

## **Conference Proceedings**

Kabarak University International Research Conference [on](#) Computing and Information Systems

Kabarak University, Nakuru, Kenya  
22<sup>nd</sup> – 23<sup>rd</sup> October 2018

**Editors**

1. Dr Christopher Maghanga
2. Dr Moses M Thiga

**Sponsors**

This conference was graciously sponsored by the National Research Fund

## **Foreword**

Dear Authors, esteemed readers,

It is with deep satisfaction that I write this foreword to the Proceedings of the Kabarak University 8<sup>th</sup> Annual International Research Conference held between 22<sup>nd</sup> and 26<sup>th</sup> October at the Kabarak University Main Campus in Nakuru, Kenya. This conference focused on the thematic areas of computer, education, health, business and music and attracted a great number of paper and poster publications. The conference also featured workshops in the areas of blockchain and digital skills for business. The participation of developing academics, undergraduate students and graduate students was particularly encouraged in this conference.

In addition to the contributed papers, the conference featured a number of invited keynote and guest speaker presentations as follows;

- 1 Mr John Walubengo, Dean Faculty of Computing at the Multimedia University of Kenya and a member of the Artificial Intelligence and Blockchain Taskforce.
- 2 Mr Derrick Rono, Senior Systems Developer with Andela Ltd and our Kabarak University Computer Science alumni
- 3 Mr John Karanja, Chief Executive Officer, Bithub Africa
- 4 Ms Roselyne Wanjiru, Education Program Coordinator EOS Nairobi, representing Mr Daniel Kimotho, Community Lead EOS Nairobi
- 5 Ms Rosemary Koech-Kimwantu, Legal and Regulatory Specialist at Oxygene Marketing
- 6 Dr Julius Jwan, the CEO Kenya Institute of Curriculum Development
- 7 Prof Ruth Otunga, Deputy Vice Chancellor, Academic Affairs, University of Eldoret.
- 8 Dr Edward Nzinga, Senior Lecturer, Instruction and Curriculum Design Scientist, Pan Africa Christian University.
- 9 Prof Peter Anyang Nyongo, Governor Kisumu County
- 10 Prof Michael Kiptoo, CEO, Kenya Medical Training College.
- 11 Dr Geoffrey Wechuli, Head, Department of Family Medicine, Kabarak University
- 12 Mr Onesmus Kamau, Head of eHealth, Ministry of Health
- 13 Ms Edna Tallam-Kimaiyo, CEO Nursing Council of Kenya
- 14 Mr Davis Njuguna Kamau, Director, East Africa Chamber of Commerce, Industry and Agriculture
- 15 Mr James Kaka, CEO Kakajames Enterprises Ltd
- 16 Mr Janet Lagat, CEO Hortigrud Ltd
- 17 Mr Raphael Osoro, CEO Sunsareg Solar Ltd
- 18 Mr Kirori Mindo, CEO Qmax Digital Ltd
- 19 Prof. Kimberly Carballo: Coordinating Opera Coach and Collaborative Piano, Jacobs School of Music, Indiana University
- 20 Dr Evelyne Mushira. Deputy Director, Permanent Presidential Music Commission
- 21 Mr Reuben Kigame; Renowned Gospel Artist and Founder of Sifa Voices International
- 22 Ms Caroline Wanjiku, A renowned Comedian aka “Teacher Wanjiku”

I trust that these proceedings will provide researchers with an excellent source of new and relevant knowledge in their respective disciplines. We thank all authors and participants for their contributions.

**Dr Moses M Thiga**

**Director, Research, Innovation and Outreach**

### **Conference Organizing Committee**

- Prof Jackson Kitetu                      Chairman
- Dr Moses Thiga                            Director, RIO & Secretary
- Dr Dave Bowen                             School of Education
- Ms Mary Muriithi                         School of Pharmacy
- Dr Geoffrey Kamau                        School of Business and Economics
- Dr Robert Mutwiri                        School of Computer Science and Bioinformatics
- Dr Pamela Kimeto                         School of Medicine and Health Sciences
- Dr Patrick Monte                          School of Music and Performing Arts
- Ms Rahab Wakuraya                       School of Law
- Prof Gladys Kiptionny                     Director, Excellence in Learning and Teaching
- Mr Anthony Somba                        Director, Quality Assurance and Institutional Planning
- Dr Betty Tikoko                             Director, Institute of Postgraduate Studies
- Ms Patricia Chebet                         University Librarian

## **Table of Contents**

A Proposed Framework for Implementing Cloud Erp System in a Developing Country Local Government: A Case of Uganda.....	7
Ab initio calculation of structural and electronic properties of 3c-Silicon Carbide: Density functional theory calculations.....	20
Computational methods in Materials Science studies.....	27
The Potential of Electronic Data Interchange at Huduma Center Acase of Nakuru County.....	35
Security and Privacy of app Permissions on Mobile eServices.....	38
RE TSA - Real Time Security Alert.....	49
The Exponentially Modified Gaussian Function as a Tool for Deconvolution of Astroparticle Physics Data.....	53
An Architecture for Detecting Information Technology Infrastructure Policy Violations in a Cloud Environment.....	62
Evaluation of mechanisms that enable self- protection on policy violation in cloud Infrastructure .....	70
Practices, Challenges and Approaches for Software Project Risk Management in Kenyan County Governments.....	79
Improving the Performance of Network Intrusion Detection Based on Hybrid Feature Selection Model.....	90
Assessing Security Risk Caused By Smart Mobile Devices In A University Network Through A Web-Based Threat Matrix.....	102
A Serial Number Based Identification Model for a Computer in a Wireless Local Area Network .....	119
Modified Regression Type Estimators in the Presence of Non-Response.....	133
A Study of the Morphology of Synthesized ZnO Nanoparticles and their Application in Photodegradation of Dyes.....	146

## **A Proposed Framework for Implementing Cloud ERP System in a Developing Country Local Government: A Case of Uganda**

David Mpanga\*, Christopher Maghanga and Rabah Kefa  
School of Science, Engineering & technology, Kabarak University

Corresponding author: [dmpangabiz@gmail.com](mailto:dmpangabiz@gmail.com)

### **ABSTRACT**

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

Key words: ERP, Cloud ERP, ERP implementing framework, Local government ERP, ERP implementation

### **INTRODUCTION**

Enterprise Resource Planning (ERP) is a software solution that assimilates business functions and data into a single system that is shared within the business (Rajeshwar, 2015). According to Matos & Alves, (2011) enterprise systems are packed software solution that have become popular in private sectors where organizations are aligning information systems with business strategy through elimination of fragmented information sources; replacing legacy information systems with Enterprise resource planning (ERP) software that cut across functional areas. Enterprise systems originated from manufacturing industry and later extended to private sector broadly. Enterprise Resource Planning software solutions are also known as Standardized Business Software Applications (Keller and Meinhardt, 1994). According to Carutasu & Carutasu(2016), ERP is multifunctional software package and extends to the entire enterprise with the same database for the entire company. Enterprise Resource Planning (ERP) systems are, generally, characterized by their complexity and wide footprint in the enterprise with regards to scope,

Ramburnet, al. (2016). Though ERP use is widely accepted in developed countries, Shaul&Tauber (2013), the market of ERP systems in developing countries is still in early stages, Hawari&Heeks (2010).

Increased demand for efficiency and effectiveness in service delivery has made the implementation of information systems and the demand for access to real time information no longer a requirement unique to private sector or large public sector entities, it is also a critical requirement for local government entities like municipalities. However, there are many substantial challenges faced by local government entities and information systems implementers, for example, municipal entities in a country are many and scattered geographically, there are insufficient technological infrastructure within these entities, highly constrained by requirements to comply with government regulations, they lack adequate funds and technical IT skills. Software providers and implementers have to address the above issues to successfully develop and deploy information systems that fit local government entities.

Municipalities are lower local government public sector entities that provide government services to local communities and businesses. Their structure consist of cells, the lowest unit, ward and division. Municipalities are entities designated to provide broadly three services: planning, garbage management and provision of social services. In many developing countries, local government entities are characterized by acute lack of adequate IT infrastructure, limited computer skills, insufficient data collection, storage and accessing mechanism, and inadequate IT budget.

To successfully implement an Information system that deliver value to the recipient organization, like a municipal entity, requires a clearly defined framework to guide the implementation process within limits of contextual constraints. Partial or total failure of information system implementation doesn't necessarily result from software design. The failure could be caused by solution – organization misfits that are contextually unique to a particular organization, Hawari&Heeks (2010).

Cloud computing is a network based service model that enable on demand network access to a shared pool of configurable computing resources; a model that provides special services over the internet; this service could be server, storage, or software (Bahssas et al., 2015). Many ERP vendors have moved to cloud computing platform, where ERP solutions are hosted. Cloud ERP is hosting an ERP system over the cloud, where hosting is done through two models IaaS (Infrastructure as a service) and SaaS (Software as a Service) (Lenart, 2011). According to Bahssas et al. (2015) cloud ERP has many advantages which are less staff, Mobility, easy expandable, cost reduction, and fewer expenses. Cloud technology under Software as a Service (SaaS) model is gaining popularity in private sector SMEs promising, low deployment costs, low price with pay-as-use, a considerably reduced time-to-deployment (Carutasu & Carutasu, 2016; Weng& Hung (2014). Local governments in developing countries could benefit from SaaS, however, a successful deployment require a comprehensive contextualized implementing framework to ensure compliance to local government regulations and unique constraints. Cloud ERP SaaS module will enable local governments to get access to a pool of cloud ERP software service through internet connection rather than each local government implement own ERP system.



## **Objective**

The paper is intended to provide a conceptual framework for a successful implementation of a cloud based ERP systems in local government, a municipality used as a case, in a developing country. This will help local government decision makers and ERP vendor when considering to implement ERP system in local government administration. The paper attempts to answer the question; what framework is appropriate to successfully implement a cloud ERP system in a developing country's local government?

## **STRUCTURE OF THE PAPER**

The following section explains the methodology used to collected data for this paper; the next explores existing ERP system implementing frameworks/methodologies; then findings are discussed; and lastly a proposed framework for implementing cloud ERP in local government in a developing country is explained.

## **METHODOLOGY**

The papers draws data from both primary and secondary sources following exploratory approach. A qualitative approach was used to understand municipality information systems, data/information standards and needs, business processes and relevant service delivery regulations. A review of reports, forms, etc. was done to understand the data and information requirements and challenges in the functions of municipality administration. A critical literature review was carried out to explore work done on implementation of information systems in local government with a focus on ERP systems in developing countries. Primary data was obtained from interviews with staff in three local government municipalities; to get an in depth understanding of the types of information systems within municipality administration, how they are implemented and managed; understand local government business processes and regulations constraining them. Three group discussions were conducted in three municipalities, and each group discussion involved 5 local government participants. Focus group discussions were focused on understanding: the functions of a municipality, key municipality business processes, framework for implementing information systems, data collection and management processes, level of awareness and acceptance of third party managed internet based enterprise systems.

## **DATA COLLECTION METHOD**

To obtain data from multiple participants, focus groups method was adopted for being economical, fast, and efficient (Krueger & Casey, 2000). For exploratory and verification purposes, emergent-systematic focus group design was adopted; three sessions were conducted, and participants purposively selected using purposive sampling techniques. Focus groups consisted of 7 participates, a number within the range of Morgan, (1997) and Baumgartner, Strong, & Hensley, (2002) recommendation, and each session lasted 1 hour 20 minutes averagely.

The focus group method was intended for an in-depth understanding of information systems and business processes in municipalities rather than behavior, opinions and attitudes of employees towards municipality information systems. Hence, interactions among focus group participants and between participants and individuals were not measure as recommended by Myers (2006) or Onwuegbuzieet. al. (2009). Understanding of municipality information systems, processes, and

ERP implementation framework/methodology will equip decision makers and ERP vendors to reduce on total or partial failure rate of ERP implementation, result from implementing framework/methodology.

## **RELATED WORK**

This section provides a discussion on existing framework/methodologies used when implementing ERP systems. The discussion cover articles ranging from 1983 to 2015, exploring approaches, frameworks, and methodologies adopted to implement ERP systems in various organizations.

## **ERP IMPLEMENTING FRAMEWORKS**

Literature on ERP implementation methodologies/frameworks is very sparse, available literature on ERP system implementing frameworks is vendor prescribed and generic. Research of ERP system focus on CSFs identified from development countries. Literature on ERP implementation on public-sector is relatively sparse more so from developing countries (Matos &Alves, 2011).ERP is realized in public sector organizations that are constituted to operate like corporate organizations. There is a need to understand the maturity level of business processes in public sectors in developing countries. Hasibuan&Dantes (2012), suggested an impact of 42.20% weight of business process reengineering on the priority key success factor of ERP implementation cycle.

Govindaraju (2012) suggest an organizational perspective framework for implementing ES; focusing on two stages in ES implementation process including project stage and post project stage. Further recommend that enterprise system implementation effectiveness need to be analyzed at two levels: short term implementation effectiveness, related to the outcome of the project stage, and the long-term implementation effectiveness, related to the outcome of the post-project stage. This framework is generic, and doesn't specifically highlight the critical factors that should be considered at each stage, and how variations in businesscharacteristics or business environments impact on the whole ES implementation process.

Dantes&Hasibuan (2011) proposed an ERP implementing conceptual framework considering two dimensions; ERP implementation process having five stages: project preparation, technology selection, project formulation, implementation and post-implementation. Somers and Nelson (2004) identified six stages of ERP implementation process: initiation, adoption, adaptation, acceptance, routinization, and infusion.

Ahituv (2002) developed a generic hybrid ERP implementation methodology combining three structured approaches: Structured Development Life Cycle (SDLC), Prototyping and application package model. He contend that the uniqueness of ERP system renders any of the three models inadequate to be adopted solely in implementation of ERP system. Implementation of ERP system touches the core process of the business. Hence, adoption of a hybrid methodology universally is likely to result into unexpected failure due to cultural, organizational and political influences experienced in environments that are characteristically different.

Maditinoset *al.*, (2011) argue that most of ERP failures are not caused by the ERP software but the complexity and massive changes caused by ERP in an organization This is line with Heloet

*al.* (2008), stating that the major impediments to successful ERP implementations are not technologically related issues such as compatibility, technological complexity, and standardization, but most are organization and human related issues including as resistance to change, organizational culture and business processes. These challenges could be dealt with by using a well contextualized framework appropriate. Universality adoption of implementing frameworks overlook organizational culture, behavior, and change management impact on ERP implementation failure.

Huang *et al.* (2004) listed the top ten risks that cause ERP implementation failures, which are related to implementing framework. ERP implementation involves more than changing an organization's software; it involves repositioning the organization and transforming its business operations, processes and practices (Rajeshwar, 2015).

### **LIMITATION OF EXISTING FRAMEWORKS/METHODOLOGIES**

Unlike the private sector where top management make decisions independently, in public sector decisions are highly influenced politically and highly constrained by government legislations. The critical success factors identified in the private sector don't translate directly into the public sector more so in developing countries. Motivating factors for implementing ERP implementation literature use concepts of framework, methodology and model interchangeably. Implementation of ERP system is based on assumption of best practices being universal; a major source of misfit of ERP and client organization business processes. There is a need to recognize the variation in characteristic business process among organizations, be it private or public, and developed economies or developing economies. Klaus *et al.* (2000) states that the transferability of ERP best practices on a global scale might be limited due to every country specific requirements relating to every fundamental processes.

Existing frameworks are private sector based and focus on what should be done at a particular stage with no consideration of variations in different domains. Characteristic variations between private sector and local government significantly impact on the way ERP implementing activities are carried out. ERP implementation in local governments in developing countries should also take into account the fact that developing countries have limited resources unlike the developed countries. Hence, ERP systems implementation process should be administered differently as suggested by Addo-Tenkorang&Helo (2011).Sommer (2011) state that public administration has characteristics including: cultural, political, and organizational factors that negatively influence successful ERP implementation in local government administration.

Most ERP vendors propose frameworks specific to their ERP solution to simplify the implementation process. Some of the major vendor specific frameworks include: Accelerated SAP (ASAP) by SAP, Application Implementation Method (AIM) by Oracle, Direct Path by PeopleSoft and Dynamic Enterprise Modeler by BAAN (Benders, Batenburg& Van der Blonk, 2006). Vendor specific frameworks coerce client organizations to compromise their core business processes for the sake of conforming to the vendor's prescribed implementing framework; a concept of isomorphism, DiMaggio and Powell (1983).

Implementing Enterprise Information Systems in local governments in developing countries requires a consideration of unique characteristics related to economic, skills and political

challenges. EIS significantly impact of business processes, hence, local government business processes, which are highly constrained; politically and financially require specific ERP implementation considerations to ensure a cost effective and successful implementation of ERP system in developing countries.

## **FINDINGS**

### **i. Context and functions**

Municipalities are instituted by Act of parliament to execute functions of local government within district territory. Functions of a municipality are broadly categorized in three: economic and physical planning for local communities, provided social services to citizenry, and environment sanitary through garbage management. These are clearly stipulated in various government Acts, which are referenced from Local government Act 2017. Municipalities consist of lower administrative units; divisions which are equivalent of sub-county, ward equivalent of a parish, and cell equivalent of village.

### **ii. Major stakeholders**

Central government is one of the major stakeholders, funding 70% of the budget to support decentralized activities. Local citizenry and business community are primary stakeholders who benefit directly from municipality functions. Development partners, both local and international, participate directly or indirectly in various development project.

### **iii. Municipality business processes**

There was no documentation of day to day business processes, though guideline on the activities within the mandate of the municipality are outlined in various Acts. However, key business processes could be identified from the description of major activities. Key business processes include: residents registration, property registration, business

### **iv. Implementing information Systems**

Municipalities don't have IT/IS office or an IT/IS personnel, and have never engaged in implementation of an information system, and are not familiar of any information implementation framework or methodology. Information Technology implementation are carried out by contractor from central government. A focal person is designated to liaise with the outside support on behalf of local information technology users.

### **v. Critical data requirements and challenges**

Execution of municipality functions requires up-to-date data on: residents to deploy government programs effectively, licensable business to correct revenues as mandated by the central government, properties for physical planning and tax collection. Though there is mechanism to collect business data for the purpose of revenue, however most data is obtained from external bodies; incomplete and outdated, hence, unreliable.

### **vi. Cloud based solutions**

Most of municipality leaders are aware of IT/IS trends, benefits and challenges. Though there is an acute lack of IT/IS resources there is a high sense of appreciation of

transformation of service delivery by implementing IT/IS solutions. Though, there is a willingness to attempt deployment of IT/IS solutions that are third party managed like cloud based ERP, readiness and preparation in terms of resources, skills, and policies are lacking.

It is fair and reasonable to conclude that, generally municipalities in Uganda lack IT/IS function with a dedicated IT/IS department, and have no appropriation of IT/IS budget specific to the development of IT/IS infrastructure, resources and skills. IT/IS activities are coordinated by a focal point person. Though all involved municipalities have internet connectivity, they lack Local Area Network (LAN) and access to any electronic information systems rather than Integrated Financial Management Information Systems (IFMIS), managed at central government level. Also, there is no knowledge of Business Process Management concept, which is critical to successfully implement enterprise systems. The municipality context in a developing country like Uganda, require a specific framework of attributes to successfully implement ERP system.

### **CONCEPTUAL FRAMEWORK FOR IMPLEMENTING CLOUD ERP**

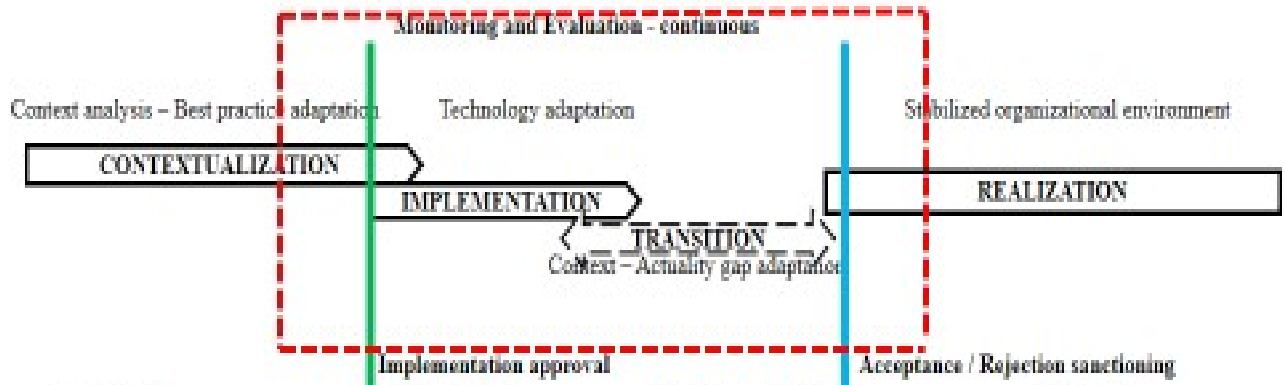
Bitsini (2015) states that the continued growth of ERP adoption in developing countries is accompanied by high failure rates. This is attributed to the complexity of ERP system and misalignment based on ERP inbuilt best practices (Bitsini, 2015). However, a methodology adopted to implement an information system may also result in information system failure. Little work is done to understand ERP implementation framework/methodology in context of local government in developing countries. Most research categorize implementation of enterprise system in three broad phases, and little is explained about the specific activities that should be done to ensure a successful implementation. An exploratory research from the three local government administration at different levels in a developing country show that ERP is a new technology being adopted in a technologically, financially and skills constrained environment.

A conceptual framework that captures the unique characteristics is proposed to include a transitive phase after implementation and before a post implementation phase is actualized. It was recognized that to complete an implementation of a full enterprise system, will all relevant modules, in local government administration could take decades. Due to lack of resources in developing countries, ERP is implemented module by module. Most local government units that have attempted to adopt ERP have implemented only financial module, hence, realization of full benefits are yet to be achieved, and some run the ERP with unresolved errors. In this situation it is difficult to establish a clear cut between implementation and post implementation phases. Failure to recognize this result in budgets that significantly reduce or totally cut off financial resources after implementation. This is a common experience in developing countries where most ERP implementation are donor funded.

A transitional phase need to be consider to allow the stabilization of users' environment; behavior, cultural and skill acquisition. Adoption of ERP lead to a paradigm shift from functional-silo environment to a process – customer centric orientation. This transition phase is critical the stabilization of the organizational and individual culture, and external forces that result from interfaces of various stakeholders. The transition phase is characterized by forward and backward activities as the organization and individuals struggle to strike an equilibrium of

change caused by: processes alignment, policy reviews, new skills demands, budget reallocations, new roles and responsibilities.

**A CONCEPTUAL FRAMEWORK FOR IMPLEMENTING A HOSTED ERP IN LOCAL GOVERNMENT IN A DEVELOPING COUNTRY**



CONTEXT	TECH FIT	BUSINESS FIT	IMPACT
Understanding the context	Technology:	Technology – Organization	Benefits realization
KPI metrix		Assess progress on KPI	KPI measurement (regular)
Resources Mobilization	Connectivity	Fit analysis and design	Process alignment
Policy review	Upgarde	Technology adjustment	Organizational impact assessment
Change management design	Change management	Change management enhancement	Cost – benefit analysis
Understanding domain best practice		Processes alignment	Process alignment
Process alignment			
Skills development	Skills development	Skills enhancement	
Stakeholders chartering			

**Contextualization phase**

The public sectors organizational complexity and structure make ERP implementation more challenging than in private sectors, Dwivedi et al. (2014). Most of the actives in this phase are focused on understanding and preparing enabling environment through policy reviews to support process alignment. Regulations in public sector require a very laborious process to change them. Political influences and interests, resources and skills availability significantly affect activities, listed in the conceptual framework, during the pre-implementation phase. Unlike the private sector where decisions are with a focus on maximizing returns, public sector decisions are highly influenced by political and registrations that are embedded in bureaucratic structures. Lack prior experience and skills in business process analysis and modeling and enterprise systems technology, also significantly affect the planning process and negatively influence the decisions made. Findings revealed that most of public sector information systems fail because of: top

down imposing pressures, political ambitions, financial challenges, unskilled staff and low motivation among the teams at operational levels of administrative structures.

Secondary, using external consultants who are not familiar with day to day challenges in local environment result into presumed challenges and solutions. Understanding local government context is very important; local government domains vary based on the political environment and government models. Hence, domain best practices could not be considered universal. Preparation for implementing an enterprise systems require a well-defined strategy for acquiring adequate financial and non-financial resources to avoid interruptions along the implementation process. In developing economies where donor funding is the major source of financing such huge projects, prior negotiations for long term financing to sustain activities have to be planned well.

Business reengineering, which is fundamental to implementing ERP system, involve overhaul of organizational structures, management systems, job descriptions, skill development, training and the use of ERP (Rajeshwar, 2015). Local government entities are required to comply with a number legislations, hence, a framework specific to local government context is critical to effectively manage structural changes for a successful implementation of ERP system. Managing changes in the way an organization work, job profile, decision making capabilities, and processes integration, which are caused by implementing ERP is complex and if not done properly can lead to ERP failure (Rajeshwar, 2015).

### **Implementation phase**

The complexity of ERP system, and the impact ERP implementation make to business processes, characterize the traditional in-house ERP implementation phase with enormous technological activities including: Hardware and Software installations and configurations; realignment of business processes; attitude and culture change activities; user training. A lot of the resources and commitments are required during this phase. Findings revealed that implementation of information systems similar to ERP systems is a new experience; secondary local government budgets are grossly inadequate to fund enterprise systems implementation. Adopting a cloud ERP system lessen the demand for in-house technological skills; significantly reduce Information Technology resources acquisition budget; distraction caused by the presence external consultants is minimized. Finding indicate that the concept of business process management is not well embraced in developing countries more so in public sector. According to Soja (2012), Infrastructure are significant barriers to ES adoption success.

Implementing ERP system in an organization without prior business process improvement work, lead to a distorted approach that focus on organization – ERP fit rather that ERP – Organization fit approach. Scarcity of BPM research in public sector, more so in developing countries make the implementation of ERP systems very complicated; only 7% of BPM research covering public sector, Houy et al (2010). It is important that local government units in a developing country embark on business process analysis and improvement prior to the ERP implementation phase. In view of this the end of the implementation phase shouldn't be considered as the end of the implementation process, rather, a stage at which critical evaluation of the ERP and Organization Fit should begin. This will enable relevant stakeholders to identify critical technological misfits or errors; review of change management strategy is examined, and tactical enhancement, if need be, are initiated. ERP system implementation is different from traditional information systems

implementation. Traditional information systems implementations don't have the constructs: technological, managerial, operational, strategic, and organizational identified by Al-Mashari et al., (2003).

### **Transition phase**

Findings show that donor funded projects in developing countries are executed within terms and conditions of the donors origin. Local terms and conditions of remunerations and services delivery are usually below the donor's conditions. When donor funding stop, usually at the end of implementation phase, it is difficult to sustain activities at the same level of standards. Lowering standards lead to loss of skilled personnel, causing a failure to realize the intended benefits. A transitive phase will help the local government unit to adjust to local situations; allow a gradual culture change, extend the monitoring and evaluation activities to enable the implementing organization access the success of the implementation.

ERP implementation success shouldn't be measure only in terms of completing the implementing project in time scheduled and budgeted resources; a critical measure of the smooth transition to operationalization of the new system, and achievement of intended business objectives need to be emphasized. Hence, a transition phase is critical to ensure the organization – technology fit.

A blue line on the conceptual framework indicate the point of certainty of the outcome of the implementation in relation to objectives achievement or worst situation where management has to decide to discard the project. It is quite challenging to determine the sustainability, just the point of completion of implementation phase, of a big donor funded project like ERP system in public sector. Constraints in local government administration adversely impact on the sustainability of projects. A well-defined and planned period, transition phase, will provide an opportunity for backward and forward assessment of the ERP system adaptation journey.

The transitioning phase allows stakeholders to assess the progress on the key performance indicator defined in the contextualization phase. Focusing of the compliance testing enable the stakeholders to ascertain the ERP fit into the business processes. To ensure a smooth adaption of the enterprise systems in public sector requires that the enterprise system comply with political, legislation and economic requirements that were identified in the contextualization phase. Data should be corrected on implementation activities to enable the planning of implementation of other modules. All errors need to be corrected during this phase before the contracted technical team disengage from the implementation project.

### **Realization**

In public sector the measure of ERP implementation success has to be against benefits realization in relation to key performance indicators based on efficiency in service delivery, rather that ROI as in private sector. Motivations for service delivery public sector are different the private sector, hence, ERP system implementation success in public sector has to be measured differently. Periodic KPI measurements have to be executed in this phase to collect data required for decision making for further: policy reviews, capacity development, process realignment and enterprise systems upgrade. The realization phase shouldn't be looked at as plan to a finishing line but a structured approach to continuous KPI measurement to ensure a continuous



improvement in service delivery. KPI measurement has to be carried out at departmental level by the department personnel to ensure benefit realization in all departments.

### **Monitoring and Evaluation**

ERP systems are complex systems whose implementation has wide impacts on a recipient organization. It is important that the ERP adoption process in local governments is monitored throughout all stages to ensure that: compliance to regulations is adhered to; adoption activities are progressing on schedule and detect indicators of success or failure; identify factors that account for the progress or constrain progress of activities; measure responses and reactions to adoption activities. The trends in effects and impact of the adoption of ERP system are analyzed to: minimize the risk of adoption partial or total failure; determine the degree of the milestones; reformulate strategies to keep the adoption process on track. Implementation of ERP systems in public sectors in most of developing countries is donor funded, hence, there is a great reliance on donor guidelines. Continuous evaluation of the adoption process help to identify and resolve non-technical issues, like further resources commitment, that may affect the implementation and sustainability of the of ERP system. Implementation of ERP system in developing countries require continuous monitoring and evaluation; risks and constraints to a successful implementation are highly prevalent in developing countries.

Though local governments at municipality level are familiar with Integrated Financial Management Information System (IFMIS), ERP is a new concept to them. Local governments have gone through a number of reforms to improve efficiency in public service delivery. However, at municipality level, Business Process Management concept is not known, and the municipalities participated in the research had never engaged in process analysis and design activity. In view of this, implementation of ERP in local governments need to imbedded monitoring and evaluation activities within ERP implementation process; implementation of ERP system lead to massive process changes. This could be effectively achieved when an Action Research model is adopted, where the core focus is continuously on planning, action and reflection as depicted in Figure 1. This is also important to ensure that the ERP implementation adhere to compliances required by various public sector regulations, impact of political influences are managed, changing requirements are anticipated, and possible failure factors are mitigated at every stage of ERP implementing process .Success of ERP systems depends on when it is measured and that success at one point in time may only be loosely related to success at another point in time (Markus et al., 2000).



Figure 1. Source: A step by step guide to monitoring and evaluation (2014)

## CONCLUSION

This paper presents exploratory focus group findings from local government municipality context in relation to information systems, organized in themes: context and function, major stakeholders, municipality business processes, implementing information systems, critical data requirements and challenges, and cloud based solutions. The paper also discusses existing frameworks/methodologies adopted to implement ERP systems, and unveils limitation of existing frameworks, which include: vendor specificity, private sector oriented, universality of best practices, and lack of consideration of developed country context. On the basis of the research findings, a conceptual framework for implementing a cloud ERP system in lower local government in a developing country is proposed, prescribing contextualization, implementation, transitive, and realization phases, with continuous monitoring and evaluation mechanism. From academic perspective, this paper contributes to ERP implementation literature, and benefits both ERP systems academicians and practitioners interested in information systems in local governments in a developing country. This study also forms a basis for further ERP research in context of a developing country local government, like validation of proposed framework, appropriate cloud ERP architecture, etc. From practical perspective, this research will be beneficial to local government decision makers and ERP implementers by providing them a comprehensive understanding of the critical need to adopt a local government contextualized framework to mitigate failure factors leading to partial or total failure of ERP system implementation, a consequence unbearable in development country context with highly constrained resources. The results can be generalized to small organizations in developing country context.

## References

- A step by step guide to monitoring and evaluation. Version 1.0 Published January 2014. Monitoring and Evaluation for Sustainable Communities' (<http://www.geog.ox.ac.uk/research/technologies/projects/monitoringandevaluation>)
- Al-Mashari, M. and Al-Mudimigh, A. (2003), "ERP Implementation:Lessons From A Case Study", Information Technology & People, Vol. 16 No. 1, 2003, pp. 21-34.
- Alves, M., G. & Matos, A., S. (2011). An Investigation into the Use of ERP Systems in the Public Sector, Journal of Enterprise Resource Planning Studies, Vol 2011

- Bahssas, D.,M., AlBar, A., M., Hoque, R. (2015). The International Technology Management Review, Vol. 5 (2015), No. 2, 72-81
- Baumgartner, T. A., Strong, C. H., & Hensley, L. D. (2002). Conducting and reading research in health and human performance (3rd ed.). New York: McGraw-Hill.
- Bitsini, N. (2015). Investigating ERP Misalignment between ERP Systems and Implementing Organizations in Developing Countries. *Journal of Enterprise Resource Planning Studies* <http://www.ibimapublishing.com/journals/JERPS/jerps.html> Vol. 2015 (2015), Article ID 570821, DOI: 10.5171/2015.570821
- Carutasu, N. &Carutasu, G. (2016). Cloud ERP implementation, Business & Management Journal, A quarterly review, volume 4, issue 1
- Constantin Houy, Peter Fettke, Peter Loos, (2010) "Empirical research in business process management – analysis of an emerging field of research", Business Process Management Journal, Vol. 16 Issue: 4, pp.619-661, <https://doi.org/10.1108/14637151011065946>
- Dwivedi, Y. K., Wastell, D., Laumer, S., Henriksen, H. Z., Myers, M., Bunker, D., ... Srivastava, S. C. (2014). Research on Information Systems Failures and Successes: Status Update and Future Directions. *Information Systems Frontiers*, 17(1), 143–157.
- Hawari, A., &Heeks, R. (2010). Explaining ERP failure in a Developing Country: a Jordanian Case Study. *Journal of Enterprise Information Management*, 23(2), 135–160.
- Helo, P., Anussornnitisarn, P., &Phusavat, K. (2008). Expectation and reality in ERP implementation: consultant and solution provider perspective. *Industrial Management & Data Systems*, 108(8), 1045-1059
- Huang, S. M., Chang, I. C., Li, S. H., & Lin, M. T. (2004). Assessing risk in ERP projects: identify and prioritize the factors. *Industrial management & data systems*, 104(8), 681-688.
- Krueger, R. A., & Casey, M. A. (2000). Focus groups: A practical guide for applied researchers (3rd ed.). Thousand Oaks, CA: Sage.
- Maditinos, D., Chatzoudes, D., &Tsairidis, C. (2011). Factors affecting ERP system implementation effectiveness. *Journal of Enterprise information management*, 25(1), 60-78.
- Markus, M. L., Axline, S., Petrie, D., & Tanis, C. (2000). Learning From Adopters' Experiences with ERP: Problems Encountered and Success Achieved. *Journal of Information Technology*, 15(4), 245–265.
- Morgan, D. L. (1997). Focus groups as qualitative research (2nd ed.). Thousand Oaks, CA: Sage.
- Myers, G. (2006). "Where are you from?": Identifying place. *Journal of Sociolinguistics*, 10, 320–343.
- Onwuegbuzie, A. J., Dickinson, W. B., Leech, N. L., & Zoran, A. G. (2009). A Qualitative Framework for Collecting and Analyzing Data in Focus Group Research. *International Journal of Qualitative Methods*, 8(3)
- Rajeshwar, V. (2015).ERP Implementation Challenges & Critical Organizational Success Factors, *International Journal of Current Engineering and Technology*, Vol.5, No.4
- Ramburn, G., A., Mwalemba, Gwamaka, M., Lisa, S. (2016). "Organizational & knowledge challenges faced during an ERP implementation: The case of a large public sector organization", *CONF-IRM 2016 Proceedings*. 29, <http://aisel.aisnet.org/confirm2016/29>
- Shaul, L., &Tauber, D. (2013). Critical Success Factors in Enterprise Resource Planning Systems: Review of the Last Decade. *ACM Computing Surveys*, 45(4), 1–39.

- Soja, P. (2012). "Determinants of Enterprise System Adoption across the System Lifecycle: Insights from a Transition Economy". *AMCIS 2012 Proceedings*. Paper 4.  
<http://aisel.aisnet.org/amcis2012/proceedings/ICTinGlobalDev/4>
- Weng, F. & Hung, M. (2014). Competition and Challenge on Adopting Cloud ERP, *International Journal of Innovation, Management and Technology*, Vol. 5, No. 4

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

Perpetua MUCHIRI\*<sup>1,2</sup>, Valid MWALUKU<sup>2</sup>, Korir KIPRONOH<sup>2,3</sup>, Nicholas MAKAU<sup>2</sup>, George AMOLO<sup>1,2</sup>

<sup>1</sup>Technical University of Kenya, Department of Physics & Space Sciences, P.O. Box 52428-00200, Nairobi. \*Tel: +254718837440, +254729401249, Email: [pshiroh2015@gmail.com](mailto:pshiroh2015@gmail.com), [georgeamolo862@gmail.com](mailto:georgeamolo862@gmail.com)

<sup>2</sup>Computational Material Science Group, Physics Department, University of Eldoret, P.O. Box 1125- 30100, Eldoret, Kenya. Tel: +254727276933, +254727462626, Email: [vmwatati@yahoo.com](mailto:vmwatati@yahoo.com), [wanimak@yahoo.com](mailto:wanimak@yahoo.com),

<sup>3</sup>Moi University, Physics Department, P.O. Box 3900-30100, Eldoret, Kenya. Tel: +254722157591, Email: [koriro1208@gmail.com](mailto:koriro1208@gmail.com)

### Abstract

Silicon Carbide has become one of the promising materials that can be used for electronic and optical applications. This is as a result of its superior properties among them structural, thermal, chemical, electronic and mechanical. This work reports both the structural such as bond length, lattice parameter and electronic properties of cubic Silicon Carbide (3C). The theoretical calculations were carried out using an ab initio approach based on Density Functional Theory framework using Ultrasoft pseudopotential as implemented in Quantum ESPRESSO computer code. The lattice parameter was found to be overestimated by +0.66% when compared to the experimental value of 8.24 Bohr while the bulk modulus was underestimated by 11.91%. Cubic Silicon Carbide was found to have an indirect band gap of 1.34 eV between W and K and L and W which is underestimated by the Density Functional Theory calculations.

Keywords: Electronic properties, mechanical properties, Density Functional Theory

### 1. Introduction

Polytypism is one of the phenomenons evident in some materials. It exists whereby a compound and elements occur in different crystal structures. The main difference between the different polytypes is the stacking sequence along one direction [1]. One of the materials that has attracted a lot of attention due to this phenomenon is Silicon Carbide (SiC) which form such stable polytypes. Another important aspect of SiC is that it is a known group-iv naturally stable compound. This material is among the prominent systems that exhibits several polytypism. It has more than 200 polytypes and among them is 3C polytype which has attracted more attention due to its favorable electronic properties. SiC is used in microelectronic devices such as high-power and high-temperature applications. However, a deep understanding of the physical properties of SiC is necessary due to technological problems that need to be addressed before the material can be used in the production of electronic devices. [2]. One of the most extreme polytype is zincblende [3] which is the main phase considered in this work. It has pure cubic package with double layers of Si-C in the [111] direction.

Silicon carbide referred to as carborundum consist of silicon and carbon atoms and occurs as the extremely rare mineral moissanite in nature. It is a high quality technical grade non-oxide ceramic possessing wide energy band gap, low density and high thermal conductivity with diverse industrial applications. It possesses exclusive properties like high hardness and strength, high elastic constants, oxidation resistance, high erosion resistance as well as chemical and thermal stability. These properties make SiC a candidate for applications such as high power, high temperature electronic devices, abrasion and cutting applications. It has a variety of polytypes which possess unique structural and electronic properties that attract attention of many researchers. The material has been of immense interest due to its hardness and being a strong ceramic it has other applications in areas requiring high endurance like car brakes, clutches and ceramic plates in bulletproof vests [4,5].

Since the 1980s the interest in the development of wide band gap materials has increased drastically, as their unique physical properties make them very attractive for high-temperature, high-power and high frequency application fields, where the requirements are beyond the limits of Si or GaAs technology. One of the most promising wide band gap semiconductors for such an application is silicon carbide (SiC) with exceptional material properties, like high-electron mobility, high-breakdown field, high saturated electron-drift velocity and high thermal conductivity.

### **The problem**

Having a large bandgap (2.3–6.2 eV), it is much more difficult to thermally excite electrons from the valence band to the conduction band. For example in SiC the probability of thermal excitation of an electron over the band gap is  $10^{-26}$  at room temperature, i.e. there are no thermally excited electrons in the conduction band [15]. In a device this causes the reduction in leakage currents and an increase in thermal stability since intrinsic-type conduction will dominate at higher temperatures (when this happen the devices fail, since there is no longer p-n junction to block the voltages.). The wide band gap is also accompanied by considerably higher breakdown voltage as compared to silicon. This means that for power devices with similar blocking voltage capabilities, the one made of silicon must have about 100 times lower doping level in a 10 times thicker layer, as compared to a SiC device. Thick layers with low doping levels will have high resistance, increasing the power loss and heat generation in the device. Therefore, the use of wide bandgap materials, like SiC, gives the possibility to increase the blocking voltages for high power devices, as well as to make devices smaller and to reduce power losses. It is because of these outstanding properties that much effort has been directed towards understanding and improving the electrical properties of SiC.

### **The objectives**

To determine the:

1. geometrical properties of SiC in the zinc blende phase
2. the electronic properties of SiC in the zinc blende phase

## Literature review

SiC has also been studied by several groups using both experimental and theoretical techniques. Chang et al. [6] using ab initio electronic structure approaches showed that the band gap of SiC with cubic phase decreases with increasing pressure while zinc-blende phase transforms to rocksalt structure at Kbar when under hydrostatic pressure. Molecular Dynamics studies have also shown that the zinc-blende phase of SiC is the most stable at ambient condition through pressure-induced structural deformation[7]. Other studies have shown an existence of high mobility in the conduction band being dominant at high temperatures and low mobility impurity conduction band being dominant at temperatures lower than 70K for heavily doped SiC ( $n \approx 10^{19} \text{ cm}^{-3}$ ) material [8]. The response of turning and twisting has also not been investigated exhaustively in SiC.

## Methodology

The first-principle calculations performed in this work were done in the framework of density functional theory. For the exchange-correlation functional the study employed the generalized gradient approximation (GGA) of Perdew-Berke-Ernzerhof [9]. The geometry optimization was done using the primitive unit cells. Through the Quantum Espresso database, the ultrasoft pseudopotential was taken to optimize the structures. They characterized the interactions occurring between the electrons and ionic core [10]. The valence electron structures for the nonmetal and metal are  $2s^2 2p^2$  for C and  $3s^2 3p^2$  for Si, respectively. The forces and stress tensors were minimized in order to optimize the atomic positions as well as lattice parameters. The calculations converged when the total energies of successive iterations agreed to within  $1 \times 10^{-4}$  Ry in the iterative solution of the Kohn-Sham equations

[11]. The Monkhorst-Pack [12] scheme was applied, and the k-point mesh of the first irreducible Brillouin-zone was used. The scheme ensures that there is an integration of the irreducible region of the zone over a mesh where the special k-points are uniformly spaced though at different sites and coverage.

## Results and discussion

This section reports on the geometrical properties such as bond angles, lattice parameter and bond lengths, bulk moduli as well as electronic properties.

### **Geometrical properties**

In this study, the optimized structure of SiC was obtained using Xcrysden program [13] following rigorous relaxation.

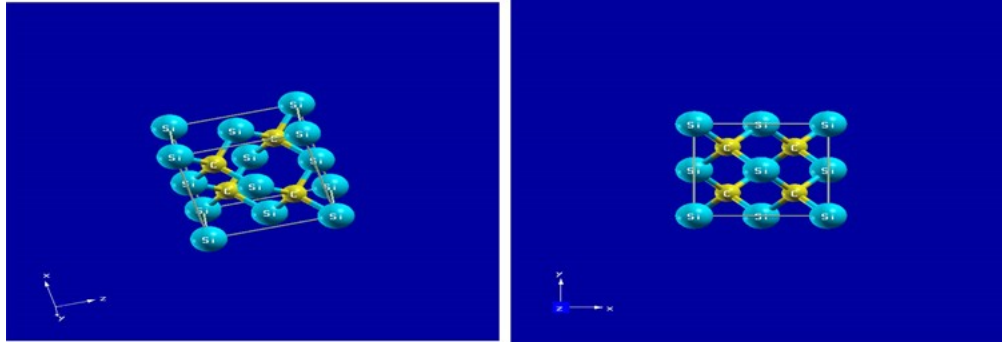


Figure 1: SiC structure in zinc blende phase snapshots. The frame shows xz (L) and yx (R) planes as displayed by Xcrysden. The frame below shows the zy plane

From Fig 1, the bond lengths and the bond angles were determined. The bond angle was  $109.471^\circ$

Table 1: Calculated DFT-GGA Bond lengths, bond angle and lattice parameter of SiC in zinc blende structure.

SiC	Bond angle (Si-C-Si, C-Si-C)	Bond length, Å (Si-C)	Lattice parameter, Å	Lattice parameter, bohrs
This work	$109.471^\circ$	1.9006	4.38	8.2344
Experimental work			4.36 <sup>a</sup>	8.1968
Other works	$109.00^\text{d}$	1.89 <sup>c</sup>	4.34 <sup>b</sup>	8.1592

%deviation

0.66

<sup>a</sup>Reference [18] <sup>b</sup>Reference [14] <sup>c</sup>Reference [15] <sup>d</sup>Reference [16]

The lattice parameter of SiC in zinc blende structure is calculated as the value corresponding to minimum total energy of the entire system at ground state and using the Murnaghan equation to extract the value.



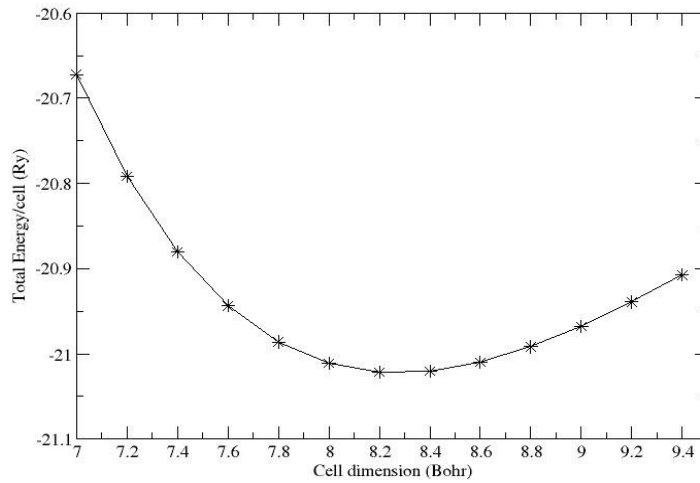


Fig 2: Total energy/cell vs cell dimension

The fitting to this equation of state extract not only the equilibrium lattice parameter but also the bulk modulus and its derivative. By use of GGA for exchange and correlation functional, the lattice parameter was overestimated by 0.66% which reveals a good agreement between the theoretical and experimental value. The bulk modulus for this system was determined to be 198.2 Gpa which is compared to an experimental value of 225 Gpa [17].

### Electronic properties

The calculated electronic band structure and the PDOS in the selected high symmetry points for the first Brillouin zone are presented in Fig 3. They were obtained using the determined equilibrium lattice constant of SiC in this study. The band structure indicate that SiC is a semiconductor.

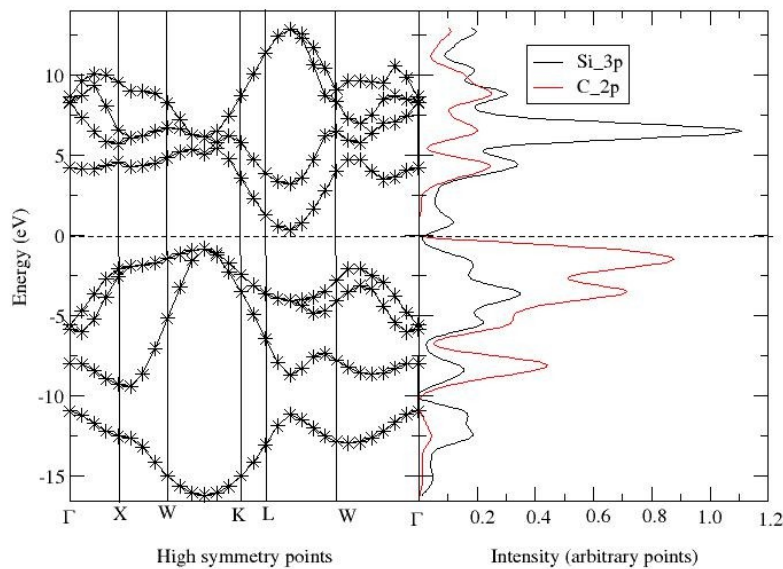


Fig 3: Superimposed graph of band structure and PDOS of SiC in the zinc blende structure.

