate**	**FP Rate**	**Precision**	**Recall**	**F-Measure**	**MCC**	**ROC**	**PRC-Area**	**Class**
	0.924	0.028	0.904	0.924	0.914	0.889	0.989	0.973	**spam**
	0.972	0.076	0.978	0.974	0.975	0.889	0.989	0.997	**ham**
	0.971	0.065	**0.961**	0.961	**0.961**	0.889	0.989	**0.991**	

4.2 Conclusion

SMS spam filtering is an important issue in mobile commerce security and machine learning techniques; The quality of performance Naıve Bayes classifier is also based on datasets used. In this thesis Naive Bayes classifier has shown highest precision in Sms Spam detection. By looking at the words that are present within the message, the classifier was able to correctly classify the message as either Spam or Not. Using a model such as these mobile users can detect Spam messages using their phones therefore reducing fraud.

This model can be improved by looking at the messages that were mis-classified and understanding why this happened.

4.3 Recommendations

i) Some WEKA Visualizations features were not very clear e.g. the J48 visualization tree, this is because the tree was too large, other commercial software such as scikit-learn, RapidMiner may be used for this purpose.
ii) To avoid loss of money through SMs Spam, the government of Kenya needs to provide user training/education on Social engineering attacks especially on mobile phone.
iii) To speed up the training and testing , the researcher recommends thorough preprocessing of data. Use of a computer at least of 1.10 GHZ , 4GB RAM or above especially when handling large data is highly recommended
iv) Profiling of frequent sms Spam phone number may also help to curb this menace
v) Client side detection may not be enough. An adoption of a server side detection mechanism from the service providers such as Safaricom, Airtel and Telkom will help to reduce the damage of SMs Spam .

4.4 Areas of Further research

This study focussed on SMs Spam detection using naive bayes machine learning algorithm. However there are almost infinite text classification ways to detect SMS Spam that needs to be researched on. In this study the accuracy of the model can be improved with considering large data set and restrict the algorithm model to ignore normal dictionary words and instead use frequently used spam words in any language including Slang language (ghetto language) and local vernacular languages.

References

A Almomani, BB Gupta, T Wan, A Altaher (2013) Phishing Dynamic Evolving Neural Fuzzy Framework for Online Detection Zero-Day Phishing Email. Indian J. Sci. Technol. 6, no. 1, 3960–3964 .

A- Kwee, et al (2009), "sentence-Level Novelty Detection in English and Mafay." in advances in knowledge and discovery and Data mining vol. 5476. T. Theeramunkong. et al. Eds., cd: Springer Berlin Heidelberg., pp. 40-51.

B..Blankertz, G. Dornhege, C. Schafer, R. Krepki, J. Kohlmorgen, K.-R. Muller, V. Kunzmann,

Delany, S. J., Buckley, M., & Greene, D. (2012). SMS spam filtering: Methods and data. *Expert Systems with Applications*, *39*(10), 9899-9908.

Mansfield-Devine, S. (2017). Bad behaviour: exploiting human weaknesses. *Computer Fraud & Security*, *2017*(1), 17-20.

Kang, A., Lee, J. D., Kang, W. M., Barolli, L., & Park, J. H. (2014). Security considerations for smart phone smishing attacks. In *Advances in Computer Science and its Applications* (pp. 467-473). Springer, Berlin, Heidelberg.

Russell, S. J., & Norvig, P. (2016). *Artificial intelligence: a modern approach*. Malaysia; Pearson Education Limited,.

Rennie, J. D., Shih, L., Teevan, J., & Karger, D. R. (2003). Tackling the poor assumptions of naive bayes text classifiers. In *Proceedings of the 20th international conference on machine learning (ICML-03)* (pp. 616-623).

Sinclair, C., Pierce, L., & Matzner, S. (1999, December). An application of machine learning to network intrusion detection. In *Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99)* (pp. 371-377). IEEE.

Wang, C., Zhang, Y., Chen, X., Liu, Z., Shi, L., Chen, G., Qiu, F., Ying, C., & Lu, W. (2010).A behavior-based SMS antispam system. IBM Journal of Research and Development , 54 , 3:1{3:16.

Yadav, K., Kumaraguru, P., Goyal, A., Gupta, A., & Naik, V. (2011, March). SMSAssassin: crowdsourcing driven mobile-based system for SMS spam filtering. In *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications* (pp. 1-6).