From Fig 3, the band structure of 3C-SiC shows that it is a semiconductor as the valence band is clearly separated from the conduction band. The system has an indirect band gap of 1.34 eV around W and L whereby VBM is between W and K, while CBM is between L and W high symmetry directions which can be compared to the experimental value of 2.36 eV. This is an underestimation of the band gap which is associated with DFT calculations. The width of CB is found to be 12.32 eV while that of VB is 15.33 eV. From this figure the levels at all symmetry points between gamma and gamma are connected by smooth curve. The Si 3p states are the most dominant states in the conduction band between 0 eV and 12 eV while in the valence band the C 2p are the most predominant between 0 eV and -10 eV. The strong hybridization of the C-2p and Si-3p orbitals contributes to the mechanical properties of the system such as high value of bulk modulus which give rise to the numerous applications of SiC. The small bandgap suggest that SiC is a semiconductor.

### Recommendation

Since DFT underestimates the value of the bandgap, I recommend the use of hybrid functionals

which provide more accurate values or DFT+U which is considerably cheaper compared to hybrid functional calculations. Hybrid functionals are a class of approximations to the exchange–correlation energy functional in density functional theory (DFT) that incorporate a portion of exact exchange from Hartree–Fock theory with exchange and correlation from other sources (ab initio or empirical). The exact exchange energy functional is expressed in terms of the Kohn–Sham orbitals rather than the density, so is termed an implicit density functional. One of the most commonly used is the B3LYP, which stands for Becke, 3-parameter, Lee–Yang–Parr, PBE0, Meta hybrid GGA. Surface calculations would provide more information since a large number of applications for SiC are related to surface properties.

### Conclusion

The thrust of this work was to investigate the geometrical and electronic properties of SiC in the zinc blende crystal phase using DFT. The obtained lattice parameter was found to be overestimated by 0.66% while the band gap was underestimated. In the crystal form it is an indirect bandgap semiconductor which allows it to be used in technological and industrial applications.

### References

- Verma, A. R., & Krishna, P. (1965). Polymorphism and polytypism in crystals. 1966, 341 P. JOHNWILEY AND SONS, INC., 605 THIRD AVENUE, NEW YORK, N. Y. 10016.
- Jepps, N. W. (1983). NW Jepps and TF Page, Prog. Cryst. Growth Charact. 7, 259 (1983). Prog.Cryst. Growth Charact., 7, 259.
- R. S. Ramsdell, Amer. Mineralogist 32, 64 (1947)

- Levinshtein, M. E., et al (2001). John Wiley & Sons.
- Parfenova, I. I. (2004). Substitutional 3d Impurities in Cubic Silicon Carbide. *Semiconductors*, 38(2).
- Chang, K. J., & Cohen, M. L. (1987). Ab initio pseudopotential study of structural and high-pressure properties of SiC. *Physical Review B*, 35(15), 8196.
- Shimojo, F., Ebbsjö, I., Kalia, R. K., Nakano, A., Rino, J. P., & Vashishta, P. (2000). Molecular dynamics simulation of structural transformation in silicon carbide under pressure. *Physical review letters*, 84(15), 3338.
- Kim, J. G., Frenkel, A. C., Liu, H., & Park, R. M. (1994). Growth by molecular beam epitaxy and electrical characterization of Si-doped zinc blende GaN films deposited on  $\beta$ -SiC coated (001) Si substrates. *Applied physics letters*, 65(1), 91-93.
- Perdew, J. P., et al (1996). *Physical review letters*, 77(18), 3865.
- Giannozzi, P., et al (2009). *Journal of Physics: Condensed Matter*, 21(39), 395502.
- 11.Kohn, W., et al (1965). *Physical review*, 140(4A), A1133.
- Monkhorst, H. J., et al (1976). *Physical Review B*, 13(12), 5188.
- Antony Kolkaji. XcrysDen X-Window CRYstalline Structure and DEN-sities. *Computational Matt ter. Sci*, 28:155, 2003.
- Mukherjee, S. (2008). *Can Silicon Carbide Nanotubes be Effective Storage Medium for HydrogenStorage?*. ProQuest.
- Kumar, A., & Aspalli, M. S. (2014). SiC: An advanced semiconductor material for power devices. *International Journal of Research In Engineering and Technology*, 3, 248-252.
- Rino, J. P., Ebbsjö, I., Branicio, P. S., Kalia, R. K., Nakano, A., Shimojo, F., & Vashishta, P. (2004). Short-and intermediate-range structural correlations in amorphous silicon carbide: a molecular dynam-ics study. *Physical Review B*, 70(4), 045207.
- Harrison, W. A. (1980). *Electronic Structure and the Physics of Solids: The Physics of the Chemical Bond*.
- Vashishta, P., Kalia, R. K., Nakano, A., & Rino, J. P. (2007). Interaction potential for silicon car-bide: a molecular dynamics study of elastic constants and vibrational density of states for crystalline and amorphous silicon carbide. *Journal of applied physics*, 101(10), 103515.

## **Computational methods in Materials Science studies**

JamesSIFUNA<sup>1</sup>, George AMOLO<sup>1</sup>, George MANYALI<sup>2</sup>

<sup>1</sup>The Technical University of Kenya, P.O. Box 52428 - 00200Nairobi- Kenya

Tel: +254 725 499 073, Email: [sifunajames@gmail.com](mailto:sifunajames@gmail.com)

Tel: +254 729 401 249, Email: [georgeamolo862@gmail.com](mailto:georgeamolo862@gmail.com)

<sup>2</sup>Masinde Muliro University of Science and Technology,

P.O. Box 190 -50100Kakamega- Kenya

Tel: +254 708 838 421, Email: [georgemanyali@gmail.com](mailto:georgemanyali@gmail.com)

### **Abstract**

Recent years have seen a great improvement in the field of density functional Theory (DFT) calculation of electronic structure and properties of crystalline materials. There are many reasons that explain the current successful application of DFT to materials science related problems: The super speed of computers, software improvements and theory advancement. Based on these three pillars, we the computing scientists were able to understand the ground state properties of cubic scandium trifluoride (ScF<sub>3</sub>) and if need arises, we willalso be able to explore the immense realm of the virtual materials. Indeed, high-throughput techniques for the search of novel crystal structures and the determination of band structure traits have become very popular in the field of computational materials science. Despite these, many challenges are still being faced. Common to all computational materials scientists is the unquenchable thirst for higher speed and better accuracy in DFT calculations. This paper aims to present recent advances in the theory and computational methods in DFT calculation of materials as well as to highlight computational results on structural properties of cubic ScF<sub>3</sub> in comparison to experimental and other theoretical studies. We employed DFT as implemented in the Quantum ESPRESSO computer code. The obtained lattice parameters of between 3.96Å to 4.06Å was in agreement with the experimental lattice parameter of 4.03Å.

**Keywords:** DFT, materials science, computational methods.

### **1. Materials science**

This is a prime field in research that entails the study of materials propertiesand how these properties are determined by a material's composition and structure. Materials science grew out of an amalgam of various fields like solid-state physics, metallurgy and chemistry just but a few(Ohring, 2001). The reason for this fusion of fields is due to the fact that the rich variety of materials properties cannot be understood within the context of any single discipline. With a basic understanding of the origins of properties, materials can be selected and tuned for enormous variety of applications, ranging from structural steels to computer microchips(Gandhi& Thompson, 1992). Materials science is fertile in engineering activities such as electronics and energy conversion among others.The many materials we study and to which materials science is applied, are usually divided into four categories: metals, polymers, semiconductors, and ceramics (Callister & Rethwisch, 2012).The advancement in quantum mechanics has given us a clear view of the behavior of matter and also the ability to guide investigation with theory. Two factors are to be applauded in relation to computational materials

science. The first factor is the exponential growth of computer-processing power. Secondly, the combined effort of Walter Kohn and John Pople, who developed simplified but accurate solutions to the equations of quantum mechanics (Kohn *et al*, 1996). The above factors have made it possible to design new materials from scratch using supercomputers and density functional theory.

The approach above is called high-throughput computational materials design, and the idea is simple: use supercomputers to virtually study hundreds or thousands of chemical compounds at a time, quickly and searching for the best building blocks for a new material, be it a battery electrode, a metal alloy or a new type of semiconductor. Recently we have seen many serious predictions such that we are nearing the end of Moore's law (Joy, 2000). Computational methods involve simulating materials at all sizes; from nanowires to bulk materials, using methods such as density functional theory and molecular dynamics, among others. In this paper, we will give a focus on density functional theory.

### 1.1 Density functional theory (DFT)

The application of density functional theory calculations is rapidly becoming a standard tool for diverse materials modelling problems in materials science (Sholl & Steckel, 2001). This is because DFT is a phenomenally successful approach to finding solutions to the fundamental equation that describes the quantum behaviour of atoms and molecules. The entire application of DFT is built on two fundamental mathematical theorems illustrated by Kohn and Hohenberg and the derivation of a set of equations by Kohn and Sham in the mid-1960s (Casida & Huix-Rotllant, 2012). The first theorem proved by Hohenberg and Kohn is: *The ground-state energy from Schrödinger's equation is a unique functional of the electron density* (Hohenberg, & Kohn, 1964). This theorem implies that there is a mapping between the ground-state wave function and the ground-state electron density. In this first theorem, we learn that the ground state electron density uniquely determines all properties in a system including the energy and the wave function of the ground state. Although Hohenberg-Kohn theorem rigorously proves that a functional of the electron density exists and that it can be used to solve the Schrödinger equation, the theorems say nothing about what the functional actually is (Sholl, & Steckel, 2001).

The second Hohenberg-Kohn theorem defines an important property of the functional: *The electron density that minimises the energy of the overall functional is the true electron density corresponding to the full solution of the Schrödinger equation* (Kohn, 1999). Let it be known that from the second theorem, if the 'true' functional were known, then we could vary the electron density until the energy from the functional is minimised. This variation principle is used in practice with approximate forms of the functional. A more precise way to write down the energy functional as described by the Hohenberg-Kohn second theorem is

$$E[\{\psi_i\}] = E_{\text{known}}[\{\psi_i\}] + E_{\text{XC}}[\{\psi_i\}], \quad (1.1)$$

Here, the functional has been split into two, the  $E_{\text{known}}[\{\psi_i\}]$ , and everything else,  $E_{\text{XC}}$ . The "known" term include the following

$$E_{\text{known}}[\{\psi_i\}] = \frac{\hbar^2}{2m} \sum_i \int \psi_i^* \nabla^2 \psi_i d^3 r + \int V(r) n(r) d^3 r + \frac{e^2}{2} \int \int \frac{n(r)n(r')}{|r-r'|} d^3 r d^3 r' + E_{\text{ion}}, \quad (1.2)$$

The terms on the RHS of *equation 1.2* are electron kinetic energies, the Coulomb interactions between the electron and the nuclei, the Coulomb interactions between the pairs of electrons and the Coulomb interactions between pairs of the nuclei. The term  $E_{\text{XC}}[\{\psi_i\}]$  in *equation 1.1* is the exchange-correlation functional and it is defined to include all the quantum mechanical effects

that are not included in the “known” terms (Wesolowski & Warshel, 1993). Assuming that we can express the as-yet undefined exchange correlation energy functional in a useful manner, it is still difficult to find the minimum energy solution of the total energy functional. This difficulty was solved by Kohn and Sham (Kohn & Sham, 1965), who showed that the task of finding the right electron density can be expressed in a way that involves solving a set of equations in which each equation only involves a single electron. The Kohn-Sham equations have the form

$$\left[ \frac{\hbar^2}{2m} \nabla^2 + V(r) + V_H(r) + V_{XC}(r) \right] \psi_i(r) = \epsilon_i \psi_i(r), \quad (1.3)$$

Equation 1.3 is superficially similar to the time independent nonrelativistic Schrödinger equation (Nelson, 1966) only that it misses the summations that appear in the full Schrödinger equation. This is because the solution to Kohn-Sham equation is a single electron wave function that depend only on three spatial variables  $\psi_i(r)$ . On the LHS of equation 1.3 are the three potentials,  $V$ ,  $V_H$  and  $V_{XC}$ .  $V$  defines the interaction between an electron and the collection of atomic nuclei,  $V_H$  is called the Hartree potential (Slater, 1951) and is defined by

$$V_H(r) = e^2 \int \frac{n(r')}{|r-r'|} d^3r', \quad (1.4)$$

Th is potential describes the Coulomb repulsion between the electron being considered in one of the Kohn-Sham equations and the total electron density defined by all electrons in the problem.  $V_{XC}$  defines the exchange correlation contributions to the single electron equations.

$$V_{XC}(r) = \frac{\delta E_{XC}(r)}{\delta n(r)}, \quad (1.5)$$

$V_{XC}$  can formally be defined as a “functional derivative” of the exchange-correlation energy. From this discussion, the process is circular. To solve the Kohn-Sham equations, we need to know the single electron wave function and to know these wave functions, we must solve the Kohn-Sham equations. To break this circle, the problem is treated iteratively using the following algorithm.

Define an initial, trial electron density,  $n(r)$ .

Solve the Kohn-Sham equations defined using the trial electron density to find the single particle wave functions,  $\psi_i(r)$ .

Calculate the electron density defined by the Kohn-Sham single particle wave functions from step 2,  $n_{KS} = 2 \sum_i \psi_i^*(r) \psi_i(r)$ .

Compare the calculated electron density,  $n_{KS}(r)$ , with the electron density used in solving the Kohn-Sham equations,  $n(r)$ . If this two densities are the same, then this is the ground state electron density and it can be used to compute the total energy. If the two densities are different, then the trial electron density must be updated in some way.

## 1.2 Challenges encountered in DFT calculations

It is important to note that DFT calculations are not exact solutions of the Schrödinger equation. This inexactness arises since the exact functional that Hohenberg-Kohn theorem applies is not known (Koentopp *et al*, 2008). Any time we perform a DFT calculation, there is always an intrinsic uncertainty that exists within the energies calculated with DFT and the true ground-state energies of the Schrödinger equation. We can't estimate the uncertainty apart from making a careful comparison with the experimental measurements. There are many physical situations

where the accuracy of a DFT calculations is good enough to make powerful predictions about the properties of complex materials but in some cases it is not expected to be accurate. We will briefly explain such cases. One such case is that DFT has a limited accuracy in the calculation of electronic excited states. This can be deduced from the Hohenberg-Kohn theorems which only apply to the ground state energy. Another inaccuracy arising from DFT calculations is the underestimation of calculated band gaps in semiconducting and insulating materials. Standard DFT calculations with existing functionals have limited accuracy for band gaps with errors larger than 1 eV being noted when comparing with experimental data. Another situation where DFT calculations will give inaccurate results is associated with the weak van der Waals attractions between atoms and molecules. Van der Waals interactions are a direct result of long range electron correlation and describing these interactions with DFT is challenging. Last but not least is the computational challenge that arise when solving the mathematical problem posed by DFT. Calculations involving a thousand or more atoms are computational expensive and are reserved for very few individuals that are able to develop or access the state of the art computer codes and equally using the world's largest computers.

### **1.3 The computation process in materials science using DFT**

Several packages have been developed in which DFT has been implemented. Right from the open source packages to the commercial packages. One is able to make a choice depending on a number of factors. One such package that is used in this work is the Quantum ESPRESSO code (Giannozzi *et al*, 2009), it falls among the many open source packages and it is written using python programming language (Van , 2007), a high-level programing language. The operation of quantum ESPRESSO package is mainly subdivided into three parts. The input (coding), processing (assembling and interpreting) and the output (build and run). In the case of DFT, input scripts are written using the shell programming language (Sobell & Helmke, 2005) or python programing language. The input script contains information regarding the system under study, i.e the cell parameters and the way the atoms are arranged, the Bravais lattice and any other relevant information on the system. During processing, the assemblers do convert the shell or python codes into machine language, a language that the computer processors understand. The speed of the processing depends on the architecture of the hardware of the computer used. After processing, interpretation and compilation of the programing code is done. In this particular case, python and shell languages are not compiled but are interpreted to check for any errors. If all is fine, the program is then 'build' and run to give the expected results readable by human as useful information.

### **1.4 Computation of Structural properties in cubic ScF<sub>3</sub>**

Scandium Trifluoride (ScF<sub>3</sub>) is a trivalent metal fluoride that belongs to the family of perovskite-type compounds that have the general formula ABX<sub>3</sub>, but in this case, A-Cation site is vacant. The crystal structure of ScF<sub>3</sub> can be cited as ReO<sub>3</sub>-type. Cubic Scandium Trifluoride (ScF<sub>3</sub>) is a material that contracts when exposed to heat. Not many materials are known to behave this way. Such materials have many interesting technological applications yet some of its properties are yet to be fully explored using computational methods. We engaged state-of-the-art *ab initio* methods based on density functional theory (DFT) to study structural and Mechanical properties of ScF<sub>3</sub>. The calculated values of the lattice parameter, atomic volumes, bulk modulus and elastic constants agree with the existing experimental and theoretical data. We did our calculation using different exchange-correlation functionals and plane augmented wave pseudo potentials. This

information will be used to show the predictive nature of DFT as a standard tool in materials science.

## 2. Computational methodology

All the calculations of full energies, optimized geometries were carried out using the quantum ESPRESSO computer code and were performed in the framework of Density Functional Theory (DFT). We did our calculations with five (5) exchange –correlations (XC); the Perdew-Burke-Ernzerhof (PBE) (Perdew *et al*, 1996), the Perdew-Wang-91 functional (PW91) (Perdew *et al*, 1992), the Wu-Cohen functional (WC) (Wu & Cohen, 2006), the enhanced Perdew-Burke-Ernzerhof functional for solids (PBEsol) (Perdew *et al*, 2008) and the Perdew-Zunger functional (PZ) (Perdew & Zunger, 1981). We picked these exchange-correlations since they are computationally efficient and no adjustable parameter was required. The core–valence electron interaction was described by Projector Augmented Wave (PAW) pseudo-potentials from the 0.3.1 version of the library of Dal Corso (Dal Corso, 2014). The crystal structure of ScF<sub>3</sub> was relaxed at 0K and 0GPa. After convergence tests, a cut-off energy of 60 Ry for the plane wave basis was chosen. The Monkhorst-Pack scheme and the Brillouin zone integration was performed at 8x8x8 k-point meshes (Monkhorst & Pack, 2005). Post-processing of data in this paper was done using the Thermo-pw software. We obtained our results by fitting the energy-volume data to the Murnaghan equation of state (Murnaghan, 1944). The energy- volume data were obtained as follows; the volume of the simple cubic structure of ScF<sub>3</sub> was deformed by a single parameter  $\epsilon$  such that the lattice spacing was defined as  $a = a_0(1 + \epsilon)$  where  $a_0$  was the theoretical equilibrium parameter that was extracted from Materials project database (Jain *et al*, 2013). We then fitted to the Murnaghan equation of state a series of total energy values for 21 sets of volumes with  $\epsilon$  ranging from -0.05 to +0.05 in steps of +0.005.

## 3. Computational results in comparison to experimental and other studies.

**Table 1:** Indicating the calculated values of the lattice parameter, Bulk modulus, the first pressure derivative the Volume per atom, minimum energy and the Bond lengths of ScF<sub>3</sub> using different exchange correlations (XC)

Exchange Correlation	Reference	$a_0$ (Å)	Dev  Of $a_0$	B <sub>0</sub> (GPa)	$B'_0$	Volume per atom (Å <sup>3</sup> )	E <sub>0</sub> (Ry)	Bond length Sc-F (Å)
PBE	This work	4.06	0.74%	92.8	4.31	16.67	-335.73	2.03
PBESOL	This work	4.01	0.05%	99.7	4.48	16.15	-332.10	2.01
PW91	This work	4.05	0.49%	93.9	4.31	16.50	-336.62	2.03
PZ	This work	3.96	1.74%	110.2	4.67	15.62	-328.87	1.98
WC	This work	4.01	0.05%	99.4	4.48	16.17	-334.18	2.01
EXPERIMENT	a	4.03	-	88.8		16.36		2.01
PBE	b	4.03	0.00%	-		16.36		2.02
HF-DFT PBE0	b	4.05	0.49%	-		16.61		2.03
LCAO method	b	4.03	0.00%	-		16.36		2.01

<sup>a</sup>Cody *et al*, 2014



<sup>b</sup>(Zhgun *et al*, 2012)

From table 1 above, the lattice parameter in the 5 XCs agreed well with the experimental data and past DFT calculations apart from PBE and PZ which gave a high and low lattice constant. The bond lengths were similar in each simulation and agreed with the experiment. It is generally well known that PBE and PZ predict ground state properties that are higher and lower respectively compared to the other exchange correlation functionals (Wu *et al*, 2004). The lattice constant obtained in PBESOL and WC agrees perfectly to the experiment one thus making DFT a standard tool in material prediction.

### Conclusion

The aim of this work was to illustrate the inclusion of computational methods in materials science. Since many studies have gone a long way to illustrate the effectiveness of DFT as a standard tool in materials modelling, we employed the theory in predicting the ground state properties of cubic ScF<sub>3</sub>. The calculated values of the lattice parameters, bulk modulus and the bond lengths were in agreement with values obtained from other related studies. From our calculation, DFT as a tool was able to complement the experimental approaches as well as predicting other properties like the volume per atom and total energy of cubic ScF<sub>3</sub>. Since the tool worked on our system, it could equally work on a different one since the theory remains unchanged. We state clearly that the future of science lies in simulation due the prowess exhibited by DFT in this study and that of other related scholars.

### Acknowledgment

The Technical University of Kenya is appreciated for laying a platform to this work. The Computational and Theoretical Physics group of Masinde Muliro is applauded for providing resources to carry out this study. Kennedy Wachira of Masinde Muliro University is applauded for the cokeful discussion on this work.

### References

- Callister Jr, W. D., & Rethwisch, D. G. (2012). *Fundamentals of materials science and engineering: an integrated approach*. John Wiley & Sons.
- Casida, M. E., & Huix-Rotllant, M. (2012). Progress in time-dependent density-functional theory. *Annual Review of Physical Chemistry*, 63, 287-323.
- Cody R. Morelock, Leighanne C. Gallington and Angus P. Wilkinson. (2014). Evolution of Negative Thermal Expansion and Phase Transitions in Sc<sub>1-x</sub>Ti<sub>x</sub>F<sub>3</sub>. *American Chemical Society*, 4(2), 1936-1973.
- Dal Corso, A. (2014). Pseudopotentials periodic table: From H to Pu. *Computational Materials Science*, 95, 337-350.
- Gandhi, M. V., & Thompson, B. D. (1992). *Smart materials and structures*. Springer Science & Business Media.

- Hohenberg, P., & Kohn, W. (1964). Inhomogeneous electron gas. *Physical review*, 136(3B), B864.
- Jain, A., Ong, S. P., Hautier, G., Chen, W., Richards, W. D., Dacek, S., ... & Persson, K. A. (2013). Commentary: The Materials Project: A materials genome approach to accelerating materials innovation. *Apl Materials*, 1(1), 011002.
- Joy, B. (2000). Why the future doesn't need us. *Wired magazine*, 8(4), 238-262.
- Koentopp, M., Chang, C., Burke, K., & Car, R. (2008). Density functional calculations of nanoscale conductance. *Journal of Physics: Condensed Matter*, 20(8), 083203.
- Kohn, W. (1999). Nobel Lecture: Electronic structure of matter—wave functions and density functionals. *Reviews of Modern Physics*, 71(5), 1253.
- Kohn, W., & Sham, L. J. (1965). Self-consistent equations including exchange and correlation effects. *Physical review*, 140(4A), A1133.
- Kohn, W., Becke, A. D., & Parr, R. G. (1996). Density functional theory of electronic structure. *The Journal of Physical Chemistry*, 100(31), 12974-12980.
- Monkhorst, H. J., & Pack, J. P. (2005). Special points for Brillouin-zone integrations. *Applied Physics*, 2(1), 5188-5193.
- Murnaghan, F. D. (1944). The compressibility of media under extreme pressures . *Pro-ceedings of the National Academy of Sciences*, 30(9), 244-247.
- Nelson, E. (1966). Derivation of the Schrödinger equation from Newtonian mechanics. *Physical review*, 150(4), 1079.
- Ohring, M. (2001). *Materials science of thin films*. Elsevier.
- P. Giannozzi, S. Baroni, N. Bonini, M. Calandra, R. Car, C. Cavazzoni, D. Ceresoli, G. L. Chiarotti, M. Cococcioni, I. Dabo, A. Dal Corso, S. Fabris, G. Fratesi, S. de Gironcoli, R. Gebauer, U. Gerstmann, C. Gougoussis, A. Kokalj, M. Lazzeri. (2009). QUANTUM ESPRESSO: a modular and open-source software project for quantum simulations of materials. *Journal of Physics: Condensed Matter*, 21, 395502.
- Perdew, J. P., & Zunger, A. (1981). Self-interaction correction to density-functional approximations for many-electron systems. *Physical Review B*, 23(10), 5048.
- Perdew, J. P., Burke, K., & Ernzerhof, M. (1996). Generalized gradient approximation made simple. *Physical review letters*, 77(18), 3865.
- Perdew, J. P., Chevary, J. A., Vosko, S. H., Jackson, K. A., Pederson, M. R., Singh, D. J., & Fiolhais, C. (1992). Atoms, molecules, solids, and surfaces: Applications of the generalized gradient approximation for exchange and correlation. *Physical Review B*, 46(11), 6671.

- Perdew, J. P., Ruzsinszky, A., Csonka, G. I., Vydrov, O. A., Scuseria, G. E., Constantin, L. A., ... & Burke, K. (2008). Restoring the density-gradient expansion for exchange in solids and surfaces. *Physical Review Letters*, 100(13), 136406.
- Sholl, D., & Steckel, J. A. (2001). *Density functional theory: a practical introduction*. John Wiley & Sons.
- Slater, J. C. (1951). A simplification of the Hartree-Fock method. *Physical review*, 81(3), 385.
- Sobell, M. G., & Helmke, M. (2005). *A practical guide to Linux commands, editors, and shell programming*. Prentice Hall Professional Technical Reference.
- Van Rossum, G. (2007). Python Programming Language. In *USENIX Annual Technical Conference*, (p. 36).
- Wesolowski, T. A., & Warshel, A. (1993). Frozen density functional approach for ab initio calculations of solvated molecules. *The Journal of Physical Chemistry*, 97(30), 8050-8053.
- Wu, Z., & Cohen, R. E. (2006). More accurate generalized gradient approximation for solids. *Physical Review B*, 73(23), 235116.
- Wu, Z., Cohen, R. E., & Singh, D. J. (2004). Comparing the weighted density approximation with the LDA and GGA for ground-state properties of ferroelectric perovskites. *Physical Review B*, 70(10), 104112.
- Zhgun, P., Bocharov, D., Piskunov, S., Kuzmin, A., & Purans, J. (2012). Electronic structure of cubic ScF<sub>3</sub> from first-principles calculations. *arXiv preprint arXiv*, 1211, 5697.

## **The Potential of Electronic Data Interchange at Huduma Center Acase of Nakuru County**

Nixon O. Nyambane\* & Moses M. Thiga  
Kabarak University

\*Corresponding author: [nixonnyambane@gmail.com](mailto:nixonnyambane@gmail.com)

### **Introduction**

Huduma Kenya is government initiative that was started in the year 2013 with the aim of transforming public services delivery by providing citizens access to various public services and information to Kenyan citizens. some of these services include; birth certificates, national identity cards, passports, registration of business names, and applications for marriage certificates, drivers' licenses, police abstracts.

Electronic data interchange is the transfer of business information between computer systems in different organization (without human intervention or with minimal human intervention) using widely agreed standards to structure the transaction or message data (Itoh,2005)

The main objective of this research is to examine the potential of electronic data interchange at huduma Kenya, what significance can it enhance on the services delivered at huduma center.

### **Discussion**

Electronic data interchange continues to prove to be a vital technology for the growth of many organizations by lowering costs, improving speed, accuracy and business efficiency. In cost saving the electronic data interchange reduces expenses associated with paper, printing, reproduction, storage, filling, postage and document retrieval or all reduced or eliminate when one switch to EDI transactions and also errors due to illegible faxes, lost orders or incorrectly taken phone orders are eliminated, saving staff valuable time from handling data disputes. With speed Electronic data interchange can speed up business cycle by 61%. Exchange transactions in minutes instead of the days or weeks time of wait time, EDI also improves data quality, delivering at least a 30-40% reduction in transactions with errors-eliminating errors from illegible handwriting, lost faxes/mail and keying and re-keying errors. EDI enables real-time visibility into transactions status, this enables faster decision-making and improved responsiveness to changing customer and market demands, and allows businesses to adopt a demand-driven business model rather than a supply-driven one.

### **The problem**

Huduma center an incentive that was started by the government in the year 2013, offer services that are meant to be offered by different government agencies or departments. In center and the consider government agency. Requests stored at electronic data interchange system at huduma center can also be accessed by consider government agency since they also have electronic data interchange system

### **Current Solution**

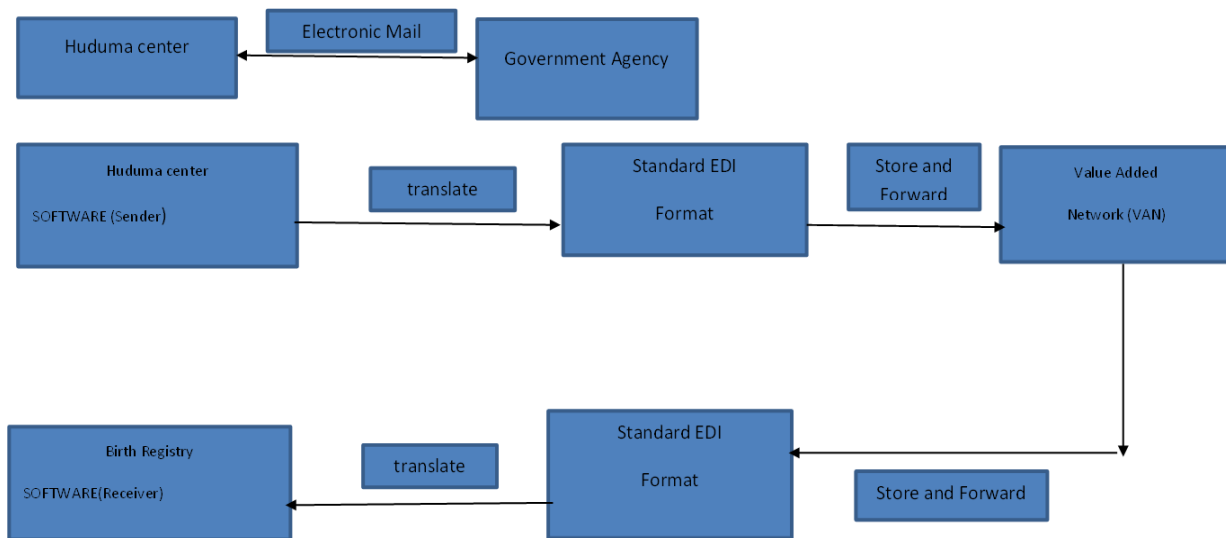
The Government of Kenya has often provided poor services to the citizens as characterized by slow pace of delivery of diverse services, corruption in service provision, loss of critical files,

and bureaucratic nature of a centralized government service infrastructure amongst other challenges (Mwangi, 2015a). Huduma center has in one or another facilitate improvement the service delivery to Kenyan citizens as compared when these services are offered by the government agencies or departments but sometimes the inefficient of systems used at huduma center delays the service delivery for Kenyans like for example the use of electronic mail.

order for huduma center to offer this services, it will need to link with the various government agencies that has data required. But huduma center uses electronic mail as a means of linking with the government agencies for example replacement of national identity card that was stolen. Sometimes Electronic mail can take a lot of time for the consider government agency to respond that is why it normally takes two or more than two weeks to replace a stolen Identity card.

The proposed electronic data interchange system can reduce the delays at huduma center and also improve the accuracy of the service delivered since this kind of the system links huduma

**Problem and proposed solution**



**Benefit of Electronic Data Interchange to Huduma center**

huduma center offer Services that need to be linked with government agencies or departments since the data needed in order to offer the service required is mostly possessed by the government agencies or departments like for example for a customer who needs a birth certificate huduma center will be required to link with birth registry since the department possess records of birth .Electronic data interchange system will facilitate this process by ensuring that there is a link between huduma center and government agency so that the required data can be exchanged.

**Research Methodology**

The study will adopt:

1. The descriptive research design and specifically a case study technique. The case study is an in-depth study on given phenomenon focusing on a particular case (Cooper & Schindler, 2011).

2. The study utilized both quantitative and qualitative research approach. The quantitative research approach is based on statistical analysis in order to depict the relationships between variables.
3. The study will also make use of expert research design since data will be collected from experts who have knowledge on the various systems existing at huduma center.

## **References**

Itoh K (2005), “UN/CEFACT Trade Facilitation and EDI activities”, Hanoi, Vietnam.

Vollmer, Ken. Forrester, “The Future of EDI.” Last modified February 04, 2011.

Kilindini Waterfront Project (2006). “Kilindini Waterfront and Terminal Operating System”. Available at <http://www.kwatos.kpa.co.ke>

Trade facilitation Project (2005). Available at <http://web.worldbank.org>

Mwangi, E. K. (2015). Employees’ perception of determinants of the effectiveness of performance contracting on service delivery in local authorities in Kenya. *Journal of Arts and Humanities*, 2 (3), 36-40.

Cooper, R. D, & Schindler, P. S. (2011). *Business Research Methods* (11<sup>th</sup>Ed.). New York, United States: McGraw-Hill Publications.

## **Security and Privacy of app Permissions on Mobile eServices**

Francis Xavier LOWU

Bugema University, P.O. Box 6529 Kampala, Uganda

Tel: +256 0752818997, Email: [hodct@bugemauniv.com](mailto:hodct@bugemauniv.com), [flowu.x@gmail.com](mailto:flowu.x@gmail.com)

### **Abstract:**

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

**Keywords:** Mobile, Apps, Eservice, Permissions, Android, Security, Privacy

### **1. Introduction**

Mobile eservices use anytime, anywhere service model in both government and private sector. Businesses have become so competitive that they need to find the equally very busy customers without inconveniencing their day-to-day work. Mobile devices that use android apps are many and users prefer them, however other mobile apps running on different mobile based operating systems like iOS are also used. Users of the mobile app eservices give to much private data and information which is captured by these mobile apps. The mobile apps also capture or use some information and data on the mobile devices without the consent of device owners.

While mobile eservices have shown a tremendous growth in the urban regions, it is still a challenge to be implemented in the rural and semi-urban areas. This is due to lack of technical knowledge by the citizens and or users and guarantee from the government on issues of privacy and security. The security concerns such as attacks by hackers, theft of data and information from eservices portals, makes users hesitant. Governments also seem to be hesitant to implement and roll out eservices, through e-Government portals due to fear of cyber attacks. Data Mining remains threatened by the security and privacy gaps in eservices, since mobile eservices need presence of confidentiality, integrity and availability. Mobile services apps that have similar functionalities are likely to have more attacks, forexample

banking eservice apps which are accessed by unsuspecting users on daily basis. Lack of technical knowledge and ability to analyse the app permission requirements has also played a big role in increasing vulnerability to mobile eservice subscribers and users. For example most of the eservices have an attachment to financial transactions. This is due to the increased pay-as-you-go and self-help services, with majority having android mobile apps developed for them. app developer need to rethink of the involvement of users requirements through service providers.

Hezal Lopes et al (2013) assert that, the rate at which mobile malware is growing is alarming. It still remains the biggest threat in the mobile device industry today. The dominance of android mobile device has put it in the path of the hackers who use malware to attach mobile devices. The largest market of mobile device users today is in Africa, and this makes it an opportunity and return in investment for malware professional to attack. Training, sensitization by mobile telecommunication company and sell of devices with malware protection software can reduce the risks of being attached. Android mobile platform normally warn users before they install mobile apps. This is to help them make decisions on whether to continue installing the app or not. However most of the users either ignore or do not understand the implication of the app permissions.

## **2. The Problem**

Private and public sector services today have adopted the use of mobile eservice model to provide self-help spot-on services. Such services require the use of mobile device such as, android mobile devices and installation of the mobile eservice app upon submission of relevant information and data about the user and device. Data and information submitted via app permissions policy infringes on the security and privacy of users of mobile eservices. With increasing use of data analytics due to availability of too much data and information of unsuspecting mobile android devices, mobile app eservices users doubt the intention of app permissions submitted during installation for usage of the eservice apps. Politics and businesses have continuously used the collected data without the knowledge of the users for campaigns, business analytics and further for competitive advantage between business competitors. This has put privacy and security of mobile app eservice users in open to vulnerabilities without their knowledge.

## **3. Objectives**

The use of eservices today can not be avoided, as most Banks, higher institution of learning, health organization among others have developed android apps that can directly be downloaded from Google play store.

This paper presents concerns on the security and privacy of app permissions on mobile eservices with the following objectives.

1. To identify the security and privacy lapses on mobile eservices and how they relate to app permission policy of android mobile devices,
2. To propose a framework for eservices based on apps permission and user involvement in their development
3. To discuss and analyze the security and privacy of each app permissions based on the use of mobile eservices.



#### **4. Literature Review**

Hezal et al (2013) studied four subjects of security, security of operating systems on mobile devices, security of mobile devices, mobile database security and security of mobile network. They acknowledge that smart phone and other mobile devices do not have pre-installed security software, which gives opportunity to cyber attackers to access the mobile devices. There is no installed security softwares such as firewalls, antivirus on the mobile devices. Further that the operating system security model of android supports the android based application distribution model, such as permissions which cannot be changed after installation of the application. However their work did not concentrate on the effect the permissions can incur on the unsuspecting users. Most of the users have no ability to evaluate permissions requested by the apps.

Jing et al (2015) identified personal information privacy, monetary risks and device stability and availability risks. "The convenience of smartphones is undeniable. But, along with that convenience comes new risks in terms of security and privacy. Smartphones contain an unprecedented amount of personal and often sensitive data including contacts, call logs, browsing history, personal photos, financial information, and personal messages. Moreover, with advanced sensors such as Global Positioning Systems (GPSs), cameras, and microphones, smartphones are capable of fine grained tracking and monitoring of a person's movements, communications, and surroundings. Thus, although smartphone apps can enable rich new functionality, they also pose risks to the personal privacy and security of smartphone users. Effective risk communication mechanisms are critical for helping users make safe and informed decisions regarding the apps that they install on their mobile devices." Jing et al (2015).

Milda et al (2017) as technology evolves, users now face different challenges, mobile devices have evolved to become a powerful tool that is connected to the internet and also cheap enough to be available to a large population of users that may be unable to afford a laptop and broadband service.

According to AVast Internet security report 2017, reveals that there is an increase in attacks that target Android smartphones and tablets. This raised to 40% in the second quarter of 2017. To address the threat, Avast upgraded its Avast mobile security and Antivirus and AVG Antivirus mobile apps to combat the threat. The top three major threats that were listed are:

- **Rooters:** These Rooters request the root access of a smartphone or sometimes use exploits and obtain the root access. When they gain control of the device, spying on the user starts and it may result in stealing information from the user.
- **Fake apps:** There are many which are illegitimate apps that pose as real ones in order to attract downloads and expose users to advertisements, hence attacking them.
- **Downloaders:** Most devices have Downloaders or droppers which use social engineering tactics to trick victims into installing more malicious apps. The Droppers also typically show full-screen ads, even outside of the app itself. These ads are not just annoying, but are often linked to suspicious sites which steal data.

However the AVast Internet security report 2017 says that users can control the app online, activate a siren if the phone has been stolen, remotely adjust settings and set custom screen messages, using;

- **App Permissions:** This help and allows the user to understand which apps installed on their phone have which permissions and what information they can access.  
However most of the users do not bother so long as the app has installed. They just delete the app in case it's not liked.
- **Wifi Speed Test:** Checks the download and upload speed of the Wi-Fi network users are connected to. This helps the attackers how much time they will use to attack successfully. Slow internet access is not good for attackers.
- **Call Blocker:** this gives the users options to block unknown callers or send them directly to voicemail. This feature has been optimized for users to not only block numbers stored in the address book but also all unknown, and hidden numbers.
- **Safe Clean:** This cleans residual data and caches to improve smartphone speed and performance.

According to Esmeralda (2017) security concern is key to mobile device management strategy today, where what the users find as convenient also becomes convenient to the attackers. The study focused on human factor as the weakest point in the security of mobile devices. The contribution of users to smartphone threats and reducing the risks brought about by the smartphones was the basis of the research.

Based on work by Adrienne et al (2011), Smartphone and browser operating systems provide development platform that support different markets to thrive on third part applications. Users get security risks from the third party applications, implying that some of the third party authors are malicious, due to their expertise in security vulnerabilities. To protect users from attack and threats due to third party codes and applications, app permission controls are used by modern app platforms to control access to relevant parts of security and privacy of a user.

## 5. Methodology

To achieve the objectives of this study, Google play store was used to identify the different android based mobile eservice apps. The data collection goal was to identify as many mobile eservices app permissions as possible. Each mobile eservices app identified was matched with its permissions and put in a relational table set. Different types of permissions were identified and grouped. there are permissions that have risk privacy of mobile users and there those that risk the security of users more.

### *Identification of Security and Privacy Lapse*

A group of three mobile eservices areas were identified and each group had different mobile eservice apps under it. These included Banking apps, eHealth & Life Insurance apps and Bill payment apps. The mobile apps that were identified under mobile banking group were; Eazzy Banking for Equity Bank, Standard/Stanbic Bank app, EcoBank Banking app, all of them had same requests such as contacts, location and others app permission. Almost all big Banks and telecom mobile network apps in the region have at least an app to be accessed by the users. This makes the users vulnerable in all directions.

As shown, in *Table 1*, each app was matched with the permissions. There are permissions that are mandatory to each app, more so for the apps that give the same services,

for example Banking apps. Digits 1 and 0 were used in *Table 1* to show that which permissions hold for a respective app or does not hold respectively.

*Table 1: Mobile Eservices and Permission that infringe on Privacy and Security*

MOBILE ESERVICES	MANDATORY APP PERMISSIONS										
	Contact	Locations	Photo/Media/Files	Identity	Storage	Phone Calls	Device ID & Call Info	SMS	WiFi	Microphone	Camera
Banking Apps											
• Stanbic	1	1	1	0	1	0	1	0	0	0	1
• EassyPay	1	1	1	0	1	0	1	0	0	0	1
• AirtelM'ney	1	1	1	1	1	1	1	1	1	1	1
• MyMTN	1	1	1	1	1	1	1	1	1	1	1
• EcoBank	1	1	1	1	1	1	1	1	1	1	1
• KCB	1	1	1	1	1	1	1	1	1	1	1
• CenteMobile	1	1	1	1	1	1	1	1	1	1	1
• MPesa	1	1	1	1	1	1	1	1	1	1	1
• Bankclays	1	1	1	1	1	0	1	0	0	0	1
• EazzyEqui	1	1	1	0	1	1	1	1	1	0	1
eHealth & Life Ins											
• Weight	1	1	1	1	1	1	1	1	1	1	1
• Nutrition	1	1	1	1	1	1	1	1	1	1	1
• FWDInsura	1	1	1	1	1	1	1	1	1	1	1
• NSSFGO	1	1	1	1	1	0	1	1	0	1	1
Bill Payments											
• Water	0	0	1	0	1	0	0	0	1	1	1
• TV	1	1	1	1	1	1	1	1	1	1	1
• Electricity/U	1	1	1	1	1	1	1	1	1	1	1
• meme	1	1	1	1	1	1	1	1	1	1	1

Each group was put in a dataset to find out which mobile app permission was mostly valued by the app developers and service providers. Mobile eservice app users have less permissions and this makes them be used without objection.

*Table 2:* shows that most eservice providers require contacts, locations, access to photos, storage, device ID and Cameras, yet these are key to the privacy of individual users.

Table 2: Mobile Eservice Groups and Frequency

MOBILE ESERVICES GROUPS	FREQUENCY PER APP PERMISSION										
	Contacts	Locations	Photo/Media/Files	Identity	Storage	Phone Calls	Device ID & Call Info	SMS	WiFi	Microphone	Camera
Banking Apps	10	10	10	7	10	7	10	7	7	6	10
eHealth & Life Ins	4	4	4	4	4	3	4	4	3	4	4
Bill Payments	3	3	4	3	4	3	3	3	4	4	4

*Cyber Attack Prune app Permissions*

To identify cyber attack prune permissions, the researcher looked at permissions that are linked directly to Internet service providers to contact or access the user through phones calls. These and others expose the mobile service users greatly. The majors ones that had similarity in all apps included;

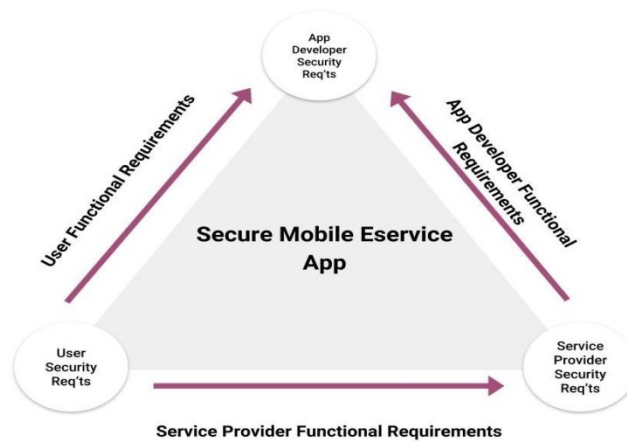
Table 3: App Permission Security Lapses

Permission Type	Security Lapse due to Permission
Receive data from Internet	This may involve malware and viruses
View network connections	Knowing the network connection of the user
	may also compromise information and connectivity to sensitive NODES
Disable your screen lock	this may come with Denial of services attacks were the owner of the mobile device may not access his/her information/contacts
Run at startup	It's always very difficult to detect malware that run at startup. They seem like app programmes
Prevent device from sleeping	This may let you starting clicking on everything that pops up. Which may be installed on your device.
Modify system settings	Most of the time users take long to modify settings from the default setting when a new device is acquired. Accepting modification by apps may be dangerous. They can restore to

	the known defaults once you had changed
View network connections	This will expose the use to know which network you are using. While some may be for data loading purposes, it may still be compromised.
Full network access	Okay,, but with high speed connectivity attack can occur very fast.Usually if the
Read Google service configuration	This will always target Google email contacts and Google drive content.
Access downloads manager	makes downloads faster to minimize detection. Which may be dangerous for users.
Download files without notification	Files downloaded without notification can be very dangerous. Apps are supposed to be installed for eservices. So any installation needs the knowledge of the user,.

All these permissions are dangerous as far as security of mobile e service users is concerned. The app developers and mobile service providers need to get a common understanding on how to develop the apps. Requirements of App developers was identified along side the user mobile eservice app security expectations. Six categories of functional and security requirements were identified to help in the design of the framework to meet objective two of the study. These included: *App Functional Requirements, User Functional Requirements, Service Provider Functional Requirements, App Security requirements, User Security Requirements and Service Provider Security requirements.*

*Proposed Framework*



*Figure 1: Secure Mobile Eservice App Development Framework*

Figure 1 shows the proposed framework that involves all stakeholders, mobile users, eservice providers and the app developers in the process of developing eservice mobile apps. User consultation is required from service providers. This makes it easy to adopt the user functional requirements in the design processes. Service provider functional requirements are normally business oriented and they tend to have coincidence with the user security requirements. Since each entity understands their security requirements better

## 6. Results

Figure 2 show that mobile eservice app permissions by frequency.

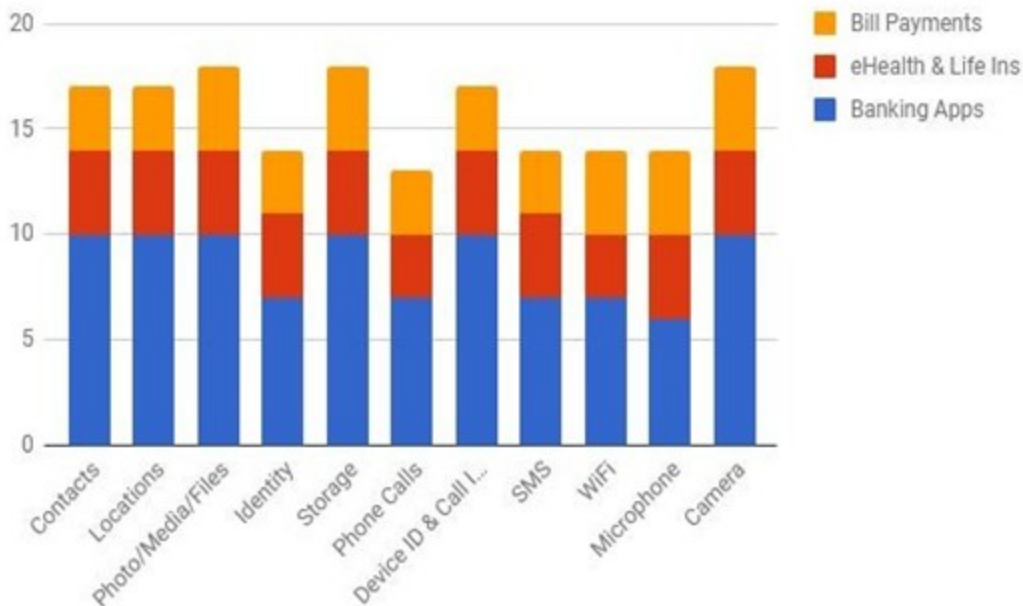


Figure 2: Frequency of Mobile Eservice Permissions

According to the graph here most of the apps require contacts from the user. This helps them to easily contact them in marketing. By using the contacts of the person without his/her consent is depriving them of the privacy. More messages will be sent frequently to the users.

Location also is required by most of the eservice apps. While this may be okay to some extent, by knowing the location of the target it becomes easy to attack the person. SO location is a security threat.

Photo and files of users contact information such as profiles of the person. This is both insecure and for privacy it becomes tricky for the person whose photo is taken by each app installed.

Storage space is normally got to scan through your device to find out if more apps can be installed. Mobile devices have limited space and therefore over usage of the space may make the device slow and this becomes problem to fast access or stop it in case of detection of malware tendencies.

Another permission that is liked by most eservice apps is the camera. However they are less security threat associated by it on a personal usage. However when someone takes your picture and puts it on a profile somewhere without your knowledge it becomes a privacy issue. The study as shown in the Chart above shows that most apps also identity, phone calls, SMS send and microphone which may equally be security and privacy breach for the service users.

## 7. Recommendations and Area for Further Study

In this study recommendation is such that; most of the users of mobile eservices show be able to take their time and read the permissions before installation of the app. Also the eservice app developers should involve the users to find out their function requirements alongside those of

the eservice providers. By understanding the functional requirements of the users through the service providers makes it easy to develop an app that will be having security requirements of users and service providers.

#### *Area for Future Study*

I hope to examine how cloud app permissions relate to mobile based app permissions. With interest on the security of Infrastructure as a service (IaaS), Software as a Service (SaaS) and platform as a service (PaaS).

#### **Conclusion**

This paper has evaluated the privacy and security of app permission on mobile eservice users. This study also analysed that the apps installed by the mobile eservices users requires installed based on similar permissions. The Researcher also found out that the permission that are required are those which infringe on the privacy of the users. In the study the eservices where grouped based on the service that are used most by the mobile eservice. Three groups were created, Banking apps, ehealth and life insurance apps, ebilling appsgroup. Most of these app groups had similarity in the app permissions requested.

A framework was developed to propose how users functional requirements can be included during development. In the frame developed its proposed that if all users have their functional requirements through the eservice provide and they also submit their functional requirements it becomes easy for the app developers to cater for the security requirements of the users.

#### **References**

- Esmeralda, K. (2017). Smartphone Security Threats. Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Hungary. *Management, Enterprise and Benchmarking in the 21st Century Budapest*.
- Milda, P., Ali, D., Gregory, E. (2017). Mobile Phone Forensics: An Investigative Framework Based On User Impulsivity And Secure Collaboration Errors. Pg. 79-89, *Contemporary Digital Forensic Investigations Of Cloud And Mobile Applications. School of Computing, Science and Engineering, University of Salford-United Kingdom*
- Jing, C., Christopher, S., Gates, Z. J., Ninghui, L., Proctor, Ting. (2015). Dimensions Of Risk In Mobile Applications: A User Study.
- Hezal, L., Rahul, L.(2013). Comparative Analysis Of Mobile Security Threats And Solution. *Department of Computer Engineering, Mumbai University, Universal College of Engineering. Int. Journal of Engineering Research and Application* 3(5) 499-502.
- Adrienne, P., Felt, K, G., David, W. (2011). The Effectiveness of Application Permissions. *University of California, Berkeley. Proc. of the USENIX Conference on Web Application Development*.
- Ondrej, V. (2017). Avast cyber security predictions for 2017. Redwood City, California, September 11, 2017  
<https://press.avast.com/avast-reports-40-increase-in-mobile-cyberattacks>.



Muhammad, I., Narseo, V., Suranga, S., Mohamed, K., Vern, P.(2016). An Analysis Of The Privacy And Security Risks Of Android Vpn Permission-Enabled Apps. *Imc 2016, November 14-16, 2016, Santa Monica, CA, USA, ACM. ISBN 978-1-4503-4526-*

Primal, W., Arjun, B., Ashkan, H., Serge, E., David, W., and Konstantin, B.(2013). Android Permissions Remystified: A Field Study On Contextual Integrity. *University Of British Columbia, Vancouver, Canada.*

## **RETSA - Real Time Security Alert**

Ronald YATOR,  
P.O. Box 0701621998-20157, Kabarak, Nakuru, Kenya  
Tel: +254 701 621 998, Email: ronald.yator@gmail.com

### **Abstract**

Insecurity is a major challenge in our current world today. Millions of shillings and property has been lost, many lives has been lost due to insecurity. It is high time to embrace innovation and invention of ways to curb the societal problems like this. That is why there is need to come up with faster security alert systems. This innovation is alert system that notifies the owner or users on an illegal access to their property. The system ensures the property access points are secured with active detectors that signal the main system to alert the owner of illegal access. Therefore ensuring that the owner can monitor his property wherever he or she is e.g. outside country, outside the locality. Due to this challenge the (RETSA – Real Time Security Alert) system that notifies the owner or users on an illegal access to their property was developed. The system ensures the property access points are secured with active detectors that signal the main system – (RETSA) to alert the owner of illegal access. Therefore ensuring that the owner can monitor his property wherever he or she is e.g. outside country, outside the locality.

**Keywords:** RETSA, Detectors, Signal, Security, Alert.

### **1. Introduction**

This is a system that is designed to work as security problem solution. The system allows the owner of the property or person in charge to get notification upon His or Her property Access without Authority. The notification is received by the owners' phone/person in charge phone. The background information of this invention is as follows: The General Concept that lead to birth of this invention came through many experiments and assumptions after an increase of a security challenge in Kenya at most.

The experiments and assumption started in 28<sup>th</sup> September, 2012 after a huge increase of Insecurity in Polyview Estate in Kisumu City in Kenya where I stayed with my Brother Josephat Yator and His Family. On thinking on how to solve the problem, Alarm installation could come in to my Mind. After that successful trial on the experiments, I took a step in developing my concept. And through advancement of it, lead to birth of many devices using the same concept to enable them work and enable them solve security problems in different fields. The invention gives a wider field of application industrially.

Its Technical field is Information Communication Technology in that it allows Network Connectivity involvement issue and Communication Device components to solve security problem. The principle uses as an information and Communication technology invention is to be applied on Access points of; Vehicle, Domestic Houses / Commercial Buildings, Financial institutions as well as Industries and Factories, including the Cow shed in areas affected by cattle rustling so as to provide Notifications in an Unauthorized Access, to the owner or person in charge within a shortest time possible.

### **2. The problem**

Currently many existing systems do not notify the owner on unauthorized access to their property immediately. This is because most systems send the notification to the emails indicating all information of security status. Other systems send data of security status to an online synchronized system thus compelling the owner to login to the site creating a waste of time for response. That is why I came up with the system to solve this by sending alert to a mobile phone via short message service popularly known as SMS.

### **3. Objectives**

#### **3.1 The main objective**

The main objective of this system is to alert the owner or user on illegal access to property on time.

#### **3.2 Specific objectives**

The specific objectives of the system is to reduce the crimes rate in Kenya and the world at large, to create thousands of jobs to thousands of technicians and installers, to safeguard property and livestock in cattle rustling areas and people lives.

### **4. Literature review**

There are some of the security systems that exist, Examples of this are Biometric locks, key code locks and CCTV Systems. There are systems that exist but are more complex. That is if you were to monitor your property accesses, it will take you more time to do so. Take a case of biometrics, when an intruder bypasses the room via a window, the owner won't be able to notice but later only to realize that something wrong is going on or a personal electronics is missing. This RETSA system will be much simple to make the users maneuver it. So it's all complex security systems with lapse and thus the reason for coming up with this security systems to curb these challenges.

This challenges has led to coming up with this system to provide an excellent system capable of sending alert in less than a minute, the system needs a simple power source of 5 voltages, user friendly system capable of meeting and handling with ease challenges faced by the current system. The purpose of this project is to identify the effect that the other systems has on insecurity trends. In CCTV, It is tedious to follow the channels while working to know who entered your house or room via the internet protocol cameras. RETSA system will solve many challenges by ensuring that the owner is notified at the right time to make a response. In addition the system is able to notify unlimited number of users or co-owners thus more effective than current systems.

### **5. Methodology**

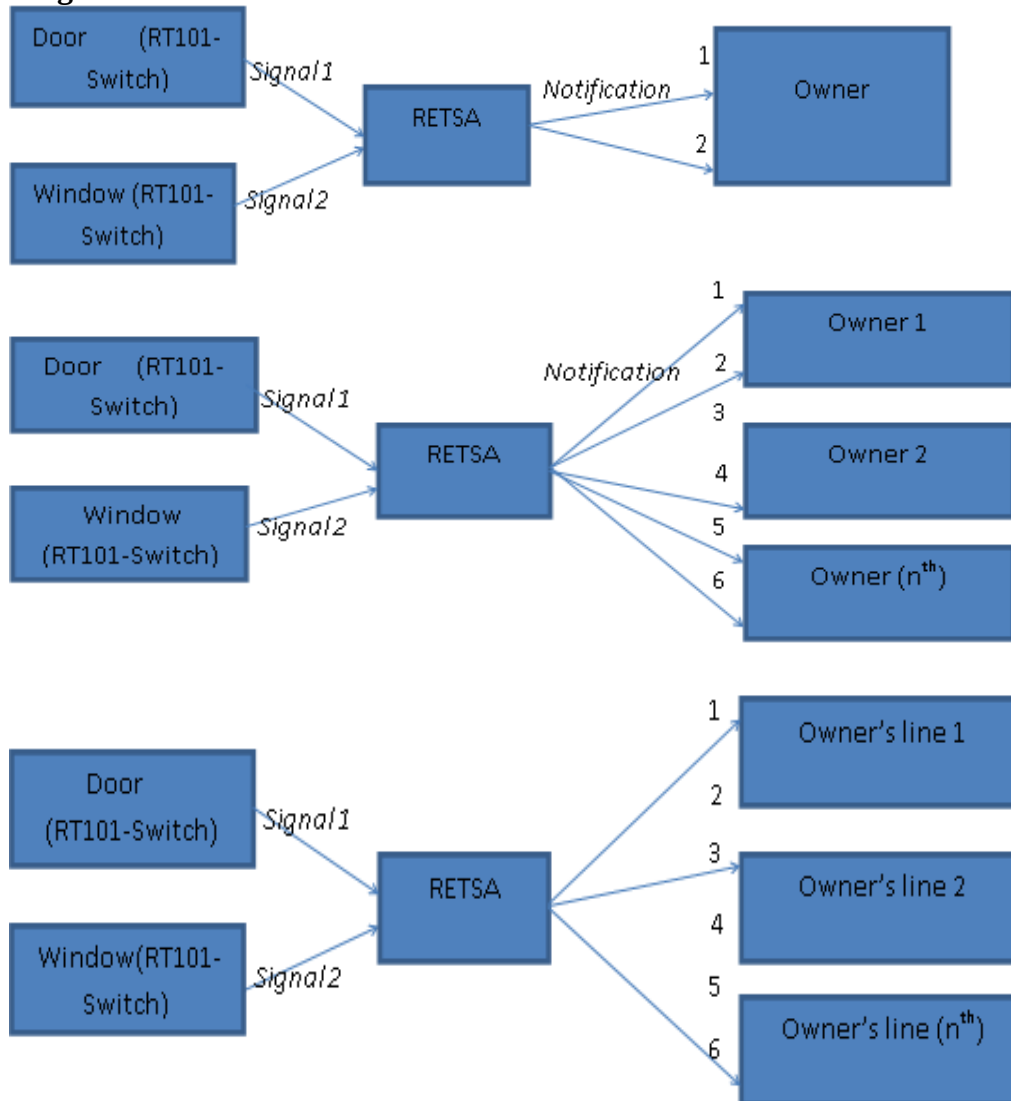
The use of questionnaires allows the analysts to collect facts from large number of people while maintaining uniform responses. Both closed and open questionnaires are to be used to obtain mainly qualitative responses from the friends and the staffs. Open ended questionnaires will be used to give a chance for the respondent to give an opinion and to give useful insight to the problem.

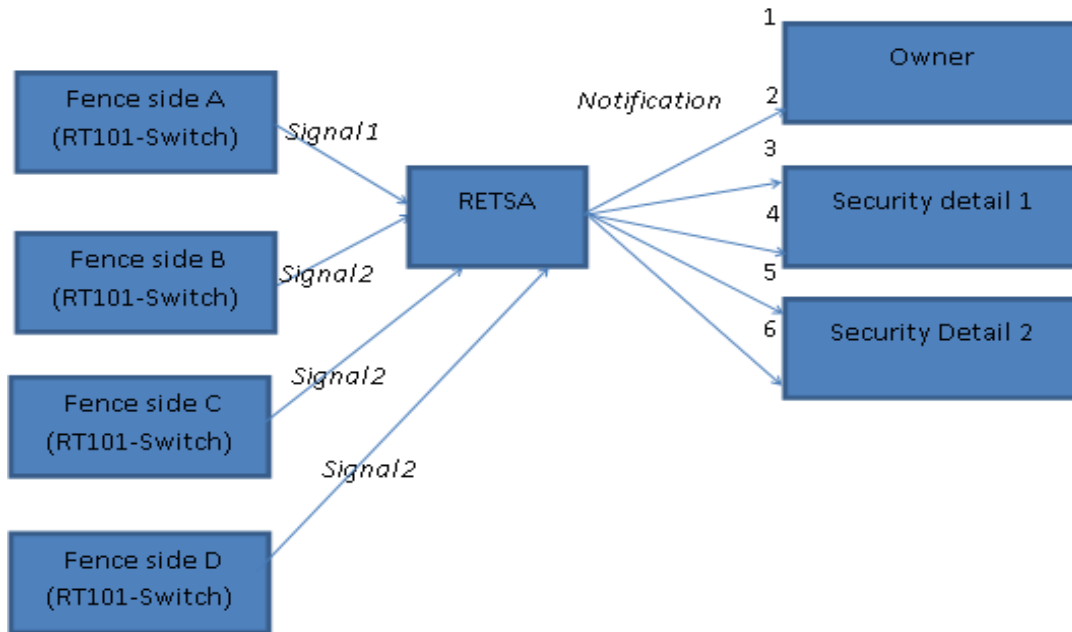
In observation method of data collection the researcher visits the proposed system and observes, records the flow of activities interested in. Observation will therefore bring more insight on how the manual system works.

### **6. Results**

This security system proves to be more effective than existing systems. It sends alert in less than a minute and also able to notify more than one person. RETSA is able to be implemented across many areas like; vehicle, homes, cow sheds, electronics and general plot fencing.

### Diagrams





### Recommendations and areas for further study

The national and county government, willing sponsors, partners and Kabarak University are urged to fully support and embrace this innovation to its full implementation like the RETSA system innovation. This will encourage students and innovators to innovate and invent thus improving livelihoods and one of the big four agenda of the government majorly industrialization. The areas for further study is; electronics and C programming to improve the whole system.

### Conclusion

The developed system should be implemented for it meets the standards of security systems required in this current world and eliminates the limitations of the existing systems thus ensuring the security alert received within a shorter time than existing systems.

## The Exponentially Modified Gaussian Function as a Tool for Deconvolution of Astroparticle Physics Data

Livingstone OCHILO<sup>1</sup>

<sup>1</sup>JOUST, P.O. Box 210, Bondo, 40601, Kenya

Tel: +254 0706 550 243, Email: livingstone.ochilo@gmail.com

### Abstract:

In the period 2004 – 2012, the Pierre Auger Observatory has recorded more than two million of ultra-high energy cosmic rays. In seeking to interpret the data recorded for the events, it is necessary to simulate the interaction of primary cosmic rays with the atmosphere. One of the software that is available for this kind of simulation is CONEX. In this study, CONEX is used to simulate various compositions of primary cosmic rays, whose interactions with the atmosphere result in air showers, with a distribution of depths of shower maximum ( $X_{max}$ ), which is treated as the true distribution. Smearing this distribution with a known  $\sigma$  gives the “measured” distribution. By using the Exponentially Modified Gaussian (EMG) function, we have obtained deconvoluted distribution which is generally in good agreement with the original distribution.

**Keywords:** Ultra-High Energy Cosmic rays, air shower, Exponentially Modified Gaussian.

### 1. Introduction

As is typical of astroparticle physics experiments, the Pierre Auger observatory in Argentina has collected a large amount of data on the most energetic cosmic rays, referred to as Ultra-High Energy Cosmic Rays (UHECR) from 2004 to 2012 (Aab, *et al.*, 2014). The total number of events and the quality cuts that have been applied to them is given in Table 1.

Table 1: Summary of the number of events remaining after the application of event selection criteria to the Auger data (Aab, *et al.*, 2014). The selection efficiency in each case is calculated relative to the previous cut.

Cut	Events	Efficiency (%)
<i>Pre-selection</i>		
air shower candidates	2573713	-
hardware status	1920584	74.6
aerosols	1569645	81.7
hybrid geometry	564324	35.9
profile reconstruction	539960	95.6
clouds	432312	80.1
$E > 10^{17.8}$ eV	111194	25.7
<i>quality and fiducial selection</i>		
P(hybrid)	105749	95.1
Xmax observed	73361	69.4
quality cuts	58305	79.5
fiducial field of view	21125	36.2
profile cuts	19947	94.4

Part of the data that has been collected include the energy of the cosmic rays impinging the observatory as a function of the atmospheric depth at which the resulting cascade of particles, called an air shower, reaches its maximum in terms of both the number of particles present and the energy deposited by the particles. The mean of such depths is normally symbolized as  $\langle X_{\max} \rangle$ . One of the fundamental physics questions that the Pierre Auger experiment seeks to unravel is the composition of cosmic rays arriving at the Earth. This can potentially be done if it can be possible to associate an observed depth of shower maximum and energy with a given particle. However, the depth of a shower maximum depends not only on the energy of the particle, but also its mass. By simulating a shower similar to the one detected by a detector, it is possible to estimate the composition of the primary particles which produced the shower in the first place.

The software CONEX (Bergmann, *et al.*, 2007) and the hadronic interaction model EPOS-LHC (T. Pierog, *et al.*) have been developed and expanded over the years for the simulation of air showers. Using CONEX code, with EPOS-LHC as the interaction model, air showers composed of different primary cosmic ray particles at different energies can be simulated. The development of the shower can then be studied, including the final particles reaching the ground.

The exponentially modified gaussian function (EMG) is defined as (Grushka, 1972):

$$f(x; \mu, \sigma, \lambda, \beta) = \beta \frac{\lambda}{2} e^{\frac{\lambda}{2}(\mu + \lambda\sigma^2 - 2x)} \operatorname{erfc}\left(\frac{\mu + \lambda\sigma^2 - x}{\sqrt{2}\sigma}\right) \quad (1)$$

where  $\operatorname{erfc}$  is the complimentary error function defined as  $\operatorname{erfc}(x) = 1 - \operatorname{erf}(x)$  and  $\lambda$  is the reciprocal of the standard deviation. EMG is a convolution of the normal and exponential probability density functions. If a reasonably good fit of the EMG is obtained on Xmax distribution (that in addition can be smeared to mimic the effect of the detector resolution), then the variance of the underlying normal distribution and hence its standard deviation may be obtained from the relation

$$\sigma_{\text{EMG}}^2 = \sigma^2 + 1/\lambda^2 \quad (2)$$

The mean of the EMG distribution is given by

$$\bar{x}_{\text{EMG}} = \mu + 1/\lambda \quad (3)$$

For a large sample of data, it is expected that the smearing of the sample should not make its mean to deviate from that of the parent distribution, hence  $\bar{x}$  in Eqn. (3) should remain the same for the sample as for the parent distribution.

## 2. The Problem

Analysis of the variation of the mean depth shower maximum  $\langle X_{\text{max}} \rangle$  with energy has already revealed a trend whereby the composition of the primary cosmic rays initially gets lighter with increasing energy,  $E$ , upto  $\lg(E/\text{eV}) = 18.26$  before beginning to get heavier. The contribution of individual nuclei to the overall composition is still uncertain. Based on different astrophysical models of acceleration of cosmic rays, a truncation of the Pierre Auger  $\langle X_{\text{max}} \rangle$  data into “light” and “heavy” components has been proposed, in order to shed more light on the contribution of protons and heavier nuclei respectively. However, this truncation causes an introduction of a bias in the characteristics of two subsets of data thus generated, due to detector resolution. This study aims at estimating this bias.

## 3. Research Objectives

1. To simulate primary cosmic rays whose depth of shower maximum correspond to that of measured data.
2. To smear the simulated distributions using standard deviations that correspond to the estimated resolutions of the detectors used in collecting experimental data.
3. To use the EMG function to deconvolute the smeared distribution so as to obtain the true distribution of Xmax.
4. To compare the characteristics of the simulated “true” distribution with the measured one.

## 4. Literature Review

Since the first observation of an UHECR event in 1962, their chemical composition has not been definitively established. As a result of the very low flux of UHECRs, they cannot be detected directly, but instead detectors which are spread out over a large area of the surface of the earth such as the Pierre Auger detector, must be used (Nagano & Watson, 2000). At energies above



$10^{14}$  eV, it is not possible to measure the abundance of individual elements in the cosmic ray spectrum directly. However, the mean mass of the cosmic rays at a given energy can be estimated by analyzing for example the mean atmospheric depth at which the resultant air shower initiated by the primary cosmic rays reaches its maximum development (Linsley, 1963; Kampert & Unger, 2012). Determination of the individual masses that give the average measured is currently the subject of ongoing research. It is however possible to deduce a change in mass with increasing energy of the primary nuclei, but only on a statistical basis (Kampert & Unger, 2012). Based on simulation studies, an estimate of the fractions of nuclei present in the air showers detected by the Pierre Auger Observatory has been obtained (Aab, *et al.*, 2014). Although this study concluded that an assumption of only two primary cosmic ray nuclei could not describe the measured data, it was a good starting point to include more primary particles in future studies. The use of the EMG function can likewise be extended to assumptions of more primary nuclei.

### 5. Methodology

A variety of mixed primary compositions of cosmic rays made of two nuclei: p-He, p-Fe and p-O were simulated using the CONEX code, with EPOS-LHC as the hadronic interaction model. To begin the procedure of EMG analysis, the smeared distribution was fitted with an EMG for various p-He, p-Fe, and p-O compositions, and hence  $\lambda_{fit}$ ,  $\sigma_{fit}$  and  $\mu_{fit}$  were obtained. In the meantime, the true mean of the light and heavy subsets were obtained from two separate histograms, filled for light and heavy <sup>events</sup> respectively without any smearing. The standard deviation of the EMG from Equation (2) is given by

$$\sigma_{fit}^{EMG} = \sqrt{\sigma_{fit}^2 + 1/\lambda_{fit}^2} \quad (4)$$

Then

$$\sigma_{true}^{EMG} = \sqrt{\sigma_{res}^2 + \sigma_{fit}^2} \quad (5)$$

where  $\sigma_{res}$  is the smearing due to resolution, and the standard deviation of the unsmeared underlying Gaussian is given by

$$\sigma_{true} = \sqrt{\sigma_{res}^2 + \sigma_{fit}^2} \quad (6)$$

The fit parameters  $\sigma_{true}$ ,  $\lambda_{fit}$  and  $\mu_{fit}$  were then substituted in the EMG, and the function integrated to obtain the deconvoluted means of the ‘light’ and ‘heavy’ subsets of the data; the two subsets being delimited by  $X_{max}^{cut}$  (see Figure 1).

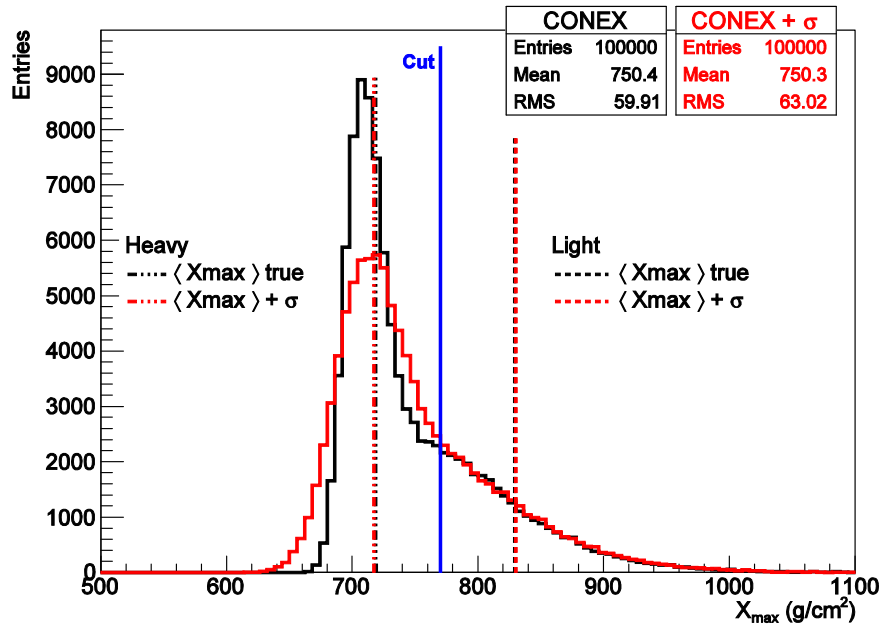


Figure 1: Simulated composition of 40% proton-60% oxygen mixture. A smear of the distribution with  $\sigma_{res} = 20 \text{ g/cm}^2$  is shown in red. The mean of the light and heavy subsets of data before and after smearing are represented by the vertical dashed lines.

The mean of Xmax for the light and heavy components are given respectively by Equations (7) and (8),

$$\langle X_{max}^{light} \rangle = \frac{\int_{X_{max}^{cut}}^{+\infty} X_{max} f(X_{max}; \mu_{fit}, \sigma_{true}, \lambda_{fit}) dX_{max}}{\beta_{light}} \quad (7)$$

$$\langle X_{max}^{heavy} \rangle = \frac{\int_{-\infty}^{X_{max}^{cut}} X_{max} f(X_{max}; \mu_{fit}, \sigma_{true}, \lambda_{fit}) dX_{max}}{\beta_{heavy}} \quad (8)$$

where  $\beta_{light}$  and  $\beta_{heavy}$  are the normalization factors given respectively by

$$\beta_{light} = \int_{X_{max}^{cut}}^{+\infty} f(X_{max}; \mu_{fit}, \sigma_{true}, \lambda_{fit}) dX_{max} \quad (9)$$

and

$$\beta_{\text{heavy}} = \int_{-\infty}^{X_{\text{max}}^{\text{cut}}} f(X_{\text{max}}; \mu_{\text{fit}}, \sigma_{\text{true}}, \lambda_{\text{fit}}) dX_{\text{max}} \quad (10)$$

By subtracting the mean in the light and heavy subsets of the true distribution from the corresponding mean in the deconvoluted distribution, an estimate of the bias is obtained. All the graphs were plotted using the ROOT software, which is designed to handle large amounts of data, and is based on C++.

## 6. Findings and discussion

A summary of the results of this procedure, showing a sample of the fits to selected compositions together with the fit parameters in each case, is contained in Figure (2), where  $\sigma_{\text{res}} = 50 \text{ g/cm}^2$ . Superposed plots of the actual true distributions give one an idea of how well this procedure unfolds the smeared distribution. It was observed that generally, when the primary distribution contains two distinct peaks, the smeared distribution does not reflect this, i.e. it has only one peak. In such cases, the true distribution obtained by the use of the EMG differs significantly from the actual true distribution. A look at the quality of fit represented by the values of  $\chi^2/\text{Ndf}$  for different compositions shown in Figure (3) suggests that compositions containing only iron and proton generally have the lowest quality fits. This is especially so when the width of smear is  $20 \text{ g/cm}^2$ . However, the procedure worked generally well, resulting in a bias in truncated  $\langle X_{\text{max}} \rangle$  close to zero as expected. A summary of the biases in  $\langle X_{\text{max}} \rangle$  for the resolutions  $\sigma_{\text{res}} = 20$  and  $\sigma_{\text{res}} = 50 \text{ g/cm}^2$  are presented in Figure (4).

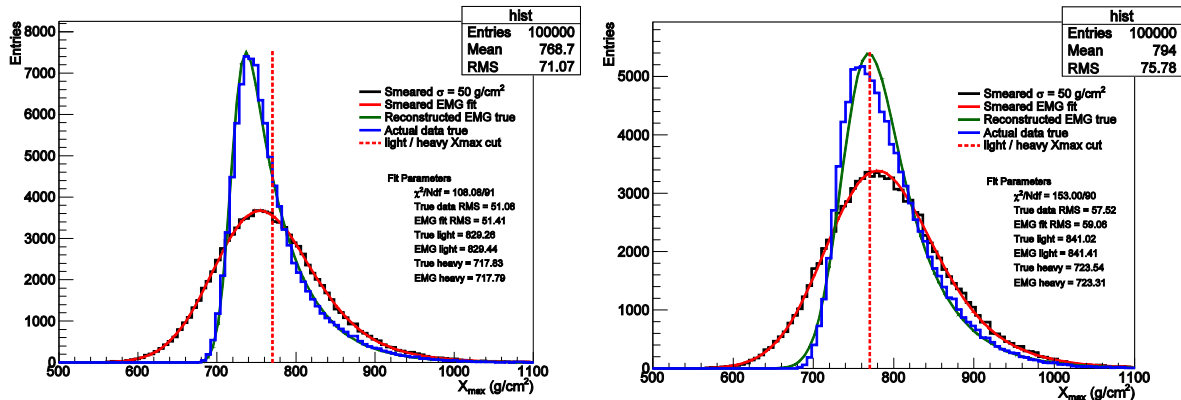


Figure 2: Smeared ( $\sigma_{\text{res}} = 20 \text{ g/cm}^2$ ) simulated 40%p-60%O and 80%p-20%O mixtures fitted with an EMG. The reconstructed true distributions as predicted by the EMG are also shown. The unit of  $\langle X_{\text{max}} \rangle$  shown on the r.h.s. of every plot is in  $\text{g/cm}^2$ .

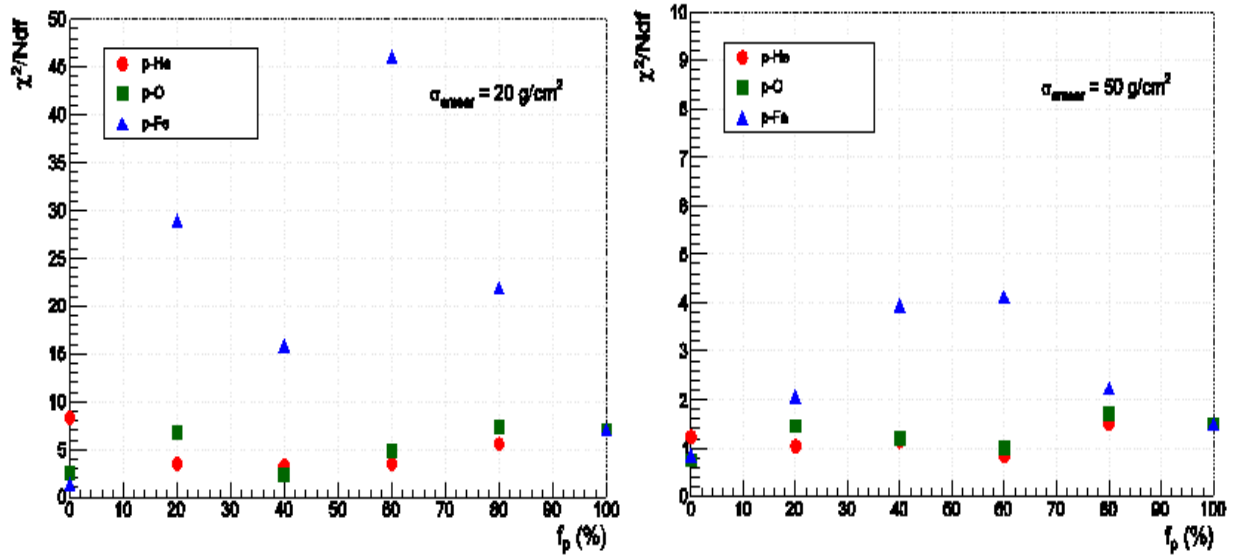


Figure 3: Evolution of the quality of EMG fit with proton fraction for p-He, p-O and p-Fe mixtures for widths of smear  $\sigma_{res} = 20 \text{ g/cm}^2$  (left panel) and  $\sigma_{res} = 50 \text{ g/cm}^2$  (right panel). The horizontal axis shows the percentage of proton in each mixture.

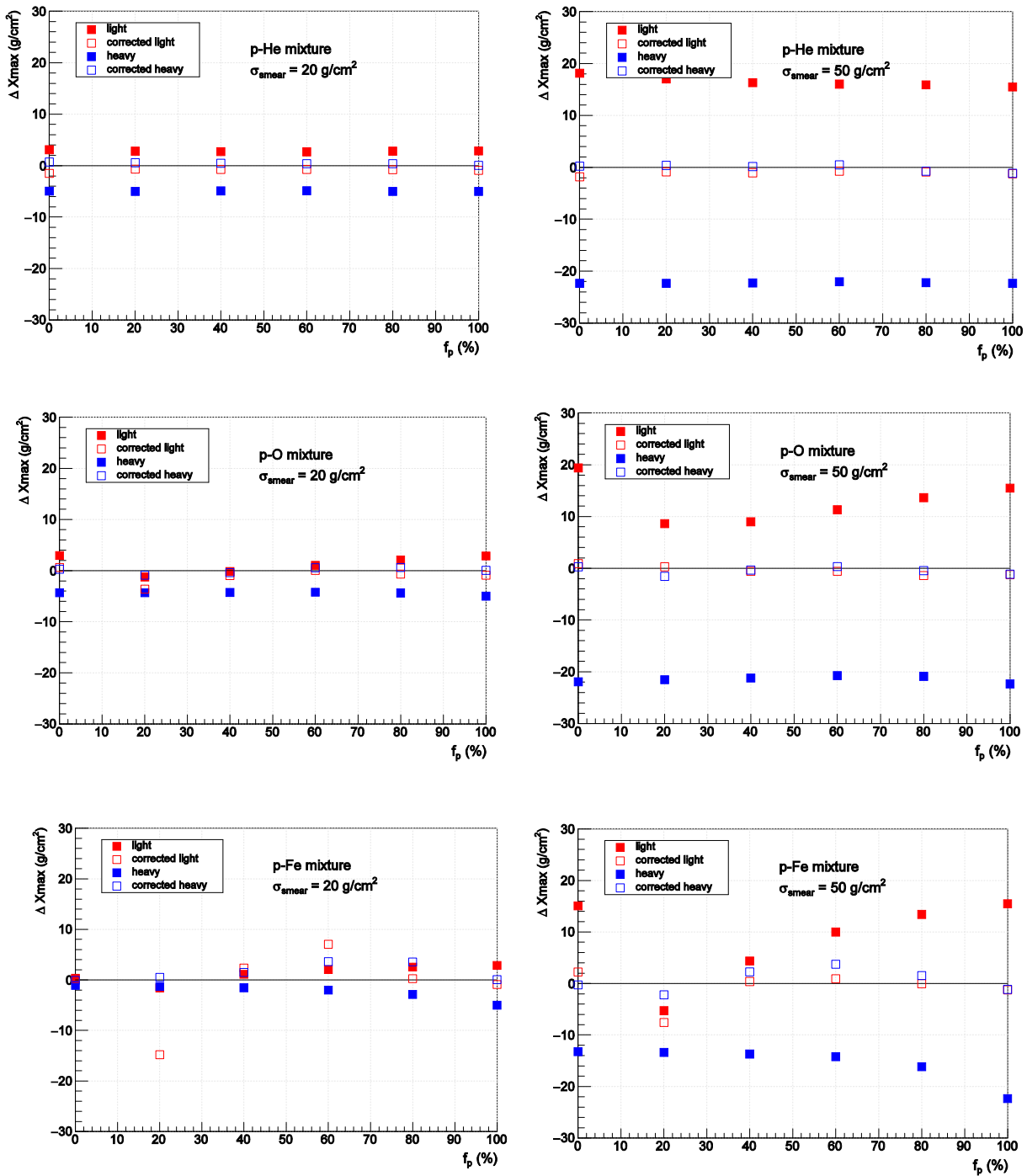


Figure 4: Bias in the light and heavy  $\langle X_{max} \rangle$  due to resolution effects (closed symbols) and results for the corrected  $\langle X_{max} \rangle$  values (open symbols).

## 7. Recommendations and areas for further research

We have investigated the possibility of using the exponentially modified gaussian function to unfold smeared simulated data produced by the CONEX code, with EPOS-LHC as the hadronic interaction model. Using a mixture of only two primary particles of p-He, p-O or p-Fe, we observe that the EMG fits the “measured” data well and hence we are able to obtain the true standard deviation and thus the true distribution with a good accuracy in cases of pure composition, compositions with  $\sigma_{\text{smear}} = 50 \text{ g/cm}^2$  or compositions containing only protons and helium. In most of the cases where the primary contains proton and iron, information gets lost during the smearing process, such that it is difficult to correlate the smeared data with the true data and hence unfolding is not easy. A further study is necessary to find a way around this. In order to represent the more realistic situation where many primary particles are involved, it would be of interest to simulate a composition containing more nuclei.

## Acknowledgement

The author gratefully acknowledges the input of Alexey Yushkov and Markus Risse of the University of Siegen in the writing of this paper.

## References

- Aab, A. *et al.* (2014). Depth of maximum of air-shower profiles at the Pierre Auger observatory: measurements at energies above  $10^{17.8}$  eV, *Physical Review D*
- Aab, A. *et al.* (2014). Depth of maximum of air-shower profiles at the Pierre Auger observatory II. Composition implications. *Physical Review D* 90, 122006.
- Bergmann, T., Engel, R., *et al.* (2007). One-dimensional hybrid approach to extensive air shower simulation. *Astropart. Phys.*, 26:420.
- Grushka, E. (1972). Characterization of exponentially modified gaussian peaks in chromatography. *Anal. Chem.*, 44(11):1733–1738.
- Kampert, K-H & Unger, M. (2012). Measurements of the cosmic ray composition with air shower experiments, *Astropart. Phys.*, 35:660–678.
- Linsley, J. (1963). The cosmic ray spectrum above  $10^{19}$  eV at Volcano ranch and Haverah park, *8th ICRC, Jaipur, volume 77*.
- Nagano, M. & Watson, A. A. (2000). Observations and implications of the ultrahigh-energy cosmic rays. *Rev. Mod. Phys.* 72(3):689–732.
- Pierog, T., *et al.* (2015). EPOS-LHC: test of collective hadronization with data measured at the CERN large hadron collider. *Phys. Rev. C*, 92:034906.

## **An Architecture for Detecting Information Technology Infrastructure Policy Violations in a Cloud Environment**

Ruth Anyango Oginga,  
School of Science, Engineering & Technology, Kabarak University

Felix Musau  
School of Computing Sciences, Riara University, Kenya

Christopher Maghanga  
School of Science, Engineering & Technology, Kabarak University

Corresponding author: [roginga@kabarak.ac.ke](mailto:roginga@kabarak.ac.ke)

### **Abstract**

Organizations are increasingly becoming aware of the business value that cloud computing brings and are taking steps towards transition to the cloud. Just like any other technology it brings new security threats and challenges. A smooth transition entails a thorough understanding of the benefits as well as challenges involved. Privacy is a concern that has risen as obstacle to widespread adoption of clouds by users. Many organizations consider the deployment of different types of protection systems to curb the various malicious activities. The systems can offer sophisticated monitoring and reporting capabilities to identify attacks against cloud environment, while stopping multiple classes of attacks before they are successful against a network. Despite the use of protection systems to detect any malicious activities, some users still find ways to violate some of the laid down IT infrastructure Acceptable Use Policies. While many cloud security research focus on enforcing standard access control policies typical of centralized systems, such policies have often proved inadequate. For this reason, an architecture has been developed to automatically detect IT infrastructure policy violation in a cloud environment. The implication of this research is that institutions would regain their trust in this paradigm and consider implementing policies in their clouds. Since policy violation is one of the major hindrances to the implementation of cloud computing, the policy violation detection architecture could be employed by institutions to ensure data security in cloud environment. The architecture uses software agents as its core components to collect evidence across cloud environment. The architecture captures any policy violation in the cloud environment when using any IT infrastructure. Therefore we discuss the policy violation detection architecture and present our findings in this paper.

**Keywords:** Architecture, Policy violation, IT infrastructure, Cloud environment, Detection

### **I. INTRODUCTION**

So many organizations today make use of Acceptable Use Policy to specify the actions prohibited to the users of an organization's IT infrastructure. Recent cloud computing models are known to be very promising internet-based computing platforms, however these models could result in a loss of security over customer data. This usually happens because the enterprise IT assets are hosted on third-party cloud computing platforms.

All users are usually required to adhere to all the policies specified in the acceptable use policy document without exception. Despite the use of intrusion detection system (IDS) is not guaranteed and cannot be considered as complete defense, the researcher believe it can play a significant role in the Cloud security architecture (Mchugh, 2000).

For this reason architecture would assist network administrators to automatically detect policy violation by gathering relevant evidence data from the node and other IT infrastructure on a cloud environment. Policy violation detection architecture provides prevention capabilities rather than just detection so it can further stop the attack itself as noted by terminating the user session that is being used for the attack, block access to the target (or possibly other likely targets) from the offending user account, IP address, or other attacker attribute, or block all access to the targeted host, service, application, or other resource. This allows the user to have self-discipline when accessing or using cloud environment.

## **II. RELATED WORK**

There are several studies have been conducted previously that aimed to integrate IT functions of Public/private University cloud computing. Most of the paper discussed private cloud computing, others public cloud computing and others hybrid. In this section, therefore, a summary of some of the most prominent efforts in previous research work is provided. To begin with, Examined about cloud computing, and a new model is introduced for cloud computing (Wyld 2010).

Vaquero (2011) focused on the effectiveness of using services cloud such as IaaS and PaaS in educational fields, especially in teaching advanced Computer Science courses. By Praveena and Betsy (2009) provided a comprehensive introduction to the application of cloud in university.

The proposed service support for campus Cloud, in which all resources are virtualized into service based on the virtualization technology, could achieve resource sharing in campus Cloud system. The service pool provides the necessary support for integration of local resources and technology environment for a variety of scattered resources, under the existing conditions to meet the users in universities. The campus cloud platform must need to give special service support for users (Ye and Chen 2011).

However, the software's are installed once, and job scheduling will control the same type of job to the respective cloud servers. To provide virtualization techniques, the cloud servers are referred to as node controller and deploy hypervisors. Local server would act as a (middleware) cluster controller containing warlrus, storage controller and session controller. The Middleware use honey bee algorithm, active clustering, and biased random sampling algorithms. Further, the local server also resolves the primary authentication and access control

### **Level of awareness on policies in cloud environment**

Despite all those IT policies and restrictions, that staff is aware of; staff wants to use personal devices for work because it allows them to be more productive. Agreeing to these IT enforced policies usually give workers the ability to access company emails, use remote desktop tools or virtualization to access their files (Schulz, 2016). An interesting finding is that only one third of staff reported about their knowledge of solutions for data protection in the cloud. This finding indicate a pattern that to an extent cloud service users are aware of privacy and security issues when storing their data, although they are less aware of solutions related to these issues. Similar results are found in which showed that there is an alarmingly high percentage of users from



Switzerland and India, who are not aware that the CSPs obtain the right to modify user data and disable user accounts at any time (Sachdeva et. al., 2011).

This outcome is derived as a result of the fact that users do not read policies violations and terms of service of the cloud services they use. In another study the Australian respondents believed that the cloud computing made it more difficult for organizations to find a way to protect customers' data and the greatest concern was regarding the risk of losing control over data locations and data unauthorized access (Quah,2013).

This possesses serious concerns from a user perspective; organizations lose control over their vital data and are not aware of any security mechanisms put in place by the provider having data in an unknown place and with no control over it are one of the leading concerns to organizations when switching to cloud computing (Behl, 2011).

### **Causes of policy violation**

Federation defense approach, in which the IDSs are deployed in each Cloud computing region, IDSs cooperate with each other by exchanging alerts, and implement a judgment criterion to evaluate the trustworthiness of these alerts. A cooperative component is used to exchange alert messages from other IDSs. Majority vote method is used for judging the trustworthiness of an alert (Chi-Chun et. al,2010).

### **Lack of policies and standards**

Network administrators often give staff policies the benefits of doubt because employees don't always break the rules of malicious or vindictive reasons. Rather workers may not even know that certain actions break company's' policy. Breaches can occur when employees store company information in third party cloud services or when they use a blacklisted app, jail broken phone or other devices that does not meet the company guidelines employees who violate policies usually do so to be more productive (schulz, 2016).

### **Theft of Service Attacks**

The Theft of Service attack utilizes vulnerabilities in the scheduler of some hypervisors. The attack is realized when the hypervisor uses a scheduling mechanism, which fails to detect and account of Central Processing Unit (CPU) usage by poorly behaved virtual machines. This failure may further allow malicious customers to obtain cloud services at the expense of others. This attack is more relevant in the public clouds where customers are charged by the amount of time their VM is running rather than by the amount of CPU time used. Since the Virtual Machine Manager (hypervisor) schedules and manages virtual machines, vulnerabilities in the hypervisor scheduler may result in inaccurate and unfair scheduling. These vulnerabilities mainly result from the use of periodic sampling or low-precision clock to measure CPU usage: like a train passenger hiding whenever ticket checkers come for tickets (Fangfei, 2011).

### **Mechanisms to enable self- protection of the cloud infrastructure**

Dynamic service provisioning using GRIA SLAs, The authors describe provisioning of services based on agreed SLAs and the management of the SLAs to avoid violations. Their approach considers only Grid environments and not Clouds.

## **Firewall**

Firewall is a combination of hardware and software that isolates an organization's internal network from other networks, allowing some packets to pass and blocking others. It functions to avoid unauthorized or illegal sessions established to the devices in the network areas it protects. Firewalls are configured to protect against unauthenticated interactive logins from the outside world. The firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. Basically, numbers of firewalls can be deployed in the proper positions of the managed network for cooperative, integrated, and in depth network security protection. Administrators that manage the firewalls have a have to be careful while setting the firewall rules (Bourducen et. al., 2009).

## **Intrusion Detection System (IDS)**

Intrusion Detection System helps information systems to deal with attacks. This is accomplished by collecting information from a variety of systems and network sources. The information collected is analyzed for possible security problems. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches. The intrusions may include attacks both from outside the organization as well as within the organization (Samrah, 2003).

## **Cyberoam**

Cyberoam is an Identity-based UTM Appliance. Cyberoam's solution is purpose-built to meet the security needs of corporates, government organizations, and educational institutions. Cyberoam's perfect blend of best-of-breed solutions includes Identity based Firewall, Content filtering, Anti-Virus, Anti-Spam, Intrusion Detection and Prevention (IDP), and VPN. Cyberoam provides increased LAN security by providing separate port for connecting to the publicly accessible servers like Web server, Mail server, FTP server etc. hosted in DMZ which are visible the external world and still have firewall protection. It also provides assistance in improving Bandwidth management, increasing Employee productivity and reducing legal liability associated with undesirable Internet content access.

## **POLICY VIOLATION DETECTION ARCHITECTURE**

The user can access the POVIDA using different technologies such as laptops and phones. The user can access different cloud services depending on cloud service providers. These serviced are put in layers. The upper layer is Software as a Service (SaaS), which is the one visible to the final user and involves applications. The next layer is Platform as a Service (PaaS) and it matters to software developers. It is composed by the operating systems, application programming interfaces (API), documentation, and basic services. Infrastructure as a Service (IaaS) refers to the usage of available resources on the cloud: memory, processors, storage and finally business process as a service (BPaaS) as the delivery of business process outsourcing (BPO) services that are sourced from the cloud and constructed for multitenancy. As a cloud service, the BPaaS model is accessed via Internet-based technologies. A cloud management platform is a suite of integrated software tools that an enterprise can use to monitor and control [cloud computing](#) resources. While an organization can use a cloud management platform exclusively for a private or public cloud deployment, these toolsets commonly target hybrid and [multi-cloud](#) models to help centralize control of various cloud-based infrastructures. Then there is policy violation detection architecture that is used to detect any violation on the cloud see figure 1.

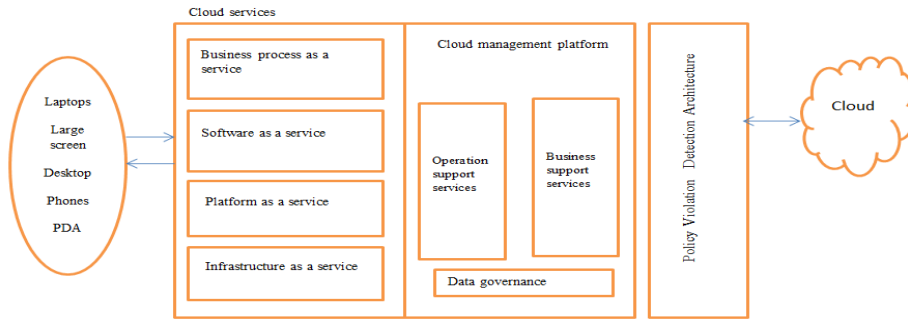


Figure 1: Policy violation detection architecture

### III METHODOLOGY

There exist different approaches that have been used in the security of data in the network. In this paper, though Design science research methodology and descriptive research design was used in this study. Descriptive research is a study designed to depict the participants in an accurate way and describes people who took part in this study (Kowalczyk, 2015). This approach was used to analyse and define the policy violation in the cloud environment. This involved closed ended questionnaires to collect views of users in the institutions. Descriptive survey was therefore chosen for this study because of the opinions of the respondents in terms of security in cloud computing. Descriptive research design enabled the study to generalize the findings to a larger population.

#### Population of the Study

The targeted population for the study was the five Universities in Kenya. This target population has been chosen purposively for this research because these Universities have sensitive and crucial data that needs to be kept secure and private as well as utilize IT infrastructures for growth. The Universities consist of those in the staff, students and Managements who are currently using cloud computing or considering the use of cloud computing due to their infrastructure size and requirement. The Universities had a focus group of people who participated in the research that filled in the questionnaires. These included the ICT managers, Staff in the department of computer Science, Fourth year students in the department computer Science and Network Administrators.

#### Pilot Experiment

Experimental method was used to attempt to detect any IT infrastructure policy violation in the cloud. There were a number of times that the architecture was tested and it was worked well. Seventy (70) participants also tested the architecture and were observed. It was testing whether the architecture was testing the violation in cloud. Data collected from the survey was checked for completeness, consistency, accuracy and uniformity. The regression analysis approach was used to analyze the data collected in order to examine the relationship between two or more variables of interest. It studies the influence of one or more independent variables on a dependent variable. Data entry, descriptive, graphical, reliability and regression analysis was done using minitab version17. This helped in explaining between the variable and which variable was more important than the other. An initial coding framework with the list of themes was first developed. By applying analytical and theoretical ideas developed during the research, these themes were refined and reduced by grouping them together. This list formed the final category

that was used to produce a list used to violate policies. Chi square was used to analyze the data on each objective. [Chi-Square test of independence](#) is used to determine if there is a significant relationship between two categorical variables.

### III. FINDINGS

Data was collected using a survey and observation on the developed architecture. The survey purpose was to know the level of awareness of users towards cloud computing and the needs of users, while the observation was intended to confirm if the needs and requirement were met on the development of the architecture. The survey was done in different institutions and the architecture was done by different group of people. The response rate was ninety five (95) out of one hundred and two (102), and seventy (70) people tested the architecture. The results are summarized in Table 1 about (42%,) of the respondents strongly agreed that the institution have strict policies on what can be accessed and what cannot be accessed on the cloud. Majority of the respondents (43%) also agreed that cloud services providers through network admin analyses the logs with response rate of 67%. The results of the respondents (63%) also significantly strongly agreed and agreed) that Policies in place conform to legal requirement. The findings also revealed that penalties are clearly outlined for violation of policies 61% of the respondents (strongly agreed and agreed).The results of the respondents (60%) significantly(strongly agreed and agreed) that Policy violation detector analyses the operations to determine whether it violates data loss prevention policy. When respondents were asked whether Policy violation detector analyses the content that is either accessed or saved onto any storage system, (34%) agreed. Policy violation detector monitors users actions by intercepting with (54%) approval.

Table 1: Policy violation

	SD(%)	D(%)	UN(%)	A(%)	SA(%)	$\chi^2$	Pr> $\chi^2$
The institution have strict policies on what can be accessed and what cannot be accessed on the cloud	2.0 2	7.0 7	15.1 5	33.3 3	42.4 2	59.1	<.0001
Cloud services providers through network admin analyses the logs	1.0 1	4.0 4	27.2 7	43.4 3	24.2 4	61.2	<.0001
Policies in place conform to legal requirement	1.0 3	8.2 5	27.8 4	32.9 9	29.9	40.1	<.0001
Penalties are clearly outlined for violation of policies	3.0 6	9.1 8	26.5 3	36.7 3	24.4 9	37.0	<.0001
Policy violation detector analyses the operations to determine whether it violates data loss prevention policy	1.0 2	9.1 8	29.5 9	38.7 8	21.4 3	45.3	<.0001
Policy violation detector analyses the content that is either accessed or saved onto any storage system	3.0 3	9.0 9	33.3 3	34.3 4	20.2	39.1	<.0001
Policy violation detector monitors users actions by intercepting	3.1 3	12. 5	30.2 1	25	29.1 7	26.6	<.0001

### Regression analysis results

The regression analysis approach was used to analyze the data collected in order to allow the study to examine the relationship between two or more variables of interest. It examines the influence of one or more independent variables on a dependent variable.

### Regression Analysis

The regression equation is

$$y = 3.91 + 0.103 \times 1 + 0.213 \times 2 + 0.591 \times 3$$

### Analysis of Variance

Table 2. Analysis of variance

Source	DF	SS	MS	F	P
Regression	3	1272.13	424.04	26.54	0.000
Residual Error	95	1517.89	15.98		
Total	98	2790.02			

S = 3.99722 R-Sq = 45.6% R-Sq(adj) = 43.9%

## IV. CONCLUSION AND FUTURE WORK

Today, cloud computing is being defined and talked about across the ICT industry under different contexts and with different definitions attached to it. However, despite the flow in activity and interest, there are significant, persistent concerns about cloud computing that are hindering the momentum and will eventually compromise the vision of cloud computing as a new IT procurement model. Additional concerns regarding privacy and security were also established and addressed through enhancements to the architecture and prototype. The research found out that most respondent was not sincere in the survey because they could imagine and indicate instead of what they really knew. The respondents were asked whether their institution have strict policies on what can be accessed and what cannot be accessed. The study found out that the majority were aware that there are policies in place. In real sense there are no outline policies in place. This was not achieved but in the recommendation it was suggested that institutions to outline penalties and conform to legal requirements. POVIDA is able to analyses policy to determine policy violation and it can also analyses the content being accessed and before saving the data. It can also monitor the users' actions by blocking. In future the studies should explore the possibility of providing suitable frameworks for capturing of screen short in cases where policy violation is detected.

## REFERENCE

- Barinder, K. and Sandeep, S. (2014) 'Parametric Analysis of various Cloud Computing Security Models', *International Journal of information and Computation Technology.*, vol. 4, no. 15, 2014, pp. 1499-1506.
- Becker, J.D. and Elana, B. (2014) 'IT Controls and Governance in Cloud Computing', 20th Americas Conference on Information systems( AMCIS), Savanah.
- Behl, A. (2011). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In Information and communication technologies (WICT), 2011 world congress on (pp. 217-222).IEEE.

- Bhardwaj, S., Jain, L., & Jain, S. (2010). Cloud computing: A study of infrastructure as a service (IAAS). *International Journal of engineering and information Technology*, 2(1), 60-63.
- Computing, C. (2010). Security–A Natural Match. *Trusted Computing Group (TCG)* <http://www.trustedcomputinggroup.org>.
- S. Pearson and T. Sander (2010), “A mechanism for policy-driven selection of service providers in SOA and cloud environments,” in *Proceedings of the 10th Annual International Conference on New Technologies of Distributed Systems (NOTERE '10)*, pp. 333–338.
- V. C. Emeakaroha, M. A. Netto, R. N. Calheiros, I. Brandic, R. Buyya, and C. A. deRose, (2012) “Towards autonomic detection of SLA violations in cloud infrastructures,” *Future Generation Computer Systems*, vol. 28, no. 7, pp. 1017–1029.
- Vaquero, L.M. (2011). *EduCloud: PaaS versus IaaS Cloud Usage for an Advanced Computer Science Course*. *IEEE Transactions on Education*. [Online]. 54 (4). pp. 590–598. Available from: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5686886>.
- Y. Chi, H. J. Moon, H. Hacigümüş, and J. Tatemura, (2011) “SLA-tree: a framework for efficiently supporting SLA-based decisions in cloud computing,” in *Proceedings of the 14th International Conference on Extending Database Technology: Advances in Database Technology (EDBT '11)*, pp. 129–140.

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

Ruth Anyango Oginga,  
School of Science, Enginnering & Technology, Kabarak University

Felix Musau  
School of Computing Sciences, Riara University, Kenya

Christopher Maghanga  
School of Science, Enginnering & Technology, Kabarak University

Corresponding author: [roginga@kabarak.ac.ke](mailto:roginga@kabarak.ac.ke)

### **Abstract**

Cloud computing is an emerging paradigm that involves all the basic components of computing such as end-user machines (PCs), communication networks, access management systems and cloud infrastructures. According to Gartner, while the hype grew exponentially during 2008 and continued since, it is clear that there is a major shift towards the cloud computing model and that the benefits may be substantial (Gartner Hype-Cycle, 2012). However, as the shape of the cloud computing is emerging and developing rapidly both theoretically and in reality, the cloud security, data and cloud infrastructure and privacy issues still pose significant challenges. It still lacks mechanism to enable itself from policy violation. In this work, we describe various mechanisms that would enable self-protection on policy violation in cloud infrastructure. In particular, we discuss five critical mechanisms: IDS, Cyberoam, Federated Identity Management System, firewall and honeypot. Some solutions to mitigate these attacks on these mechanisms are also proposed along with a brief presentation on the future trends in cloud computing deployment. Finally we evaluate these mechanisms based on the data collected from users in case they know how to protect their data in cloud environment.

**Keywords:** Policy violation, cloud infrastructure, evaluating and self-protection

### **INTRODUCTION**

So many organizations today make use of Acceptable Use Policy to specify the actions prohibited to the users of an organization's IT infrastructure. Recent cloud computing models are known to be very promising internet-based computing platforms, however these models could result in a loss of security over customer data. All users are usually required to adhere to all the policies specified in the acceptable use policy document without exception. Despite the use of intrusion detection system (IDS) is not guaranteed and cannot be considered as complete defense, the researcher believe it can play a significant role in the Cloud security architecture (Mchugh, 2000). The authors describe provisioning of services based on agreed SLAs and the management of the SLAs to avoid violations. Their approach considers only Grid environments and not Clouds. Moreover, they do not detail how the low-level metric are monitored and mapped to high-level SLAs to enforce the SLA objectives at runtime. Moreover, with the rapid changing technology environment it is clear that, more speedy changes in the way security

incidences are detected and the way security data is analyzed needs to be done (Markus et. Al., 2012). This paper, therefore, presents mechanisms that enable self- protection on policy violations in cloud infrastructure. The primary objective is to evaluate the mechanisms that enable self- protection on policy violation in developed tools and techniques that can be part of cloud infrastructures to detect policy violations. This paper is made up of:- Introduction, related studies, critical mechanisms, future trend in cloud computing, evaluation mechanisms to enable self- protection in cloud and finally conclusion and future work.

## **RELATED STUDIES**

There exists various research works from different scholars which have made valuable contributions towards the study in this paper. In this section, therefore, a summary of some of the most prominent efforts in previous research work is provided. Discussion on autonomous QoS management using a proxy-like approach, their implementation is based on WS-Agreement. Thereby, SLAs can be exploited to define certain QoS parameters that a service has to maintain during its interaction with a specific customer Also, their approach is limited to Web services and does not consider other applications types (Koller and Schubert 2007)

In an effort towards fighting IT infrastructure policy violations and collect relevant incidence information in a LAN environment, law enforcement agencies have also started incorporating the collection and analysis of digital evidence data into their infrastructures. However they do not consider application deployment and provisioning strategies (Dobson and Sanchez 2011).

Creating a security policy is the first step in protection and enforcement. While it may seem excessive, enterprises need to define which assets users are entitled to access and under what conditions as well as which resources and applications are prohibited. Especially important is establishing individual accountability. Beth Israel Deaconess Security policy details everything from the protection of confidential information to large files transfers, misuse of software, protection of passwords and malware prevention. Increasing awareness about the risks resulting from unchecked trust is resulting in stronger more visible security policies, rather than allowing acceptable use policies and non-disclosure agreements to dictate consequence of inappropriate actions. Organizations are drafting policies that specifically list misuse of computer equipment and data as an offense that can result in punitive actions including termination (Anon, 2014).

According to Bruneton et al. (2006) demonstrated the viability of component-based design to build complex systems from heterogeneous building blocks and reach flexible security. We explore that approach to orchestrate and adapt security services in a cloud (e.g., as Web Services) to compose individual security services flexibly inside a unified security architecture. Security properties provided by individual security services are expressed as flexible contracts, e.g., Service-Level Agreements, to derive overall security objectives guaranteed by the cloud infrastructure.

Computing approach for self-managed security also proved its interest to build security infrastructures with minimal security administration overheads. It satisfies multiple security requirements, and reacts rapidly to detected threats: security parameters are autonomously negotiated with the environment to match the ambient estimated risks and achieve an optimal level of protection (Chess, 2003). A first generic component-based framework for self-



protection has been defined Lacoste et al. (2010). The first part of this dissertation work study whether this framework is sufficient for self-management of cloud security, and define the necessary extensions for that purpose.

### **Critical mechanisms**

There five critical mechanisms to enable self- protection in cloud infrastructure these are IDS, Cyberoam, federated Identity management, firewall and honey pot.

### **Intrusion Detection Systems**

Intrusion Detection System helps information systems to deal with attacks. This is accomplished by collecting information from a variety of systems and network sources. The information collected is analyzed for possible security problems. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches. The intrusions may include attacks both from outside the organization as well as within the organization (Samrah, 2003).

### **Cyberoam**

Cyberoam is an Identity-based UTM Appliance. Cyberoam's solution is purpose-built to meet the security needs of corporates, government organizations, and educational institutions. Cyberoam's perfect blend of best-of-breed solutions includes Identity based Firewall, Content filtering, Anti-Virus, Anti-Spam, Intrusion Detection and Prevention (IDP), and VPN. Cyberoam provides increased LAN security by providing separate port for connecting to the publicly accessible servers like Web server, Mail server, FTP server etc. hosted in DMZ which are visible the external world and still have firewall protection. It also provides assistance in improving Bandwidth management, increasing Employee productivity and reducing legal liability associated with undesirable Internet content access.

### **Federated Identity Management System**

The backbone of cloud computing security is tightly coupled with identities used to access cloud infrastructure. Management of identities (IDM) is about maintaining the integrity of identities, throughout their life cycle, to make it and its related data (e.g., authentication and authorization results) available to different services in secure and privacy-protected manner (Bishop, 2002). The concept of federated identity management (FIM) is about managing identities by allowing an identity subject to establish links between his/her identities, each of which can be used for a different service, across geographical and organizational borders (Bishop 2002). Establishing a logical link between identities is called identity federation. The federation is a group of organizations that establish trust among themselves in order to cooperate safely in business (Leandro, 2012).

### **Firewall**

Firewall is a combination of hardware and software that isolates an organization's internal network from other networks, allowing some packets to pass and blocking others. It functions to avoid unauthorized or illegal sessions established to the devices in the network areas it protects.

Firewalls are configured to protect against unauthenticated interactive logins from the outside world. The firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. Basically, numbers of firewalls can be deployed in the proper positions of the managed network for cooperative, integrated, and in depth network security protection. Administrators that manage the firewalls have a have to be careful while setting the firewall rules (Benkhelifa et. al., 2009).

## **Honeypot**

Honeypot is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers. A honeypot works by fooling attackers into believing that it is a legitimate system. The attackers attack the system without knowing that they are being observed. When an attacker attempts to compromise a honeypot, its attack related information, such as the IP address of the attacker, will be collected. This activity done by the attacker provides valuable information and analysis on attacking techniques, allowing system administrators to trace back to the source of attack if required (Levin & Labella 2003)

In general honeypots can be divided into two categories. Production Honeypots: Production honeypots are used to assist an organization in protecting its internal IT infrastructure. These secure the organization by policing its IT environment to identify attacks. These honeypots are useful in catching hackers with criminal intentions. The implementation and deployment of these honeypots are relatively easier than research honeypots because these have less purpose and require fewer functions. As a result, they also provide less evidence about hacker"s attack patterns and motives. Research Honeypots: Research honeypots are complex. They are designed to collect as much information as possible about the hackers and their activities. Their primary mission is to research the threats organization may face, such as who the attackers are, how they are organized, what kind of tools they use to attack other systems, and where they obtained those tools. While production honeypots are like the police, research honeypots act as their intelligence counterpart and their mission is to collect information about the attacker. The information gathered by research honeypots helps the organization to better understand the hackers attack patterns, motives and how they function (Zhan et. al., 2013).

## **FUTURE TRENDS IN CLOUD COMPUTING**

### **Growth in Cloud Services Solutions**

[Cloud computing](#) future growth all began when the growth of infrastructure as a service, IaaS, and platform as a service, PaaS, expanded the number of cloud solutions available in public and private sectors. As IaaS and PaaS continue to be used worldwide to achieve diverse goals, we will see these solutions as the most deployed cloud services around the world. Cisco predicts that SaaS, software as a service, solutions will account for more than 60% of all cloud-based workloads this year. They also predict that PaaS and IaaS solutions will increase throughout 2018. Any business looking to simplify their operations and make services easier to access for customers will most likely move toward cloud services solutions.

### **Increased Storage Capacity**

A huge aspect affecting the [future of cloud computing](#) is the amount of storage cloud computing will offer companies and individuals. This growth is because many businesses are adopting cloud technology as a huge part of doing business. It is predicted that providers will bring more data centers online with larger-capacity storage equipment throughout this year. Cisco estimates the storage capacity of the cloud will double this year alone. With this increased storage, more businesses will be able to store large data sets and perform analytics using cloud computing. Being able to perform analytics on this massive amount of data will allow companies to gain valuable insights into customer behavior, human systems, and strategic financial investments, just to name a few.

## **Introduction of the Internet of Everything (IoE)**

Most of us have heard the buzzword, internet of things, IoT. With continuous innovations in real-time data analytics and cloud computing, we will see the newest technology buzzword, internet of everything, be used more often as 2018 progresses. Cloud computing will play a major role in the way IoE develops as it relies heavily on machine to machine communications, data, processes and the way humans interact with things in their environment. A major trend we will see this year is the significant role cloud computing will play in IoE's ability to simplify all interactions.

### **Enhanced Internet Quality**

The quality of the internet has been getting immensely better every year since it was created. 2018 is expected to be no different, as the amount of data generated and stored around the world increases. Customers today already expect high-quality, fast-loading services and apps and this expectation will enhance network quality and cloud computing. This high-quality expectation will also lead businesses to upgrade their platforms and services to be more responsive to the needs of their customers. As the quality of the internet is enhanced, IoT and IoE industries will benefit a great deal from the faster network speeds and the ability to receive and deliver data more efficiently in real time.

### **Cloud Solutions to Security Challenges**

One of the most important cloud computing trends 2018 will see is the increased solutions the cloud will bring to security. 2017 saw the most cyber-attacks ever recorded in the history of the internet and 2018 should be no different. Many experts predict 2018 will see more individual and state-sponsored attacks aimed at undermining cloud infrastructure security. Cyber-attacks are also becoming more sophisticated which means anyone in charge of their company's security will need to become more sophisticated in the way they detect and prevent these attacks. Cloud services will be able to help companies with their security measures by offering managed security services

### **EVALUATING MECHANISM TO ENABLE SELF- PROTECTION IN CLOUD INFRASTRUCTURE**

In this paper, though Design science research methodology and descriptive research design was used in this study. Descriptive research is a study designed to depict the participants in an accurate way and describes people who took part in this study (Kowalczyk, 2015). This approach was used to analyse and define the policy violation in the cloud environment. This involved closed ended questionnaires to collect views of users in the institutions. Descriptive survey was

therefore chosen for this study because of the opinions of the respondents in terms of security in cloud computing. Descriptive research design enabled the study to generalize the findings to a larger population.

#### Population of the Study

The targeted population for the study was the five Universities in Kenya. This target population has been chosen purposively for this research because these Universities have sensitive and crucial data that needs to be kept secure and private as well as utilize IT infrastructures for growth. The Universities consist of those in the staff, students and Managements who are currently using cloud computing or considering the use of cloud computing due to their infrastructure size and requirement. The Universities had a focus group of people who participated in the research that filled in the questionnaires. These included the ICT managers, Staff in the department of computer Science, Fourth year students in the department computer Science and Network Administrators.

#### Pilot Experiment

Experimental method was used to attempt to detect any IT infrastructure policy violation in the cloud. There were a number of times that the architecture was tested and it was worked well.

Seventy (70) participants also tested the architecture and were observed. It was testing whether the architecture was testing the violation in cloud. Data collected from the survey was checked for completeness, consistency, accuracy and uniformity. The regression analysis approach was used to analyze the data collected in order to examine the relationship between two or more variables of interest. It studies the influence of one or more independent variables on a dependent variable. Data entry, descriptive, graphical, reliability and regression analysis was done using minitab version17. This helped in explaining between the variable and which variable was more important than the other. An initial coding framework with the list of themes was first developed. By applying analytical and theoretical ideas developed during the research, these themes were refined and reduced by grouping them together. This list formed the final category that was used to produce a list used to violate policies. Chi square was used to analyze the data on each objective. [Chi-Square test of independence](#) is used to determine if there is a significant relationship between two categorical variables.

#### Findings

Data was collected using a survey and observation on the developed architecture. The survey purpose was to know the level of awareness of users towards cloud computing and the needs of users, while the observation was intended to confirm if the needs and requirement were met on the development of the architecture. The survey was done in different institutions and the architecture was done by different group of people. The response rate was ninety five (95) out of one hundred and two (102), and seventy (70) people tested the architecture. The results are summarized in Table 1 where Respondents never agreed on whether data/information on transit is always safe regardless of the deployment model used. They never agreed that the architecture allows unauthorized access to data/information in the cloud. Respondents (strongly agreed and agreed) 65%, those hackers can manipulate weakness in data security model to get an illegitimate access to data or application. Majority of the respondents also strongly agreed 45% that applications created without policies followed are potential security risks due to incompatibility and integration issues, there is only (2%) who strongly disagreed. Respondents

(strongly agreed and agreed) 79%, that Intrusion Detection System approach also improves security by helping to capture the overall extent of an attack. Minority of the respondents strongly disagreed 2%, that the architecture contain both detection and reaction mechanisms this was supported .When the respondents were asked if all monitoring operations are done outside the virtual machines so the attacker cannot modify the architecture, majority of the respondents strongly agreed and agreed 49%, that all monitoring operations are done outside the virtual machines so the attacker cannot modify the architecture.

**Table 1: Mechanisms to enable self-protection of the cloud infrastructure**

	SD(%)	D(%)	UN(%)	A(%)	SA(%)	$\chi^2$	Pr> $\chi^2$
Data/information on transit is always Safe regardless of the deployment model used.	12.1 2	14.1 4	36.36	18.1 8	19.1 9	18. 2	0.001 1
The architecture allows unauthorized access to data /information in your cloud.	14.1 4	27.2 7	16.16	27.2 7	15.1 5	8.8	0.065 5
Hackers can manipulate weakness in data security model to get an illegitimate access to data or application	9.09	6.06	20.2	40.4	24.2 4	37. 0	<.000 1
Applications created without policies followed are potential security risks due to incompatibility and integration issues.	2.04	4.08	15.31	33.6 7	44.9	68. 8	<.000 1
Intrusion Detection System approach also improves security by helping to capture the overall extent of an attack	2.02	4.04	15.15	41.4 1	37.3 7	67. 4	<.000 1
The architecture contain both detection and reaction mechanisms	2.02	6.06	32.32	37.3 7	22.2 2	48. 3	<.000 1
All monitoring operations are done outside the virtual machines so the attacker cannot modify the architecture	3.06	10.2	37.76	27.5 5	21.4 3	37. 1	<.000 1

#### CONCLUSION AND FUTURE WORK

Security measures should be dynamic and autonomous. Cloud computing infrastructure is changing fast requiring security measures and policies to be updated regularly at the same pace to match the changing behavior of the clouds. Furthermore, licensing is crucial to the security of clouds. Standard policies should be strictly implemented in clouds and organizational/governing bodies should visit clouds' staff and infrastructure on regular bases to evaluate the efficiency of the security precautions adopted by the purveyors. The statistics for attacks, occurring in any cloud, should be publically available to determine the reliability of cloud purveyors. This type of sharing helps other cloud's security experts to guard against new attacks. Also, it is extremely important to holistically investigate the various cloud security related parameters including risks, threats, challenges, vulnerabilities, and attacks. The mechanisms chosen should at all cost self-protect you when you are using cloud. The possibility of being attacked can be reduced by deeply understanding the dependencies among these considerations. Finally, note that virtualization is a backbone of cloud computing. However, the concept of using virtualization in cloud computing is not yet mature as there are numerous number of attacks that target the

virtualization environment. Examples of these attacks include information leakage during VM migration, service theft by manipulating VMs, uploading malicious VMs on cloud server, and rolling back VMs. Therefore, it is extremely important to develop reliable schedulers that, by design, contain sufficient security mechanisms. We have identified a few areas that are still unattended in cloud computing security such as auditing, and migration of data from one cloud to another which can be tackled in future.

## REFERENCE

- S. Bouchenak,(2010) “Automated control for SLA-aware elastic clouds,” in Proceedings of the 5th International Workshop on Feedback Control Implementation and Design in Computing Systems and Networks (FeBiD '10), pp. 27–28.
- Cappos, J., Beschastnikh, I., Krishnamurthy, A., & Anderson, T. (2009). Seattle: A platform for educational cloud computing. SIGCSE Bulletin, 41, 111-115
- Malik, S., Huet, F. & Caromel, D. (2012). Cooperative cloud computing in research and academic environment using Virtual Cloud. In: 2012 International Conference on Emerging Technologies. [Online]. October 2012, Islamabad: IEEE, pp. 1–7. Available from: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6375445>.
- A. Samrah, “Intrusion Detection Systems; Definition, Need and Challenges,” [http://www.sans.org/reading\\_room/whitepapers/detection/intrusion-detection-systems-definition-challenges\\_343](http://www.sans.org/reading_room/whitepapers/detection/intrusion-detection-systems-definition-challenges_343), October 31, 2003.[8].
- Bishop, M. *Computer Security: Art and Science*; Addison-Wesley Professional: Reading, MA,
- Chou, T. (2013): security threats on cloud computing vulnerabilities, international journal of computer science & information technology (IUCSIT) vol. 5 No3.
- E. Benkhelifa and T. Welsh, “Towards Malware Inspired Cloud Self-Protection,” proceedings of the 2014 International Conference on Cloud and Autonomic Computing (ICCAC 14), 2014, pp. 1–2.
- Leandro, M.A.P.; Nascimento, T.J.; dos Santos, D.R.; Westphall, C.M.; Westphall, C.B. Multitenancy authorization system with federated identity for cloud-based environments using
- Leavitt, N. (2009) 'Is cloud computing really ready for prime time?', *Computer*, vol. 42, 2009, pp. 15- 20.
- Levin, J. and Labella, R., “The Use of Honeynets to Detect Exploited Systems across Large Enterprise Networks”, IEEE Proceedings, pp.92-99, 18 June 2003.[10].“Honey-pot Security”, <http://www.infosec.gov.hk/english/technical/files/honeypots.pdf>. [11].
- Khorshed, M.T.; Ali, A.B.M.S.; Wasimi, S.A. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Gener. Comput. Syst.* **2012**, 28, 833–851.

D. Chess, C. Palmer, and S. White. Security in an Autonomic Computing Environment. IBM Systems Journal,42(1):107–118,2003.Truehost.<https://www.truehost.co.ke/cloud-providers-kenya/>

Gartner (2012). Gartner Highlights Five Attributes of Cloud Computing. [Online]. 23 June. Available from: <http://www.gartner.com/newsroom/id/1035013>.

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

Kilisio Mercy and Moses Thiga

Kabarak University, 13 P.O. Box Private Bag, Kabarak, 20157, Kenya

### **Abstract**

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

**Keywords:** county government, risk management, software project

### 1. Introduction

Risks are inevitable, and there is always a degree of risk involved in every project. Project Management Book Of Knowledge defines project risk as “an uncertain event or condition, that if, it occurs causes a negative or positive effect on at least one of the projects objective such as time, cost, quality or scope.” Risk management and success of a project are intertwined. Better approaches to project risk management tend to increase chances of software project success in terms of achieving scope, quality, schedule and cost constraints (Bhoola, Hiremath, & Mallik, 2014). Risk management is considered to be an important component of software project management. However, in spite of its importance it’s the least practiced (Mnkandla, 2012).

Risk management process was introduced in software development as an explicit process in 1980(Wallmüller, Wiczorek, Naujoks, & Bartlett, 2002). Barry Boehm is known as the father of risk management in software engineering. Software project risk management is the process of identifying, analysing, managing and controlling issues and risks that may arise during the software project life cycle. The first step is identifying all the risks and adding them to the list of possible risks. After identification, the risks are analysed and prioritised both in terms of likelihood of it happening and the impact it might have on the project. The third step is the management or planning of the software risks which involves risk response strategies; the process of responding to risk factors. The most common response strategies are acceptance, mitigation, transfer or avoidance. The last step is risk control which involves monitoring of the status of the risks and the actions taken against them.

There can be many risks in creating quality software systems. They cannot be completely eliminated but project managers can reduce these risks and their impact on software products by



calculating these risks. Increases in project size and complexity in return increases the risks. The software industry is one of the largest industries in the world. To achieve a successful outcome, project leadership must identify, assess, prioritize, and manage all of the major risks. Tom Gilb put it as “If you don’t actively attack the risks, the risks will attack you.”

The software management study showed that industry wide, only 16.2% of software projects are on time and on budget. The rest, 52.7% are delivered with reduced functionality and 31.1% are cancelled before completion(international, 2013). The main reason stated for this large amount of less quality software and failure of software projects is the lack of proper software risk management(Dedolph, 2003). Many projects with all the ingredients for success fails. It happens when stakeholders, managers and project teams are not used to evaluating the uncertainties, risks and complexities involved beforehand, and fail to adapt their management style to the situation (Shenhar & Dvir, 2007). Uncertainty has no independent existence, it is not something that can be identified and eliminated in the same way that a bug which invades a project can. The uncertainty arises naturally from complex situations (Cleden, 2009).

The Standish Group 2004 Report indicated that the main reason for project failure in developed countries is not the absence of general resources or financial resources, but the lack of project management capability (Berg & Karlsen, 2007). According to (Jekale, 2004), projects in developing countries are highly influenced by their external environment. The project environment in many developing countries is unstable and characterized by rapid change of markets, shift of funding sources, frequent change of government policies and the business environment.

In Kenya, the county governments were introduced through the promulgated constitution of Kenya in 2010. The implementation was carried out in the 2013 general election whereby 47 county governments were enacted. Like many other developing countries, the software development in Kenya is a fast developing and rapidly growing industry that is facing a lot of challenges. It is seen as a solution to issues that are facing the society, and the automation of a lot of processes within different organisations especially the government institutions. The county governments are still at its’ early stages of growth meaning that they face a lot of challenges in software project management such as delays, underperformance, cost overrun, incomplete or volatile software requirements, employees’ turnover, poor schedule, complex projects, lack of skills and lack of formal risk management practices (Kipyegen, Mwangi, & Kimani, 2012).

According to the County Integrated Development Plan (2013-2017), the projects that were to be undertaken by the County Government of Nakuru were: Automation of revenue collection, Automation of county operations, Website Design and Development, Purchase of ICT equipment, Networking, Telephone Communication Systems, Media Centre, Security Systems, Digital villages and ICT Centres (Nakuru County Integrated Development Plan 2013-2017, 2013).

The county government of Nakuru through the ICT department, has plans to come up with innovating ways to improve systems and processes within the county. It believes that ICT has the capacity to transform the county government into an effective system. Those plans include improving Wireless Access Networks within all Sub-County offices; install CCTV surveillance

systems within urban centres; establishing digital information; establishing Wi-Fi zones within Sub-County headquarters; creating online portals to effect online payments and service access as well as developing ICT solutions and platforms to facilitate ease of doing business with and accessing services from the County Government of Nakuru (Kimani, 2017). For these projects to be successful, there need to a risk management plan in place.

Risk management is very important especially in software and IT projects because they can be vehicles of delivering organisational change, so achieving the business objectives can be dependent on their success.

## 2. Problem Statement

Software development projects have an increased rate of failure and, like other businesses, software development involves technical and expensive resources. The success of software development depends on the criteria: functionality, quality and timelines. These are the three major constraints to a project success. Software is developed to perform a specific function. If the software does not perform intended function effectively, then the purpose of the software will be defeated. Software development organisations suffer problems from delayed and over budget projects. Risk can occur in any project and can harm the final product and its functionality. For reducing or avoiding risks, project managers should take appropriate countermeasures. If there are no proper risk management techniques, the failure of a large-scale system can affect the stakeholders of that software. Failure of the final product can waste the budget and time of its customers, employees and organization. The failure can reduce the profits of the business or an organisation.

### 1. Objectives

1. To survey the number and types of software projects that have been undertaken by the County Government of Nakuru since inception.
2. To determine the structures, practices and personnel for software project management in the County Government of Nakuru.
3. To establish the challenges and related outcomes associated with software projects in the County Government of Nakuru.
4. To determine the software risk management practices undertaken by the County Government of Nakuru during their software development projects.

## 2. Literature review

### 2.1 *Software risk management practices*

The ever increasingly competitive markets, business and enterprises have led to reliance in information technology systems to achieve effectiveness and efficiency. Project management is concerned with the application of tools, skills, knowledge and techniques to achieve effectiveness and efficiency to survive in competitive market (PMI, 2000). The dynamic nature of the IT industry makes it hard to manage software projects (Maniuk, 2017). For the project managers, it is not enough to have knowledge of project management practices, but also be up to date with the latest trends in the software industry. There are several practices and as a project

manager, one has to be conversant with all of them to be able to choose best practices for the project.

Seven risk management principles (Rathod, Chim, & Chawan, 2012) have been identified to be important to achieve the objectives of risk prevention, mitigation, correction and safe system failure:

*Product vision:* Product vision is based on the common purpose, ownership, and collective commitment; it focuses on product results.

*Teamwork:* No single person can anticipate all the risks that face a project. Risk management requires that project members find, analyse, and work on potential risks together. For this to be effective communication skill is needed.

*Global perspective:* Potential impacts of adverse effects, such as cost overrun, time delays, or failure to meet product specifications are included.

*Future view:* This principle develops the ability to look into the future, beyond today's crisis and into the likely consequences and impacts of current decisions on future options. It thinks about the risks that may arise in the future and try to minimize them as early as possible.

*Communication skills:* It defines and improves formal and informal communication. Communication with all stakeholders through meetings is of great value to the project.

*Integrated management:* This principle helps to assure that risk management processes, paperwork, and discipline are consistent with established project culture and practice. Ensures the habit of using risk management methods and tools in project development process.

*Continuity:* Continuous process requires sustaining constant vigilance, identifying and managing risks routinely throughout all phases of the projects' life cycle. The processes must be part of daily, weekly, monthly, and quarterly project management.

## *2.2 Software risk management challenges*

According to ProofHub, (@proofhub, 2017) only 2.5% of companies successfully complete their projects. This is a very disappointing figure. This low percentage is because beside being able to plan, manage resources and meet deadlines, one must be able to foresee the challenges that may derail the progress of the overall project.

Despite availability and existence of software development risk management tools, risks are still prevalent. Risks that are common in software development are incomplete requirements or requirements that keep changing, under skilled employees, tight timelines, insufficient resources, poor schedule, and complexity of the project, poor design, cost estimates and lack of formal risk management approach. (Kipyegen, Mwangi, & Kimani, 2012). The main objective of risk management is to reduce the impact and probability of the effects and increasing the impact and probability of opportunities. All projects have a certain degree of risk, so risk management is an important activity in project management. Risk management is a process that involves software risk identification, analysis, planning, monitoring and control.

IT projects are risk-prone, and it's not due to technological failure but mainly due to its' complexity (M. Marinho, S. Sampaio, Lima, & Moura, 2014). One of the major reasons that a software project can fail is due to weak risk management. Others being lack of senior management, unclear project objectives, scope creep, gaps in communication and lack of visibility of all projects. (Abbasi, Wajid, Z. Iqbal, & Zafar, 2014).

## *2.3 Software risk management approaches*

There are three main approaches to software risk management(Otniel, Nicolae, & Claudiu, N.d);evaluation, contingency and management approaches.

*Evaluation approach to IT/software project risk management*

According to this approach, the process of risk management is an analysis for determining the risk factors and causes of project failure. It aims to learn from past projects, by evaluating risks that have already occurred. The evaluation may result in modifying the use of previous framework of risk management or even changing the framework. The contribution of the evaluation approach of risk management to project success is indirect, as the information gathered is used in future projects(Bakker, Boonstra, & Wortmann, 2010).

This approach answers the question what causes projects to fail. It assumes that it is likely that knowledge of the risks and their causes will have a positive impact on the project outcome. The aim of this approach is to create project predictability in new projects by using information regarding risks and causes of project failure gathered from previous projects.

*Management approach to IT/software project risk management*

Management approach answers the question how to deal with risks in order to prevent project failure. This approach to risk management has processes based on rational decision making. It focuses on identifying the events and situations specific to projects that can interfere with the original plan and developing measures to keep the current project on track. The contribution of the management approach of risk management to project success is direct, as it focuses on the relevant and specific risks of the current project.

*Contingency approach to IT/software project risk management*

The contingency approach to risk management considers project success to be dependent on how well the project as a whole is able to deal with uncertainties in the project environment (Jun, Quizhen, & Qingguo, 2011)as project uncertainty is negatively associated with project success. According to the contingency approach, risk management is not considered to be a separate management process. Instead it is embedded in the various processes and procedures of the project.

Regardless of the approach, a standard method for identifying, assessing, and responding to risks should be included in any project as this influences the outcome of the project.

#### *4.4 Nakuru County Government*

Nakuru County lies within the Great Rift Valley and borders eight other counties namely; Kericho and Bomet to the west, Baringo and Laikipia to the north, Nyandarua to the east, Narok to the south-west and Kajiado and Kiambu to the south. The county covers an area of 7,495.1 Km<sup>2</sup> and is located between Longitude 35 ° 28` and 35° 36` East and Latitude 0 ° 13 and 1° 10` South. The county headquarter is Nakuru town.

The county is divided into nine administrative Sub-Counties namely; Naivasha, Gilgil, Nakuru, Rongai, Nakuru North, Subukia, Njoro, Molo, and Kuresoi. Njoro and Kuresoi were hived off from Molo Sub-County, Gilgil from Naivasha, Rongai from Nakuru Town, and Subukia from Nakuru North.The county is divided into 11 constituencies namely; Naivasha, Gilgil, Nakuru town West, Nakuru Town East, Rongai, Bahati, Subukia, Njoro, Molo, and Kuresoi North and Kuresoi South. In total Nakuru County has 55 electoral county wards(Nakuru County Government ICT Roadmap (2015-2020), 2015).

The ICT and E-government is under the Ministry of Education, ICT and E-government, which was established to deliver services to the citizens of the county government of Nakuru. A CEC Member heads the ministry. He is supported by the Chief Officer. Under the ICT

department, there is a Director and a County ICT manager. The County ICT Manager is the one to oversee the projects being undertaken.

The concept of project success varies from different scholars and practitioners as to what constitute it. In most cases, a project success is measured in terms of three requirements: time, budget and quality. However, (Prabkhar, 2008) argues that the three are measures of project management success and project success be best measured on the overall objectives of the project. In Brazil, a study was conducted where it examined risk management practices among several projects across different industrial sectors and states. The study revealed that adopting best practices in risk management had a significant positive impact on project success (Junior & Carvalho, 2013).

A project management team should learn to deal with and plan for risks as no project is free of risks. Risk management is not a new concept to an experienced project manager. Management experts can judge a project manager based on his/her ability to oversee risks that might creep up in a project anytime. These risks can be incomplete software requirements or volatile requirements, employees' turnover, lack of formal risk management approach, poor schedule, cost estimates, complex projects and lack of skills among others. Risks are not one-time event, one has to constantly manage risks (Kipyegen, Mwangi, & Kimani, 2012). Contingency plans should be in place while planning the risks because ambiguous contingencies can be a huge challenge in risk management. If contingencies are not identified, the entire project can be mixed up in an unexpected set of problems.

### **3. Methodology**

The research is based on collected data which is then analysed and organised to reveal the risk management practices, challenges and approaches in software development at the county level. The primary data collection was through questionnaires and interviews. The questionnaires provide a better way of gathering and recording data while interviews aids to obtain detailed information about personal feelings, perceptions and opinions regarding the issue. It also allows more detailed questions to be asked, yields a high response rate and at the same time, respondents' own words are recorded, ambiguities are clarified and incomplete answers followed up, thus, enabling clarification which gives precise meaning of the asked questions. The questionnaires used in this study were structured and open-ended.

The collected data was due to an expert interview to the County Ict manager who has overseen all the projects done by the county government since its' inception. Nakuru County was chosen as a pilot study to check on software risk management on all counties in the country.

### **4. Results**

#### *4.1 The number and types of software projects that have been undertaken by the County Government of Nakuru since inception.*

The county government has outsourced five software systems from vendors. Most of the software systems acquired are automated process systems to facilitate services provided by the county government to the public. Examples of these systems are; revenue collection system, hospital management system, and lands information management system.

#### *4.2 The structures, practices and personnel for software project management in the County Government of Nakuru.*

Since the organisation outsource all its software projects, the ICT manager is the project manager in charge of all projects. He chooses who participates in the project management team based on experience and their qualifications. The minimum number of staffs involved at a project at a time is 7 and the maximum is 11. There isn't a standard software project management practice observed in the projects.

### *22.3 The challenges and related outcomes associated with software projects in the County Government of Nakuru.*

The following were found to be the main challenges affecting the software projects at the County Government of Nakuru:

- Budget allocation and approvals.

The County Assembly is the body tasked by the Constitution of Kenya to allocate and approve all the monetary needs of the County Governments. The main challenge with this arrangement is that sometimes the department is not given the amount they requested to acquire the software systems they need. This may result in challenges with acquiring the system that is of high quality they had set their eyes on. Delayed approvals delay the timelines set for the delivery of a software system.

- Lack of capacity

The organisation does not have software developers within the department, forcing them to outsource their software projects. Outsourcing projects might result in cost escalation.

### *22.4 The software risk management practices undertaken by the County Government of Nakuru during their software development projects.*

There isn't a standard or a formal risk management practice. Results from the study showed that some of the respondents are not aware of the existence of formal risk management practices. It was also clear that there is no policy to address risk management practices and policies to govern the processes. There might not be a formal risk management plan, but they do have a response strategy to several risks that may arise.

To avoid some of the risks that arise in software development, the organisation chooses to outsource their projects. The main reason they outsource is lack of capacity within the department. The motivation behind outsourcing is to get products developed faster and also to tap into expert skills from vendors. The process of outsourcing is through tendering. Outsourcing comes with its own challenges and business risks and to deal with the risks they apply the four strategies which are; avoiding, mitigating, transfer of risks and acceptance.

*Avoidance response strategy:* Eliminating activities with a high probability of loss by making it difficult for risk to occur, or by executing the project in a different way which will achieve the same objectives but which insulates the project from the effect of the risk can be termed as risk avoidance (Bhoola, Hiremath, & Mallik, 2014).

It is suggested that the key to managing risks at each stage of the project is to assign an experienced project manager skilled in change management and monitoring progress. This can act as an avoidance strategy to provide risk solutions (Tesch, Timothy, & Mark, 2007).

The business risks that may arise, chosen by the organisation to use this strategy include instances where the project doesn't have a defined project charter, when the project does not have senior management sponsoring, when the metrics of project success are not clear to all stakeholders of the project, when the internal team is not involved in the outsourcing process, when vendor contracts are not adequately detailed. The reason for the decision to choose this strategy on the above instances, given was mostly because it is the technically viable approach. The other reasons were that it is the most agreeable approach and the only legally acceptable approach.

On management risks, the avoidance strategy will be used on instances when the project manager selected to oversee the project does not have the relevant knowledge and skills, when misunderstandings on the expectations arising from unclear specifications or deliverables, where conflicts are not resolved amicably, and where the stakeholders do not adhere to the project development processes. Similar to the reasons given to avoidance response to the business, the popular reason is that, it is the only viable approach. In the case of conflict resolutions and incompetent project manager with respect to outsourced projects, the reason for avoiding the project was that, it is the convenient approach.

The technological risks like certifications and the relevant experience of the vendor team not being considered during the evaluation process, undefined final functionality of the system, lack of discussion between the vendors and the business team, lack of a quality assurance process and the lack of quality assurance checks during the development process, the organisation choose to use this strategy mainly because it is the most convenient approach. The other reason is because it is the technically viable approach.

*Mitigation response strategy:* This strategy tries to minimise the impact the risk might have on the project. Risk mitigation is one or more reinforcing actions designed to reduce a threat to a project (Bannerman, 2008).

This response strategy was preferred for business risks such as; when some key players in the organisation have been left out of the project, when projects have no quantifiable or verifiable measures of success, when there is no consistent support from stakeholders, when the internal team is not supportive of the outsourcing process, when the vendors' contracts are not strictly enforced or when the vendors are not demonstrating desire to adhere to contracts, when the vendor companies does not understand the organisational goals towards the project. This response was preferred mainly because it is the only technically viable approach. The other reason was, it is the most convenient approach.

Management risks such as unclear deliverables between vendors and the organisation, when the assigned project manager does not have time and resources to perform the duty, miscommunication and misunderstanding on project milestones by stakeholders, communication challenges among the stakeholders, unclear project development processes in use for the project by stakeholders, utilises this strategy response. It is the preferred response for these risks mainly because it is the viable approach and the most agreeable approach.

The technological risks like when inconsideration of ongoing training of the vendor, system handing over modalities are not clearly understood, realization that there hasn't been constant system review during its' development, when requirements creep is not managed, and whereby the vendors expectations are not managed, the mitigation response strategy is preferred because it is the viable approach and the most convenient approach.

## **5. Recommendations**

General recommendations for area of further research include:

- There is need for clear and proper policies and framework to guide in the implementation of formal risk management techniques and approaches.
- Software risk management plan solely for government institutions, like county governments that rely on the county assemblies for budgeting, and that which outsource their projects.

The best framework to adopt in software risk management would be:

Identify risks

Strategize

Manag

This means that the project manager identifies all the risks that might face the project with the help of the team and notes them down. After identification, the team may then classify the risks and strategize on how to react to the risks depending on the impact it might have on the project. Management involves monitoring the risks during the project life's cycle.

## 6. Conclusions

Risk management in software projects is very important and different than in other projects. Formal software risk management process techniques provide multiple benefits to both the project team and the organization and these benefits can only be achieved if all stakeholders become aware of these techniques. Creating policies and awareness of the formal software risk management process techniques and tools is crucial in the software development process. Also, educating young software engineers will not only help improve software projects but can lead to innovation of other better ways of handling risks in the industry. Handling risks will lead to more success in software projects.

## References

- @proofhub. (2017, 04 27). *Project Management Challenges*. Retrieved from <https://www.proofhub.com/articles/project-management-challenges>
- Abbasi, N., Wajid, I., Z.Iqbal, & Zafar, F. (2014, January). Project Failure Case Studies and suggestion. *International Journal of Computer Applications*, 86(6), 34-39.
- Ariasa., G., Vilchesa, D., Banchoff, C., Hararia, I., Harari, V., & Iuliano., P. (2012). The 7 key Factors to get successful results in IT development projects. *Conference on Enterprise Information Systems* (pp. 199-207). San Martin: Elsevier Limited.
- B., B. J., & W., G. R. (1992). *The Management of Organizations*. Boston: Houghton Mifflin Company.
- Bakker, K., Boonstra, A., & Wortmann, H. (2010). Does Risk Management Contribute to Success? *International of Project Management*, 28(5), 493-503.
- Bannerman, P. L. (2008). Risk and risk management in software projects: A reassessment. *Journal of Systems and Software*, 81, 2118-2133.
- Berg, M. E., & Karlsen, J. T. (2007). Mental models in project management coaching. *Engineering Management Journal*, 19(3), 3-14.
- Bhoola, V., Hiremath, S. B., & Mallik, D. (2014). An Assessment of Risk Response Strategies Practiced in Software Projects. *Australasian Journal of Information Systems* , 18(3).
- Bpayne., & Watt, A. (2012). *Project Management*. British Columbia: Open Book Publishing.
- Cleden, D. (2009). *Managing Project Uncertainty*. Gower Publishing Company.



- Costa, H., Barros, M. O., & Travassos, G. H. (2007). Evaluating software project portfolio risks. *Journal of Systems and Software*, 80(1), 16-31.
- Dedolph, M. (2003). The Neglected Management Activity: Software Risk Management. *Bell Labs Technical Journal*, 8(3), 91-95.
- Demir, K. A. (2009). *A survey on Challenges of Software Project Management*. Naval Postgraduate School, Department of Computer Science, Monterey, Ca.
- international, S. g. (2013). Retrieved from <http://standishgroup.com>.
- Jekale, W. (2004). *Performance for public construction projects in developing countries: Federal road and educational building projects in Ethiopia*. Norwegian University of Science & Technology.
- Jun, L., Quizhen, W., & Qingguo, M. (2011). The Effects of Project Uncertainties and Risk Management on IS development Project Performance: A Vendor Perspective. *International Journal of Project Management*, 29, 923-933.
- Junior, R., & Carvalho, M. (2013). Understanding the impact of project risk management on project performance. *Journal of Technology Management & Innovation*, 8(1), 64-78.
- Kendrick, T. (2003). *Identifying and managing project risk: essential tools for failure-proofing your project*. New York: Amacom.
- Kimani, D. (2017, Dec 04). Retrieved from County Government of Nakuru: [http://www.nakuru.go.ke/harnessing-ict-resources-for-improved-systems-and-processes/Kipyegen, N., Mwangi, W., & Kimani, S. \(2012, May\). Risk Management Adoption Framework for Software Projects. \*International Journal of Computer Issues\*, 9, 365-374.](http://www.nakuru.go.ke/harnessing-ict-resources-for-improved-systems-and-processes/Kipyegen, N., Mwangi, W., & Kimani, S. (2012, May). Risk Management Adoption Framework for Software Projects. International Journal of Computer Issues, 9, 365-374.)
- M.Marinho, S.Sampaio, Lima, T., & Moura, H. (2014, October). A Guide to Deal with Uncertainties in Software Project Mangement. *International Journal of Computer Science & Information Technology*, 6(5), 1-20.
- Maniuk, I. (2017, 04 11). Retrieved from Project Management: <https://hygger.io/blog/challenges-in-software-projectmanagement/>
- Mnkandla, E. (2012). Assessing a Methodology's Project Risk Management Competence. *Journal of Contemporary Management*, 9, 279-299.
- Nakuru County Government ICT Roadmap (2015-2020)*. (2015, September). Retrieved from <http://icta.go.ke/pdf/28.pdf>
- Nakuru County Integrated Development Plan 2013-2017*. (2013, September 27). Retrieved from <http://www.nakuru.go.ke/wp-content/uploads/2014/03/Nakuru-COUNTY-INTERGRATED-DEV-PLAN-2013-2017.pdf>
- Otniel, D., Nicolae, B., & Claudiu, B. (N.d). RISK MANAGEMENT APPROACHES AND PRACTICES IN IT PROJECTS. *West University of Timisoara, Faculty of Economics and Business Administration*, 1014-1020.
- PMI. (2000). *A Guide to Project Management Body of Knowlegde*. The Project Management Institute. Sylva,NC: PMI, Publishing Division.
- Prabhkar, G. (2008). What is Project Success: A literature review. *International Journal of Business and Management*, 3(9), 3-10.
- Rathod, V., Chim, M., & Chawan, P. (2012, May). An Overview of Software Risk Management Principles. *Journal of Advanced Research in Computer Engineering & Technology*, 1(3), 51-54.
- Shenhar, A., & Dvir, D. (2007). *Reinventing project management: the diamond approach to successful growth and innovation*. Harvard: Harvard Business Press.

- Sheu, D. D., & Lee, H.-K. (2011). A proposed process for systematic innovation. *International Journal of Production Research*, 49(3), 847-868.
- Shukla, A. (2016, April 1). Retrieved from Gate6 Digital Product Development Company: <https://www.gate6.com/blog/top-6-challenges-software-development/>
- Teklemariam, M., & Mnkandla, E. (2017). Software Project Risk Management Practice in Ethiopia. *The Electronic Journal of Information Systems in Developing Countries*, 79(7), 1-14.
- Tesch, D., Timothy, K. J., & Mark, N. F. (2007). IT project risk factors: the project management professionals perspective. *Journal of Computer Information Systems*, 47(4), 61-69.
- Valdellon, L. (2017, January 17). *Project Management*. Retrieved from <https://www.wrike.com/blog/top-challenges-it-project-management/>
- Wallmüller, E., Wiczorek, M., Naujoks, U., & Bartlett, B. (2002). "Risk management for IT and software projects" in *Business Continuity*. Berlin, Germany: Springer.

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

Joseph MBUGUA<sup>1</sup>, Joseph SIROR<sup>2</sup>, Moses THIGA<sup>3</sup>

Kabarak University, 13 P.O. Box Private Bag, Kabarak, 20157, Kenya

<sup>1</sup>[Jmbugua80@yahoo.com](mailto:Jmbugua80@yahoo.com), <sup>2</sup>[josephsiror@gmail.com](mailto:josephsiror@gmail.com) <sup>3</sup>[mthiga@kabarak.ac.ke](mailto:mthiga@kabarak.ac.ke)

### **Abstract:**

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

Key words: Intrusion detection, Performance, hybrid, feature selection, classifier.

### **Introduction**

Network Intrusion Detection System (IDS) [1] monitors the use of computers and networks over which they communicate, searching for unauthorised use, anomalous behaviour, and attempt to deny users, machines or portions of networks access to the services. Although the intrusion detection systems are increasingly deployed in the computer network, they deal with a huge amount of data that contains null values, incomplete information, and irrelevant features. The analysis of the large quantities of data can be tedious, time-consuming and error-prone. Data mining and machine learning [2] provides tools to select best relevance features subset which improves detection accuracy and removes distractions.

Feature selection procedures require four basic stages in a simple feature selection method [3].

- (1) Generation procedure in order to generate the upcoming candidate subset
- (2) Evaluation function so that it can evaluate the subset
- (3) Stopping criterion to decide when to stop
- (4) Validation procedure used for validates the subset.

The existing feature selection techniques in machine learning can be broadly classified into two categories i.e. wrappers and filters. Wrappers selection techniques evaluate the worth of features using the learning algorithm applied to the data while filters evaluate the worth of features by using heuristics based on general characteristics of the data. Feature selection algorithms can be further differentiated by the exact nature of their evaluation function, and by how the space of feature subsets is explored. Wrappers often give better results in terms of the final predictive accuracy of a learning algorithm than filters because feature selection is optimized for the

particular learning algorithm used. However, since a learning algorithm is employed to evaluate each and every set of features considered, wrappers are prohibitively expensive to run, and can be intractable for large databases containing many features. Furthermore, since the feature selection process is tightly coupled with a learning algorithm, wrappers are less general than filters and must be re-run when switching from one learning algorithm to another.

The advantages of filter approaches in feature selection outweigh their disadvantages. Filters execute many times faster as compared to wrappers and therefore applicable in databases with a large number of features [4]. They do not require re-execution for different learning algorithms and can provide an intelligent starting feature subset for a wrapper in case improved accuracy for a particular learning algorithm is required [5]. Filter algorithms also exhibited a number of drawbacks. Some algorithms do not handle noise in data, and others require that the level of noise be roughly specified by the user a-priori [5], [6]. In some cases, a subset of features is not selected explicitly; instead, features are ranked with the final choice left to the user. In other cases, the user must specify how many features are required, or must manually set a threshold by which feature selection terminates. Some algorithms require data to be transformed in a way that actually increases the initial number of features. This last case can result in a dramatic increase in the size of the search space [6].

The rest of the paper is organized as follows: Section II presents some related researches on intrusion detection which cover the feature selection and data mining. Section III briefly describes the KDD dataset used in this research. Section IV explains the details of the dataset pre-processing phase of the proposed model. The proposed model is presented in Section V. Finally, the experimental results and analysis are presented in Section 6 followed by some conclusions in the final section.

## RELATED WORK

Recent study indicates that machine learning algorithms can be adversely affected by irrelevant and redundant training information [7]. The simple nearest neighbour algorithm is sensitive to irrelevant attributes, its sample complexity (number of training examples needed to reach a given accuracy level) grows exponentially with the number of irrelevant attributes [8][9]. Sample complexity for decision tree algorithms can grow exponentially on some concepts (such as parity) as well. The naive Bayes classifier can be adversely affected by redundant attributes due to its assumption that attributes are independent given the class [10]. Decision tree [11], [12] algorithms such as C4.5 overfit training data, resulting in large trees. In many cases, removing irrelevant and redundant information can result in C4.5 producing smaller trees. As a result, most researchers combine the feature selection and classification algorithms to improve the detection accuracy and make intelligent decisions in determining intrusions. Siraj et al. [16] proposed new, automated and intelligent hybrid clustering model called Improved Unit Range and Principal Component Analysis with Expectation Maximization (IPCA-EM) to aggregate similar alerts as well as to filter the low quality alerts. Panda et al. [2] proposed a hybrid intelligent approach using combination of classifiers in order to make the decision intelligently, so that the overall performance of the resultant model is enhanced. These two models use hybrid classifiers to make intelligent decisions and the filtering process is applied after adding supervised or unsupervised learning techniques to obtain the final decision. Agarwal et al. [47]

proposed hybrid approach for anomaly intrusion detection system based on combination of both entropy of important network features and support vector machine.

Lin et al. (2015) studied the importance of feature representation method on classification process. They proposed cluster centre and nearest neighbour (CANN) approach as a novel feature representation approach. In their approach, they measured and summed two distances. The first distance measured the distance between each data sample and its cluster centre. The second distance measured the distance between the data and its nearest neighbour in the same cluster. They used this new one-dimensional distance to represent each data sample for intrusion detection by a k-nearest neighbour (k-NN) classifier. The proposed approach provided high performance in terms of classification accuracy, detection rates, and false alarms. In addition, it provided high computational efficiency for the time of classifier training and testing

### Methodology

The proposed model has four phases as shown in figure 1:

- Phase 1 data pre-processing
- Phase 2 feature selection techniques.
- Phase 3 classification techniques.
- Phase 4 evaluation.

### Data Preprocessing

To make efficient use of the available dataset for analysis the data preprocessing is required to provide solutions to Clean the data to remove noise and duplicate information and then deal with any incomplete or missing data an efficient algorithm based on normalization and discretization techniques. Data normalizaion is a process of scaling the value of each feature into a well-proportioned range, so that the bias in favor of features with greater values is eliminated from the dataset [13]. Every attribute within each record is scaled by the respective maximum value and falls into the same range of [0-1]. Normalization follows equation 1,

$$\text{Normalized}(x_i) = \frac{(X_i - X_{\min})}{(X_{\max} - X_{\min})} \dots\dots\dots \text{Eq. (1)}$$

where  $X_{\min}$  is the minimum value for variable X,  $X_{\max}$  is the maximum value for variable X. For a specific symbolic feature, we assigned a discrete integer to each value and then used equation 1 to normalize it.

Discretization transforms continuous valued attributes to nominal [14][15]. The main benefit is that some classifiers can only take nominal attributes as input, not numeric attributes and also some classifiers can only take numeric attributes and hence can achieve improved accuracy if the data is discretized prior to learning.

### Feature Selection Techniques

The feature selection techniques help to identify some of the important attributes in a data set, thus reducing the memory requirement, increase the speed of execution and improves the classification accuracy[16]. The purpose of this work is to find out which data feature selection algorithm gives better results with decision trees classifiers. Several feature subset selection techniques have been used in data mining.

i. Correlation based feature selection (CFS)

CFS is considered as one of the simplest yet effective feature selection method which is based on the assumption that features are conditionally independent given the class, where feature subsets are evaluated according to a correlation based heuristic evaluation function.[17]. A good feature subset is one that contains features highly correlated with the class, yet uncorrelated with each other. The major advantage of CFS, it is a filter algorithm, which makes it much faster compared to a wrapper selection method since it does not need to invoke the learning algorithms [18],[19].

$$\rho(X, Y) = \frac{\sum_i (x_i - \bar{x})(y_i - \bar{y})}{[\sum_i (x_i - \bar{x})^2 \sum_i (y_i - \bar{y})^2]^{\frac{1}{2}}} \dots\dots\dots(2)$$

Pearson’s correlation coefficient (2), where all variables have been standardized shows that the correlation between a composite and an outside variable is a function of the number of component variables in the composite and the magnitude of the inter-correlations among them, together with the magnitude of the correlations between the components and the outside variable.

ii. Information Gain

Information gain is used as a measure for evaluating the worth of an attribute based on the concept of entropy (1), the higher the entropy the more the information content. Entropy can be viewed as a measure of uncertainty of the system. The largest mutual information between each feature and a class label within a certain group is then selected (2). The performance evaluation results show that better classification performance can be attained from such selected features [20],[18].

$$- \sum_i P(c_i) \log_2 P(c_i). \tag{Eq. (3)}$$

$$IG(A) = I(D) - \sum_{j=1}^p \frac{|D_j|}{|D|} I(D_j^A) \tag{Eq. (4)}$$

**Algorithm 1: Feature selection according to information gains**

Input: A training dataset T = D(F,C), number of features to be selected L

Output: Selected features S

1. Initialize relative parameters: F ← fi, i =1, 2, ...n, C ← 'class labels', S =? ;
2. for each feature fi ∈ F do
  - a. Calculate its information gain IG( fi ) ;
  - b. insert fi into S in descending order with regard to IG( fi ) ;
3. Retain first L feature in S, and delete the others ;
- 4 Return Selected features: S.

iii. Chi-square

Chi-square [18] test is commonly used method, which evaluates features individually by measuring chi-square statistic with respect to the classes. The statistic is

$$\chi^2 = \sum_{i=1}^k \sum_{j=1}^k \frac{(A_{ij} - E_{ij})^2}{E_{ij}}$$

$E_{ij}$  value i for attribute and j for the class,

$E_{ij}$  = the expected No. of instances for  $A_{ij}$ .

The larger value of the  $\chi^2$ , indicates highly predictive to the class.

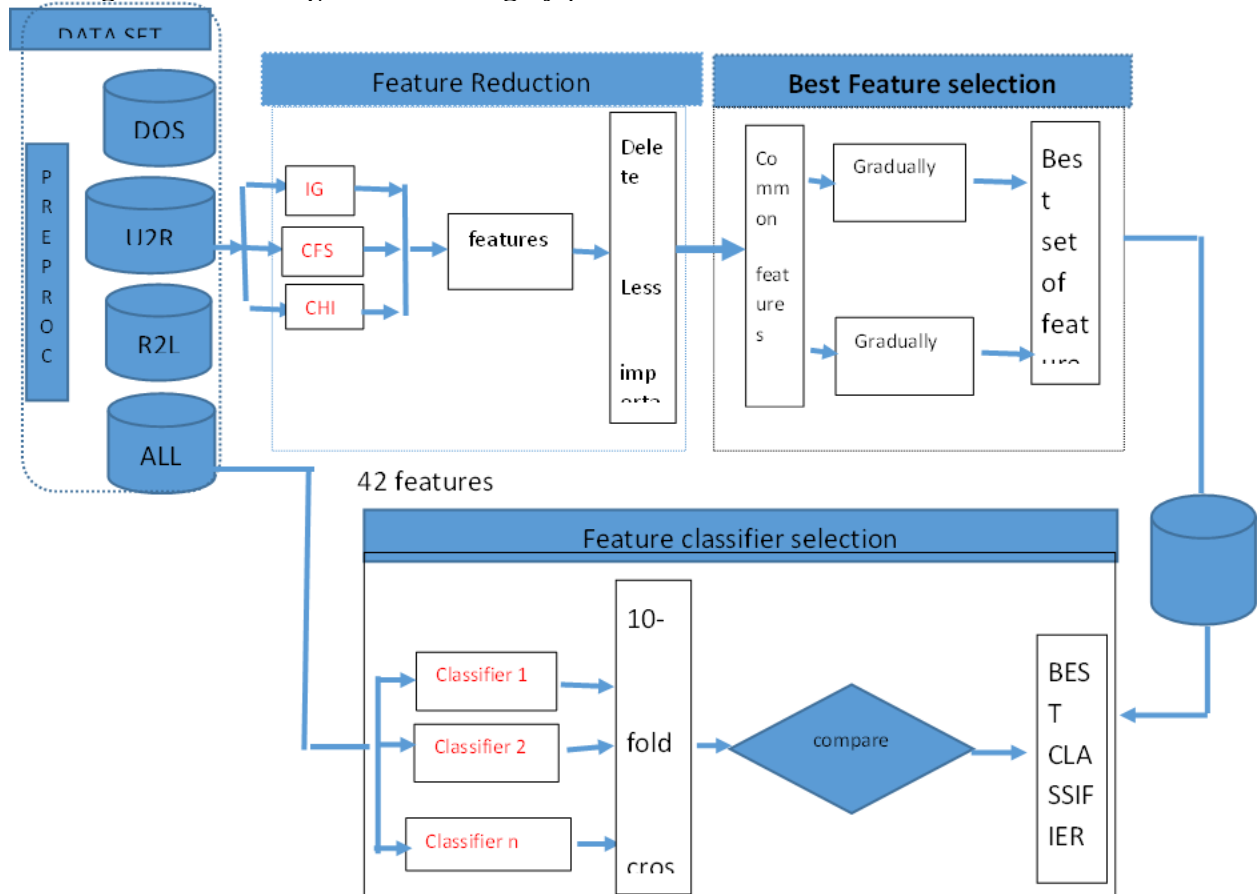


Figure 1 best feature selection process

**Classification techniques**

Classification [21] is a machine learning technique where similar type of samples are grouped together in supervised manner and can classify the intrusion data as normal or attack.

**Random Forest**

Random Forest is an ensemble learning technique for classification and predictive modeling. It is also an approach to data exploration and generates many trees by using recursive partitioning

then aggregate the results[22]. Each of the trees is constructed separately by using a bootstrap sample of the data and the bagging technique[23] is applied to combine all results from each of the trees in the forest. The method used to combine the results can be as simple as predicting the class obtained from the highest number of trees.

### Bayesian Network

Bayesian reasoning provides a probabilistic approach for inference and is based on the assumption that the quantities of interest are governed by probability distributions and that optimal decisions can be made by reasoning about these probabilities together with observed data [24]. A Bayesian network is a graphical model that encodes probabilistic relationships among variables of interest. When used in conjunction with statistical techniques, Bayesian networks have several advantages for data analysis (Kaur & Sachdeva, 2016; Assi & Sadiq, 2017). First, the Bayesian networks encode the interdependencies between variables and hence they can handle situations where data are missing. Secondly, the Bayesian networks have the ability to represent causal relationships. Therefore, they can be used to predict the consequences of an action. Lastly, the Bayesian networks have both causal and probabilistic relationships; they can be used to model problems where there is a need to combine prior knowledge with data. The disadvantages of Bayesian networks includes [27]. First, the classification capability of naïve Bayesian networks is identical to a threshold-based system that computes the sum of the outputs obtained from the child nodes. Secondly, the child nodes do not interact between themselves and their output only influences the probability of the root node and hence incorporating additional information becomes difficult as the variables that contain the information cannot directly interact with the child nodes. Lastly, the accuracy of this method is dependent on certain assumptions that are typically based on the behavioral model of the target system and deviating from those assumptions will decrease its accuracy. Therefore, selecting an accurate model will lead to an inaccurate detection system as typical systems and/or networks are complex.

### J48

J48 [22] is an open source Java implementation of the C4.5 algorithm in the WEKA data mining tool. C4.5 is a program that creates a decision tree based on a set of labeled input data. The decision trees generated by C4.5 can be used for classification, and for this reason, C4.5 is often referred to as a statistical classifier. J48 classifier algorithms [26] are used to compare and built, using the information entropy process, a decision tree from a set of training dataset. These algorithms adopt a top down technique and inductively built the decision tree for classification. It's extremely efficient when handling large datasets. [28]. The extra features of J48 [29] includes accounting for missing values, decision trees pruning, continuous attribute value ranges and derivation of rules.

To make actual decisions regarding which path of the tree to replace is based on the error rates used. The reserved portion can be used as test data for the decision tree to overcome potential overfitting problem (reduced-error pruning).

Now, among the possible values of this feature, if there is any value for which there is no ambiguity that is for which the data instances falling within its category have the same value for the target variable then terminate that branch and allocate to it the target value that have obtained.

### EXPERIMENT & DISCUSSION



## Data Set

The experiments is conducted on MIT Lincoln's Lab's DARPA 2000 Scenario Specific NSL-KDD, 2014 which contains simulated attack scenarios in a protected environment an off-site server. KDD'99 testing set includes 37 attack types that are included in the testing set.

The simulated attacks in the NSL-KDD dataset fall in one of the following four categories[8], [30]–[32].

- i. Denial of service attack (Dos), where attempts are to shut down, suspend services of a network resource remotely making it unavailable to its intended users by overloading the server with too many requests to be handled. e.g. syn flooding. Relevant features includes source bytes and percentage of packets with errors. Examples of attacks includes back,land, neptune, pod, smurf, teardrop
- ii. Probe attacks, where the hacker scans the network of computers or DNS server to find valid IP, active ports, host operating system and known vulnerabilities with the aim discover useful information. Relevant features includes duration of connection and source bytes. Examples includes Ipsweep, nmap, portsweep, satan
- iii. Remote-to-Local (R2L) attacks, where an attacker who does not have an account with the machine tries to gain local access to unauthorized information through sending packets to the victim machine exfiltrates files from the machine or modifies in transit to the machine. Relevant features includes number of file creations and number of shell prompts invoked. Attacks in this category includes ftp\_write, guess\_passwd, imap, multihop, phf, spy, warezclient, warezmaster
- iv. User-to-Root (U2R) attacks, where an attacker gains root access to the system using his normal user account to exploit vulnerabilities. Relevant features includes Network level features – duration of connection and service requested and host level features - number of failed login attempts. Attacks includes buffer\_overflow, loadmodule, perl, rootkit

## Experimental Setup

In the experiment, we apply full dataset as training set and 10-fold cross validation for the testing purposes. The available dataset is randomly subdivided into 10 equal disjoint subsets and one of them is used as the test set and the remaining sets are used for building the classifier. In this process, the test subset is used to calculate the output accuracy while the  $N_1$  subset is used as a test subset and to find the accuracy for each subset. The process is repeated until each subset is used as test set once and to compute the output accuracy of each subset. The final accuracy of the system is computed based on the accuracy of the entire 10 disjoint subsets.

For our experiment, we selected attribute set based on the repetition of attribute from four scheme. Existing FS that are employed in experiments are Correlation Feature Selection (CFS) based evaluator with Best-first searching method, Gain Ratio (GR) Attributes based Evaluator with Ranker searching method, Information Gain (IG) based Attributes Evaluator with ranker searching method, and Chi Squared Eval and Ranker searching method we obtained.

Table 1: The best set of relevant features

ALL	8	2,3,4,26,27,36,39,41
DOS	9	2,3,9,26,41,4,26,27,41
PROB	7	2,3,9,30,34,38,40
E		
R2L	8	1,2,7,33,3,40,34,30,21
U2R	7	6,11,29,30,3,10,14
Best	1	1,2,3,9,26,27,29,30,34,36,3
Featur	2	9,40
e		

### Evaluation Metrics

The performance of the proposed feature selection technique is tested with different evaluation metrics such as: True Positive rate (TR), accuracy (Acc) also known as correctly classified instances (CC), Precision (Pr), false alarm rate (FAR) also known as false positive rate (FPR), ROC and F measure rate (MR).

- i. True positive rate (TPR):  
 $TP/(TP+FN)$ , also known as detection rate (DR) or sensitivity or recall.
- ii. False positive rate (FPR):  
 $FP/(TN+FP)$  also known as the false alarm rate.
- iii. Precision (P):  
 $TP/(TP+FP)$  is defined as the proportion of the true positives against all the positive results.
- iv. Total Accuracy (TA):  
 $(TP+TN)/(TP+TN+FP+FN)$  is the proportion of true results (both true positives and true negatives) in the population.
- v. F-measure:  $2PR/(P+R)$  is the harmonic mean of precision and recall

### Experimental Results and Analysis

In this experiment the time required for the classifiers to build the training model based on several feature selection techniques, namely: ALL, CFS, chi-squared, Information Gain and proposed features are compared with four different classifiers i.e. random forest, Bayes, J48, Parts as shown in Table 8. The experiments indicate that using random forest as a classifier in the training phase takes longer time train the model and hence the results can best illustrate the enhancement of the proposed feature selection technique in the overall performance of intrusion detection. Using all 41 features without selecting important features increases the overhead of the classifiers which subsequently increases the time to build the model. It can be observed that correlation features selection has the most efficient time across most classifiers with exception of chi-squared and Bayes Net (0/16). J48, Bayes and parts presents the most time efficient classification algorithm for all the filter selection methods. As observed, the proposed scheme outperforms the existing techniques with significantly less training time with exception of correlation based feature selection technique and the performance of the overall system is not degraded and its effectiveness is not compromised.

Table 8 Training times for different feature selection techniques

Feature selection	Bayes	J48	Random forest	PART
CFS	0.21	0.32	5.68	1.38
ALL	0.8	2.16	10.04	2.39
CHI	0.16	0.95	9.86	5.24
IG	0.28	0.98	9.52	5.07
<b>PROPOSED</b>	<b>0.35</b>	<b>0.82</b>	<b>6.99</b>	<b>1.36</b>

The work also compares the performance of proposed technique in terms of True Positive rate, false positive rate, precision, F measures and ROC with other schemes as indicated in Table 7. Comparing our proposed technique against using the full dataset with 42 features, the table indicates some enhancement has been obtained and even no degradation is observed. For instance, the false positive and accuracy have been decreased around 3% and improved about 5% respectively. Additionally, it is shown that the proposed technique has the best performance among other feature selection techniques.

Table 10 and Table 11 presents the performance of different classification algorithms with the proposed selected feature and full dataset, respectively. It is apparent that, with regard to the decrease in the training time, the overall performance of the model is enhanced comparing to using 42 features although with some exceptions. The false alarm rate for PART classifier, for example, with an increase about 1 % has a negative impact on the performance of proposed features set, however since the other evaluation metrics has increased or maintained at the same level, this adverse impact can be considered negligible. Moreover, among all classifiers, J48 classifier has the highest accuracy and precision and the lowest miss and false alarm rate, hence considered to be the best classifier for the proposed feature selection technique.

Table 11 and 12 demonstrate the performance of different feature selection techniques tested with different classification algorithms namely: J48, Random forest, PART and Bayesian in terms of detection rate and false positive rate, respectively. As it can be observed, regardless of the classification algorithms, the performance of the proposed technique significantly improves comparing to other schemes. For instance, the detection rate of our proposed technique is averagely 99% for all the classifiers as compared to the ALL, CFS, CHI and IG feature selection technique with average detection rate of 98 %, 98%, 91% AND 92% respectively. Similarly, Table 9 shows that the false alarm rate for the proposed technique with a significant drop comparing to other schemes helps to enhance the performance. For example, on average the proposed scheme with 1% has significantly less false alarm rate than ALL, CFS, CHI and IG feature selection technique with 2, 2, 10 and 8 %, respectively.

Classification Results Using All 42 Features of NSL-KDD Dataset

Table 9 Classification Results Using All Features of NSL KDD Dataset

Classifier	TP	FP	PR	RECALL	FM	ROC
J48	99	0.8	98	97	97	99
R Forest	99	0.8	96	98	98	99
Bayesian	97	1.7	97	97	97	99
PART	99	0.7	98	98	97	99

Table 10 Classification Results Using Proposed Features of NSL KDD Dataset

Classifier	TP	FR	PR	RECALL	FM	ROC
J48	99	0.4	99	99	99	99
R Forest	99	0.2	99	99	99	1
Bayesian	95	1.6	96	95	96	99
PART	99	0.3	99	99	99	99

Table 11 The Performance of five Feature Selection Techniques with Different Classifier in Terms of Detection Rate

FST	J48	RF	PAR T	BAYES
Full	99	99	99	95
CFS	99	99	98	97
Chi square	92	93	93	88
IG	93	93	93	88
PROPOSE D	99	99	99	97

Table 12 The performance of feature selection techniques with different classifier in terms of false positive rates

FST	J48	RF	PART	BAYESIAN
FULL	1	1	1	5
CFS	1	1	2	3
PROPOSE D	1	1	1	3
CHI	8	7	7	12
IG	7	7	7	12

## Conclusions

This work examines the features included in NSL- KDD dataset to identify the significant features and reduce the number of features in the NSL- KDD dataset. Therefore, a subset of significant features in detecting intrusion can be proposed by using machine learning techniques. These features then can be used in the design of Intrusion Detection Systems (IDS), working towards automating anomaly detection with less overhead. The most important features to detect cyber-attacks are basic features such as source byte, destination byte, the used service, a flag to indicate the status of the connection. Moreover, time-based traffic features are important to analysis and detect cyber-attacks, such as information about the percentage of connections in the past 2 seconds with a different service than current connection. To detect R2L and U2R attacks it is important to study content features.

The proposed feature selection technique is compared with other well-known feature selection algorithms namely: CFS, IG, and chi-squared on NSL-KDD dataset. The results indicate that the proposed technique has considerably less training time while maintaining accuracy and precision. In addition, to demonstrate the effect of pre-processing dataset on classification rate using filter feature selection methods, different feature selection techniques are tested with four different classification algorithms namely: J48, Random forest, PART and Bayesianin terms of detection rate and False Alarm Rate. Regardless of the classification algorithm, the results indicate that the proposed scheme out performs other techniques. Another observation from comparison results between the proposed technique and using the full dataset is that J48 classification algorithm performs better with proposed feature selection algorithm than other classifiers. This is expected as random forest is an ensemble classifier that combines a collection of classifiers to make a forest.

### References

- [1] M. M. Siraj, H. Hussein, T. Albasheer, and M. M. Din, "Towards Predictive Real-time Multi-sensors Intrusion Alert Correlation Framework," *Indian J. Sci. Technol. ISSN*, vol. 8, no. 12, pp. 974–6846, 2015.
- [2] M. C. Belavagi and B. Muniyal, "Performance Evaluation of Supervised Machine Learning Algorithms for Intrusion Detection," *Procedia Comput. Sci.*, vol. 89, pp. 117–123, 2016.
- [3] H. Singh and D. Kumar, "A study on Performance analysis of various feature selection techniques in intrusion detection system," *Int. J. Adv. Res. Comput. Sci. Manag. Stud.*, vol. 3, no. 6, pp. 2321–7782, 2015.
- [4] M. Othman and T. Maklumat, "Mobile Computing and Communications: An Introduction," *Malaysian J. Comput. ...*, vol. 12, no. 2, pp. 71–78, 1999.
- [5] K. Kumar, "Network Intrusion Detection with Feature Selection Techniques using Machine-Learning Algorithms," vol. 150, no. 12, pp. 1–13, 2016.
- [6] J. Song, "Feature Selection for Intrusion Detection System Jingping Song Declaration and Statement," p. 132, 2016.
- [7] N. A. Noureldien and I. M. Yousif, "Accuracy of Machine Learning Algorithms in Detecting DoS Attacks Types," vol. 6, no. 4, pp. 89–92, 2016.
- [8] A. Thesis, "Using Support Vector Machines in Anomaly Intrusion Detection by," 2015.
- [9] P. Verma, "Performance of Detection Attack using IDS Technique," vol. 4, no. 3, pp. 624–629, 2016.
- [10] J. Juanchaiyaphum, N. Arch-int, and S. Arch-int, "A Novel Lightweight Hybrid Intrusion Detection Method Using a Combination of Data Mining Techniques," *Int. J. Secur. its Appl.*, vol. 9, no. 4, pp. 91–106, 2015.
- [11] P. Manandhar, "A Practical Approach to Anomaly - based Intrusion Detection System by Outlier Mining in Network Traffic By," 2014.
- [12] A. I. Madbouly, A. M. Gody, and T. M. Barakat, "Relevant Feature Selection Model Using Data Mining for Intrusion Detection System," *Int. J. Eng. Trends Technol.*, vol. 9, no. 10, pp. 501–512, 2014.
- [13] M. A. Ambusaidi, X. He, Z. Tan, P. Nanda, L. F. Lu, and U. T. Nagar, "A Novel Feature Selection Approach for Intrusion Detection Data Classification," *2014 IEEE 13th Int. Conf. Trust. Secur. Priv. Comput. Commun.*, pp. 82–89, 2014.
- [14] D. a. M. S. Revathi, "A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion Detection," *Int. J. Eng. Res. Technol.*, vol. 2, no. 12,

- pp. 1848–1853, 2013.
- [15] S. K. Sahu, S. Sarangi, and S. K. Jena, “A detail analysis on intrusion detection datasets,” *Souvenir 2014 IEEE Int. Adv. Comput. Conf. IACC 2014*, no. December, pp. 1348–1353, 2014.
  - [16] Z. Dewa and L. A. Maglaras, “Data Mining and Intrusion Detection Systems,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 1, no. 1, p. 1:7, 2016.
  - [17] Y. Wahba, E. ElSalamouny, and G. ElTaweel, “Improving the Performance of Multi-class Intrusion Detection Systems using Feature Reduction,” *Ijcsi*, vol. 12, no. 3, pp. 255–262, 2015.
  - [18] V. Barot, S. Singh Chauhan, and B. Patel, “Feature Selection for Modeling Intrusion Detection,” *Int. J. Comput. Netw. Inf. Secur.*, vol. 6, no. 7, pp. 56–62, 2014.
  - [19] M. B. Shahbaz, X. Wang, A. Behnad, and J. Samarabandu, “On Efficiency Enhancement of the Correlation-based Feature Selection for Intrusion Detection Systems,” 2016.
  - [20] A. AliShah, M. Sikander Hayat Khiyal, and M. Daud Awan, “Analysis of Machine Learning Techniques for Intrusion Detection System: A Review,” *Int. J. Comput. Appl.*, vol. 119, no. 3, pp. 19–29, 2015.
  - [21] S. Thaseen and C. A. Kumar, “Intrusion Detection Model using PCA and Ensemble of Classifiers,” vol. 16, no. 2, pp. 15–38, 2016.
  - [22] R. Pradhan, “Performance Assessment of Robust Ensemble Model for Intrusion Detection using Decision Tree Techniques,” vol. 3, no. 3, pp. 78–86, 2014.
  - [23] S. L. Pundir and Amrita, “Feature Selection Using Random Forest in Intrusion Detection,” *Int. J. Adv. Eng. Technol.*, vol. 6, no. 3, pp. 1319–1324, 2013.
  - [24] A. A. Ramaki, M. Khosravi-Farmad, and A. G. Bafghi, “Real time alert correlation and prediction using Bayesian networks,” *2015 12th Int. Iran. Soc. Cryptol. Conf. Inf. Secur. Cryptol.*, vol. 978, pp. 98–103, 2015.
  - [25] R. Kaur and M. Sachdeva, “International Journal of Advanced Research in An Empirical Analysis of Classification Approches for Feature Selection in Intrusion Detection,” vol. 6, no. 9, 2016.
  - [26] J. H. Assi and A. T. Sadiq, “NSL-KDD dataset Classification Using Five Classification Methods and Three Feature Selection Strategies,” vol. 7, no. 1, pp. 15–28, 2017.
  - [27] Kamesh and N. Sakthi Priya, “Security enhancement of authenticated RFID generation,” *Int. J. Appl. Eng. Res.*, vol. 9, no. 22, pp. 5968–5974, 2014.
  - [28] M. K. Gambo and A. Yasin, “Hybrid Approach for Intrusion Detection Model Using Combination of K-Means Clustering Algorithm and Random Forest Classification,” *Ijes*, vol. 6, no. 1, pp. 93–97, 2017.
  - [29] Dubb Shruti and Sood Yamini, “Feature Selection Approach for Intrusion Detection System,” *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 2, no. 5, pp. 47–53, 2013.
  - [30] N. Shahadat, I. Hossain, A. Rohman, and N. Matin, “Experimental Analysis of Data Mining Application for Intrusion Detection with Feature reduction,” pp. 209–216, 2017.
  - [31] A. Jain and J. L. Rana, “Classifier Selection Models for Intrusion Detection System (Ids),” *Informatics Eng. an Int. J.*, vol. 4, no. 1, pp. 1–11, 2016.
  - [32] M. R. Parsaei, S. M. Rostami, and R. Javidan, “A Hybrid Data Mining Approach for Intrusion Detection on Imbalanced NSL-KDD Dataset,” vol. 7, no. 6, pp. 20–25, 2016.

## **Assessing Security Risk Caused By Smart Mobile Devices In A University Network Through A Web-Based Threat Matrix**

Irene WanjiruWanja  
School of Computer Science and Bioinformatics  
Kabarak University, Private Bag 20157 Kabarak, Kenya  
Email: iwanja@kabarak.ac.ke

### **ABSTRACT**

The need by staff and students to use smart mobile devices in university network is indisputable. This is because they help them to work and study more effectively as well as achieve better work-life balance. However smart mobile devices pose a security challenge as they continue to expand the corporate network unchecked thus increasing the attack surface. The purpose of this study is to develop a web-based threat matrix that computes likelihood of threat attack. The matrix indicates risk exposure levels and provide recommendations that maximize the protection of confidentiality, integrity and availability of university data while still providing functionality and usability of smartmobile devices.

### **Introduction**

A university local area network comprise of interconnected key departments and other offices within a university campus or campuses. Computers and other smart mobile devices use LAN connection to share resources such as a printer or network storage. The nodes are usually interconnected either through wired or wireless means. Smart mobile devices (SMD) refers to any physical object associated with computing resources and is capable of transmitting data to other similar objects either through physical transmission medium and logical protocols or with human through the device user interface (Somayya&Hema, 2016). BYOD (Bring Your Own Device) is a technology, concept or strategy for employees and in this case students prefer working with their personal smartmobile devices such as smart phones, tablet PCs and laptop computers to access corporate internal resources such as database and applications.

The use of smartmobile devices in a corporate network has introduced the need manage and control devices and data not only in an IT department inside a company but also by individual users. Hence security policies should be focused on both user-centered security policies and devices-centered security policies. With the advent of BYOD it has become necessary to supervise not only a specific point of access but also all points of access to corporate network.

To enhance the benefits brought about by use of smart mobile devices in a corporate environment security issues must be addressed. According to Miller, Voas and Hurlburt (2012) smartmobile devices contain a wealth of personal information which may be mixed with corporate information stored on the same device. This creates the need to control access to these devices to protect the privacy of information. When both organization and personal information coexist in one device, it becomes a challenge to find a balance between security control for organization's data and privacy of personal data (Ghosh, Gajar&Rai, 2013).

### **Problem statement**

Despite of the fact that use of smartmobile devices increases convenience and efficiency of work and study, they pose a security challenge as they continue to expand the corporate network unchecked thus increasing the attack surface. One of the major reasons for increased security threats is the concern of managing disparate smartmobile devices which are heterogeneous.

In an environment where bring your own device (BYOD) policy is encouraged, it is important to consider a flexible security policy that accommodates the numerous types of terminals and their diverse use. This can easily be done if there is a threat assessment tool that can inform the level of exposure to attack and hence provide some policy review advisory notes or guideline. In addition such a tool can help to provide guidelines on technical security mechanisms or otherwise to aid in enforcing the security policy. This is the sole purpose of this study.

### **Research objective**

- (i) To develop a threat matrix to compute likelihood of threat attack on a university network and provide security requirements based on the computed likelihood of attack

### **Research Question**

- (i) How can a threat matrix that computes likelihood of threat attack be developed?

## **2. LITERATURE REVIEW**

### **2.1 Smart mobile Devices Security Threats**

(Goguen&Fringa, 2002) define threat as the likelihood of a particular threat-source to exercise vulnerability or a weakness that can be accidentally triggered or intentionally exploited. Computing devices connect to the Internet in a variety of ways such as wirelessly using a Wi-Fi card and a wireless internet connection or hotspot, through a broadband connection such as third generation (3G) or fourth generation (4G) wireless connections provided by a cellular network, or by tethering using a cellphone as a modem (Pinola, 2012).

The benefits of using smartmobile devices also come with various cyber security threats and vulnerabilities. These vulnerabilities can be related to the hardware of the device, the internet connections (Bluetooth or wireless), installed applications, stored data and information transfer. Threats can be rated as low, medium or high depending on the likelihood to occur and the impact to the user (Bosworth, Kabay&Whyne, 2009).

Malware threats include viruses, Trojans, worms, spyware and other malicious software which severely degrades and destroy computer's operating system. Most malware target laptops but threats against mobile phones have also increased recently (Friedman & Hoffman, 2008). Smartmobile devices with activated Bluetooth and set to discoverable mode are vulnerable to bluesnarfing attacks (Blue jacking Tools, 2012).

### **2.2 Security Requirement for Smart Mobile Devices**

Employers need to consider this risk when drafting security policies to ensure the rules on the use or prohibition of personal devices for company purposes are spelled out. Hardware and software of the device should be known to the employer and employees they are also required to



follow minimal secure practices on their devices before accessing company websites or e-mail (NZ Business, 2011).

It is hard to prevent theft or loss of devices, but the loss of data can be minimized by encrypting the information on the device, requiring a password, biometrics, or an access key to use and configuring the device to erase data after a number of failed logon attempts. The cost of these mitigations is minimal since most operating systems offer password protection and biometric systems are also relatively inexpensive (Milligan & Hutcheson, 2008).

Another option is to install software that allows remote wipe of the data such as Lojack for laptops and Sophos for smartphones (Barcelo, 2011). Users may not want to take the extra steps in logging on to their devices but the pay-off is rewarding if the device is lost or stolen.

Although some phishing attacks may be hard to recognize, the best prevention strategies are to read e-mail carefully to ensure it is from a reputable source, look for grammatical errors and avoid opening attachments unless their receipt is expected (Newman, 2011).

### **2.3 Security Solutions for Smart Mobile Devices**

According to (Antonio, 2012) there exists two main ways of addressing security concerns in a BYOD environment, this include access control where people are at the center and device control where devices are at the center. The research identifies three different security approaches that can be used to control smartmobile devices. Mobile Device Management (MDM) provides support to full device control through software solutions that companies can use to control, lock down, enforce policies and encrypt mobile devices. Mobile Application Management (MAM) according to this research acts like MDM but it is only applied to specific applications on a device. MAM can enable IT security personnel to control and secure specific corporate applications and leave the rest of the things contained on a smartmobile device to the user. Mobile Information Management (MIM) on the other hand allow files and documents synchronization across different devices to manage security.

Network Access Control (NAC) is a security framework which limits the number of connected devices while determining permissions and denying unrecognized devices access to a company's internal network (Downer & Bhattacharya, 2015). According to this research, NAC is useful in ensuring that likelihood of data leakage, infection of malware and other related attacks are avoided or minimized.

Desktop virtualization is a type of security framework which enables desktop computers, virtual machines of servers to host sessions for remotely located smartmobile devices (Downer & Bhattacharya, 2015). These models centralize resources, data as well as security management. This reduces or eliminates the need to transmit data onto smartmobile devices and hence reduces the likelihood of data leakage.

Containerization is used as a security framework to partition smartmobile device storage into different independent sections which separates personal data from work data (Rhodes, 2013). Each section has its own security policies and allows remote access for company control without affecting personal data.

Remote wiping is a reactive solution which is triggered when a device is lost or stolen or when the owner leaves the company (Downer & Bhattacharya, 2015). This is done by removing all company applications and data contained in the smartmobile device. Some MDM and MAM solutions already contain remote wiping procedures.

## **2.4 Research Gap**

From the security solution for smart mobile devices presented in section 2.3 above, none of them integrates a threat assessment as part of their proposed solution. Before designing and deploying smartmobile device security solutions, it would be prudent to assess the security status in order to implement the most suitable solution. However there seems to be no tool designed to assess risks and threats brought about by use of smartmobile devices before proposing a solution.

Using ISO 27001 best practices as benchmark framework, the researcher aimed at designing a matrix with a more comprehensive approach that comprised five of the domains of ISO 27001. This includes; information security policy, asset management, access control, operations security and communications security.

The developed security matrix will act as a risk assessment tool to determine likelihood of attack from various threats introduced to university network through use of smartmobile devices. After submitting the assessment questions included in the matrix, feasible threats and vulnerabilities will be identified. The computed likelihood of attack information will help the university determine the security controls that need to be improved or to be added to the network.

## **3. METHODOLOGY**

### **3.1 Matrix implementation and discussion**

The matrix which is in the form of a web-based model is developed using rapid prototyping approach which will enable testing and evaluation at an early stage. The matrix will have various module including; user registration module to allow new users to register in order to access other system functionalities. User login module to allow only authorized users to access the system functionalities after submitting the correct credentials. Assessment module to allow users to answer the assessment questions; the results are then submitted to the database and are used to compute the likelihood of attack. Reports module to allow users to view their scores and recommendations of the submitted assessment.

### **3.2 System Design and Testing**

A logical design of the STM web-based model is presented in this section. It is comprised of several sections to expound on the system design and testing. Figures 1 to 6 presents flowcharts for the system.

#### **3.2.1 User Registration**

This is the first section of the STM model where every user is expected to register in-order access the system. Personal details such as user name, email address, name of organization, user category and password are required in this interface. Figure 1 below provides flowchart of the registration process while figure 2 provides the graphical user interface of the registration module.

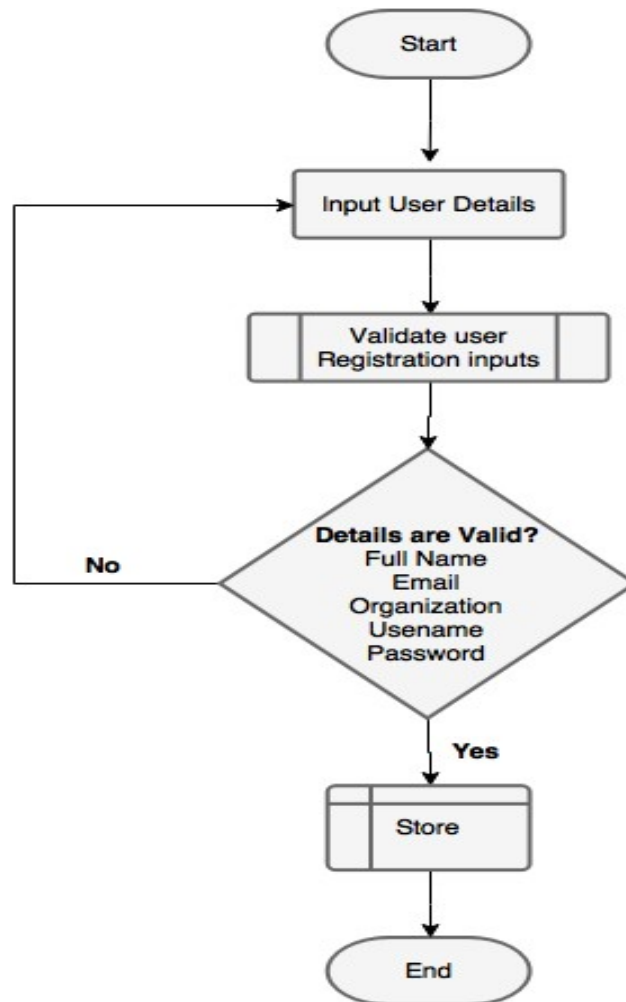
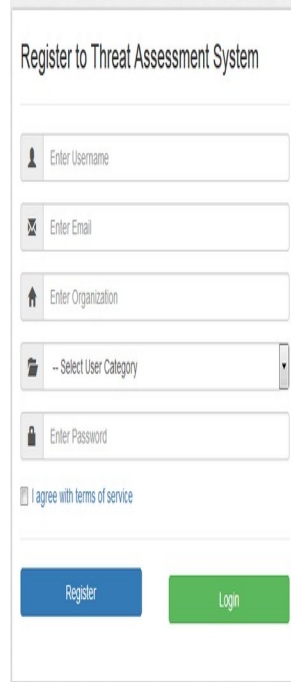


Figure 1. Registration Process Flowchart  
Source: Researcher (2018)



The image shows a web form titled "Register to Threat Assessment System". It contains several input fields: "Enter Username" with a person icon, "Enter Email" with an envelope icon, "Enter Organization" with a house icon, and a dropdown menu labeled "-- Select User Category" with a folder icon. Below these is an "Enter Password" field with a lock icon and a checkbox labeled "I agree with terms of service". At the bottom, there are two buttons: a blue "Register" button and a green "Login" button.

Figure 2: Registration Process GUI  
**Source: Researcher (2018)**

### 3.2.2 Login Module

In this module, user sessions and logins are managed. When a user attempts to login, this module refers to the users' table in the database to determine if the user is registered or not and whether the user has provided the correct password. Figure 3 below shows a flowchart representing the logic of the login system whereas figure 4 presents a graphical user interface of the login system.

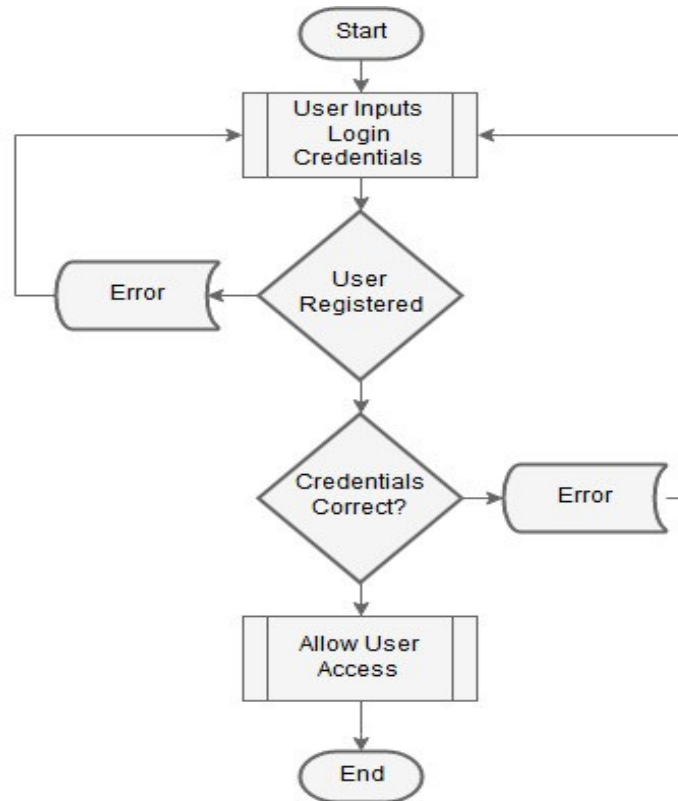


Figure 3: Login Process Flowchart  
Source: Researcher (2018)

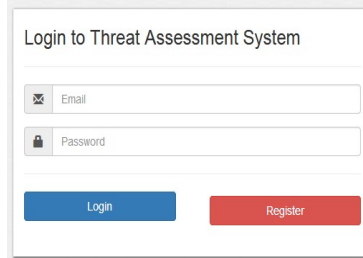


Figure 4: Login GUI  
Source: Researcher (2018)

### 3.2.3 Threat Assessment Module

This is a self-assessment module for staff and students in which the system displays questions which are retrieved from the database and has five choices to allow the user to select their preferred choice. Once the user has completed the assessment they are allowed to submit the results in the database from which the likelihood of attack is computed. Figure 5 below shows a flowchart presentation of the assessment logic whereas figure 6 is the presentation of the graphical user interface of the risk assessment module.

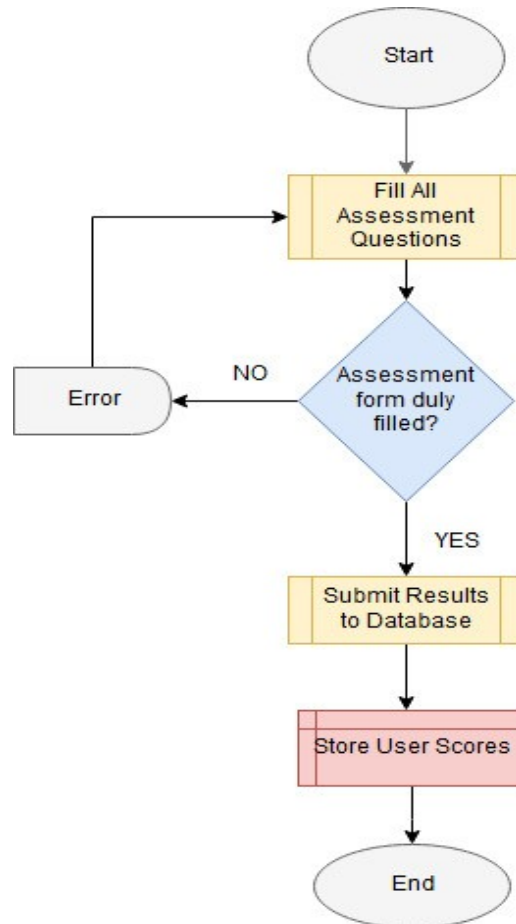


Figure 5: Threat Assessment Flowchart  
Source: Researcher (2018)

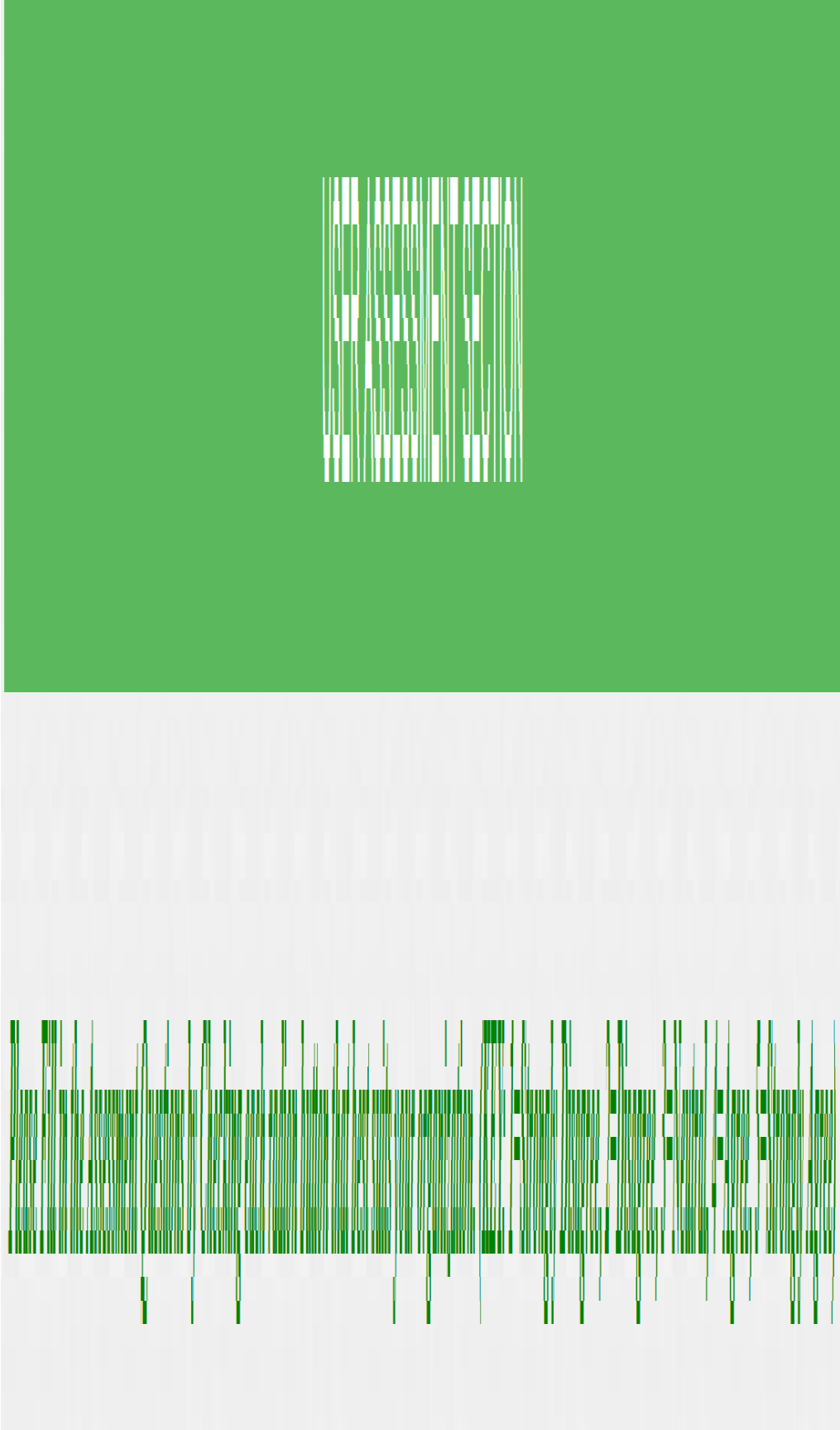


Figure 6: Threat Assessment GUI  
Source: Researcher (2018)

### 3.2.4 Likelihood of Attack Assessment Module

This module computes likelihood of threat attack depending on the scores obtained from the submitted assessments. Likelihood of attack was computed as a function weight derived from chapter 4 of this document as demonstrated below;

$$\text{Likelihood of Attack} = 5.233 + (-0.084 * \text{Information Security Policy}) + (0.199 * \text{Asset Management}) + (-0.003 * \text{Access Control}) + (-0.101 * \text{Operations Security}) + (-0.530 * \text{Communications Security}) + 0.335. \quad \text{Equation 1}$$

A threat is very likely to attack the university network if the user scores 1 for all the 45 assessment questions. Similarly a threat is very unlikely to attack if the user scores 5 for all the assessment questions. Possible likelihood of attack is achieved if the user scores 3 in every assessment question. Figure 6 shows a flowchart presentation of likelihood of attack computation and figure 8 displays its GUI representation.

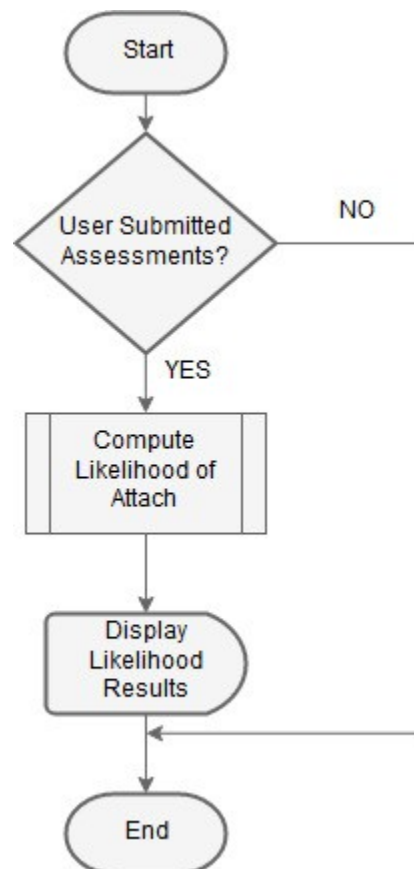


Figure 7: Likelihood of Attack Computation  
Source: Researcher (2018)



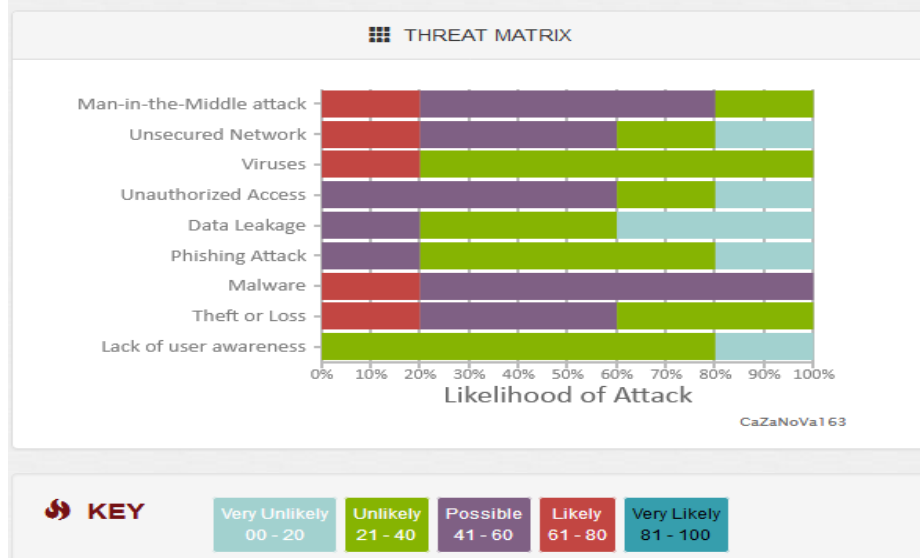


Figure 8: Threat Matrix GUI  
 Source: Researcher (2018)

### 3.2.5 Recommendations Component

Based on the user or professional assessments, this module suggests a number of recommendations necessary to mitigate threats resulting from use of smartmobile devices. This module filters the recommendations for all the questions whose user assessment scores goes below the threshold and allows the user to download the recommendations in printable document format (pdf). The figures 9 and 10 shows logic flowchart and GUI presentations respectively.

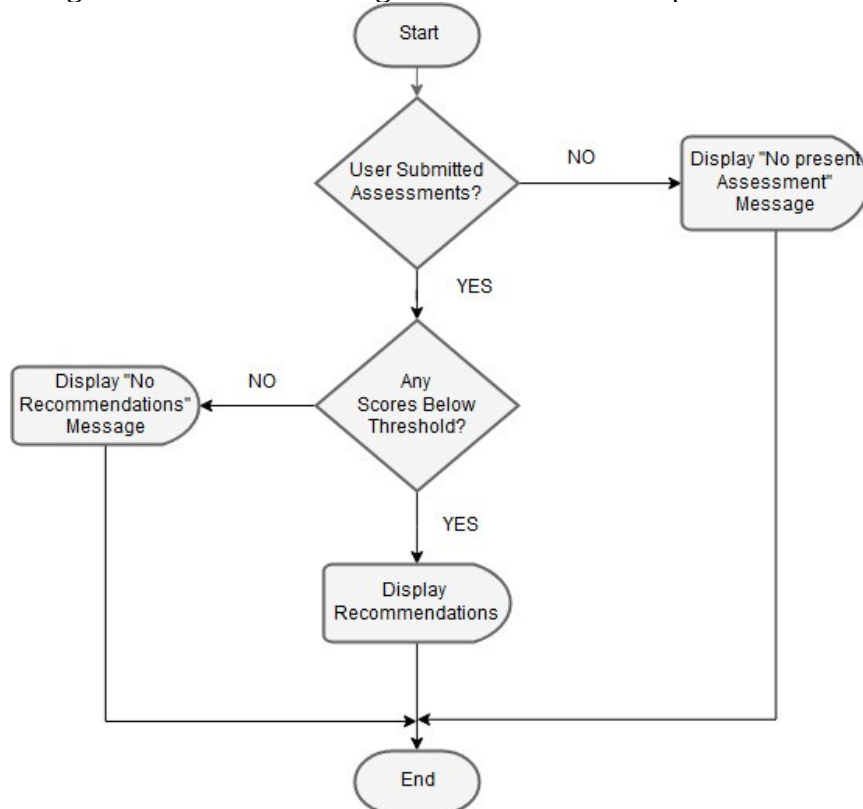
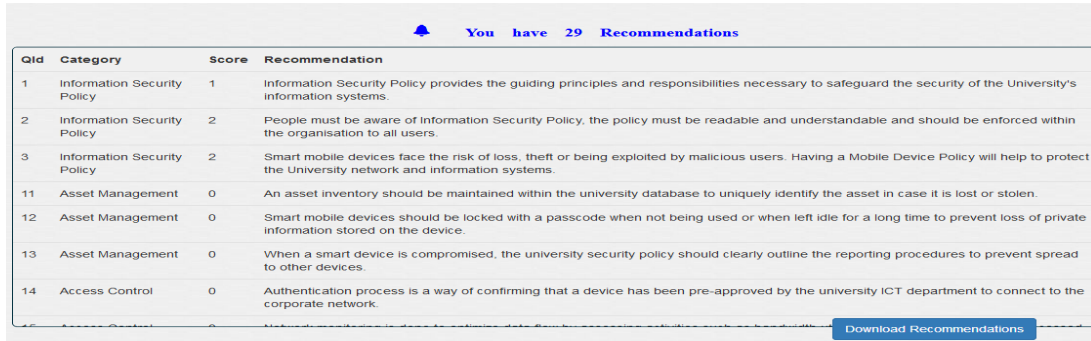


Figure 9: Recommendations Flowchart  
Source: Researcher (2018)



QId	Category	Score	Recommendation
1	Information Security Policy	1	Information Security Policy provides the guiding principles and responsibilities necessary to safeguard the security of the University's information systems.
2	Information Security Policy	2	People must be aware of Information Security Policy, the policy must be readable and understandable and should be enforced within the organisation to all users.
3	Information Security Policy	2	Smart mobile devices face the risk of loss, theft or being exploited by malicious users. Having a Mobile Device Policy will help to protect the University network and information systems.
11	Asset Management	0	An asset inventory should be maintained within the university database to uniquely identify the asset in case it is lost or stolen.
12	Asset Management	0	Smart mobile devices should be locked with a passcode when not being used or when left idle for a long time to prevent loss of private information stored on the device.
13	Asset Management	0	When a smart device is compromised, the university security policy should clearly outline the reporting procedures to prevent spread to other devices.
14	Access Control	0	Authentication process is a way of confirming that a device has been pre-approved by the university ICT department to connect to the corporate network.

[Download Recommendations](#)

Figure 10: Recommendations GUI  
Source: Researcher (2018)

### 3.2.5 Proof of Concept

The STM system prototype was developed as a proof of concept using MySQL as the database engine and PHP as server side-scripting language. Bootstrap 4 which is a framework of CSS was used to style user interface for the purpose of user interaction with the system. phpStorm was used as program editor to write and test the code. Apache web server assisted in running the application locally. The application was later deployed online and is accessible through [www.irenewanja.com](http://www.irenewanja.com)

## 4. CONCLUSION

The study sought to assess security threats introduced to the university information systems and data through use of smartmobile devices. A Threat Matrix which was a web-based model was developed to show levels of likelihood of attack for various threats that were found to be common. This assisted in determining the security gap that needed to be addressed to enhance security of the university network. The matrix also provided recommendations on security requirements that were needed to improve the security status of the university network.

### 4.1 Suggestions for Further Research

#### 4.1.1 Likelihood of Attack versus Impact Assessment

The main purpose of the developed Threat Matrix was to determine the possibility of threat attack to the university network. To advance the system operations, further research on how to compute the impact created by the threat in the event that it succeeds in launching the attack. This would help the university ICT security experts to prioritize on the risks that have high impact while employing the countermeasures.

### References

- Abdelrahman, O. H., Gelenbe, E., Görbil, G., & Oklander, B. (2013). Mobile network anomaly detection and mitigation: The NEMESYS approach. In *Information Sciences and Systems 2013* (pp. 429-438). Springer, Cham
- Abomhara, M., & Kjøien, G. M. (2014, May). Security and privacy in the Internet of Things: Current status and open issues. In *Privacy and Security in Systems (PRISMS), 2014 International Conference on* (pp. 1-8). IEEE.
- Arabo, A., & Pranggono, B. (2013, May) malware and smart device security: Trends, challenges and solutions. In *Control Systems and Computer Science (CSCS), 2013 19th International Conference on* (pp. 526-531). IEEE.
- AT&T State of IoT Security survey, (2015). *Exploring IoT Security*. The CEO's guide to securing the Internet of Things. Volume 2 retrieved from <https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf> (accessed 10th march, 2017)
- Aware, W. T. A., Documentation, T. P. S., & Logical, C. (2005). Information technology–Security techniques–Information security management systems–Requirements.
- Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011, February). Proposed embedded security framework for internet of things (iot). In *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE), 2011 2nd International Conference on* (pp. 1-5). IEEE.
- Barcelo, Y. (2011, September). Insecurity. *CA Magazine*, pp. 36-38.

- Beach, A., Gartrell, M., & Han, R. (2009, August). Solutions to security and privacy issues in social networking. In *Computational Science and Engineering, 2009. CSE'09. International Conference on* (Vol. 4, pp. 1036-1042). IEEE.
- Bernabe, J. B., Hernández, J. L., Moreno, M. V., & Gomez, A. F. S. (2014, December). Privacy-preserving security framework for a social-aware internet of things. In *International Conference on Ubiquitous Computing and Ambient Intelligence* (pp. 408-415). Springer International Publishing.
- Bluejacking Tools. (2012). *Phone Spy*. Retrieved from Bluejacking Tools: <http://www.bluejackingtools.com/bluesnarf--spy/-phone-spy/>(accessed 11<sup>th</sup> September, 2017)
- Bosworth, S., Kabay, M., & Whyne, E. (2009). Physical Threats to the Information Infrastructure. In F. Platt, *Computer Security Handbook*. New York: John Wiley & Sons Inc.
- Business Insider, (2016). IoT-Ecosystem, what is the internet of things, retrieved from <http://www.businessinsider.com/iot-ecosystem-what-is-the-internet-of-things-2016>(accessed 4<sup>th</sup> March, 2017)
- Calder, A. and Watkins, S. (2008). *IT Governance: A Manager's guide to Data Security and ISO27001/ISO 27002, 4th Edition*. London: Kogan Page Limited.
- Cisco.com (2014). *Cyber Threat Management from the Boardroom Risk*: Retrieved from [blogs.cisco.com: https://blogs.cisco.com/security/cyber-threat-management-from-the-board-room-risk-lost-in-translation](https://blogs.cisco.com/security/cyber-threat-management-from-the-board-room-risk-lost-in-translation)(accessed 8<sup>th</sup> November, 2017)
- Cisco.com (2017) *LAN Solutions Guide for Higher Education/Universities*. Retrieved from [Cisco.com:https://www.cisco.com/c/en/us/products/wireless/-office-net-software/index.html](https://www.cisco.com/c/en/us/products/wireless/-office-net-software/index.html) (accessed 11<sup>th</sup> September, 2017)
- Computer Weekly. (2010, July 12). *iTunes hack could affect thousands, say experts*. Retrieved from Computer Weekly: <http://www.computerweekly.com/news/1280093237/iTunes-hack-could-affect-thousands-say-experts>(accessed 11<sup>th</sup> September, 2017)
- Delac, G., Silic, M., & Krolo, J. (2011, May). Emerging security threats for mobile platforms. In *MIPRO, 2011 Proceedings of the 34th International Convention* (pp. 1468-1473). IEEE.
- Ernst & Young Global Limited, (2015). *The multiplying effect of today's cybersecurity challenges*. Cybersecurity and the Internet of Things.
- Friedman, J., & Hoffman, D. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. *Information Knowledge Systems Management*, 159-180.
- Gelenbe, E., Gorbil, G., Tzovaras, D., Liebergeld, S., Garcia, D., Baltatu, M., & Lyberopoulos, G. (2013, June). Security for smart mobile networks: The NEMESYS approach. In *Privacy and Security in Systems (PRISMS), 2013 International Conference on* (pp. 1-8). IEEE.
- Hossain, M. M., Fotouhi, M., & Hasan, R. (2015, June). Towards an analysis of security issues, challenges, and open problems in the internet of things. In *Services (SERVICES), 2015 IEEE World Congress on* (pp. 21-28). IEEE.
- Huang, X., Craig, P., Lin, H., & Yan, Z. (2015). SecIoT: a security framework for the Internet of Things. *Security and Communication Networks*.
- IEEE Standard Association, (2015). *Executive summary*, Internet of Things (IoT) Ecosystem study retrieved from <http://standards.ieee.org/innovate/iot/study.html>(accessed 4<sup>th</sup> March, 2017)

- Infosecinstitute.com (2014). Cyber Threat Analysis: Retrieved from: <http://resources.infosecinstitute.com/cyber-threat-analysis/#gref>(accessed 8<sup>th</sup>November,2017)
- Jha, A., & Sunil, M. C. (2014). Security considerations for Internet of Things. *L&T Technology Services*.
- Kim, D. H., Cho, J. Y., Kim, S., & Lim, J. (2015). A Study of Developing Security Requirements for Internet of Things (IoT). *Advanced Science and Technology Letters*, 87, 94-99.
- Kim, J. T. (2015). Requirement of Security for IoT Application based on Gateway System. *International Journal of Security and Its Applications*, 9(10), 201-208.
- Kim, J., & Lee, J. W. (2014, March). OpenIoT: An open service framework for the Internet of Things. In *Internet of Things (WF-IoT), 2014 IEEE World Forum on* (pp. 89-93). IEEE.
- Koh, E. B., Oh, J., & Im, C. (2014). A study on security threats and dynamic access control technology for BYOD, smart-work environment. In *Proceedings of the International MultiConference of Engineers and Computer Scientists* (Vol. 2, pp. 1-6).
- KPMG, (2015). *Focus on Security, Privacy and Trust*. Security and the IoT Ecosystem
- Lee, Y., & Kim, D. (2015). Threats Analysis, Requirements and Considerations for Secure Internet of Things. *International Journal of Smart Home*, 9(12), 191-198.
- Madakam, S., & Date, H. (2016). Security mechanisms for connectivity of smart devices in the internet of things. In *Connectivity Frameworks for Smart Devices* (pp. 23-41). Springer International Publishing.
- Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S., & Frye, J. (2012). Cyber threat metrics. *Sandia National Laboratories*.
- Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *It Professional*, 14(5), 53-55.
- Milligan, P. M., & Hutcheson, D. (2008). Business Risks and Security Assessment for Devices. *Information Systems Control Journal*, 1-5.
- Mohammed, L. A. (2010). ICT Security Policy: Challenges and Potential Remedies. *Handbook of Research on Information Communication Technology Policy: Trends, Issues and Advancements: Trends, Issues and Advancements*, 337.
- Newman, J. (2011, June 3). *4 Security Tips Spurred by Recent Phishing Attacks*. Retrieved from PC World: [http://www.pcworld.com/article/229361/4\\_security\\_tips\\_spurred\\_by\\_recent\\_phishing\\_attacks\\_on\\_gmail\\_hotmail\\_and\\_yahoo.html](http://www.pcworld.com/article/229361/4_security_tips_spurred_by_recent_phishing_attacks_on_gmail_hotmail_and_yahoo.html)(accessed 12<sup>th</sup> September, 2017)
- NIST, G. S., Goguen, A., & Fringa, A. (2002). Risk Management Guide for Information Technology Systems. *Recommendations of the National Institute of Standards and Technology*.
- NZ Business. (2011, September). Are mobile devices compromising your business security? *NZ Business*, p. 60.
- O'Dell, J. (2010, April 13). *New Study Shows the Web Will Rule by 2015*. Retrieved from Mashable: <http://mashable.com/2010/04/13/-web-stats>(accessed 11<sup>th</sup> September, 2017)
- Open Web Application Security Project (OWASP) IoT Top Ten Vulnerabilities. 2014. DOI [https://www.owasp.org/images/7/71/Internet\\_of\\_Things\\_Top\\_Ten\\_2014-OWASP.pdf](https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf)
- Pinola, M. (2012). *Internet Access Comparison*. Retrieved from About.com Office Technology: Pros and cons of different Internet-on-the-Go options:

- <http://office.about.com/od/wificonnectivity/a/wireless-internet-comparison.html> (accessed 12<sup>th</sup> September, 2017)
- PTC Cloud Services, (2016). *Seven Steps to Minimize IoT Risk in the Cloud*. Securing the Internet of Things. White paper
- Rahman, A. F. A., Daud, M., & Mohamad, M. Z. (2016, March). Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework. In *Proceedings of the International Conference on Internet of things and Cloud Computing* (p. 79). ACM.
- Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z., & Bouabdallah, A. (2013, May). A systemic approach for IoT security. In *Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on* (pp. 351-355). IEEE.
- Sabale, R. G. & Dani, A. R. (2012). Comparative study of prototype model for software engineering with system development life cycle. *IOSR Journal of Engineering*, 2(7), 21-24.
- Saif, I., Peasley, S., & Perinkolam, A. (2015). *Being secure, vigilant and resilient in the connected age*. Safeguarding the Internet of Things. *The Internet of Things*, 41 retrieved from <https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-17/internet-of-things-data-security-and-privacy.html> (accessed 10th March, 2017)
- Shafagh, H., & Hithnawi, A. (2014, May). Security Comes First, A Public-key Cryptography Framework for the Internet of Things. In *Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on* (pp. 135-136). IEEE.
- Shukla, I. (2011, September 21). *Advantages of Computing*. Retrieved from Buzzle.com: <http://www.buzzle.com/articles/advantages-of-computing.html> (accessed 13<sup>th</sup> September, 2017)
- Sopori, D., Pawar, T., Patil, M., & Ravindran, R. (2017) Internet of Things: Security Threats.
- Souppaya, M., & Scarfone, K. (2013). Guidelines for managing the security of devices in the enterprise. *NIST special publication*, 800, 124.
- Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In *Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on* (Vol. 3, pp. 648-651). IEEE.
- TechTarget.com (2016). *Managing Online Risk*. Retrieved from Techtarget.com: <http://searchsecurity.techtarget.com/feature/Managing-Online-Risk> (accessed 8<sup>th</sup> November, 2017)
- TechTarget.com. (2007). *Search Security Policy*. Retrieved from Techtarget.com: <http://searchsecurity.techtarget.com/definition/security-policy> (accessed 2<sup>nd</sup> October, 2017)
- TechTarget.com. (2012). *Search Computing*. Retrieved from Techtarget.com: <http://searchcomputing.techtarget.com> (accessed 11<sup>th</sup> October, 2017)
- TechTarget.com. (2017). *Search Mobile Computing*. Retrieved from Techtarget.com: <https://searchmobilecomputing.techtarget.com/definition/nomadic-computing> (accessed 11<sup>th</sup> October, 2017)
- Trendmicro.com (2015). *The Increasing Cyberattack Surface*. Retrieved from trendmicro.com: <https://blog.trendmicro.com/the-increasing-cyberattack-surface/> (accessed 2<sup>nd</sup> October, 2017)
- U.S. Department of Homeland Security, (2016). *Prioritizing IoT security*. Strategic principles for security Internet of Things (IoT) version 1.0 retrieved from

[https://www.dhs.gov/.../Strategic\\_Principles\\_for\\_Securing\\_the\\_Internet\\_of\\_Things-](https://www.dhs.gov/.../Strategic_Principles_for_Securing_the_Internet_of_Things-)  
(accessed 11th march, 2017).

- Vermesan, O., & Friess, P. (Eds.). (2013). *Internet of things: converging technologies for smart environments and integrated ecosystems*. River Publishers.
- Warwick, A. (2010, July 30). *Millions downloaded suspicious Android wallpaper*. Retrieved from Computer Weekly: <http://www.computerweekly.com/news/1280093401/Millions-download-suspicious-Android-wallpaper>(accessed 11<sup>th</sup> October, 2017)
- Westervelt, R. (2011, December 8). *Android app security: Study finds developers creating flawed Android apps*. Retrieved from SearchSecurity: <http://searchsecurity.techtarget.com/news/2240112235/Android-app-security-Study-finds--developers-creating-flawed-Android-apps>(accessed 11<sup>th</sup> October, 2017)
- Westervelt, R. (2011, December 9). Top 5 phone security threats in 2012. Retrieved from Search Security: <http://searchsecurity.techtarget.com/news/2240112288/Top-5--phone-security-threats-in-2012> (accessed 11<sup>th</sup> October, 2017)
- Youker, B. W. (2014). Goal-free Evaluation and Goal-Based Evaluation. *The Foundation Review* 5(4) 50-61.
- Zaidi, S. F. A., Shah, M. A., Kamran, M., Javaid, Q., & Zhang, S. (2016). A Survey on Security for Smartphone Device. *International Journal of Advanced Computer Science and Applications-2016*.
- Zhao, K., & Ge, L. (2013, December). A survey on the internet of things security. In *Computational Intelligence and Security (CIS), 2013 9th International Conference on* (pp. 663-667). IEEE.

## A Serial Number Based Identification Model for a Computer in a Wireless Local Area Network

Joseph Chebor  
Kabarak University

### 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. Apart from port numbers and IP addresses at application and network layers respectively, devices in a network use MAC addresses for identification at the physical layer. However MAC addresses can be altered thereby compromising the security, robustness and uniqueness qualities of a device identifier. This study therefore examined the inbuilt access and use of a serial number prototype system as an alternative method of identifying devices in a network. The model was constructed using evolutionary prototyping and proof of concept methods through test runs and was found to actually identify a device in a network based on a computer's serial number. It is then recommended that prototype be scaled up then adopted as network device identification method

**Key Words:** Computer, Serial Number-Based Identification, Wireless Local Area Network

### 1. Introduction

Wireless LANs (WLAN) also known as Wireless Fidelity (WiFi) or 802.11 standard is a type of a local area network that allows users access network services using mobile devices (wireless stations) such as laptops, personal digital assistance and even smart phones. The wireless stations use a base station usually an access point (AP) as an entry point to the network services. Unlike wired LANs, WLANs uses radio wave frequencies to transmit information over the local area network.

According to Mohapatra *et al.* 2014, currently most deployed WiFi technologies include Tri-band WiFi or WiGig or IEEE802.11ad, Light Fi (LiFi), Advanced Enterprise WiFi, WiFi CERTIFIED™ AC and Wi-Fi CERTIFIED Passpoint™ in the order of their technological advancement. Something common about all these technologies is in the improvements of speed of transmission in each subsequent technology. In addition to speed improvement, Advanced Enterprise WiFi allows users log in to a WiFi network using their social credentials. Wi-Fi CERTIFIED Passpoint™ ultimately allows online-sign up for mobile devices without a SIMM card.

WLAN come with a number of benefits as compared to wired LANs, notably mobility, rapid deployment, reduction in infrastructure and operational cost, flexibility and scalability (Idris & Kassim, 2010; Mandy, 2002; Nicopolitidis *et al.*, 2001). Due to these benefits hotspots are now virtually found everywhere; in enterprises, at homes and in public places. Wireless devices come with WiFi features integrated in 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. Frankel *et al.* (2007) points 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 (Vollbrecht & Moskowitz, 2002; Idris & Kassim, 2010; Stallings, 2011). Mandy, 2002 describes the reasons for the threats as default configurations, network architecture, encryption weaknesses, and physical security.

Identification, authentication and authorization as identified by Bruhn *et al.* (2003), are essential functions in providing the required services in a network. The essential network services as suggested by Frankel *et al.* (2007) are confidentiality, integrity, availability and access control. The most common authentication and authorization techniques that are currently applied as a security measure in wireless LANs include WEP, WPA, WPA2 and RADIUS together with usernames and passwords.

Yet for authentication and authorization 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 or MAC address. 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, 2006).

#### Problem Statement

Normally, every product (including a computer) or a thing of concern to an institution has an identifier to identify the product uniquely. In normal circumstances, hosts are identified by either a MAC Address or an IP address. Takahashi *et al.* (2010), refers to such identifiers as explicit or indirect identifiers because the identifiers are actually not meant to identify the devices rather they identify processes running in the devices and location of the devices. As such, 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 (Kurose & Ross, 2006).

In particular, a MAC address at the physical layer is usually hard coded or ‘burned’ into the network hardware therefore it is difficult to alter it. However copy of the MAC address in the operating system can easily be modified by an attacker to suit the valid MAC addresses spoofed.

If devices in a network cannot be correctly identified, then it can go a long way in contributing to security flaws in as far as authentication and authorization is concerned. It is for this reason then that the study seeks to investigate how a serial number may be used for physical identification of devices in a wireless LAN

#### Research Objectives

The main aim of the study was to investigate how a serial number may be used for physical identification of a computer in a wireless LAN. The specific objectives are:

1. To analyse the suitability of network device identifiers that are currently in use
2. To develop an algorithm that can obtain a remote computer’s serial number in a wireless LAN

3. To Design a model that uses a computer's serial number to identify the computer in a wireless LAN
4. To implement the prototype that uses a computer's serial number to identify the computer in a wireless LAN

### 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.* (2005) further cites examples of identifiers as could be a code (identification number, serial number, ISBN) name (domain name) or an address (IP, MAC or Port Number). Clark, 2003 cites port numbers, IP addresses and MAC addresses as the most commonly used identifiers or what is referred to as service access point identifiers (SAPs) for network address and hardware addresses.

An attribute should possess uniqueness, universality, collectability, security, data dependence, robustness and mnemonic (Danev *et al.* 2015, Leo, 2004 and Bolle *et al.* 2003) qualities to be a good identifier. Whereas uniqueness ensures that no two devices have the identifier, 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.

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 pose 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 (Canvan, 2000).

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, 2003. An IPv4, which is currently in use (Kurose & Ross, 2006), 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, 2006). DHCP assigns devices IP addresses on demand, therefore two devices can use the same IP address but on different occasions.

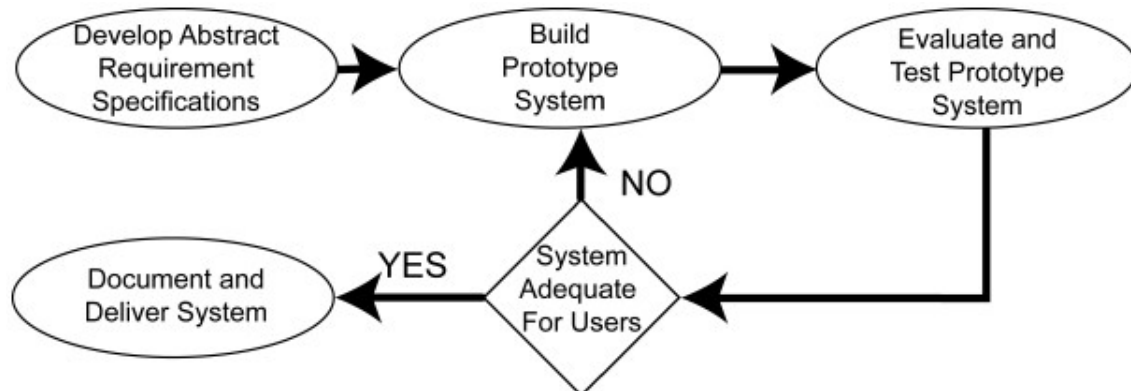
MAC address also known as LAN address or a physical address is a number used to identify a network adaptor on a LAN. As Kurose & Ross, 2006 puts it "it is not hosts and routers that have link-layer addresses but rather their adapters (that is, network interfaces) that have link-layer addresses." In other 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, 2006 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.

Identification is the process of association an object or an individual with an identity (Jain *et al.* 2000), thus establishing the identity of the entity. Identification answers the question that concerns who or what the entity is. It's a means of series of identification that the identity of an entity is constituted and specified. Luis-Garcia *et al.* 2004, sites examples of identification strategies as could be something known to the entity such as password or a personal identification number (PIN) or something owned by the entity such as a card, a token or a key. From the time of the use of identification friend or foe (IFF) during the Second World War, (Lehtonen *et al.*, 2008), identification technologies advances such as barcode readers, optical character recognition (OCR), biometric identification system (BIS) and radio frequency identification (RFD) took effect.

### Methodology

The study adopted a proof of concept (PoC) evolutionary prototyping approach to proof that a serial number can be used to identify a computer in a WLAN. Apart from proofing the functionality of the system (Yang and Epstein, 2005), evolutionary prototyping is used when an initial version of a system is developed using the best known and highly prioritized requirements. The method involved (1) Development of the abstract requirements specifications, (2) Building of the prototype system, (3) Evaluation and testing of the prototype system and (4) Documenting and delivering the prototype. The figure 1 below summarizes the research design procedure.



**Figure 1: Research design (Source: AlWahhab, 2014)**

Despite the fact that the prototype was based on a client-server architectural design, the prototype was developed to run on the server. The components of the prototype were the serial number collection module, the computer identification details processing module and the identification details display module.

The identification details collection module is code on the server that loads the computer name, IP address and serial number of client when logged on to a network. The loaded details are then processed in the identification details processing module the displayed on connected device interface using the identification details display module running at the server as well. Java

development kit (JDK) NetBeans was used for creating and implementing the computer identification interface and in the construction of the prototype modules. The identification details were managed using MySQL database on the authentication server.

Eventually evaluation and testing of the prototype was basically based on whether a serial number of logged computer can be collected and displayed on an interface using different access points.

## Results

The key findings from the literature review indicated that between port numbers, IP addresses and MAC addresses, devices in a network use MAC address as an identifier at the physical layer. The initial encoding of a 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). But due to some valid reasons (testing out networks for configurations, security applications or new protocols, workarounds and nefarious means), a copy of the MAC address in the operating system can be altered. For whichever reasons in changing a MAC address, it leads to the conclusion that a MAC address is not unique, not secure, not permanent and therefore unreliable. It is for these reasons then that the study was carried out with an aim of investigating to how serial numbers may be used for physical identification of computers in a wireless LAN.

Although computers have their serial numbers is tagged on them as part of serialization of the product, modern laptop models have their serial numbers coded into their basic input output (BIOS) chips. This makes it possible for the identifier to inwardly be accessed using a program so that it can be processed for a given desired function

## The Serial Number Based Identification (SNID) System

For a serial number to be collected from the system then displayed for purpose of identification, the database that contains the identification details has to be started first. This then is followed by establishing a connection to the database, then the existing details have to be deleted to pave way for the newly connected computers, prepare database for new records, fetch identification details of connected computers, post the details to the database, retrieve and display the details on an interface for identification, in that order as illustrated in the algorithm below.

1. Start the database
2. Connect to the database
3. Delete existing records to pave way for the newly connected device records
4. Prepare the interface for the new records
5. Get connected computer details
  - 5.1 Get computer name
  - 5.2 Get computer raw IP address
  - 5.3 Get computer serial number
6. Process computer serial number
7. Post Connected Computer Details to the Database
8. Retrieve and Display the Connected Computer Details from Database

The nature of these tasks prompted the employment of divide and conquer algorithm design technique to simplify the design and deployment of the problem. In a nutshell, divide and conquer algorithm design paradigm enables a problem to be divided smaller, more easily solvable sub problems, solve and combine the problems into the overall solution (Skiena, 2008).

This way, the problem was firstly divided into the application part and the database part. The application section used a code that was able to collect the computers name the then computers IP address which was used to fetch and process the computer’s serial number. For the serial number to be displayed for identification purposes, the database had to be started, connected then prepared for newly logged on device details to be captured and managed. The illustration in the figure 2 below show how the divide and conquer algorithm was employed

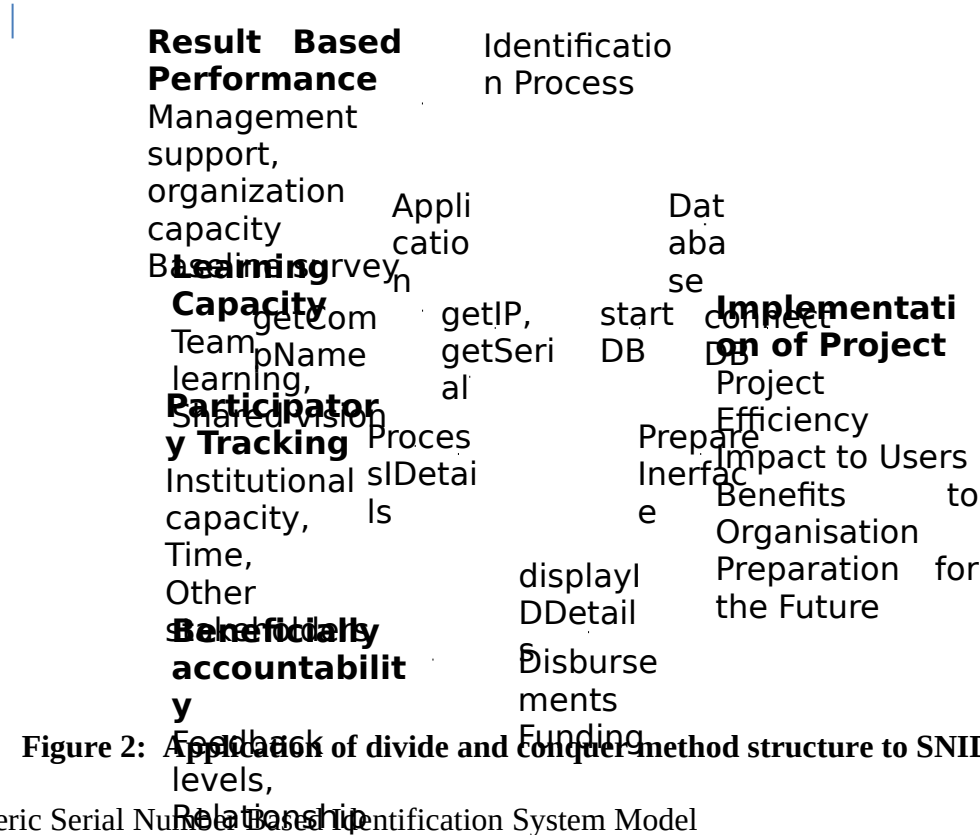
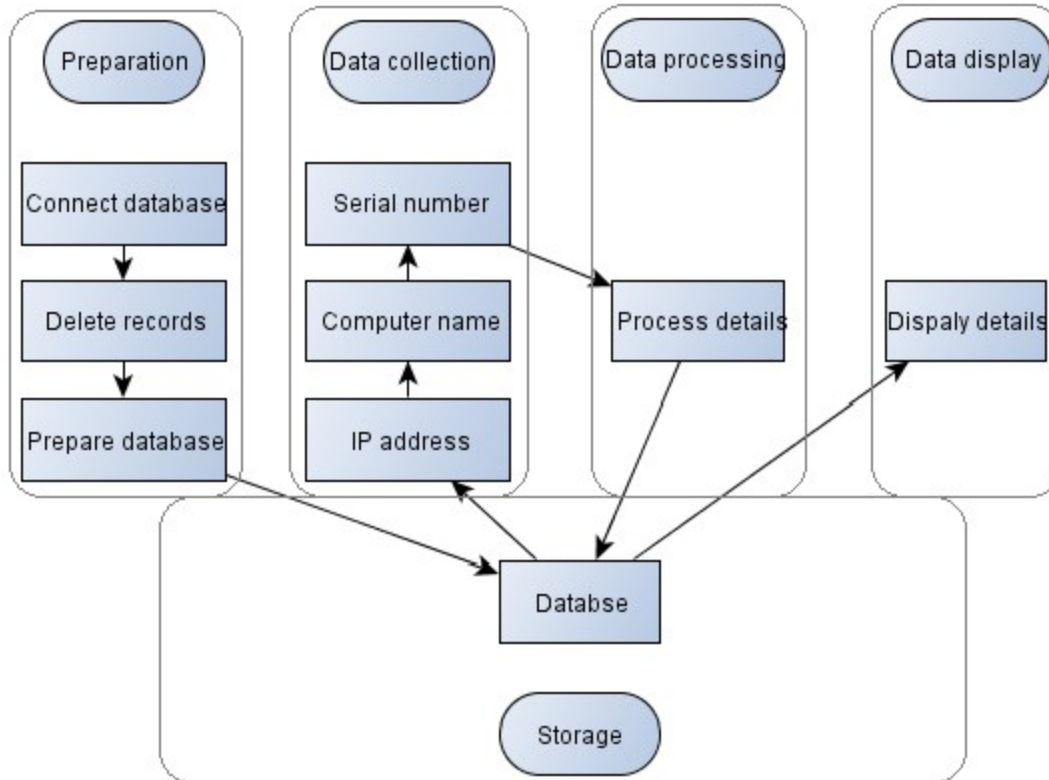


Figure 2: Application of divide and conquer method structure to SNID

The Generic Serial Number Based Identification System Model  
 The generalized model for identifying computers based on the serial numbers comprise the Data storage, database initialization, data collection, and data processing and data display modules.

Whereas the storage subsystem contains the structure that facilitates the storage and access of IP address, computer name and serial number details, initialization module involves database connection, deleting of existing records and preparing the database for new records. The responsibility of the data collection module is to fetch the IP address, computer name and serial number details necessary of computer identification process. The IP address, computer and serial number details are both from the local host computer and other computers connected to the network. As a part of the other subsystems, the serial number processing system can be said to be the pivot or the engine of the SNID system. It is at this section that the DNS resolves the host names and IP addresses, then performs IP address format conversions and ultimately uses the IP address to the get the serial number of the corresponding computer. The ultimate detail for identification is the serial number record. But for the number to be used as an identifier, then it must be displayed on an interface. The display subsystem is designed therefore to access apart from serial number, the hostname and IP address details that are essential for device identification. All these are illustrated in the figure 3 below



**Figure 3: General model for a serial number based identification system**

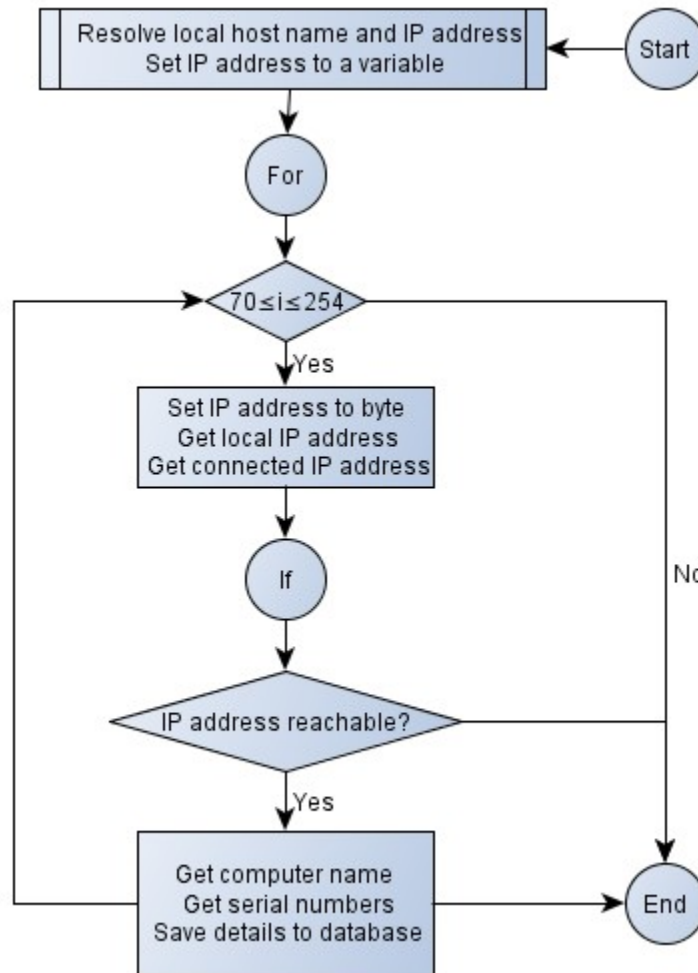
### The SNID System Design and Implementation

Processing of the computers serial number is the core component of this study. The system relies on the computers IP address to get the serial number. All these are circumvented in a Java network programming class called the inetAddress. This class is used with other networking java classes to manipulate the computer’s hostnames and IP addresses (Harold, 2013).

In this section, the function getCompName() was created to processes the serial number basing on the hostname and IP address of both the local and remote hosts. The class is enabled to throw an UnknownHostException error if an address is not found. The code running on the DNS then starts by connecting to the DNS to resolve local host name from the IP address. This is followed a variable creation for the IP address assignment. After representing the IP address in a byte format, the code gets the local IP address, the connected computer IP addresses, the connected computers serial numbers then posts the details to a database. All these is illustrated in the algorithm and corresponding flow chart below

1. Start
2. Resolve local host name and IP address
3. Assign the IP address a variable
4. For IP address between 70 and 254
  - 4.1 Set byte representation from string representation of the IP address
  - 4.2 Get local IP address
  - 4.3 Get connected computers IP address
  - 4.4 If the address is reachable, then
    - 4.4.1 Set Computer name
    - 4.4.2 Get computer serial number

- 4.4.3 Post IP address, Computer Name and serial number to a dataset
- 5. Else end
- 6. End



**Figure 4: Processing of the computer's serial number chart**

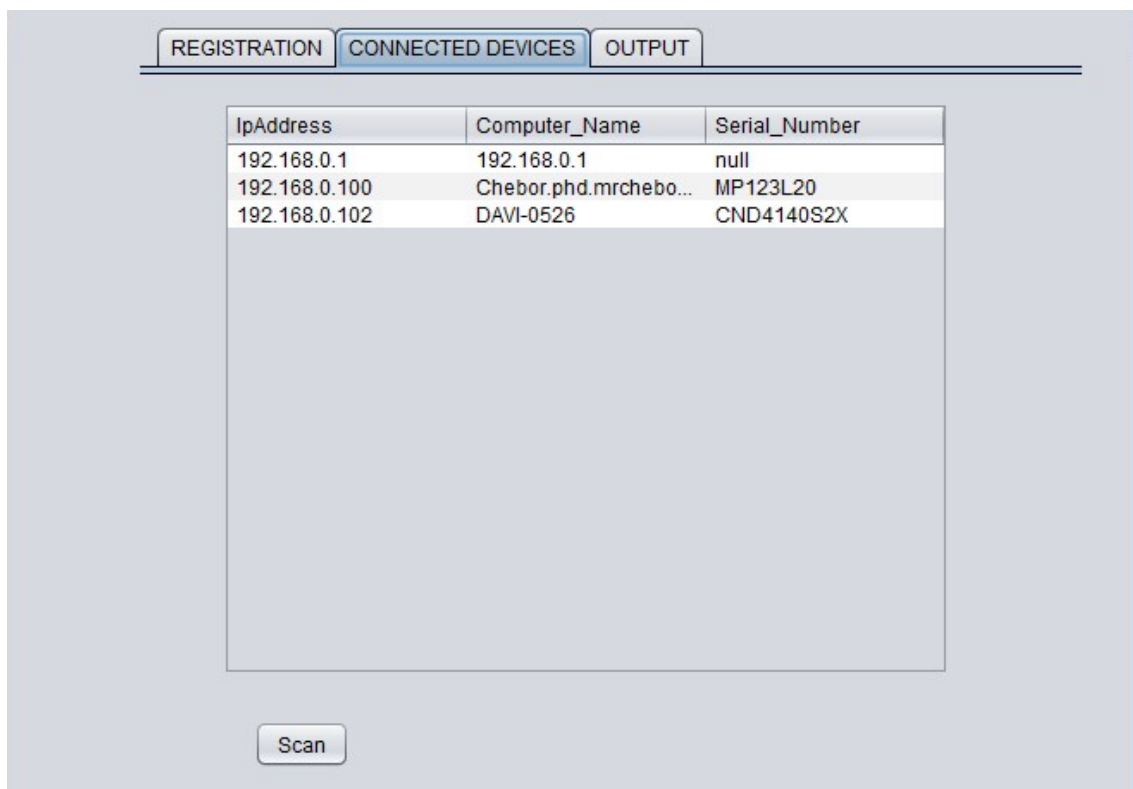
The corresponding code is as follows:

```

public void getCompName() throws UnknownHostException {
    InetAddress localhost = InetAddress.getLocalHost();
    byte[] ip = localhost.getAddress();
    for (int i = 70; i <= 254; i++) {
        try {
            ip[3] = (byte) i;
            InetAddress address = InetAddress.getByAddress(ip); //local ip address(server ip)
            ipoutput = address.toString().substring(1); //get the computer ipaddress
            if (address.isReachable(500)) {
                Computer_Name = address.getCanonicalHostName();
                getSerial();
                System.out.println("COMPUTER NAME: " + Computer_Name);
                System.out.println("COMPUTER IP: " + ipoutput);
            }
        } catch (Exception e) {}
    }
}
    
```

```
String sqlins = "INSERT INTO condevices  
(IpAddress,Computer_Name,Serial_Number)values('" + ipoutput + "','" + Computer_Name +  
"',"' + serial + "')";  
    pst = con.prepareStatement(sqlins);  
    pst.execute();  
    String sql1 = "SELECT IpAddress,Computer_Name,Serial_Number FROM  
condevices";  
    PreparedStatement pst1 = con.prepareStatement(sql1);  
    ResultSet rs1 = pst1.executeQuery();  
TblConnectedDevices.setModel(DbUtils.resultSetToTableModel(rs1));  
    }  
    } catch (Exception er) {  
    }  
    }  
(rs1));
```

Eventually the identification details are displayed in an interface as in the figure below



IpAddress	Computer_Name	Serial_Number
192.168.0.1	192.168.0.1	null
192.168.0.100	Chebor.phd.mrchebo...	MP123L20
192.168.0.102	DAVI-0526	CND4140S2X

**Figure 5: Identification details interface**

#### Research Contributions

This method should not be used as a replacement for device identifiers but primary as an alternative method to MAC address in device identification. It can actually added to the existing MAC address at data link, IP address at the network, and port number at the transport OSI reference layer model of identification especially at the physical layer

#### Alternative Identification Method



SNID can go a long way in providing alternative identification method to MAC address at the physical TCP/IP reference model layer. As an identifier, a serial number is unique, robust and more secure than a MAC address therefore providing a better alternative device identifier to network devices.

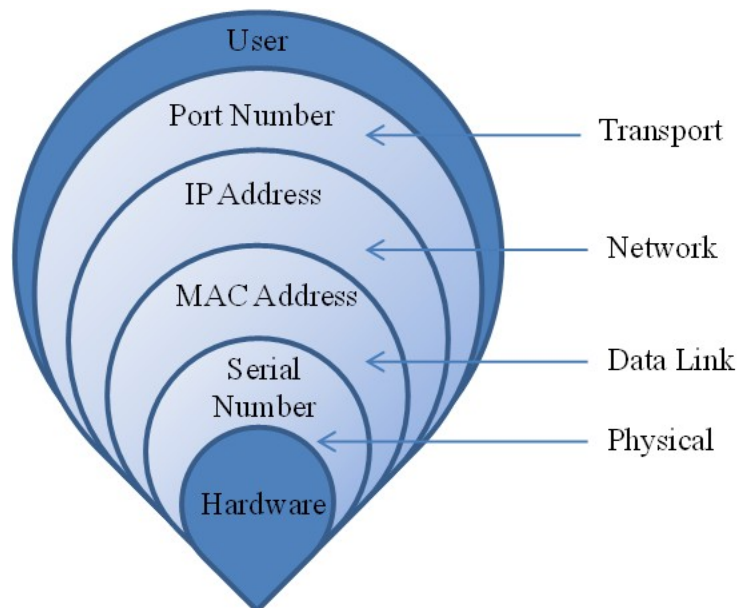
#### Additional Identification Layer

A notable contribution of the study to research is on the additional layer to existing network device identifiers. The identifiers identified earlier on are an IP address, MAC address and port number. Of course the identifiers are implicit as they are primarily used to identify devices indirectly through their locations rather the actual device.

Due to it's in process communication identification, port number identifiers are transport layer of OSI reference model. IP address identifier, of course, is a network issue as far as OSI layer model is concerned because it identifies devices in the internet. MAC addresses on the other hand identify devices in a particular network, therefore placed at data link layer of the same model.

A serial number is hard coded onto the system board BIOS of a computer by the products manufacturer. Its association with the pure hardware makes it be a physical layer issue in the OSI reference model. In this case, the serial number becomes an additional not only as a mere identifier to the existing port numbers, IP address and MAC address identifiers but more so as an actual identifier to the product (computer).

Modern computer networks are full of complexities as a result of the internet exponential growth (Behringer, 2009). A particular concern is the tremendous growth of computer hardware capacities, software sizes and so their configurations. One way of simplifying this complexity is by layering although it comes with an overhead. This way functions are devolved to each layer relieving other layers some other additional responsibilities that would have otherwise performed.



**Figure 6: Device identifiers layering**

Recommendations

The following three recommendations are proposed

#### Improvement and Deployment of SNID

The ultimate goal of the study was to demonstrate that a computer's serial number could be used for identification. The prototype was therefore developed with the emphasis on test runs to prove this concept. No much regard was considered for the usability and actual implementation design of the system in an ideal environment. It is with this regard therefore that the system is recommended to undergo through GUI enhancement, user acceptability testing process and eventually deployment of the system

#### Development of a System that Caters for other Network Device Identifiers

Laptops and computers in general like any other products are serialized for product differentiation. Other wireless network devices such tablets and smart phones use IMEIs rather serial numbers for identification. The study therefore focused on laptops to argue its case that a serial number can be used for identification. Development of an overall model/system that caters for the varieties of identifiers whether it is a serial number or an IMEI or any other related identifier is recommended

#### Integrating of SNID into an Access Point

The SNID system for the sake of the study was implemented in a server. But due to the functions and nature of servers, it is recommended that the SNID be implemented in an AP. In most cases DNS resolve domain names and IP addresses. In addition, there could be a number of servers communicating through the same AP that might require the SNID system. Access points (AP) on the other hand is an ideal home to SNID. Apart from an AP being the entry point to all devices connecting to the network it also acts as good security control in what is commonly referred to as identification, authentication, authorization and accounting (IAAA).

#### Areas for Further Research

Using a serial number for identification in isolation is not good enough. But if it results to authentication, authorization and accounting in that order then its mission will be accomplished. Actually, identification, authentication, authorization and accounting (IAAA) are essential in providing the network services required. Therefore, to accomplish the mission of network service provision, the following areas for further research are forwarded:

#### Using a Serial Number for Network Authentication

The serial number used to identify a network device can as well be used to authenticate the device. Authentication simply establishes of the validity of a logged on device. This can be achieved by creating a look up system that validates a device when logged on.

#### Using a Serial Number for Network Authorization

The reliability of a serial number puts it in a better position to be used as field to authorize devices to a network. Furthermore, its ability to carry with it aliases like computer name makes it easier to identify who the responsibility of the device lies on therefore authorized to access the appropriate network services. To achieve this, a study on a system that allows/disallows access network services depending on who the user is at authentication stage is proposed.

#### Using a Serial Number for Network Accounting

The serial number based identification will not be complete without the accounting component of network services provision. Accounting or auditing traces the device actions right from identification, authentication and authorization as well as track the activities performed. Once again a serial due to its reliability can be used as base for accounting.

### Conclusions

The mere fact that MAC address can be spoofed and altered affects robustness and uniqueness attributes of a MAC address. Uniqueness factor 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. Basing on the study objective on whether existing network device identifiers (MAC address) is suitable for network device identification, it can be concluded then that MAC address is not suitable for network device identification.

The study that was carried out with an aim of investigating how a serial number could be used to identify a computer in a WLAN revealed that a serial number can actually be used to identify a computer in a wireless LAN by displaying the identification details on an interface. For the identification details to be displayed then the database has to be created, started, connected and details interface created in that order. At the same time codes to get computer name, get IP address and eventually get and process the computer's serial number had to be developed. The processes were made possible by employing divide and conquer algorithm design

First, the overall system was divided into two sections: the application and the database parts. The application section was further divided into get computer name and IP address that resulted to getting and processing of the computers serial number. On the other hand the database was split into starting and connecting the database followed by preparing the interface to accept the identification details. Finally the identification details are displayed on the created identification details interface.

To better understand the system as well ensure the inclusion of all possible system components, SNID was put into preparation, details collection, details processing, details display and details storage sub sections. Starting, connecting, and cleaning the database and creation the interface were placed under the preparation section. The details collection section ensures that the fundamental details for identification (IP address, computer name and serial number) are factored in. The serial number has to process from the IP address and computer name that is taken care of by the processing sub section. The display section then is responsible for displaying identification details. All these would only happen with a storage location that stores and manages the details.

To make the model complete, relationships between the processes and the sections were indicated. A diagram that shows the all the components and their relation using analogue model was used to model the system

A prototype had to be developed to demonstrate the fact that a serial number can actually be used as a device identifier. As a prototype, the model had to be simple and be able proof the intended concept. This then called for implementation of the prototype using MySQL database and Java's NeatBeans IDE tools. And from the test runs, it was proofed that a serial number can actually be used as an identifier to identify network devices.

### References

- Behringer, M.H, (2009), Classifying network Complexity, Cisco Systems, [conferences.sigcomm.org/co-next/2009/workshops/research/papers/Behringer.pdf](http://conferences.sigcomm.org/co-next/2009/workshops/research/papers/Behringer.pdf). Accessed on 09/08/2018
- Bruhn, M. Gettes, M. and Ann, W. (2003). Identity and Access Management and Security in Higher Education. *EDUCAUSE QUARTERLY*. <http://net.educause.edu/ir/library/pdf/eqm0342.pdf>. Accessed on 21/03/2015.
- Canvan, J.E. (2000). *Fundamentals of Network Security*. Artech House. Boston, London.
- Coulouris, G. Dollimore, J. and Kindberg, T. (2005). *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.
- Frankel, S. Eydt, B. Owens, L. and Scarfone, K. (2007). Establishing Wireless and Robust Security Networks: A Guide to IEE 802.11i. *NIST Special Publication*. 800-97.
- Harold, E.R., (2013), *Java Network Programming*, 4<sup>th</sup> Edition, O'Reilly Media. ISBN: 9781449365936
- Idris, N.A. and Kassim, N.M. (2010). *Wireless Local Area Network (LAN) Security Guideline*, <http://www.cybersecurity.my/data/content/files/11.649.pdf> Accessed on 14/3/2015
- 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
- Jain, A., Hong, L. and Pankanti, S., (2000), Biometric Identification, *Communications of the ACM*, Vol.43, No.2
- Kurose, J.K. and Ross K.W. (2006). *Computer Networking: A Top-down Approach Featuring the Internet*. 3rd ed. Addison Wesley.
- 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.
- Lehtonen, M. Staake, T. and Michahelles, F. (2008). From identification to authentication—a review of RFID product authentication techniques. In *Networked RFID Systems and Lightweight Cryptography* (pp. 169-187). Springer Berlin Heidelberg
- Luis-Garzia, R., Albero-Lopez, C., Aughzout, O. and Ruiz-Alzola, J., (2003), Biometric Identification Systems, *Signal Processing* 83, 2539-2557

- Mandy, A. (2002). Wireless LAN Security. *Information Systems Security*, 11:3, 29-33
- Nicopolitidis, P., Papadimitriou, G. I. and Pomportsis, A. S., (2001), Design alternatives for wireless local area networks, *INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS*, 14:1-42
- Shay, W. A. (2004). *Understanding Data Communication and Networks*. Third Edition. Thomson Learning
- Skiena, S. S., (2008), *The Algorithm Design Manual*, Second Edition, Springer, London
- Stallings, W. (2011). *Network Security Essentials, Applications and Standards*. Fourth Edition. Pearson Education. New Jersey, 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.
- Tanenbaum, A. S. (2003b). *Computer Networks*, Fourth Edition, Prentice-Hall, India.
- Vollbrecht, J. and Moskowitz, R. (2002). Wireless LAN Access Control and Authentication. *Interlink Networks White Paper*. [http://www.interlinknetworks.com/whitepapers/WLAN\\_Access\\_Control](http://www.interlinknetworks.com/whitepapers/WLAN_Access_Control). Accessed on 10/01/2014.

## Modified Regression Type Estimators in the Presence of Non-Response

### Abstract

It is a common experience in sample survey that data cannot always be collected for all units selected in the sample at the first attempt and even after some call-backs. An estimate obtained from such incomplete data may be misleading because of the non-response in the data. In addition, the population mean of the auxiliary variable from the previous census may not be available. In this paper, Modified regression type estimators proposed by Tum *et al.* (2014) in single phase sampling, assuming complete response, have been proposed to estimate the population mean of the study variable in the presence of non-response under two phase sampling scheme. The expression of mean squared errors (MSE) based on the proposed estimators have been derived under two phase sampling to the first degree of approximation. A comparison of the proposed estimators with the usual unbiased estimator and existing estimators under two phase sampling scheme have been carried out. The proposed Modified regression type estimators have been found to be the most efficient compared to the existing estimators and they are recommended for use in practice.

**Keywords:** Modified regression type estimators, Study variable, Auxiliary variables, Mean Square Error, Non-response.

### INTRODUCTION

It is a common experience in sample survey that data cannot always be collected for all units selected in the sample. For example in a household survey, the families may not be found at home at the first attempt and some may refuse to cooperate with the interviewer even if contacted. In general, during surveys, it is observed that information in most cases is not obtained at the first attempt even after some call-backs. The failure to measure or get information from some of the units in the selected sample is referred to as non-response. An estimate obtained from such incomplete data may be misleading because of the non-response. There are various practical reasons for this incomplete information due to non-response like unwillingness of the respondent to answer some particular questions, accidental loss of information caused by unknown factors and failure on the part of investigator to collect the correct information, etc. The usual approach to face the non-response is to re-contact the non-respondents and obtain the information. Hansen and Hurwitz (1946) were the first authors to contract the problem of non-response while conducting mail surveys. They suggested a technique, known as 'sub-sampling of non-respondents', to deal with the problem of non-response and its adjustments. In fact they developed an unbiased estimator for population mean in the presence of non-response by dividing the population into two groups, viz. response group and non-response group. To avoid bias due to non-response, they suggested taking a sub-sample of the non-responding units. Neyman (1938) developed the concept of double phase sampling in sample survey. This sampling scheme is used to obtain the information about auxiliary variable cheaply from a larger sample at first phase and relatively small sample at the second stage. Khare and Srivastava (1993,1995) proposed ratio, product and regression estimators when population mean of auxiliary variable  $X$  is known and non-response occur only in the study variable in two phase sampling. Singh *et al.* (2010) proposed Exponential ratio and Exponential product estimators when population mean of auxiliary variable  $X$  is known and non-response occur only in the

study variable in two phase sampling. Kumar and Bhogal (2011) proposed Exponential ratio-product estimator when population mean of auxiliary variable  $X$  is known and non-response occur only in the study variable in two phase sampling. Khare and Srivastava (1993, 1995) also proposed ratio, product and regression estimators when population mean of auxiliary variable  $X$  is unknown and non-response occurs in both the study variable and auxiliary variable in two phase sampling. Singh et al. (2010) also proposed Exponential ratio and Exponential product estimators when population mean of auxiliary variable  $X$  is unknown and non-response occur in both the study variable and auxiliary variable in two phase sampling. Kumar and Bhogal (2011) also proposed Exponential ratio-product estimator when population mean of auxiliary variable  $X$  is unknown and non-response occurs in both the study variable and auxiliary variables in two phase sampling. Tum *et al.* (2014) proposed a regression type estimator that combined regression estimator and ratio - product type exponential estimator to form a new modified regression estimator. This study will focus on Tum *et al.* (2014) in presence of non-response in the study variable only and in both the study variable and auxiliary variables and develop their mean squared errors.

## 2. Notation

Consider a finite population of size  $N$  and a random sample of size  $n$  drawn without replacement.

In surveys on human populations, frequently  $n_1$  units respond on the items under examination in the first attempt while remaining  $n_2 (= n - n_1)$  units do not provide any response. When non-response occurs in the initial attempt, Hansen and Hurwitz (1946) proposed a double sampling scheme for estimating population mean comprising the following steps:

- i) a simple random sample of size  $n$  is selected and the questionnaire is mailed to the sampled units;
- ii) a sub sample of size  $r = (n_2/k)$ , ( $k \geq 1$ ) from the  $n_2$  non-responding units in the initial attempt is contacted through personal interviews.

Consider a finite population of size  $N$ . We draw a sample of size  $n$  from a population by using simple random sample without replacement (SRSWOR) sampling scheme. Let  $y_i$  and  $x_i$  be the

observations on the study variable ( $y$ ) and the auxiliary variable ( $x$ ) respectively. Let  $\bar{Y} = \frac{1}{N} \sum_{i=1}^N y_i$

and  $S_y^2 = \frac{1}{N-1} \sum_{i=1}^N (y_i - \bar{Y})^2$  denote the population mean and the population variance of the survey variable  $y$ .

When information on  $\bar{X}$  is unknown then double sampling or two phase sampling is suitable to estimate the population mean. In the first phase sample we select a sample of size  $n'$  by SRSWOR from a population to observe  $x$ . In the second phase, we select a sample of size  $n$  from  $n'$  such that  $n < n'$  by SRSWOR also. Non-response occurs on second phase in which  $n_1$  units respond and  $n_2$  do not out of  $n$  units. From  $n_2$  non-respondents a sample of  $r = (n_2/k)$ , ( $k > 1$ ) units are selected, where  $k$  is the inverse sampling rate at the second phase sample of size  $n$ .

Let  $\bar{Y}_1 = \frac{1}{N_1} \sum_{i=1}^{N_1} y_i$  and  $S_{y(1)}^2 = \frac{1}{N_1-1} \sum_{i=1}^{N_1} (y_i - \bar{Y}_1)^2$  denote the mean and variance of the response

group. Similarly,  $\bar{Y}_2 = \frac{1}{N_2} \sum_{i=1}^{N_2} y_i$  and  $S_{y(2)}^2 = \frac{1}{N_2 - 1} \sum_{i=1}^{N_2} (y_i - \bar{Y}_2)^2$  denote the mean and variance of the non-response group. The population mean can be written as  $\bar{Y} = W_1 \bar{Y}_1 + W_2 \bar{Y}_2$ , where  $W_1 = (N_1 / N)$  and  $W_2 = (N_2 / N)$ . Let  $\bar{y}_1 = \frac{1}{n_1} \sum_{i=1}^{n_1} y_i$  and  $\bar{y}_2 = \frac{1}{n_2} \sum_{i=1}^{n_2} y_i$  denote the means of the  $n_1$  responding units and the  $n_2$  non-responding units. Further, let  $\bar{y}_{2r} = \frac{1}{r} \sum_{i=1}^r y_i$  denote the mean of the  $r = n_2/k$  sub sampled units. Thus, an unbiased estimator, due to Hansen and Hurwitz (1946) of the population mean  $\bar{Y}$  of the study variable  $y$  is given by

$$\bar{y}^* = w_1 \bar{y}_1 + w_2 \bar{y}_{2r} \quad (1)$$

Where  $w_1 = (n/n_1)$ ,  $w_2 = (n/n_2)$  are responding and non-responding proportions in the sample. The variance of  $\bar{y}^*$  to terms of order  $n^{-1}$  is given by,

$$V(\bar{y}^*) = \bar{Y}^2 \left\{ \theta C_y^2 + \lambda C_{y(2)}^2 \right\} \quad (2)$$

where  $\theta = \frac{N - n}{Nn}$ ,  $\lambda = \frac{W_2(k - 1)}{n}$ ,  $C_y^2 = (S_y^2 / \bar{Y}^2)$  and  $C_{y(2)}^2 = (S_{y(2)}^2 / \bar{Y}^2)$

Let  $\bar{x}_1 = \frac{1}{n_1} \sum_{i=1}^{n_1} x_i$  and  $\bar{x}_2 = \frac{1}{n_2} \sum_{i=1}^{n_2} x_i$  denote the means of the auxiliary variable of  $n_1$  responding units and the  $n_2$  non-responding units. Further, let  $\bar{x}_{2r} = \frac{1}{r} \sum_{i=1}^r x_i$  denote the mean of the  $r = n_2/k$  sub sampled units. Thus, an unbiased estimator, due to Hansen and Hurwitz (1946) of the population mean  $\bar{X}$  of the study variable  $x$  is given by

$$\bar{x}^* = w_1 \bar{x}_1 + w_2 \bar{x}_{2r} \quad (3)$$

Where  $w_1 = (n/n_1)$ ,  $w_2 = (n/n_2)$  are responding and non-responding proportions in the sample.

The variance of  $\bar{x}^*$  to terms of order  $n^{-1}$  is given by,

$$V(\bar{x}^*) = \bar{X}^2 \left\{ \theta C_x^2 + \lambda C_{x(2)}^2 \right\} \quad (4)$$

Where  $C_x^2 = (S_x^2 / \bar{X}^2)$ ,  $C_{x(2)}^2 = (S_{x(2)}^2 / \bar{X}^2)$ ,  $S_x^2 = \frac{1}{N - 1} \sum_{i=1}^N (x_i - \bar{X})^2$  and  $S_{x(2)}^2 = \frac{1}{N_2 - 1} \sum_{i=1}^{N_2} (x_i - \bar{X}_2)^2$

The expectation includes,

$$\bar{y} = \bar{Y} (1 + e_y) \quad \bar{x} = \bar{X} (1 + e_x) \quad \bar{z} = \bar{Z} (1 + e_z)$$

$$E(e_0) = E(e_1) = 0 \quad E(e_0^2) = V(\bar{y}^*) = \bar{Y}^2 \left\{ \theta C_y^2 + \lambda C_{y(2)}^2 \right\}$$

$$E(e_1^2) = V(\bar{x}^*) = \bar{X}^2 \left\{ \theta C_x^2 + \lambda C_{x(2)}^2 \right\}$$



$$E(e_1 e_0) = V(\bar{y}^*, \bar{x}^*) = \bar{Y} \bar{X} \left[ \theta \rho_{yx} C_x C_y + \lambda \rho_{yx(2)} C_{x(2)} C_{y(2)} \right]$$

Where  $\rho_{yx} = S_{yx} / S_y S_x$ ,  $\rho_{yx(2)} = S_{yx(2)} / S_{y(2)} S_{x(2)}$ ,  $\rho_2 = \frac{S_{2xy}}{S_{2y} S_{2x}} k_{yx} = \rho_{yx} \frac{C_y}{C_x} k_{yx2} = \rho_{yx2} \frac{C_{y2}}{C_{x2}}$

$$S_{yx} = \frac{1}{N-1} \sum_{i=1}^N (y_i - \bar{Y})(x_i - \bar{X}) \quad S_{yx(2)} = \frac{1}{N_2-1} \sum_{i=1}^{N_2} (y_i - \bar{Y}_2)(x_i - \bar{X}_2) \quad S_{2yx} = \frac{1}{N-1} \sum_{i=1}^N (y_i - \bar{Y}_2)(x_i - \bar{X}_2)$$

$$S_{2x} = \frac{1}{N-1} \sum_{i=1}^N (x_i - \bar{X}_2)^2 \quad S_{2y} = \frac{1}{N-1} \sum_{i=1}^N (y_i - \bar{Y}_2)^2$$

$$\theta = \frac{N-n}{Nn}, \quad \theta' = \frac{n'-n}{n'n}, \quad \lambda = \frac{N-n'}{Nn'} \quad \text{and} \quad \delta = \frac{W_2(k-1)}{n}$$

$$A^{-1} = \frac{1}{|A|} (C^T)_{ij} = \frac{Adj(A)}{|A|}$$

$$\frac{|R|_{y^xq}}{|R|_{xq}} = (1 - \rho^2_{y \cdot xq})$$

Arora and Lai (1989) (5)

The following notations will be used in deriving the mean square errors of proposed estimator

$|R|_{y^xq}$  Determinant of population correlation matrix of variables  $y, x_1, x_2$

$|R|_{xq}$  Determinant of population correlation matrix of variables  $x_1, x_2$

**CASE 1: When there is incomplete information on the study variable  $y$  and complete information on the auxiliary variable  $x$ .**

When the population mean  $\bar{X}$  of the auxiliary variable ‘ $x$ ’ is known, the two phase ratio estimator by Khare and Srivastava (1993) is given by,

$$t_{R1} = \bar{y}^* \frac{\bar{x}}{\bar{x}'} \quad (6)$$

The MSE of the estimator  $t_{R1}$ ;

$$MSE(t_{R1}) = \bar{Y}^2 \left[ \theta C_y^2 + (\theta - \lambda) C_y^2 (1 - 2k_{yx}) C_x^2 + \delta C_{y(2)}^2 \right] \quad (7)$$

When the population mean  $\bar{X}$  of the auxiliary variable ‘ $x$ ’ is known, the two phase product estimator by Khare and Srivastava (1993) is given by,

$$t_{P1} = \bar{y}^* \frac{\bar{x}}{\bar{x}'} \quad (8)$$

The MSE of the estimator  $t_{P1}$ ;

$$MSE(t_{P1}) = \bar{Y}^2 \left[ \theta C_y^2 + (\theta - \lambda) C_y^2 (1 + 2k_{yx}) C_x^2 + \delta C_{y(2)}^2 \right] \quad (9)$$

When the population mean  $\bar{X}$  of the auxiliary variable ‘x’ is known, the two phase regression estimator by Khare and Srivastava (1995) is given by,

$$t_{RE1} = \bar{y}^* + \beta \left( \frac{\bar{y}' - \bar{y}}{\bar{x}' - \bar{x}} \right) \tag{10}$$

The MSE of the estimator  $t_{RE1}$ ;

$$MSE(t_{RE1}) = \bar{Y}^2 \left( \theta C_y^2 + (\theta - \lambda)(1 - \rho_{yx}^2) + \delta C_{y(2)}^2 \right) \tag{11}$$

When the population mean  $\bar{X}$  of the auxiliary variable ‘x’ is known, the two phase exponential ratio estimator by Singh et al. (2010) is given by,

$$t_{ER1} = \bar{y}^* \exp \left( \frac{\frac{\bar{y}' - \bar{y}}{\bar{x}' - \bar{x}}}{\frac{\bar{y}' - \bar{y}}{\bar{x}' + \bar{x}}} \right) \tag{12}$$

The MSE of the estimator  $t_{ER1}$ ;

$$MSE(t_{ER1}) = \bar{Y}^2 \left[ \theta C_y^2 + (\theta - \lambda) \left\{ C_y^2 + \frac{1}{2}(1 - 2k_{yx}) C_x^2 \right\} + \delta C_{y(2)}^2 \right] \tag{13}$$

When the population mean  $\bar{X}$  of the auxiliary variable ‘x’ is known, the two phase exponential product estimator by Singh et al. (2010) is given by,

$$t_{EP1} = \bar{y}^* \exp \left( \frac{\frac{\bar{y}' - \bar{y}}{\bar{x}' - \bar{x}}}{\frac{\bar{y}' - \bar{y}}{\bar{x}' + \bar{x}}} \right) \tag{14}$$

The MSE of the estimator  $t_{EP1}$ ;

$$MSE(t_{EP1}) = \bar{Y}^2 \left[ \theta C_y^2 + (\theta - \lambda) \left\{ C_y^2 + \frac{1}{2}(1 + 2k_{yx}) C_x^2 \right\} + \delta C_{y(2)}^2 \right] \tag{15}$$

When the population mean  $\bar{X}$  of the auxiliary variable ‘x’ is known, the two phase exponential ratio-product estimator by Kumar and Bhogal (2011) is given by,

$$t_{ERP1} = \bar{y}^* \exp \left( \alpha \left( \frac{\bar{y}' - \bar{y}}{\bar{x}' - \bar{x}} \right) + (1 - \alpha) \left( \frac{\bar{y}' - \bar{y}}{\bar{x}' + \bar{x}} \right) \right) \tag{16}$$

The MSE of the estimator  $t_{ERP1}$ ;

$$MSE(t_{ERP1}) = \bar{Y}^2 \left[ \theta \left\{ C_y^2 + \frac{B_2}{A_2} \left( \frac{B_2}{A_2} - 2k_{yx} \right) C_x^2 \right\} + \delta C_{y(2)}^2 \right] \tag{17}$$

Where

$$A_2 = \theta C_x^2, \quad B_2 = \theta k_{yx} C_x^2 \quad \text{and} \quad \alpha = \frac{A_2 + 2B_2}{2A_2}$$

### 3. Modified Regression Type Estimator in Two Phase Sampling in the Presence of Non-Response in the Study Variable Only

The modified regression estimator proposed by Tum *et al.* (2014) is given by,

$$t_{ERP} = \left( \bar{y} + \beta (\bar{X} - \bar{x}) \right) \left( \alpha \exp \left( \frac{\bar{Z} - \bar{z}}{\bar{Z} + \bar{z}} \right) + (1 - \alpha) \exp \left( \frac{\bar{z} - \bar{Z}}{\bar{Z} + \bar{z}} \right) \right) \quad (18)$$

We will consider the above estimator in presence of non-response in the study variable only and in both the study variable and auxiliary variables.

When there is incomplete information on the study variable  $y$  and complete information on the auxiliary variable  $x$ , our proposed Modified regression type estimator in the presence of non-response will be given by,

$$t_7 = \left( \bar{y}_2^* + \beta (\bar{X} - \bar{x}_2) \right) \left( \alpha \exp \left( \frac{\bar{Z} - \bar{z}_2}{\bar{Z} + \bar{z}_2} \right) + (1 - \alpha) \exp \left( \frac{\bar{z}_2 - \bar{Z}}{\bar{Z} + \bar{z}_2} \right) \right) \quad (19)$$

Substituting (5) equation in (19) we get,

$$t_7 = \left( \bar{Y} (1 + \bar{e}_{y_2}^*) - \beta \bar{e}_{x_2} \right) \left( \alpha \exp \left( \frac{\bar{Z} - \bar{Z} (1 + \bar{e}_{z_2})}{\bar{Z} + \bar{Z} (1 + \bar{e}_{z_2})} \right) + (1 - \alpha) \exp \left( \frac{\bar{Z} (1 + \bar{e}_{z_2}) - \bar{Z}}{\bar{Z} + \bar{Z} (1 + \bar{e}_{z_2})} \right) \right) \quad (20)$$

Simplifying (20), we get

$$t_7 = \left( \bar{e}_{y_2}^* + \bar{Y} - \beta \bar{e}_{x_2} \right) \left( \alpha \exp \left( - \frac{\bar{e}_{z_2}}{2} \left( 1 + \frac{\bar{e}_{z_2}}{2} \right)^{-1} \right) + (1 - \alpha) \exp \left( \frac{\bar{e}_{z_2}}{2} \left( 1 + \frac{\bar{e}_{z_2}}{2} \right)^{-1} \right) \right) \quad (21)$$

Expanding and ignoring the second and higher terms for each expansion of product and after simplification we can write

$$t_7 = \bar{Y} + \bar{e}_{y_2}^* - \beta \bar{e}_{x_2} + \bar{Y} \left( \frac{1}{2} - \alpha \right) \bar{e}_{z_2} \quad (22)$$

The mean squared error of  $t_{ERP}$  is given by,

$$MSE(t_7) = E(t_7 - \bar{Y})^2 = E \left( \bar{e}_{y_2}^* - \beta \bar{e}_{x_2} + \bar{Y} \left( \frac{1}{2} - \alpha \right) \bar{e}_{z_2} \right)^2 \quad (23)$$

Squaring the right sides of (23) and taking expectation and using (5), we get,

$$\begin{aligned} MSE(t_7) = & \theta \bar{Y}^2 C_y^2 + \lambda \bar{Y}^2 C_{y(2)}^2 + \beta^2 \theta \bar{X}^2 C_x^2 + \bar{Y}^2 \left( \frac{1}{2} - \alpha \right)^2 \theta \bar{Z}^2 C_z^2 \\ & + 2\bar{Y} \left( \frac{1}{2} - \alpha \right) \theta \bar{X} \bar{Y} C_y C_z \rho_{yz} - 2\beta \theta \bar{X} \bar{Y} C_y C_x \rho_{yx} - 2\bar{Y} \left( \frac{1}{2} - \alpha \right) \beta \theta \bar{X} \bar{Z} C_x C_z \rho_{xz} \end{aligned} \quad (24)$$

Expanding (24) by opening brackets we get,

$$\begin{aligned} MSE(t_7) = & \theta \bar{Y}^2 C_y^2 + \lambda \bar{Y}^2 C_{y(2)}^2 + \beta^2 \theta \bar{X}^2 C_x^2 + \frac{1}{4} \bar{Y}^2 \theta \bar{Z}^2 C_z^2 - \alpha \bar{Y}^2 \theta \bar{Z}^2 C_z^2 \\ & + \bar{Y}^2 \alpha^2 \theta \bar{Z}^2 C_z^2 + \bar{Y}^2 \theta \bar{X} C_y C_z \rho_{yz} - \alpha 2\bar{Y}^2 \theta \bar{Z} C_y C_z \rho_{yz} \\ & - 2\beta \theta \bar{X} \bar{Y} C_y C_x \rho_{yx} - \bar{Y} \beta \theta \bar{X} \bar{Z} C_x C_z \rho_{xz} + \alpha 2\bar{Y} \beta \theta \bar{X} \bar{Z} C_x C_z \rho_{xz} \end{aligned} \quad (25)$$

Differentiating (25) with respect to  $\alpha$  and  $\beta$  and equating to zero gives

$$\beta = \frac{\bar{Y}C_y}{\bar{X}C_x |R_{2 \times 2}|} (-1)^{1+1} |R_{yx}|_{yxz} \quad \text{and} \quad \alpha = \frac{1}{2} + \frac{C_y}{\bar{Z}C_z |R_{2 \times 2}|} (-1)^{2+1} |R_{yz}|_{yxz} \quad (26)$$

Using normal equations that are used to find the optimum values of  $\alpha$  and  $\beta$  (26) can be written in simplified form as

$$MSE(t_7) = E \left[ \bar{e}_y^* \left( \bar{e}_y^* - \beta \bar{e}_x + \bar{Y} \left( \frac{1}{2} - \alpha \right) \bar{e}_z \right) \right] \quad (27)$$

Simplifying and taking expectation, we get,

$$MSE(t_7) = \theta \bar{Y}^2 C_y^2 + \lambda \bar{Y}^2 C_{y(2)}^2 - \beta \theta \bar{X} \bar{Y} C_y C_x \rho_{yx} + \bar{Y} \alpha \theta \bar{Y} \bar{Z} C_y C_z \rho_{yz} \quad (28)$$

Substituting the optimum value in (26), we get

$$MSE(t_7) = \theta \bar{Y}^2 C_y^2 + \lambda \bar{Y}^2 C_{y(2)}^2 - \left( \frac{\bar{Y}C_y}{\bar{X}C_x |R_{2 \times 2}|} (-1)^{1+1} |R_{yx}|_{yxz} \right) \theta \bar{X} \bar{Y} C_y C_x \rho_{yx} + \bar{Y} \left( \frac{1}{2} - \left( \frac{1}{2} + \frac{C_y}{\bar{Z}C_z |R_{2 \times 2}|} (-1)^{2+1} |R_{yz}|_{yxz} \right) \right) \theta \bar{Y} \bar{Z} C_y C_z \rho_{yz} \quad (29)$$

Simplifying (29) we get

$$MSE(t_7) = \theta \bar{Y}^2 C_y^2 \left( 1 - \frac{(-1)^{1+1} |R_{yx}|_{yxz}}{|R_{2 \times 2}|} \rho_{yx} - \frac{(-1)^{2+1} |R_{yz}|_{yxz}}{|R_{2 \times 2}|} \rho_{yz} \right) + \lambda \bar{Y}^2 C_{y(2)}^2 \quad (30)$$

We can rewrite (30) as,

$$MSE(t_7) = \frac{\theta \bar{Y}^2 C_y^2}{|R_{2 \times 2}|} \left( |R_{2 \times 2}| + (-1)^1 |R_{yx}|_{yxz} \rho_{yx} + (-1)^2 |R_{yz}|_{yxz} \rho_{yz} \right) + \lambda \bar{Y}^2 C_{y(2)}^2 \quad (31)$$

We can also rewrite (31) as,

$$MSE(t_7) = \frac{\theta \bar{Y}^2 C_y^2}{|R_{2 \times 2}|} |R_{yxz}| + \lambda \bar{Y}^2 C_{y(2)}^2 \quad (32)$$

Using (5) in (32) we get

$$MSE(t_7) = \theta \bar{Y}^2 C_y^2 (1 - \rho_{y.xz}^2) + \lambda \bar{Y}^2 C_{y(2)}^2 \quad (33)$$

### CASE 2: When there is incomplete information on both the study variable $y$ and the auxiliary variable $x$ .

Khare and Srivastava (1993) proposed ratio and product estimators under case 2. When the population mean  $\bar{X}$  of the auxiliary variable 'x' is unknown, the two phase ratio estimator is given by,

$$t_{R2} = \bar{y}^* \frac{\bar{x}}{\bar{x}^*} \quad (34)$$

The MSE of the estimator  $t_{R2}$ ;

$$MSE(t_{R2}) = \bar{Y}^2 \left[ \theta' \left\{ C_y^2 + (1 - 2k_{yx}) C_x^2 \right\} + \delta \left\{ C_{y(2)}^2 + (1 - 2k_{yx(2)}) C_{x_2}^2 \right\} + \lambda' C_y^2 \right] \quad (35)$$

When the population mean  $\bar{X}$  of the auxiliary variable 'x' is unknown, the two phase product estimator is given by,

$$t_{P2} = \bar{y}^* \frac{\bar{x}^*}{\bar{x}} \quad (36)$$

The MSE of the estimator  $t_{P2}$ ;

$$MSE(t_{P2}) = \bar{Y}^2 \left[ \theta' \left\{ C_y^2 + (1 + 2k_{yx}) C_x^2 \right\} + \delta \left\{ C_{y(2)}^2 + (1 + 2k_{yx(2)}) C_{x_2}^2 \right\} + \lambda' C_y^2 \right] \quad (37)$$

When the population mean  $\bar{X}$  of the auxiliary variable 'x' is unknown, the two phase regression estimator by Khare and Srivastava (1995) is given by,

$$t_{RE2} = \bar{y}^* + \beta \left( \frac{\bar{x}' - \bar{x}^*}{\bar{x}' + \bar{x}^*} \right) \quad (38)$$

The MSE of the estimator  $t_{RE2}$ ;

$$MSE(t_{RE2}) = \bar{Y}^2 \left( \theta' C_y^2 + \lambda(1 - \rho^2) C_x^2 + \delta \left( C_{y(2)}^2 + k_{yx} (k_{yx} - 2k_{yx(2)}) C_{x(2)}^2 \right) \right) \quad (39)$$

When the population mean  $\bar{X}$  of the auxiliary variable 'x' is unknown, the two phase exponential ratio estimator by Singh et al. (2010) is given by,

$$t_{ER2} = \bar{y}^* \exp \left( \frac{\frac{\bar{x}' - \bar{x}^*}{\bar{x}' + \bar{x}^*}}{\frac{\bar{x}' - \bar{x}^*}{\bar{x}' + \bar{x}^*}} \right) \quad (40)$$

The MSE of the estimator  $t_{ER2}$ ;

$$MSE(t_{ER2}) = \bar{Y}^2 \left[ \theta' \left\{ C_y^2 + (1 - 4k_{yx}) \frac{C_x^2}{4} \right\} + \delta \left\{ C_{y(2)}^2 + (1 - 4k_{yx(2)}) \frac{C_{x_2}^2}{4} \right\} + \lambda' C_y^2 \right] \quad (41)$$

When the population mean  $\bar{X}$  of the auxiliary variable 'x' is unknown, the two phase exponential product estimator by Singh et al. (2010) is given by,

$$t_{EP2} = \bar{y}^* \exp \left( \frac{\frac{\bar{x}^* - \bar{x}'}{\bar{x}^* + \bar{x}'}}{\frac{\bar{x}^* - \bar{x}'}{\bar{x}^* + \bar{x}'}} \right) \quad (42)$$

The MSE of the estimator  $t_{EP2}$ ;

$$MSE(t_{EP2}) = \bar{Y}^2 \left[ \theta' \left\{ C_y^2 + (1 + 4k_{yx}) \frac{C_x^2}{4} \right\} + \delta \left\{ C_{y(2)}^2 + (1 + 4k_{yx(2)}) \frac{C_{x_2}^2}{4} \right\} + \lambda' C_y^2 \right] \quad (43)$$

When the population mean  $\bar{X}$  of the auxiliary variable 'x' is unknown, the two phase exponential ratio-product estimator by Kumar and Bhogal (2011) is given by,

$$t_{ERP2} = \bar{y}^* \exp \left( \alpha \left( \frac{\bar{x}' - \bar{x}^*}{\bar{x}' + \bar{x}^*} \right) + (1 - \alpha) \left( \frac{\bar{x}^* - \bar{x}'}{\bar{x}^* + \bar{x}'} \right) \right) \quad (44)$$

The MSE of the estimator  $t_{ERP2}$ ;

$$MSE(t_{ERP2}) = \bar{Y}^2 \left[ \theta' \left\{ C_y^2 + \frac{B_2}{A_2} \left( \frac{B_2}{A_2} - 2k_{yx} \right) C_x^2 \right\} + \delta \left\{ C_{y(2)}^2 + \frac{B_2}{A_2} \left( \frac{B_2}{A_2} - 2k_{yx} \right) C_x^2 \right\} + \lambda' C_y^2 \right] \quad (45)$$

Where

$$A_2 = \theta C_x^2 + \delta C_{x(2)}^2, \quad B_2 = \theta k_{yx} C_x^2 + \delta k_{yx2} C_{x(2)}^2 \quad \text{and} \quad \alpha = \frac{A_2 + 2B_2}{2A_2}$$

### 3.2 Modified Regression Estimator with Non-Response in both study variable and the auxiliary variable

Following Tum *et al.* (2014), we define the following estimator for  $\bar{Y}$  in the presence of non-response in the study variable and auxiliary variables as:

$$t_8 = \left( \bar{y}^* + \beta (\bar{X} - \bar{x}^*) \right) \left( \alpha \exp \left( \frac{\bar{Z} - \bar{z}^*}{\bar{Z} + \bar{z}^*} \right) + (1 - \alpha) \exp \left( \frac{\bar{z}^* - \bar{Z}}{\bar{Z} + \bar{z}^*} \right) \right) \quad (46)$$

The study variable (Y) is highly positively correlated with the auxiliary variable (X) and the relationship is linear and regression line does not pass in the neighborhood of the origin. While Z is an auxiliary variable which is also highly positively or negatively correlated with the study variable (Y) and the relationship is linear and regression line passes through the origin.

Substituting (5) equation in (46) we get,

$$t_8 = \left( \bar{Y} (1 + e_y^*) - \beta \bar{e}_x^* \right) \left( \alpha \exp \left( \frac{\bar{Z} - \bar{Z} (1 + \bar{e}_z^*)}{\bar{Z} + \bar{Z} (1 + \bar{e}_z^*)} \right) + (1 - \alpha) \exp \left( \frac{\bar{Z} (1 + \bar{e}_z^*) - \bar{Z}}{\bar{Z} + \bar{Z} (1 + \bar{e}_z^*)} \right) \right) \quad (47)$$

Opening brackets and ignoring the second and higher terms for each expansion of product and after simplification we can write  $t_{ERP}$  as

$$t_8 = \bar{Y} + \bar{e}_y^* - \beta \bar{e}_x^* + \bar{Y} \left( \frac{1}{2} - \alpha \right) \bar{e}_z^* \quad (48)$$

The mean squared error of  $t_8$  is given by,

$$MSE(t_8) = E(t_8 - \bar{Y})^2 = E \left( \bar{e}_y^* - \beta \bar{e}_x^* + \bar{Y} \left( \frac{1}{2} - \alpha \right) \bar{e}_z^* \right)^2 \quad (49)$$

Squaring the right sides of (49), we get,

$$MSE(t_8) = E \left( \bar{e}_y^{*2} + \beta^2 \bar{e}_x^{*2} + \bar{Y}^2 \left( \frac{1}{2} - \alpha \right)^2 \bar{e}_z^{*2} + 2\bar{Y} \left( \frac{1}{2} - \alpha \right) \bar{e}_z^* \bar{e}_y^* - 2\bar{e}_y^* \beta \bar{e}_x^* - 2\bar{Y} \left( \frac{1}{2} - \alpha \right) \bar{e}_z^* \beta \bar{e}_x^* \right) \quad (50)$$

Taking expectation and using (5) in (50), we get,

$$\begin{aligned}
 MSE(t_8) = & \theta \bar{Y}^2 C_y^2 + \lambda \bar{Y}^2 C_{y(2)}^2 + \theta \bar{X}^2 \beta^2 C_x^2 + \lambda \bar{X}^2 \beta^2 C_{x(2)}^2 + \bar{Y}^2 \left( \frac{1}{2} - \alpha \right)^2 \left( \theta \bar{Z}^2 C_z^2 + \lambda \bar{Z}^2 C_{z(2)}^2 \right) \\
 & + 2\bar{Y} \left( \frac{1}{2} - \alpha \right) \left( \bar{Y} \bar{X} \left( \theta \rho_{yz} C_z C_y + \lambda \rho_{yz(2)} C_{z(2)} C_{y(2)} \right) \right) - 2\beta \bar{X} \bar{Y} \left( \theta \rho_{yx} C_x C_y + \lambda \rho_{yx(2)} C_{x(2)} C_{y(2)} \right) \\
 & - 2\bar{Y} \beta \left( \frac{1}{2} - \alpha \right) \left( \bar{Y} \bar{X} \left( \theta \rho_{xz} C_z C_x + \lambda \rho_{xz(2)} C_{x(2)} C_{z(2)} \right) \right)
 \end{aligned} \tag{51}$$

Expanding and differentiating (51) with respect to  $\alpha$ ,  $\alpha^*$ ,  $\beta$  and  $\beta^*$  and equating to zero gives

$$\begin{aligned}
 \beta &= \frac{\bar{Y} C_y}{\bar{X} C_x |R_{2 \times 2}|} (-1)^{1+1} |R_{yx}|_{yxz} \quad \beta^* = \frac{\bar{Y} C_{y(2)}}{\bar{X} C_{x(2)} |R_{2 \times 2}^*|} (-1)^{1+1} (-1)^{1+1} |R_{yx}^*|_{yxz} \\
 \alpha &= \frac{1}{2} + \frac{C_y}{\bar{Z} C_z |R_{2 \times 2}|} (-1)^{2+1} |R_{yz}|_{yxz} \quad \alpha^* = \frac{1}{2} + \frac{C_{y(2)}}{\bar{Z} C_{z(2)} |R_{2 \times 2}^*|} (-1)^{2+1} |R_{yz}^*|_{yxz}
 \end{aligned} \tag{52}$$

Using normal equations that are used to find the optimum values of  $\alpha$  and  $\beta$ , (52) can be written in simplified form as

$$MSE(t_8) = E \left[ \bar{e}_y^* \left( \bar{e}_y^* - \beta \bar{e}_x^* + \bar{Y} \left( \frac{1}{2} - \alpha \right) \bar{e}_z^* \right) \right] \tag{53}$$

Expanding and Taking expectation and using (5) in (53) we get

$$\begin{aligned}
 MSE(t_8) = & \theta \bar{Y}^2 C_y^2 + \lambda \bar{Y}^2 C_{y(2)}^2 - \beta \bar{X} \bar{Y} \theta \rho_{yx} C_x C_y - \lambda \beta^* \bar{X} \bar{Y} \rho_{yx(2)} C_{x(2)} C_{y(2)} \\
 & + \bar{Y} \left( \frac{1}{2} - \alpha \right) \theta \bar{Y} \bar{X} \rho_{yz} C_z C_y + \bar{Y} \left( \frac{1}{2} - \alpha^* \right) \lambda \bar{Y} \bar{X} \rho_{yz(2)} C_{z(2)} C_{y(2)}
 \end{aligned} \tag{54}$$

Substituting the optimum value in (52), we get

$$\begin{aligned}
 MSE(t_8) = & \theta \bar{Y}^2 C_y^2 - \left( \frac{\bar{Y} C_y}{\bar{X} C_x |R_{2 \times 2}|} (-1)^{1+1} |R_{yx}|_{yxz} \right) \theta \bar{X} \bar{Y} C_y C_x \rho_{yx} + \bar{Y} \left[ \frac{1}{2} - \left( \frac{1}{2} + \frac{C_y}{\bar{Z} C_z |R_{2 \times 2}|} (-1)^{2+1} |R_{yz}|_{yxz} \right) \right] \theta \bar{Y} \bar{Z} C_z C_y \rho_{yz} \\
 & + \lambda \bar{Y}^2 C_{y(2)}^2 - \left( \frac{\bar{Y} C_{y(2)}}{\bar{X} C_{x(2)} |R_{2 \times 2}^*|} (-1)^{1+1} (-1)^{1+1} |R_{yx}^*|_{yxz} \right) \lambda \bar{X} \bar{Y} C_{y(2)} C_{x(2)} \rho_{yx(2)} \\
 & + \bar{Y} \left[ \frac{1}{2} - \left( \frac{1}{2} + \frac{C_{y(2)}}{\bar{Z} C_{z(2)} |R_{2 \times 2}^*|} (-1)^{2+1} |R_{yz}^*|_{yxz} \right) \right] \lambda \bar{Y} \bar{Z} C_{y(2)} C_{z(2)} \rho_{yz(2)}
 \end{aligned} \tag{55}$$

Simplifying (55) we get

$$\begin{aligned}
 MSE(t_8) = & \theta \bar{Y}^2 C_y^2 \left[ 1 - \frac{(-1)^{1+1} |R_{yx}|_{yxz}}{|R_{2 \times 2}|} \rho_{yx} - \frac{(-1)^{2+1} |R_{yz}|_{yxz}}{|R_{2 \times 2}|} \rho_{yz} \right] + \\
 & \lambda \bar{Y}^2 C_{y(2)}^2 \left[ 1 - \frac{(-1)^{1+1} |R_{yx}^*|_{yxz}}{|R_{2 \times 2}^*|} \rho_{yx(2)} - \frac{(-1)^{2+1} |R_{yz}^*|_{yxz}}{|R_{2 \times 2}^*|} \rho_{yz(2)} \right]
 \end{aligned} \tag{56}$$

$$MSE(t_8) = \frac{\theta \bar{Y}^2 C_y^2}{|R_{2 \times 2}|} |R|_{yxz} + \frac{\lambda \bar{Y}^2 C_{y(2)}^2}{|R_{2 \times 2}^*|} |R^*|_{yxz} \quad (57)$$

Or

Using (5) in (57) we get

$$MSE(t_8) = \theta \bar{Y}^2 C_y^2 (1 - \rho_{y.xz}^2) + \lambda \bar{Y}^2 C_{y(2)}^2 (1 - \rho_{y.xz}^{*2}) \quad (58)$$

#### 4. Simulation, Result and Discussion

In this section, we carried out some data simulation experiments using R statistical program to compare the performance of modified regression estimators in two phase sampling with non-response in either the study variable only or both the study variable and the auxiliary variable with already existing estimators in two phase sampling for finite population. In the simulated population, the study variable and auxiliary variables are normally distributed.

- i) Study variable  $N = 500$ ,  $n_1 = 75$ ,  $n = 50$   $\mu = 75$   $\sigma = 10$
- ii) For ratio estimator the auxiliary variable is strongly positively correlated with the study variable and the line passes through the origin.

$$N=500, n_1=75, n=50 \mu = 55 \sigma =9.4 \rho_{yx} =0.7018$$

- iii) For regression estimator the auxiliary variable was strongly positively correlated with the study variable and the regression line does not pass through the origin.

$$N = 500, n_1 = 75 \text{ and } n = 50 . \mu = 22 \sigma = 3.29 \rho_{yx} = 0.8114$$

- iv) For product estimator the auxiliary variable was strongly negatively correlated with the study variable.

$$N = 500, n_1 = 75 \text{ and } n = 50 , \mu = 34 \sigma = 5.10 \rho_{yx} = - 0.7477$$

The percent relative efficiencies (PREs) of different proposed estimators were computed with respect to a usual unbiased estimator  $\bar{y}^*$  for different values of  $k$ .

$$\text{Percent Relative Efficiencies}(\hat{t}) = \frac{\text{Var}(\bar{y}^*)}{\text{MSE}(\hat{t})} * 100 \quad (59)$$

**Table 1:** Percent relative efficiency of different  $\bar{Y}$  estimators with respect to  $\bar{y}^*$  when the non-response is on the study variable only in two phase sampling.

Estimators	$\frac{1}{k}$			
	$\frac{1}{5}$	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{1}{2}$
$\bar{y}^*$	100	100	100	100
$t_{R1}$	110	114	116	117
$t_{P1}$	101	101	102	105
$t_{RE1}$	129	140	143	157



$t_{ER1}$	126	135	138	150
$t_{EP1}$	106	107	110	111
$t_{ERP1}$	126	136	139	151
<b><math>t_7</math> (Proposed)</b>	<b>139</b>	<b>155</b>	<b>161</b>	<b>183</b>

---

The Percent relative efficiencies of all the estimators in the Table I increases as k increases. Our proposed estimator ( $t_7$ ) is the most efficient among all the estimators since it has the highest Percent relative efficiency when the non-response is on the study variable only in two phase sampling.

**Table 2:** Percent relative efficiency of different  $\bar{Y}$  estimators with respect to  $\bar{y}^*$  when the non-response is on the study variable and also in auxiliary variable in two phase sampling.

Estimators	$\frac{1}{k}$			
	$\frac{1}{5}$	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{1}{2}$
$\bar{y}^*$	100	100	100	100
$t_{R2}$	104	105	133	119
$t_{P2}$	102	105	106	106
$t_{RE2}$	202	205	213	219
$t_{ER2}$	176	180	191	181
$t_{EP2}$	154	138	133	124
$t_{ERP2}$	197	174	182	180
<b><math>t_8</math> (Proposed)</b>	<b>269</b>	<b>268</b>	<b>273</b>	<b>261</b>

---

The Percent relative efficiencies of all the estimators in the table II increases as  $k$  increases apart from  $t_{ERP2}$  whose Percent relative efficiencies decreases. Our proposed estimator ( $t_8$ ) is the most efficient among all the estimators since it has the highest Percent relative efficiency when the non-response are on the study variable and the auxiliary variable in two phase sampling.

## 5.0 Conclusion

Based on these study results, the proposed estimators  $t_7$  and  $t_8$  are recommended for use in practice when non-response is on the study variable only and on both the study variable and the auxiliary variable in two phase sampling respectively.

## Reference

1. Hansen, M. H. and Hurwitz, W. N., 1946. The problem of non-response in sample surveys. *J. Amer. Statist. Assoc.*, 41, 517-529.
2. Khare, B. B. and Srivastava, S. (1993). Estimation of population mean using auxiliary character in presence of non-response, *The National Academy of Sciences, Letters, India*, 16, 111–114.
3. Khare, B. B. and Srivastava, S. (1995). Study of conventional and alternative two phase sampling ratio, product and regression estimators in presence of non-response, *Proceedings of the National Academy of Sciences*,
4. Singh, H. P. and Kumar, S. (2010). Estimation of mean in presence of non-response using two phase sampling scheme, *Statistical Papers*, 50, 559–582.
5. Singh, H. P., Kumar, S. and Kozak, M. (2010). Improved estimation of finite population mean when sub-sampling is employed to deal with non-response, *Communication in Statistics - Theory and Methods*, 39, 791–802.
6. Tum, E.C., Kung'u, J. and Odongo, L. (2014) A New Regression Type Estimator with Two Auxiliary Variables for Single-Phase Sampling. *Open Journal of Statistics*, 4, 789-796.
7. Neyman, J. (1938). Contribution to the theory of sampling human populations. *J. Amer. Statist. Assoc.*, 33, 101-116.
8. Kumar1, S and Bhougal, S (2011) Estimation of the Population Mean in Presence of Non-Response, Vol. 18, No. 4, 537–548, *Communications of the Korean Statistical Society*

## **A Study of the Morphology of Synthesized ZnO Nanoparticles and their Application in Photodegradation of Dyes**

Lucy J. Chebor\*, Lusweti Kituyi, Dickson Andala  
University of Eldoret, Kenya

Corresponding author: email: [lucychebor@yahoo.com](mailto:lucychebor@yahoo.com)

### **Abstract**

Environmental pollution by toxic organic contaminants is a global menace and its magnitude is increasing significantly and so declining water quality has become a global issue. Waste products produced from the textiles, dyeing, paper and plastic industries are predominantly responsible for contaminating the water bodies. Organic dyes produce toxic aromatic amines that are carcinogenic to human beings and harmful to the environment yet they are non-biodegradable. In an effort to lessen the environmental effects of these dyes, various techniques have been utilized. However, these methods are expensive and ineffective resulting in intensively coloured discharge and high concentration of dyes from the treatment facilities. Nanotechnology is a promising field in waste water treatment. The aim of this study thus was to assess the use of synthesized ZnO nanoparticles in photo degradation of dyes. This involves the degradation of methyl orange dye using sunlight and fluorescent light as sources of radiation on the surface of zinc oxide nanoparticles. The basis of ZnO/UV photo-catalytic process is the semi-conduct optical stimulation of ZnO as a result of electromagnetic ray absorption. Precipitation technique was used to synthesize ZnO nanoparticles. By varying experimental conditions, two samples L<sub>1</sub> and L<sub>2</sub> were synthesized and characterized using Power X-ray Diffraction (PXRD), Fourier Transform Infra-Red (FTIR), Scanning Electron Microscopy (SEM) and Energy Dispersive X-ray Spectroscopy (EDX) methods of analysis. The PXRD results showed diffraction peaks which were indexed to ZnO reference as per JCPIDS file 80-0075. The size of ZnO nanoparticles was found to be 26 nm. FTIR spectra showed a broad band at around 430 cm<sup>-1</sup> with shoulder shape, characteristics of Zn-O bond. The images obtained by SEM showed rod shaped clusters of nanoparticles were distributed well within a range of 100 nm which is a favourable property to exhibit better photo catalytic activity. The EDX results showed elemental composition of ZnO nanoparticles and showed 54% Zn, 44.07% O and 1.93% Mn impurities for L<sub>1</sub> and 55.34% Zn, 42.3% O and 2.37% Mn impurities for L<sub>2</sub>. The effect of process parameters like amount of the photocatalyst, initial dye concentration and contact time on the extent of photodegradation has also been investigated. The results showed that percentage removal of the dye increases with increase in contact time and amount of photocatalyst, it decreases with increase in initial dye concentration. The results revealed that dyes could be removed by semiconducting nanomaterials assisted by photocatalytic degradation. Biosynthesis of nanoparticles is an approach of synthesizing nanoparticles using microorganisms and plants having biomedical applications. This approach is an environment-friendly, cost-effective, biocompatible, safe, green approach. Green synthesis includes synthesis through plants, bacteria, fungi, algae etc. They allow large scale production of ZnO NPs free of additional impurities. NPs synthesized from biomimetic approach show more catalytic activity and limit the use of expensive and toxic chemicals.

**Key Words:** Photodegradation, ZnO, nanoparticles, organic dyes, green approach

## INTRODUCTION

Dyes are important class of synthetic organic compounds used in textile industry, paper, dyeing and plastic industries as colour for dyeing their products. A huge amount of water is used which results in production of dye-containing wastewater[1]. One of the main sources of severe pollution problems worldwide is the textile industry and its dye-containing wastewaters. These industries use approximately 10,000 dyes and pigments [2]. Between 10-25% of the textile dyes and pigments are lost during the dyeing process, and 2-20% are directly discharged as aqueous effluents in different environmental components [3]. These residual dyes pose a great danger to the environment especially the natural water resources. The discharge of dye-containing effluents into the water environment is undesirable, not only because of their colour, but also because many of dyes released and their breakdown products are toxic, carcinogenic and mutagenic to life [2]. Without adequate treatment, these dyes can remain in the environment for a long period of time. For instance, the half-life of hydrolyzed reactive methyl blue is about 46 years at pH 7 and 25°C [4].

The treatment and recycling of dye-containing wastewater has been highly recommended by environmental protection agencies like WHO and UNEP. This is due to the high levels of pollutants in dyeing and finishing processes, that is, dyes and their breakdown products, pigments, dye intermediates, auxiliary chemicals and heavy metals. In an effort to reduce the environmental effects of organic dyes, various techniques have been employed. These techniques include coagulation and sedimentation in which sediments again create disposal problems. These methods are not only expensive but also highly ineffective. The use of synthesized nanoparticles in photo degradation of dyes is a new promising field in waste water treatment. This involves the degradation of organic dyes by irradiating them with ultraviolet light on the surface of zinc oxide. The entire process is called photo-catalytic degradation of dyes on ZnO. The basis of ZnO/UV photo-catalytic process is the semi-conduct optical stimulation of ZnO as a result of electromagnetic ray absorption. ZnO has an energy band of 3.2 eV which can be activated by radiation of UV in the wavelength of 387.5 nm. On the earth's surface, sunlight begins in the wavelength of 300 nm and only 4-5 percent of solar radiation may be used by ZnO[5].

The use of ZnO nanoparticles in photo catalytic colour removal is cheaper and does not pose disposal challenge, also the technology uses small amount of energy. The use of nanomaterials like ZnO nanoparticles offers a promising technology for reduction of global environmental pollutants. This semi-conductor catalyst has been preferred because of its wide energy band gap, high photo sensitivity, stability and low cost (Nishio *et al.*, 2006).

This study examined the use of synthesized ZnO nanoparticles in photodegradation of dyes. Methyl orange (MeO) was used as a model dye since it is an organic dye similar to that used in the textile and paper industries. Methyl orange is an organic dye with a chemical formula of  $C_{14}H_{14}N_3SO_3Na$  and characterized by sulphonic groups, which are responsible for high solubility of these dyes in water (Guettai & Amar, 2005).

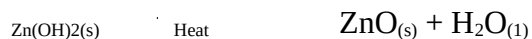
## MATERIALS AND METHODS

ZnO nanoparticles were synthesized using precipitation method. In this method, ZnO nanoparticles were prepared in two ways. In the first set, 100 ml of 1 M ZnSO<sub>4</sub> solution was added to 100ml of 2M NaOH solution in drops. When the addition was complete, the mixture was kept at room temperature under constant stirring using magnetic stirrer for a period of 2-4 hours.

The constant stirring using magnetic stirrer made the precipitation homogeneous and minimal particles which reduce the specific surface free energy of crystal nucleus which inhibit agglomeration and growth of the crystal nucleus so the particle size of the product is reduced (Zhang *et al.*, 2008).

The resultant precipitate obtained was filtered then rinsed with distilled water. The formed white precipitate of Zn(OH)<sub>2</sub> was allowed to settle, filtered using filter paper of pore size 0.4µm in a suction pump, washed with distilled water several times and dried in hot oven at 150°C for 45 minutes. The synthesized ZnO nanoparticles were further irradiated at 180 W with microwave radiation in a microwave oven for 30 minutes. This was named as sample L<sub>1</sub>. The procedure was repeated to synthesize ZnO nanoparticles in different experimental conditions. ZnSO<sub>4</sub>, NaOH and oxalic acid were used as stabilizing agents. Thus one more sample was obtained and referred to as L<sub>2</sub>.

The precipitation reaction was represented as



The resultant ZnO nanoparticles particles after irradiation were collected and stored in brown bottles. The synthesized ZnO nanoparticles were subjected to SEM, PXRD, FTIR and EDX, to confirm the nanostructure.

### Preparation of Dye Solution

The stock solution (1,000ppm) was prepared and stored in brown bottles. The stock solution was diluted to get different required initial concentrations of the dye used. Dye concentration was determined by using absorbance measured before and after the treatment using UV-Vis spectrometer.

The stock solution was diluted to different initial concentrations 10, 20, 30, 40 and 50 ppm for methyl orange in standard measuring flasks by making necessary dilutions with required volume of distilled water. The optical density of each dye solution was measured using UV-Vis spectrophotometer (model – No-SL-150 Elico) at maximum wavelength value for MeO dye. A plot of optical density versus initial concentration was drawn. This plot was used as standard graph for estimation of dye by interpolation technique. The values of optical density for dye solutions before and after removal of dye were obtained by using UV-Vis spectrophotometer. Using these optical densities the corresponding dye concentration was obtained from the graph. Stock solution of MeO dye (1,000ppm) was suitably diluted to get the required initial concentration from 15 – 45ppm. A 10ml of the dye solution of known initial concentration (C<sub>1</sub>) was transferred to 50ml beaker. Required amount of the photo-catalyst (L<sub>1</sub> and L<sub>2</sub>) was exactly

weighed and then transferred to the dye solution with different  $C_1$ . The beaker was then exposed to fluorescent light and direct sunlight for a fixed period of contact time.

After bleaching, the optical density (OD) of these solutions was measured using UV-Vis spectrophotometer and the final concentrations ( $C_2$ ) obtained from the standard graph. The extent of removal of the dye in terms of percentage removal was calculated using the following relationship:

$$\text{Percentage removal} = \frac{100(C_1 - C_2)}{C_1}$$

Where

$C_1$  = initial concentration of dye (ppm)

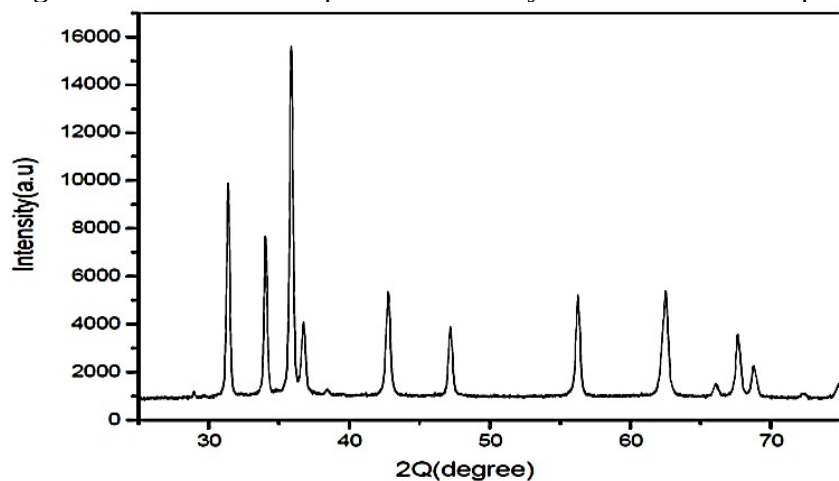
$C_2$  = final concentration of dye (ppm)

Factors that govern degradation process: The effect of various experimental parameters on degradation of MeO dye in the aqueous suspension by ZnO nanoparticles were studied by varying the experimental conditions; concentration of the dye, amount of the sample ( $L_1$  and  $L_2$ ) and contact time.

## RESULTS AND DISCUSSION

### Powder X-Ray Diffraction (PXRD)

Figure 1 shows the XRD patterns of the synthesized ZnO nanoparticles.



**Figure 1: XRD patterns of the synthesized ZnO nanoparticles**

The diffraction peaks at 31.7, 34.4, 36.2, 47.4, 56.4, 62.5, 67.6, and 68.7 can be indexed to ZnO as per the standard JCPDS file 80-0075. Powder diffraction patterns are characteristic of a particular substance and its “fingerprint” and can be used to identify a compound. Powder diffraction data from known compounds have been compiled into a database by the JCPDS. The synthesized sample can be confirmed to be ZnO nanoparticle. Clear crystallinity of the ZnO nanoparticles was observed. The samples had similar patterns. This suggests that the oxalic acid added as stabilizing agent had no effect on the Wurtzite structure of ZnO (Herrmann & Helmoltz, 2010).

Similar results were obtained (Gu *et al.*, 2004) and XRD peaks occurred at scattering angles ( $2\theta$ ) of 31.3670, 34.0270, 35.8596, 47.1635, 56.2572, 62.5384, 67.6356, and 68.7978, corresponding

to reflection from 100, 002, 101, 102, 110, 103, 200 and 112 crystals. They indexed the XRD patterns to ZnO nanoparticles reference JCPDS file 80-0075 as well.

The average crystallite size of ZnO nanoparticles was estimated according to the diffraction reflection by using Debye-Scherrer equation (Holzwarth& Gibson, 2011):

$$T = \frac{0.9 \lambda}{\beta \cos \theta}$$

Where

$\lambda$  - wavelength of incident X- ray (1.5406Å<sup>0</sup>)

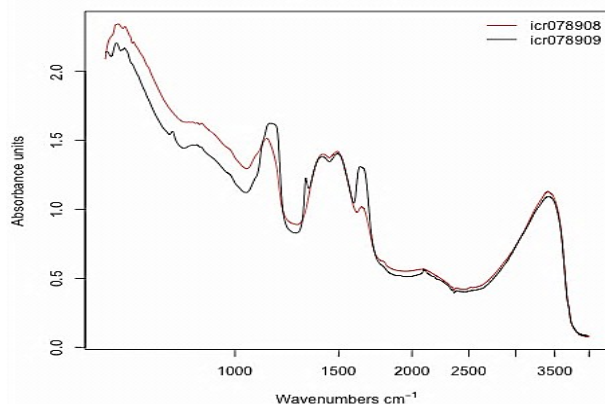
$\beta$  - full width for half maximum (FWHM),

$\Theta$  - Bragg's angle for the peak

$\beta$ - can be calculated using the equation  $\beta = (2 \theta_2 - 2 \theta_1)$ , obtained to be 0.2755 radians. The average crystallite sizes of synthesized ZnO nanoparticles were found to be around 26 nm. Similar results were obtained by Shanthi and Kuzhalosai (2012), who characterized synthesized nano-ZnO using PXRD for their three samples prepared. The sizes obtained were about 18nm, 16nm and 12nm.

The FTIR analysis

Figure 2 shows the FTIR spectrum of the synthesized ZnO nanoparticles by precipitation method, which was acquired in the range of 400-4000 cm<sup>-1</sup>. The red and black lines represent L<sub>1</sub> and L<sub>2</sub>, respectively.



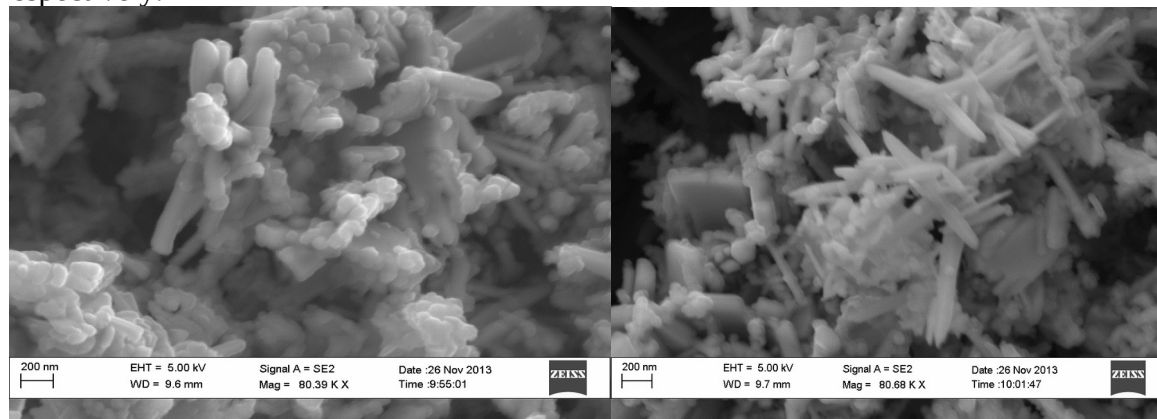
**Figure 2: Observed FTIR pattern**

FTIR of the ZnO nanocatalyst indicates the presence of water molecule adsorbed on the surface due to bands at around 3400 cm<sup>-1</sup> which may be assigned to OH stretching vibration of adsorbed H<sub>2</sub>O or due to residual Zn(OH)<sub>2</sub> present in the powder. The absorption band at 430cm<sup>-1</sup> correlated to metal oxide bond (Zn-O).

Kant and Kumar (2012) carried out similar study and FTIR spectra of ZnO obtained showed absorption band at 432.0 cm<sup>-1</sup> which could be attributed to (Zn-O) stretching frequency. Likewise peaks at 3401.3 cm<sup>-1</sup> represent (OH) stretching mode. Shanthi and Kuzhalosai (2012) also carried out a similar study and their analysis showed a broad band between 419-430cm<sup>-1</sup>.The spectra showed bands at (3250 and 3500cm<sup>-1</sup>) which was assigned to OH stretching vibrations.

### SEM Analysis

Figure 3 and Figure 4 shows the SEM diagram for sample L<sub>1</sub> and L<sub>2</sub> at high magnification respectively.



**Figure 3: Magnified L<sub>1</sub> SEM diagram**

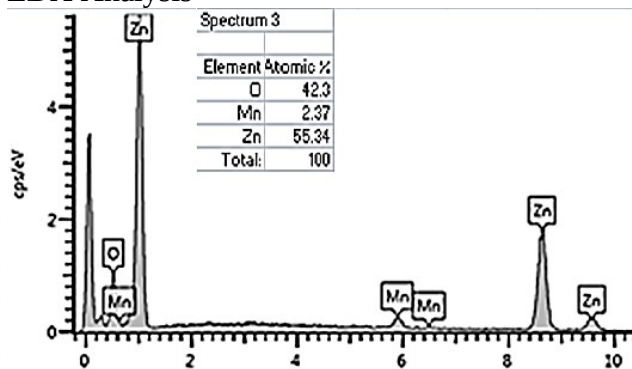
**Figure 4: Magnified L<sub>2</sub> SEM diagram**

These images showed that the ZnO nanoparticles obtained formed rod shaped clusters distributed within the range of 100nm. The diagrams also show that the surface was not uniform but porous in nature. It shows that the nanocatalyst has considerable number of pores where there is a good possibility for the heavy metals to be trapped and adsorbed onto these pores and it is a good sign for effective adsorption of heavy metals (Joshi and Shrivastava, 2012). The photographs also showed different surfaces for L<sub>1</sub> and L<sub>2</sub>. The L<sub>1</sub> showed round ended while L<sub>2</sub> showed sharp ended nanoclusters. This showed that the stabilizing agent had an influence on the morphology of the samples.

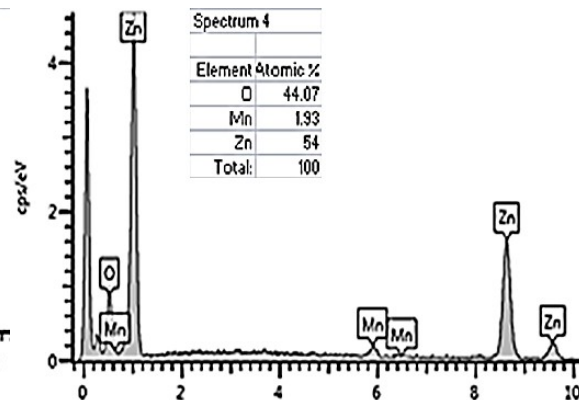
Similar studies were made by Soltaninezhad and Amrnifar (2011) who studied surface morphology of ZnO nanoparticles produced by Spray Pyrolysis. The pictures observed showed particles that were spherical in shape. However Joshi and Shrivastava, (2012) determined the surface texture which was found to be rough and porous in nature.

Due to these close similarities, the ZnO nanoparticles were confirmed. The difference in distribution range is attributed to the level of accuracy during synthesis and also method of synthesis (Joshi and Shrivastava, 2012).

### EDX Analysis



**Figure 5: EDX Pattern ZnO L<sub>1</sub>**



**Figure 6: EDX Pattern ZnO L<sub>2</sub>**

The EDX spectra indicated that the samples were made up of Zn, O and traces of Mn impurities. The peak at the spectrum peak is assigned to the bulk ZnO and the less intense one to the surface



ZnO. The peak at 0.5 KeV can only be attributed to O and not Mn due to overall position of the peaks. The elemental composition of the nanomaterial was found to be 55.34% Zn, 42.3% O and 2.37% Mn for L<sub>1</sub> and 54% Zn, 44.0% O and 1.93% Mn for L<sub>2</sub>.

Similar work has been done by Joshi and Shrivastava (2012) who characterized nano ZnO synthesized by precipitation technique. Their EDX spectra showed a peak at 0.5 KeV for oxygen 1 KeV for ZnL<sub>α</sub>, 8.6 for ZnK<sub>α</sub> and 9.6 KeV for ZnK<sub>β</sub>. The elemental composition was found to be 71% Zn, 18.5% CO and 10% C with C as the impurity.

### Photodegradation Studies

The optical density of each dye was measured using UV-Vis spectrophotometer at maximum wavelength of 480 nm. A plot of optical density versus initial concentration was done and used as a standard graph for estimation of dye concentration by interpolation technique.

### Effect of variation of initial concentration of dye on photo degradation of methyl orange dye

Table 1 shows the effect of variation of initial concentration of methyl orange dye on photodegradation.

**Table 1: Effect of variation of initial concentration of dye on photo degradation of methyl orange dye**

Radiation	Sample	Concentration of dye		
		15 mgL <sup>-1</sup>	30 mgL <sup>-1</sup>	45 mgL <sup>-1</sup>
Sunlight	L <sub>1</sub>	0.85	2.68	10.77
	% removal	98.4%	96.1%	94.7%
	L <sub>2</sub>	2.49	6.83	20.89
	% removal	97.4%	97.2%	93.6%
Fluorescent	L <sub>1</sub>	14.23	26.40	41.31
	% removal	92.0 %	89.0%	88.2%
	L <sub>2</sub>	14.04	29.81	38.03
	% Removal	91.8%	88.9%	88.0%

Photo catalytic degradation of the dye was found to decrease with increase in initial concentration of methyl orange. This could be due to more dye molecules than ZnO nanoparticles; in this case the photo-catalyst became the limiting factor. It was noted that degradation rate decreased with increase in dye concentration. The decrease in dye degradation could be attributed to reduction of OH<sup>-</sup> radicals on the catalyst surface when covered by dye ions (Poulis & Tsachpinis, 1999).

The results agree with those reported by Li *et al.* (2005) when methyl orange was irradiated with sunlight source, the degradation of the dye decreased as the dye concentration increased. This is due to the generation of OH radicals on the catalyst surface which is reduced since the active sites are covered by dye ions. Also Kansalet *al.* (2006) concluded that photo-catalytic degradation of methyl orange decreased as the dye concentration increased.

This decrease is as a result of increasing the number of photons absorbed by catalyst's slower concentration (Davis, 2006). According to Shanthi and Muthuselvi (2012), the decrease in photo

degradation is as a result of dye molecules imparting darker colour to the solution which acts as a filter to the incident light reaching the photo catalyst surface. Sampa and Biney (2004) further explained that the increase in the concentration of a dye solution results in the photons getting intercepted before they can reach the catalyst surface, thus decreasing the absorption of photons.

**Effect of variation of dose of photo catalyst ( $L_1$  and  $L_2$ ) on photo degradation of MeO dye**

The initial concentration  $30 \text{ mgL}^{-1}$  of the dye and pH in all beakers were kept constant at pH 7.0 and the dose of photo-catalyst was varied from 200 mg to 400mg with a contact time of four hours and the results are shown in Table 2.

**Table 2: Effect of variation of dose of photo catalyst ( $L_1$  and  $L_2$ ) on photo degradation of MeO dye**

Radiations	Sample	Amount of photo-catalyst		
		200mg	300mg	400mg
Sunlight	$L_1$	6.57	2.39	1.50
	% removal	92.1	94.2	96.0
	$L_2$	10.99	6.83	4.06
	% removal	93.4	97.2	96.5
Fluorescent	$L_1$	26.40	26.88	26.55
	% removal	92.0	96.4	98.5
	$L_2$	29.81	27.46	25.23
	% removal	92.6	97.5	97.9

Photo catalytic degradation of methyl orange dye increased with an increase in concentration of ZnO particles. This is due to increase in photo-catalyst molecules available to degrade the dye. Further increase of ZnO concentration increased turbidity of the solution and decreases light penetration into the solution and therefore, removal efficiency decreases (Kartalet al., 2001). The results of this study are similar to those of Joshi and Shrivastava (2012) who studied removal of methylene blue using ZnO nano particles, by varying the dose of photo catalyst from 2.0 g/l to 5.0 g/l and degradation increased from 86.0% to 92.8%. The increase in the amount of catalysts increased the number of active sites of the photo catalyst surface, which in turn increased the number of hydroxyl and superoxide radicals (Sampa and Biney, 2004).

**Effect of variation of contact time on photo degradation of MeO dye**

The results are presented in Table 3:

**Table 3: Effect of variation of contact time on photo degradation of MeO dye**

Radiations	Sample	Contact time in hours				
		1	2	3	4	5
Sunlight	$L_1$	11.84	6.83	5.99	1.45	0.58
	% removal	60.5	77.2	80.0	95.2	98.0
	$L_2$	9.12	4.23	2.68	0.97	0.53
	% removal	69.6	85.9	91.1	96.8	98.2
Fluorescent	$L_1$	10.95	8.77	5.95	2.68	1.32
	% removal	63.5	70.8	80.2	91.1	95.6
	$L_2$	11.57	8.15	5.33	2.06	0.70

% Removal	61.4	72.8	82.2	93.1	97.7
-----------	------	------	------	------	------

The results indicated that, the percentage removal of dye increased with increased contact time. This is in agreement with the results reported by Shanthi and Muthuselvi(2012), who studied the effects of contact time on removal of malachite green using ZnOnano particles. The increased contact time causes the photo-generated OH radicals and other peroxide radicals all being highly oxidant species decompose the dyes completely to mineral end products (Hofman, 1995).

### Conclusion

Photocatalytic degradation of dye was found to decrease with increase in initial concentration of methyl orange. Photocatalytic degradation of methyl orange dye increased with an increase in amount of ZnO nanoparticles. The optimum photocatalyst concentration was found to be 45mg/l with dye removal of 96.0% at contact time of 2 hours. The contact time for maximum removal of methyl orange was four hours.

### Recommendations

In future, researchers should focus on the development of novel nanomaterials/nanocomposites with a high surface area, sufficient surface functional groups and high sorption ability, for the removal of organic dyes. The environmental threat of organic dyes is becoming more and more thus; further improvements must be made in the direction of the development of materials with greater stability (resistance to pH changes and concentrations of chemicals present in contaminated water) and the capacity for the simultaneous removal of multiple contaminants, such as toxic metal ions, organic dyes and bacterial pathogens.

Considering the economics of adsorbents, it is necessary to synthesize low-cost effective and recyclable adsorbents for their extensive application in our daily life. Treatment technologies should be developed for the purification of water in order to meet the demand of increased environmental pollution.

### Acknowledgments

The authors are grateful for the supports from International Centre for Research in Agroforestry (ICRAF), University of Eldoret and University of Western Cape, South Africa which provided the laboratory space and equipment for the work.

### References

- Ali, H. (2010). Biodegradation of synthetic dyes—a review. *Water, Air, & Soil Pollution*, 213(1-4), 251-273.
- Chatterjee, D. and Dasgupta, S. (2005). Visible light induced photocatalytic degradation of organic pollutants. *Journal of Photochemistry and Photobiology C: Photochemistry Reviews*, 6(2), 186-205.
- Davis, J.C. (2006). *Managing the effects of nanotechnology*. Woodrow Wilson International Centre for Scholars, National institutes of health, Washington D.C., USA

- dos Santos, A. B., Cervantes, F. J. and van Lier, J. B. (2007). Review paper on current technologies for decolourisation of textile wastewaters: perspectives for anaerobic biotechnology. *Bioresource Technology*, 98(12), 2369-2385.
- Fazli, M. M., Mesdaghinia, A. R., Naddafi, K., Nasserli, S., Yunesian, M., Assadi, M. M. and Hamzehei, H. (2010). Optimization of reactive blue 19 decolorization by ganoderma sp. using response surface methodology. *Iranian Journal of Environmental Health Science & Engineering*, 7(1), 35-42.
- Gu, F., Wang, S. F., Lü, M. K., Zhou, G. J., Xu, D. and Yuan, D. R. (2004). Photoluminescence properties of SnO<sub>2</sub> nanoparticles synthesized by sol-gel method. *The Journal of Physical Chemistry B*, 108(24), 8119-8123.
- Guettaï, N. and Amar, H. A. (2005). Photocatalytic oxidation of methyl orange in presence of titanium dioxide in aqueous suspension. Part I: Parametric study. *Desalination*, 185(1), 427-437.
- Herrmann, V. and Helmoltz, P. (2010). Influence of stabilizers in ZnO nanodispersions on the performance of the nano particles. *Phys Status Solid*, 207(7), 1684 – 1688
- Hofman, A. (1995). Shades of green. *Stanford Soci. Innov. Rev.*, Spring: 40–49.
- Holzwarth, U. and Gibson, N. (2011). The Scherrer equation versus the 'Debye-Scherrer equation'. *Nature Nanotechnology*, 6(9), 534-534.
- Joshi, K.M. and Shrivastava V.S. (2012). Removal of methylene blue dye aqueous solution using photo catalysis, *Int.J.nano Dim*, 2(4): 241-252
- Kansal, S.K., Singh M. and Sudc, D. (2006). Studies on photodegradation of two commercial dyes in aqueous phase using different photocatalysts. *J Hazardous material*, in press.
- Kant, S. and Kumar, A. (2012). A comparative analysis of structural, optical and photocatalytic properties of ZnO and Ni doped ZnO nanospheres prepared by sol gel method. *Adv Mat Let*, 3(4), 350-354.
- Kartal, O.E., Erol, M. and Oguz, H. (2001). Photo catalytic destruction of phenols by ZnO powders. *Chen Eng Technol.*, 24, 645-649
- Li, Y., Xiaodong, L., Junwen, L. and Jing, Y. (2005). Photocatalytic degradation of methyl orange by TiO<sub>2</sub> coated with activated carbon, *Catalysis Communications*, 40; 1119-1126
- Nishio, J., Tokumura, M., Znad, H. T. and Kawase, Y. (2006). Photocatalytic decolorization of azo-dye with zinc oxide powder in an external UV light irradiation slurry photoreactor. *Journal of hazardous materials*, 138(1), 106-115.
- Poulis, I. and Tsachpini, J. (1999). Photocatalytic degradation of the textile dye Reactive Orange in the presence of TiO<sub>2</sub> suspensions *Chem Technol Biotechnol*, 74; 349-357

- Sampa, C. and Biney, K. (2004). *Photo-catalytic degradation of modern textile dyes in waste water using ZnO nanocatalyst*, Kolkata, India.
- Shanthi, M. and Kuzhalosai, V. (2012). Photocatalytic degradation of an azo dye, Acid Red 27, in aqueous solution using nanoZnO. *Indian Journal of Chemistry-Part A Inorganic Physical Theoretical and Analytical*, 51(3), 428.
- Shanthi, S. and Muthuselvi, U. (2012). A study of morphology of synthesized NanoZnO and its application in photodegradation of malachite green dye using different sources of energy 4 39-52
- Soltaninezhad, M. and Aminifar, A. (2011). Study of nanostructures of ZnO as photocatalysts for degradation of organic pollutants. *Int. J. Nano Dim*, 2(2) 137-145
- Wojnarovits, L. and Takacs, E. (2008). Irradiation treatment of azo dye containing wastewater: an overview. *Radiation Physics and Chemistry*, 77(3), 225-244.
- Zhang, H., Fung, K. H., Hartmann, J., Chan, C. T. and Wang, D. (2008). Controlled chainlike agglomeration of charged gold nanoparticles via a deliberate interaction balance. *The journal of physical chemistry C*, 112(43), 16830-16839.